

# Server Hardware Console Reference 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**

**May 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. Getting started</b> .....                        | <b>1-1</b> |
| 1.1. Overview .....  | 1-1        |
| 1.2. Connecting to the Server Hardware Console (SHC) .....     | 1-2        |
| 1.3. Logging in to the Server Hardware Console (SHC) .....     | 1-3        |
| 1.4. The Server overview page .....                            | 1-4        |
| 1.5. Server Hardware Console (SHC) features .....              | 1-5        |
| 1.6. Changing the default password .....                       | 1-6        |
| 1.7. Stopping the Server Hardware Console (SHC) .....          | 1-7        |
| <b>Chapter 2. Monitoring the server</b> .....                  | <b>2-1</b> |
| 2.1. Checking event logs .....                                 | 2-1        |
| 2.2. Adding a remote BMC log server .....                      | 2-2        |
| 2.3. Checking the hardware status .....                        | 2-3        |
| 2.4. Collecting BMC logs .....                                 | 2-5        |
| 2.5. Checking the sensors .....                                | 2-8        |
| <b>Chapter 3. Controlling the server</b> .....                 | <b>3-1</b> |
| 3.1. Checking the power state .....                            | 3-1        |
| 3.2. Setting boot options for host OS .....                    | 3-4        |
| 3.3. Powering on the server .....                              | 3-5        |
| 3.4. Powering off the server .....                             | 3-6        |
| 3.5. Managing power usage .....                                | 3-7        |
| 3.6. Enabling / disabling the identification LED .....         | 3-8        |
| 3.7. Rebooting the Baseboard Management Controller (BMC) ..... | 3-9        |
| 3.8. Connecting to the Serial over LAN (SoL) console .....     | 3-10       |
| 3.9. Connecting to the Keyboard Video Mouse (KVM) .....        | 3-11       |
| 3.10. Managing intrusions .....                                | 3-12       |
| 3.10.1. Checking intrusions detected .....                     | 3-12       |
| 3.10.2. Clearing intrusions detected .....                     | 3-13       |
| 3.10.3. Configuring actions for intrusions .....               | 3-14       |
| 3.11. Enabling port security controls .....                    | 3-15       |
| 3.12. Creating a virtual media session .....                   | 3-16       |
| <b>Chapter 4. Configuring the server</b> .....                 | <b>4-1</b> |
| 4.1. Configuring network settings .....                        | 4-1        |
| 4.1.1. BMC network settings overview .....                     | 4-2        |
| 4.1.2. Configuring common settings .....                       | 4-4        |
| 4.1.3. Configuring IPV4 address with DHCP .....                | 4-5        |

|                   |  |            |
|-------------------|--|------------|
| 4.1.4.            | Assigning a static IP address .....                  | 4-6        |
| 4.1.5.            | Configuring an IPV4 custom route .....               | 4-7        |
| 4.1.6.            | Configuring DNS settings .....                       | 4-8        |
| 4.1.7.            | Configuring WIFI settings .....                      | 4-9        |
| 4.2.              | Managing firmware versions .....                     | 4-10       |
| 4.2.1.            | Checking firmware versions .....                     | 4-11       |
| 4.2.2.            | Checking the firmware is up-to-date .....            | 4-12       |
| 4.2.3.            | Updating the BMC firmware .....                      | 4-13       |
| 4.2.4.            | Updating the BIOS and CPLD firmware .....            | 4-15       |
| 4.3.              | Configuring date and time settings .....             | 4-17       |
| <b>Chapter 5.</b> | <b>Managing Access .....</b>                         | <b>5-1</b> |
| 5.1.              | LDAP settings .....                                  | 5-1        |
| 5.2.              | Managing users .....                                 | 5-3        |
| 5.2.1.            | Viewing a user list .....                            | 5-3        |
| 5.2.2.            | Viewing privilege roles .....                        | 5-4        |
| 5.2.3.            | Setting the account policy .....                     | 5-5        |
| 5.2.4.            | Creating a new user account .....                    | 5-6        |
| 5.2.5.            | Modifying a user account .....                       | 5-8        |
| 5.2.6.            | Deleting a user account .....                        | 5-9        |
| 5.2.7.            | Disabling/enabling user accounts .....               | 5-10       |
| 5.2.8.            | Manually unlocking a user account .....              | 5-11       |
| 5.3.              | User roles and privileges .....                      | 5-12       |
| 5.4.              | Managing SSL certificates .....                      | 5-13       |
| 5.4.1.            | Viewing certificate list .....                       | 5-13       |
| 5.4.2.            | Adding a certificate .....                           | 5-14       |
| 5.4.3.            | Deleting a certificate .....                         | 5-15       |
| 5.4.4.            | Updating a certificate .....                         | 5-15       |
| 5.4.5.            | Generating a Certificate Signing Request (CSR) ..... | 5-16       |

---

## Preface

This guide explains how to use the Server Hardware Console (SHC) to manage a BullSequana Edge 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>

---

---

## Intended Readers

This guide is intended for use by system administrators and operators



---

## Chapter 1. Getting started

### 1.1. Overview

The BullSequana Edge Server Hardware Console (SHC) provides a web based interface to manage, configure and monitor the server.

The SHC is powered by OpenBMC, an open source implementation of the Baseboard Management Controller (BMC) firmware stack.

## 1.2. Connecting to the Server Hardware Console (SHC)

---

**See** The Getting Started Guide 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

### Procedure

#### 1. Open a web browser on the laptop

Enter the host name or IP address into the address bar.

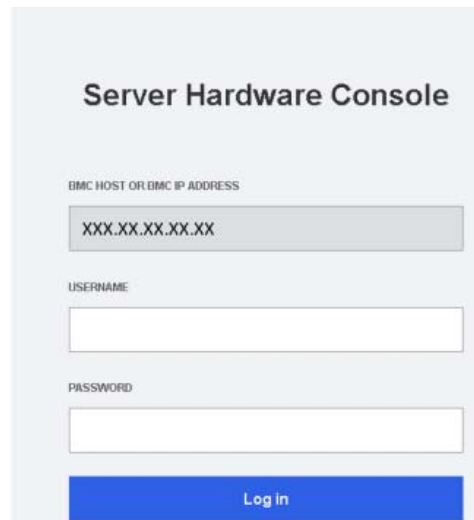
- 
- Notes**
- The factory default host name is in the following format  
http://bullsequanaedge-bmc-<Serial\_Number>.
  - The serial number is written on the label on the side.
- 

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

Ignore all security warning messages including advanced messages.

The Server Hardware Console (SHC) authentication page opens.

**Atos**  
BullSequana Edge





## 1.3. Logging in to the Server Hardware Console (SHC)

### Prerequisites

- A laptop is IP connected with the BullSequana Edge server SHC
- Chrome or Firefox are used to make the connection from the laptop

### Procedure

#### 1. Connect to the SHC

The Server Hardware Console (SHC) authentication page opens.

**Atos**  
BullSequana Edge



Server Hardware Console

BMC HOST OR BMC IP ADDRESS

XXX.XX.XX.XX.XX

USERNAME

PASSWORD

Log in

| 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

---

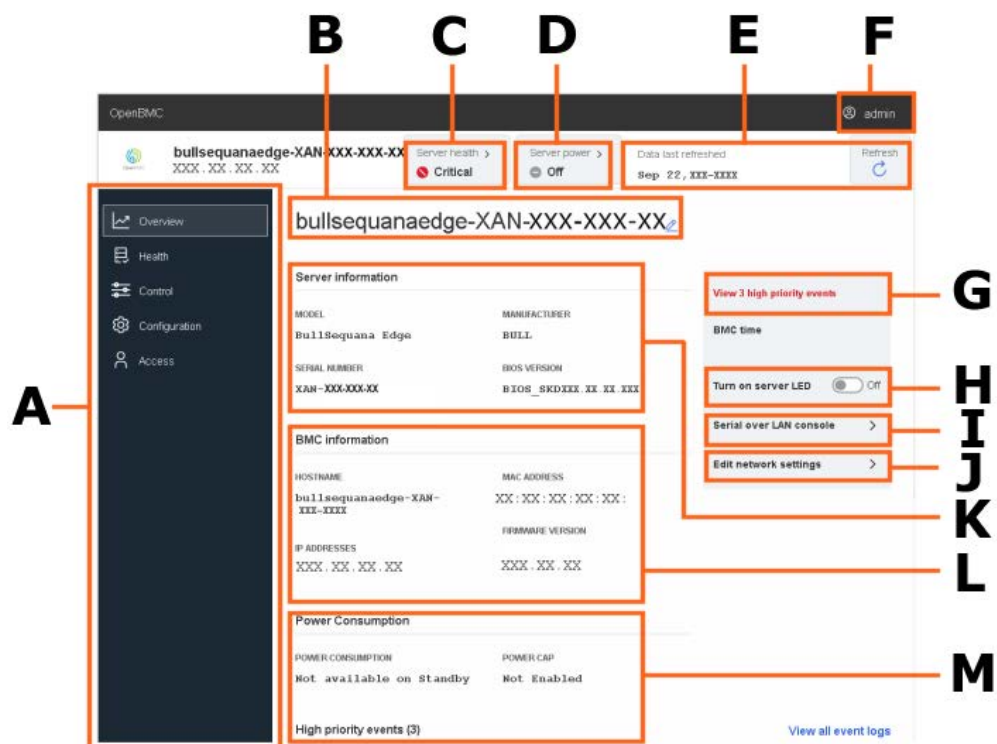
**Important** It is strongly recommended to change the default user password once initial setup is completed, taking care to record the new account details for subsequent connections.

---

## 1.4. The Server overview page

The Server overview page provides a summary of the BullSequana Edge system details and status. It also includes links to some server management and configuration features.

**Note** Some operations, for example, turning on the server LED, can be performed both from the shortcut (H) on the Server overview page or via the feature tab on the left hand side (A).



| Mark | Description   |
|------|---|
| A    | Feature tabs with sub-items used to monitor, manage and configure a BullSequana Edge server |
| B    | The host name of the server. Click <b>Edit</b> to change the host name                      |
| C    | Summary of the server health status with a link to the <b>System Logs</b> page              |
| D    | Server power state with a link to the <b>Server power operations</b> page                   |
| E    | Refresh button for the overview page with the date and time of the last refresh             |
| F    | User profile button to profile password and to log out                                      |
| G    | View high priority SELs. Click the link for more details                                    |
| H    | Button to turn on the server identification LED on the front of the server                  |
| I    | Link to the Serial over LAN (SoL) console page  |
| J    | Link to the Network Settings page   |
| K    | Summary of the server information   |
| L    | Summary of the BMC information  |
| M    | Summary of the power information  |

## 1.5. Server Hardware Console (SHC) features

The SHC tabs include features to:

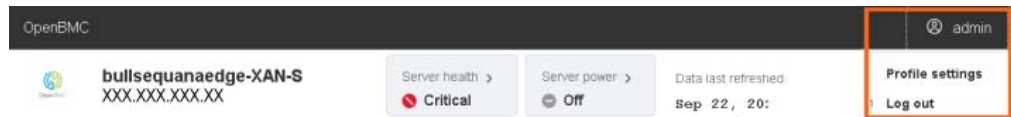
- Provide an overview of the server
- Monitor the health of the server
- Manage the server
- Configure the server
- Configure access and user settings for the server

| Tab           | Item                    |
|---------------|-------------------------|
| Overview      | Server information      |
|               | BMC information         |
|               | Power consumption       |
|               | Events                  |
| Health        | Event log               |
|               | Hardware status         |
|               | Sensors                 |
| Control       | Server power operations |
|               | Manage power usage      |
|               | Server LED              |
|               | Reboot BMC              |
|               | Serial over LAN console |
|               | KVM                     |
|               | Intrusion Detection     |
|               | Security Settings       |
|               | Virtual Media           |
| Configuration | Network settings        |
|               | Firmware                |
|               | Date and time settings  |
| Access        | LDAP                    |
|               | Local users             |
|               | SSL certificates        |

## 1.6. Changing the default password

**Note** The user must have administrator privileges to change the default password.

1. From the **admin** button, click **Profile settings**.



2. The **Profile settings** page opens.

### Profile settings

#### Profile information

USERNAME  
root

#### Change password

##### CURRENT PASSWORD

Enter the Current User Password

##### NEW PASSWORD

Password must between 8 – 20 characters

##### CONFIRM NEW PASSWORD

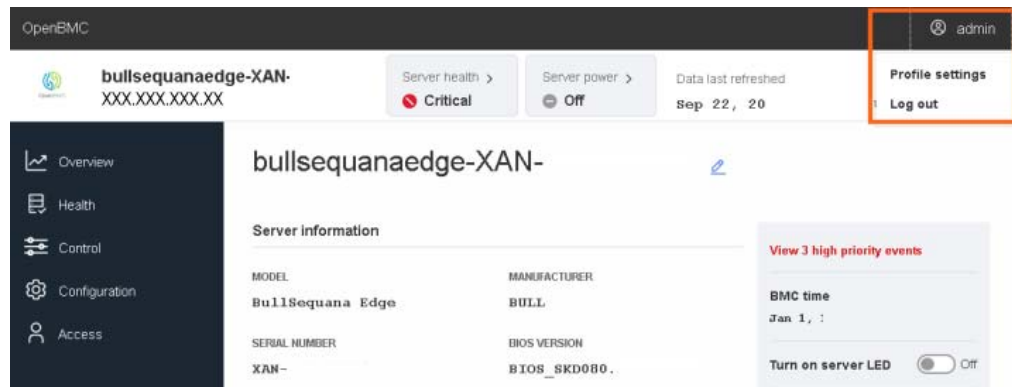
Change password

3. Enter the current password.
4. Enter and confirm the new password. Click **Change password**.

**Note** The password must be between eight and twenty characters long. The password must be different from the user name and not be the word 'password'.

## 1.7. Stopping the Server Hardware Console (SHC)

From the **admin** button, click **Log out** to stop the SHC.





## Chapter 2. Monitoring the server

### 2.1. Checking event logs

#### Prerequisites

The server is in the powered on state

#### Procedure

1. From the **Health** tab, click **Event log**. The **Event log** page opens.

The screenshot shows the 'Event log' page. At the top right, there is a link for 'REMOTE LOGGING SERVER' and a '+ Add server' button. Below this, it says 'All events from the BMC' with a 'USER TIMEZONE' dropdown. A 'FILTER EVENTS' section contains a search bar with a magnifying glass icon, a close 'X' button, and a 'Filter' button. Below the search bar 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 date input fields separated by a minus sign. Below these is a 'FILTER BY EVENT STATUS' dropdown menu currently set to 'All events'. A summary bar shows '3 Events are logged' with icons for 'Delete', 'Mark as resolved', and 'Export'. The event list below shows two entries: #3, 'LOW' severity, 'NOTICE' type, 'Host power is ON', dated 'Nov 30, 2020 08:26:03 UTC+1'; and #2, 'LOW' severity, 'NOTICE' type, dated 'Nov 30, 2020 08:25:36 UTC+1'. Each entry has a checkbox on the left and a dropdown arrow on the right.

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

## 2.2. Adding a remote BMC log server

### Prerequisites

The BullSequana Edge server is in the powered on state

### Procedure

1. From the **Health** tab, click **Event log**. The **Event log** page opens.
2. Click **Add server**.

The screenshot shows the 'Event log' interface. At the top right, there is a 'REMOTE LOGGING SERVER' section with a red box around the '+ Add server' button. Below this is a 'USER TIMEZONE' dropdown. The main area has a 'FILTER EVENTS' search bar and a 'Filter' button. Below the search bar are two filter sections: 'FILTER BY SEVERITY' with buttons for 'All', 'High', 'Medium', and 'Low', and 'FILTER BY DATE RANGE' with two date input fields. Below these is a 'FILTER BY EVENT STATUS' dropdown set to 'All events'. A summary bar indicates '25 Events are logged' with options to 'Delete', 'Mark as resolved', and 'Export'. The event list shows three entries, all with a severity of 'LOW' and status of 'NOTICE'. The first two entries are '[BIOSEvent] CMOS Checksum Validation OK' from July 25, 2019. The third entry is 'Host Force Power OFF Initiated' from June 16, 2020.

3. Enter the server host name or IP address and port parameters.

The screenshot shows a modal dialog box titled 'Add remote logging server'. It has two input fields: 'HOSTNAME OR IP ADDRESS' and 'PORT'. The 'PORT' field has a tooltip that says 'Value must be between 0 - 65535'. At the bottom of the dialog are 'Cancel' and 'Add' buttons. The background shows the 'Event log' page with the 'Add server' button highlighted.

4. Click **Add**.



## 2.3. Checking the hardware status

### Prerequisites

The server is in the powered on state

### Procedure

1. 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      | ▼ |

2. Enter the hardware component in the search field.
3. Click **Filter**.

- Click the downward pointing arrow on the right hand side to expand the information details for a component. Full details including the presence status for the component is displayed.

## Hardware status

**All hardware in the system**

Export

FILTER HARDWARE COMPONENTS

×

Filter

Hardware

System

Motherboard

|                       |                |                |
|-----------------------|----------------|----------------|
| BUILD DATE            | CUSTOM FIELD 1 | CUSTOM FIELD 2 |
| 2019-04-19 - 17:00:00 | XXXXXXXXXX     | 12345678       |
| CUSTOM FIELD 3        | CUSTOM FIELD 4 | CUSTOM FIELD 5 |
| 1234                  | SFOK           | 12001665-002   |
| CUSTOM FIELD 6        | MANUFACTURER   | PART NUMBER    |
| BULL                  | PLEXUS         | 11540978-002   |
| PRESENT               | PRETTY NAME    | SERIAL NUMBER  |
| Yes                   | MIPCS          | XXXXXXXXXX     |
| VERSION               |                |                |
| 02                    |                |                |

- Export** the hardware details, as required.

---

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

---

## 2.4. Collecting BMC logs

### Prerequisites

The BullSequana Edge server is in the powered on state

### Procedure

1. From the **Health** tab, click **Hardware status**. The **Hardware status** page opens.

## Hardware status

All hardware in the system [Export](#)

FILTER HARDWARE COMPONENTS

×Filter

| Hardware    |
|-------------|
| System      |
| Motherboard |
| CPU 0       |
| DIMM 0      |
| DIMM 1      |
| DIMM 2      |
| DIMM 3      |
| Fan 0_ PCI  |
| Fan 1_ CPU  |
| Fan 2_ PSU  |

### Collect BMC logs

[Create log file](#)[Download log file](#)

2. Click **Create log file**.

|           |   |
|-----------|---|
| DIMM 1    | <div><div>✓</div><div>Success!</div><div>Creating log file.</div><div>×</div></div> |
| DIMM 2    |   |
| DIMM 3    | ▼   |
| Fan 0_PCI | ▼   |
| Fan 1_CPU | ▼   |
| Fan 2_PSU | ▼   |
| HDD_0     | ▼   |
| HDD_1     | ▼   |
| PCI_0     | ▼   |
| PCI_1     | ▼   |

**Collect BMC logs**

Creating log file...

Create log file

Download log file

**Note** This operation may take a long time to complete.

3. Wait for the BMC log file to be created.

|           |   |
|-----------|---|
| CPU 0     | <div><div>✓</div><div>Success!</div><div>Log file is ready to download.</div><div>×</div></div> |
| DIMM 0    |   |
| DIMM 1    | ▼   |
| DIMM 2    | ▼   |
| DIMM 3    | ▼   |
| Fan 0_PCI | ▼   |
| Fan 1_CPU | ▼   |
| Fan 2_PSU | ▼   |

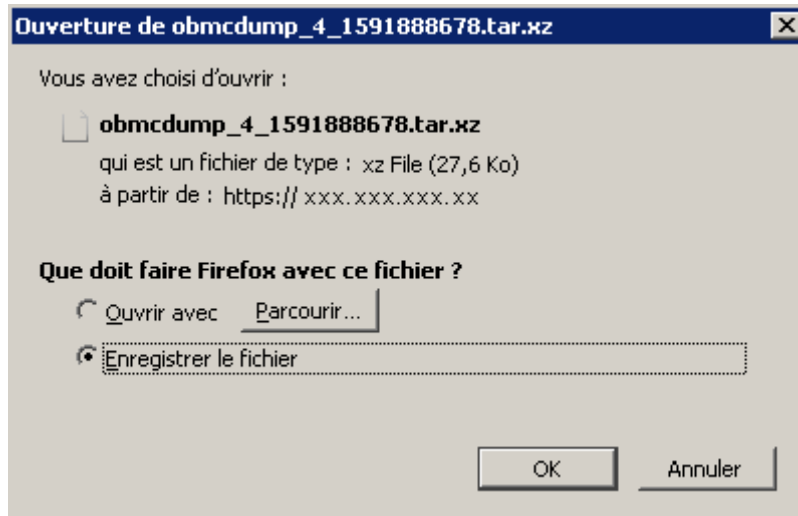
**Collect BMC logs**

Create log file

Download log file

4. When the **Success** message appears, click **Download log file**

5. Save the archive of the BMC logs, as required.



# 2.5. Checking the sensors

## Prerequisites

The server is in the powered on state

## Procedure

1. 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<br>Operation correct. No problem has been detected.   |
| ORANGE               | WARNING<br>A problem has been detected that may need preventive or corrective action.              |
| RED                  | CRITICAL<br>A problem has been detected.<br>Immediate preventive or corrective action is required. |

2. Enter the sensor name in the search field.
3. Set the severity parameter.
4. Click **Filter**.
5. Click **Export** to export the sensor states, as required.

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

---

## Chapter 3. Controlling the server

### 3.1. Checking the power state

#### Procedure

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

#### Server power operations

**Current status** Last power operation at Jan 10, 2020 00:11:11 UTC+1

bullsequanaedge-XXX-XXX-XXXXX - XXX.XX.XX.XX

Running

#### Host OS boot settings

##### BOOT SETTING OVERRIDE

None

☐ Enable one time boot

##### TPM REQUIRED POLICY

Enable to ensure the system only boots when the TPM is functional.

☐ Off

Save

Cancel

#### 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)

| Current Status        |   |
|-----------------------|---|
| Last power operation  | Date and time of last power operation   |
| Host name             | The host name of the server   |
| Power status          | <ul style="list-style-type: none"> <li>• Unreachable</li> <li>• Off</li> <li>• Running</li> </ul>   |
| Host OS boot settings |   |
| Boot Setting Override | <ul style="list-style-type: none"> <li>• None</li> <li>• Pxe - Boots from a PXE server</li> <li>• Hdd - Boots from a hard disk</li> <li>• Cd - Boots from a CD</li> <li>• Diags - Boots from the diagnostic partition</li> <li>• BiosSetup - Boots from the BIOS menu</li> <li>• Usb - Boots from a USB key</li> </ul>  |
| Enable one time boot  | Select to apply the boot setting once   |
| TPM Required Policy   | Ensures the system will only boot if the TPM is fully functional. This feature can be enabled or disabled with the On / Off slider button.  |
| Save button           | Saves the Host OS boot settings   |
| Cancel button         | Cancels the Host OS boot settings   |
| Operations            |   |
| Power on button       | Only active / visible when the server is in standby power mode. Powers on the server  |
| Reboot server         | <p>Only active / visible when the server is in powered on mode</p> <ul style="list-style-type: none"> <li>• Orderly - Shuts down the operating system before the server reboots</li> <li>• Immediate - Server reboots immediately without the operating system shutting down. <b>N.B. Risk of data loss and corruption.</b></li> </ul> <p>Reboot button - reboots the server applying the reboot option selected</p>                |
| Shutdown server       | <p>Only active / visible when the server is in powered on mode</p> <ul style="list-style-type: none"> <li>• Orderly - Shuts down the operating system before the server shuts down</li> <li>• Immediate - Server shuts down immediately without the operating system shutting down. <b>N.B. Risk of data loss and corruption.</b></li> </ul> <p>Shut down button - shuts down the server applying the shut down option selected</p> |



| System Power Restore Policy |  |
|-----------------------------|--|
| Power Restore Policy        | Description  |
| Always On                   | Returns the server to power on mode with the BMC ON and the OS launched.             |
| Always Off                  | Returns the server to standby power mode with the BMC ON but the OS is not launched. |
| Restore                     | Returns the server to the power mode already in place before the reboot.             |

- In the **Current status** section, check the power state. Three power states are possible **Unreachable**, **Off** or **Running**. The date and time of the last power operation is also indicated.

## Server power operations

### Current status

Last power operation at Jan 10, 2020 00:11:11 UTC+1

bullsequanaedge-XXX-XXX-XXXXX - XXX.XX.XX.XX

✓ Running

### Host OS boot settings

## 3.2. Setting boot options for host OS

### Procedure

1. From the **Control** tab, click **Server power operations**. The **Server power operations** page opens.
2. In the **Host OS boot settings** section, from the boot setting override drop-down list select the boot setting required.

#### Host OS boot settings



BOOT SETTING OVERRIDE

None

**None**

Pxe

Hdd

Cd

Diags

BiosSetup

Usb

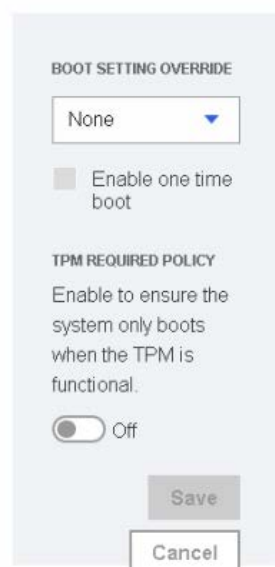
Off

Save

Cancel

3. If required, enable the option so that the system only boots when the Trusted Platform Module (**TPM**) is functional.

#### Host OS boot settings



BOOT SETTING OVERRIDE

None

☐ Enable one time boot

TPM REQUIRED POLICY

Enable to ensure the system only boots when the TPM is functional.

Off

Save

Cancel

4. Click **Save**.

## 3.3. Powering on the server

### Prerequisites

The server is in standby power mode

### Procedure

1. From the **Control** tab, click **Server power operations**. The **Server power operations** page opens.
2. 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)

3. Click **Power on**.

## 3.4. Powering off the server

### 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.

---

**Note** A BullSequana Edge server can also be powered off by pushing the front power button or via the Machine Intelligence System Management (MISM) console.

---

---

**See** The Getting Started Guide or the Management Console User's Guide for more information.

---

### Prerequisites

The server is in the powered on state

### Procedure

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

#### 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)

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

## 3.5. Managing power usage

### Procedure

1. From the **Control** tab, click **Manage power usage**. The **Manage Power Usage** page opens.

### Manage Power Usage

#### Power information

POWER CONSUMPTION

73 W

#### Server power cap setting

Set a power cap to keep power consumption at or below the specified value in watts.

☐ Off

POWER CAP VALUE IN WATTS

0

Cancel

Save settings

2. To set a power cap:
  - a. Enable the **Server power cap setting**.
  - b. Set the power cap value in the **Power Cap Value in Watts** box.
3. Click **Save settings**.

---

**Note** The power consumption and power cap value are indicated on the Server overview page.

---

## 3.6. Enabling / disabling the identification LED

### Procedure

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

#### Server LED

##### LED light control

---

###### Server LED light

Turn the LED light on or off. If the server has an LCD, use this control to display text (on) or not to display text (off) on the LCD.



2. Turn the server identification LED off / on.

---

**See** The Description Guide to locate the blue server identification LED at the front of the server.

---

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

### Procedure

1. 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

2. 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.

## 3.8. Connecting to the Serial over LAN (SoL) console

### Procedure

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.



### 3.9. Connecting to the Keyboard Video Mouse (KVM)

KVM is used by the remote console to transmit the screen data to the administrator machine and the keyboard and mouse data back to the host.

#### Procedure

From the **Control** tab, click **KVM**. The **IP KVM** page opens.

IP KVM



| IP KVM Actions                 |   |
|--------------------------------|---|
| Send Ctrl+Alt+Del              | Click the link to send the Ctrl+Alt+Del key combination to the server OS interface. |
| Send   (Bar)                   | Click the link to enter   within the server OS interface.                           |
| Send @ (at)                    | Click the link to enter @ within the server OS interface.                           |
| Open in new window             | Click the link to open the IP KVM page in a new window.                             |
| Click here to type in the host | Click to enter the OS desktop and perform server operations.                        |

---

**Important** The Send Ctrl+Alt+Del command is for Windows systems only. If the command is launched twice on a Red Hat system the server will reboot.

---

## 3.10. Managing intrusions

Different actions can be configured in the event of an intrusion being detected by the BullSequana Edge server intrusion detection switch. The history and of the intrusions detected are recorded in the System Event Logs.

### 3.10.1. Checking intrusions detected

#### Procedure

1. From the **Control** tab, click **Intrusion Detection**. The **Chassis Intrusion** page opens.

#### Chassis Intrusion

##### CURRENT INTRUSION STATUS

---

NO INTRUSION DETECTED

##### CLEAR INTRUSION

---

CLEAR

NOTE: Intrusion status will be updated during next boot up. Make sure the chassis is properly closed before pressing CLEAR button.

##### ACTION

---

Ignore

Cancel

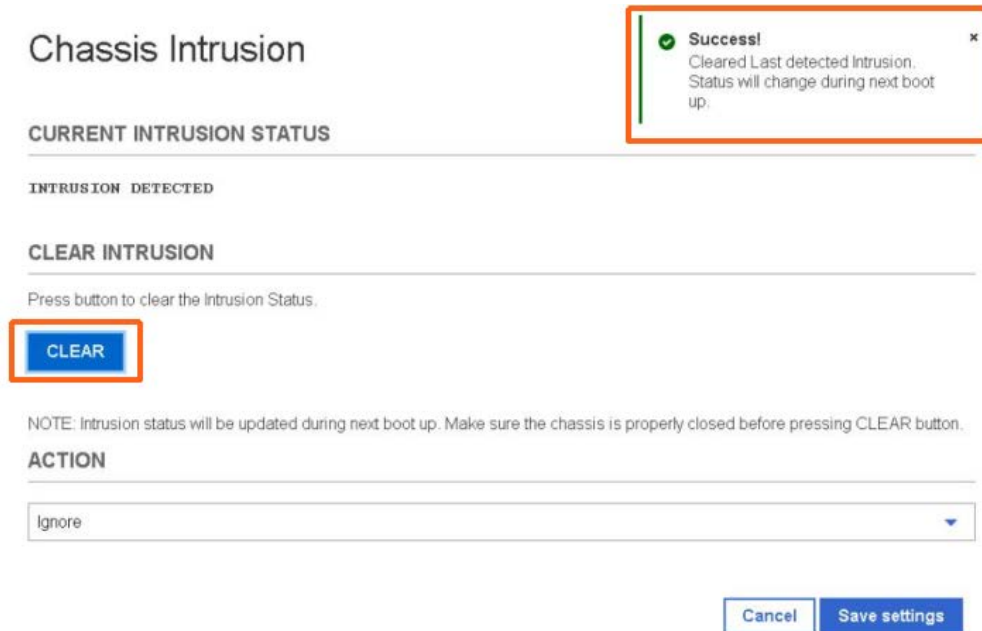
Save settings

2. All intrusions detected are listed under **Current Intrusion Status**.

### 3.10.2. Clearing intrusions detected

#### Procedure

1. From the **Control** tab, click **Intrusion Detection**. The **Chassis Intrusion** page opens.



The screenshot shows the 'Chassis Intrusion' page. At the top right, a green success message box states: 'Success! Cleared Last detected intrusion. Status will change during next boot up.' Below the title, the 'CURRENT INTRUSION STATUS' section shows 'INTRUSION DETECTED'. The 'CLEAR INTRUSION' section contains the instruction 'Press button to clear the Intrusion Status.' and a blue 'CLEAR' button, which is highlighted with an orange box. Below this, a note reads: 'NOTE: Intrusion status will be updated during next boot up. Make sure the chassis is properly closed before pressing CLEAR button.' The 'ACTION' section features a dropdown menu currently set to 'Ignore'. At the bottom right, there are 'Cancel' and 'Save settings' buttons.

2. Click **CLEAR** to remove any actions detected from the list.
3. Wait until the Success message appears.

---

**Note** The intrusion(s) detected will only be cleared from the intrusion status list following a reboot of the host server.

---

### 3.10.3. Configuring actions for intrusions

#### Procedure

1. From the **Control** tab, click **Intrusion Detection**. The **Chassis Intrusion** page opens.

Chassis Intrusion

**CURRENT INTRUSION STATUS**

NO INTRUSION DETECTED

**CLEAR INTRUSION**

CLEAR

NOTE: Intrusion status will be updated during next boot up. Make sure the chassis is properly closed before pressing CLEAR button.

**ACTION**

Ignore  
Power Off  
Ignore

Cancel Save settings

2. In the **Action** section, select either **Power Off** or **Ignore** from the drop down list, for any intrusions detected.

---

**Important** If the **Power Off** action is set, the server will not start until the intrusion is removed from the **Current Intrusion Status** list.

---

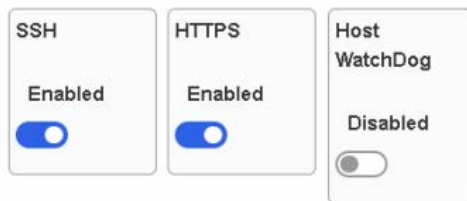
3. Click **Save settings**.

## 3.11. Enabling port security controls

### Procedure

1. From the **Control** tab, click **Security Settings**. The **Ports Control** page opens.

### Ports Control



2. Enable / disable the SSH, HTTPS and Host WatchDog controls as required.

---

**Notes**

- If SSH is disabled, the OpenBMC console will not respond until it is enabled.
- If HTTPS is disabled, neither the web interface or any of the REST commands will respond. HTTPS can only be re-enabled from the OpenBMC console.

---

## 3.12. Creating a virtual media session

### Procedure

1. From the **Control** tab, click **Virtual Media**. The **Virtual Media** page opens.

### Virtual media

Specify image file location to start session.

Virtual media device

Choose file

No file selected

Start

2. Click **Choose file**.
3. Select an ISO file for the boot.
4. Click **Start**.

---

## Chapter 4. Configuring the server

### 4.1. Configuring network settings

#### Prerequisites

- A laptop computer with the Chrome or Firefox browser installed
- The laptop is connected to the BullSequana Edge BMC port
- The server BMC has an IP address allocated
- The laptop computer is connected to the LAN

### 4.1.1. BMC network settings overview

#### Procedure

From the **Configuration** tab, click **Network settings**. The **BMC network settings** page opens.

### BMC network settings

COMMON SETTINGS

HOSTNAME

DEFAULT GATEWAY

bulsequanaedge

XXX.XX.XX.X

IPv4 SETTINGS

NETWORK INTERFACE

MAC ADDRESS

eth0

X:XX:XX:XX:XX:XX

☒ OBTAIN AN IP ADDRESS AUTOMATICALLY USING DHCP

☐ ASSIGN A STATIC IP ADDRESS

Add IPv4 address

☒ ENABLE LINK LOCAL ADDRESSING

Note: Link-Local address will be enabled on one ethernet interface at a time.

IPv4 CUSTOM ROUTE

IPv4 ADDRESS

GATEWAY

NETMASK PREFIX LENGTH

Add

Interface

IPv4 Address

Gateway

DNS SETTINGS

Add DNS server

BMC WIFI SETTINGS

Scan

AVAILABLE NETWORK

PASSWORD

Connect

☐ AUTO CONNECT AFTER BMC REBOOT

Cancel

Save settings



| <b>Common settings</b>                        |  |
|---|--|
| Hostname                                      | The server hostname  |
| Default gateway                               | Default gateway IP address   |
| <b>IPV4 settings</b>                          |  |
| Network interface                             | Select the option required: <ul style="list-style-type: none"> <li>• Eth1</li> <li>• Eth2</li> </ul> |
| MAC address                                   | The server MAC address   |
| Obtain an IP address automatically using DHCP | When enabled, network IP address is retrieved from a DHCP server                                     |
| Assign a static IP address                    | When enabled, network IP address is static   |
| Add IPV4 address button                       | Click to add a static IPV4 address   |
| Enable link local addressing                  | When enabled a link local address will be assigned to the interface.                                 |
| <b>IPV4 custom route</b>                      |  |
| IPV4 address                                  | Valid IP address of the host or Network ID of the Network.   |
| Gateway                                       | Valid IP Address of the gateway.   |
| Netmask prefix length                         | Valid netmask of the Network or the host   |
| Add button                                    | Click to add the IPV4 address  |
| <b>DNS settings</b>                           |  |
| DNS server 1                                  | DNS server IP address  |
| Remove  | Click to remove the DNS server   |
| Add DNS server button                         | Click to add a DNS server  |
| <b>BMC WIFI settings</b>                      |  |
| Scan button                                   | Click to discover the available wireless networks  |
| Available network                             | Lists the available networks. From the drop-down list, select the network required                   |
| Password                                      | Enter the password of the network selected   |
| Connect button                                | Click to connect to the network selected   |
| Autoconnect after BMC reboot                  | Enable to connect automatically to the network selected after a BMC reboot                           |
| <b>Buttons</b>                                |  |
| Cancel  | Click to cancel the operation  |
| Save settings                                 | Save the configuration   |

## 4.1.2. Configuring common settings

### Procedure

1. From the **Configuration** tab, click **Network settings**. The **BMC network settings** page opens.

## BMC network settings

### COMMON SETTINGS

HOSTNAME

bullsequanaedge

DEFAULT GATEWAY

XXX.XX.XX.X

---

**Note** The default gateway for the BMC is configured automatically.

---

2. If required, change the settings for the default gateway.
3. Click **Save settings**.

### 4.1.3. Configuring IPV4 address with DHCP

#### Procedure

1. From the **Configuration** tab, click **Network settings**. The **BMC network settings** page opens.
2. Select the network interface from the drop-down list.
3. In the **IPV4 settings** section, click **OBTAIN AN IP ADDRESS AUTOMATICALLY USING DHCP**.
4. Click **Add IPV4 address**.

#### IPV4 SETTINGS

| NETWORK INTERFACE | MAC ADDRESS       |
|-------------------|-------------------|
| eth0              | XX:XX:XX:XX:XX:XX |

☒ OBTAIN AN IP ADDRESS AUTOMATICALLY USING DHCP

☐ ASSIGN A STATIC IP ADDRESS

**Add IPV4 address**

☒ ENABLE LINK LOCAL ADDRESSING

Note: Link-Local address will be enabled on one ethernet interface at a time.

5. Click **Save settings**.

## 4.1.4. Assigning a static IP address

### Prerequisites

The network parameters for static IP addresses are known

### Procedure

1. From the **Configuration** tab, click **Network settings**. The **BMC network settings** page opens.
2. In the **IPV4 settings** section, click **ASSIGN A STATIC IP ADDRESS**.
3. Click **Add IPV4 address**.

4. Click **Remove** to remove the existing IP address, if one exists.
5. Enter the network parameters for the static IP address.
6. Click **Add IPV4 address** if additional addresses are to be configured.
7. Click **Save settings**.

### 4.1.5. Configuring an IPV4 custom route

It is possible to customize a SSH connection to the BMC from a different network.

#### Procedure

1. From the **Configuration** tab, click **Network settings**. The **BMC network settings** page opens.
2. In the **IPV4 Custom Route** section, enter the network parameters for customized connection.

IPV4 CUSTOM ROUTE

IPV4 ADDRESS

GATEWAY

NETMASK PREFIX LENGTH

Add

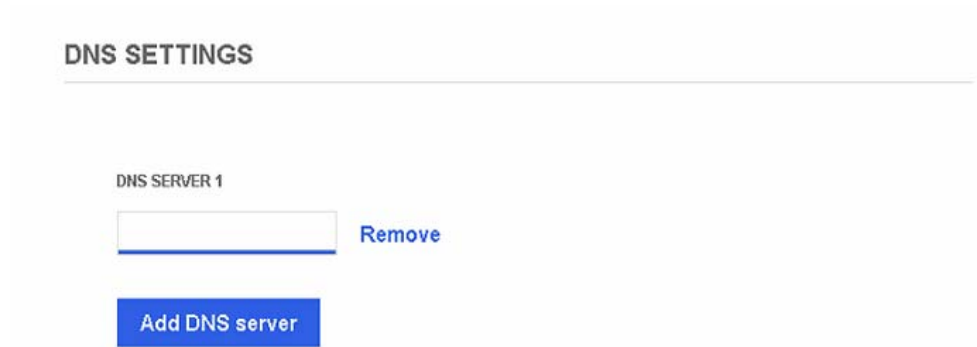
| Interface | IPv4 Address    | Gateway     |                        |
|-----------|-----------------|-------------|------------------------|
| eth0      | xxx.xx.xx.xx/xx | xxx.xx.xx.x | <a href="#">Remove</a> |
| eth0      | xxx.xx.xx.xx/xx | xxx.xx.xx.x | <a href="#">Remove</a> |

3. Click **Add**.
4. If required, click **Remove** to delete existing custom routes.

## 4.1.6. Configuring DNS settings

### Procedure

1. From the **Configuration** tab, click **Network settings**. The **BMC network settings** page opens.
2. In the **DNS settings** section, click **Remove** to remove the existing DNS server



The screenshot shows the 'DNS SETTINGS' section of a web interface. It features a header 'DNS SETTINGS' with a horizontal line below it. Underneath, there is a label 'DNS SERVER 1' above a text input field. To the right of the input field is a blue 'Remove' link. Below the input field is a blue button labeled 'Add DNS server'.

3. Enter the DNS server to be used.
4. Click **Add DNS server**.
5. Click **Save settings**.

## 4.1.7. Configuring WIFI settings

### Prerequisites

- The laptop computer is connected to the WIFI LAN
- The WiFi network and password are known

### Procedure

1. From the **Configuration** tab, click **Network settings**. The **BMC network settings** page opens.
2. In the **BMC WIFI Settings** section, click **Scan**.

**BMC WIFI SETTINGS**

**Scan**

AVAILABLE NETWORK

Not listed? ▼

ENTER SSID

PASSWORD

**Connect**

☐ AUTO CONNECT AFTER BMC REBOOT

**Cancel** **Save settings**

3. From the list of available networks displayed, select the network required.
4. Enter the password and the SSID, as required.
5. Click **Connect**.
6. Check the **Auto Connect after BMC reboot** box to reconnect after a BMC reboot.
7. Click **Save Settings**.

## 4.2. 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.



## 4.2.1. Checking firmware versions

### Prerequisites

The server is in the powered on state

### Procedure

1. 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 |        |

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

## 4.2.2. 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. From the **Configuration** tab, click **Firmware**. The **Firmware** page opens.
2. 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.

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

### 4.2.3. Updating the BMC firmware

#### Prerequisites

The server power status is Off or Running

#### Procedure

1. **Check the server power status**
2. **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

### 3. 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 | <b>Activate</b> <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.

## 4.2.4. 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 power status is Off or Running

### Procedure

#### 1. Check the server power status

#### 2. 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"/> |  |

#### 3. 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 | <a href="#">Activate</a> <a href="#">Delete</a> |

4. **Wait two to three minutes and then refresh the page**

The firmware is now active.

5. **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**.

## 4.3. Configuring date and time settings

### Procedure

1. From the **Configuration** tab, click **Date and time settings**. The **Date and time settings** page opens.

### Date and time settings

Set date and time manually or configure a Network Time Protocol (NTP) Server

☒ OBTAIN AUTOMATICALLY FROM A NETWORK TIME PROTOCOL (NTP) SERVER

NTP SERVER ADDRESS 1 (PRIMARY)

129.184.124.7

Remove

NTP SERVER ADDRESS 2

129.184.124.8

Remove

NTP SERVER ADDRESS 3

129.184.124.9

Remove

Add new NTP server

☐ MANUALLY SET DATE AND TIME

BMC TIME

08/12/2020

16:10:05.000

Central European Standard Time (UTC+01:00)

HOST TIME

08/12/2020

15:59:03.000

Central European Standard Time (UTC+01:00)

TIME OWNER

Split

BMC

Host

Both

Split

Cancel

Save settings

2. Set the data and time, either:
  - a. Either select **Obtain automatically from a Network Time Protocol (NTP) server**.
  - b. Or select **Manually set date and time** and use the **Time owner** drop-down list to set the time owner according to system requirements.

| Time owner | Description   |
|------------|---|
| BMC        | Configure the date and time for the BMC                           |
| Host       | Configure the date and time for the host                          |
| Both       | Configure the date and time for both the BMC and the host         |
| Split      | Configure the BMC date and time settings separately from the host |

3. Click **Save settings**.



## Chapter 5. Managing Access

### 5.1. LDAP settings

From the **Access** tab, click **LDAP**. The **LDAP** settings page opens.

#### LDAP

Configure LDAP settings and manage role groups.

##### Settings

☐ **Enable LDAP authentication**  
LDAP authentication must be enabled to modify role groups.

☐ **Secure LDAP using SSL**  
  
A CA certificate and LDAP certificate are required. One or more are missing.  
  
**Go to SSL certificates**

SERVICE TYPE

☐ Open LDAP  
☐ Active directory

SERVER URI

BIND DN

BIND PASSWORD

BASE DN

USER ID ATTRIBUTE  
(OPTIONAL)

GROUP ID ATTRIBUTE  
(OPTIONAL)

Reset

Save

##### Role groups

Add role group

Remove role groups

| Group name   | Group privilege |
|--|-----------------|
| LDAP authentication must be enabled before creating role groups. |                 |

| Settings                  |   |
|---------------------------|---|
| Enable LDP authentication | Allows LDAP authentication to be configured   |
| Secure LDAP using SSL     | Secures LDAP server using a Secure Socket Layer certificate   |
| Go to SSL certificates    | Redirects to the <b>SSL certificates</b> page. The link is active when LDAP authentication is enabled                           |
| Service type              | Selects the LDAP service type: <ul style="list-style-type: none"><li>• Open LDAP</li><li>• Microsoft Active Directory</li></ul> |
| Server URI                | ldap://<LDAP Server IP>   |

| <b>Settings</b>  |  |
|--|--|
| Bind DN  | Bind Distinguished Name  |
| Bind password  | Bind user password   |
| Base DN  | Base Distinguished Name. The point from which a server will start searching for users. |
| User ID attribute  | The log in attribute that uniquely identifies a single user record.                    |
| Group ID attribute   | The log in attribute that uniquely identifies a group user record.                     |
| Reset button   | Clears the fields  |
| Save button  | Saves the configurations   |
| <b>Role groups</b>   |  |
| Role groups enable a set of permissions to be assigned to a group of administrators or specialist users. |  |
| Group name   | Group name   |
| Group privilege  | Role assigned to the group   |

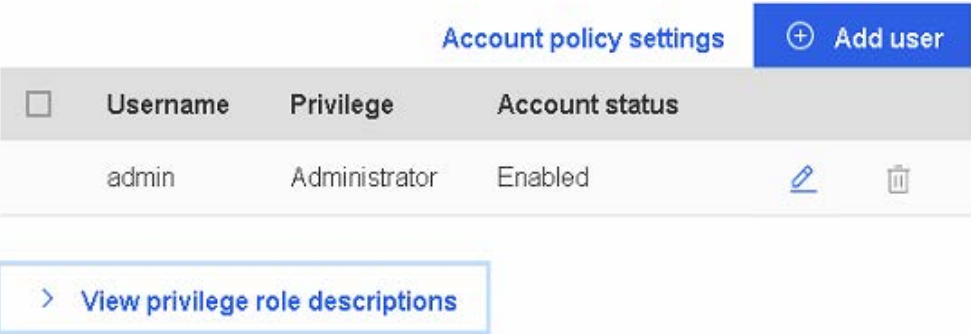
## 5.2. Managing users

### 5.2.1. Viewing a user list

#### Procedure

1. From the **Access** tab, click **Local users**. The **Local user management** page opens.

### Local user management



| Local user management |   |
|-----------------------|---|
| Username              | Name the user uses to log on  |
| Privilege             | Role assigned to the user   |
| Account status        | When enabled, the user account is active and the user is able to log on. When disabled, the user's account is unavailable: the user's account is maintained but it is no longer possible to log on using this account |
| Buttons               |   |
|                       | Edit button to display and modify the user account  |
|                       | Remove button to delete the user  |

## 5.2.2. Viewing privilege roles

### Procedure

1. From the **Access** tab, click **Local users**. The **Local user management** page opens.
2. Click **View privilege role descriptions** to display the roles.

### Local user management

[Account policy settings](#) [+ Add user](#)

| <input type="checkbox"/> | Username | Privilege     | Account status |   |
|--------------------------|----------|---------------|----------------|---|
| <input type="checkbox"/> | admin    | Administrator | Enabled        | <a href="#">Edit</a> <a href="#">Delete</a> |

▼ Hide privilege role descriptions

|  | Admin | Operator | ReadOnly | NoAccess |
|--|-------|----------|----------|----------|
| Configure components managed by this service | ✓     |          |          |          |
| Configure manager resources                  | ✓     |          |          |          |
| Update password for current user account     | ✓     |          |          |          |
| Configure users and their accounts           | ✓     |          |          |          |
| Log in to the service and read resources     | ✓     | ✓        | ✓        |          |
| IPMI access point                            | ✓     | ✓        | ✓        |          |
| Redfish access point                         | ✓     | ✓        | ✓        |          |
| SSH access point                             | ✓     |          |          |          |
| WebUI access point                           | ✓     | ✓        | ✓        |          |

### 5.2.3. Setting the account policy

#### Procedure

1. From the **Access** tab, click **Local users**. The **Local user management** page opens.

## Local user management

| <input type="checkbox"/> | Username | Privilege     | Account status |
|--------------------------|----------|---------------|----------------|
|                          | admin    | Administrator | Enabled        |

[View privilege role descriptions](#)

2. Click the **Account policy settings** tab. The **Account policy settings** page opens.

**Account policy settings**

MAX FAILED LOGIN ATTEMPTS  
Value must be between 0 - 65535  
0

USER UNLOCK METHOD  
☒ Automatic after timeout  
TIMEOUT DURATION (SECONDS)  
Must be at least 1

☒ Manual

Cancel Save

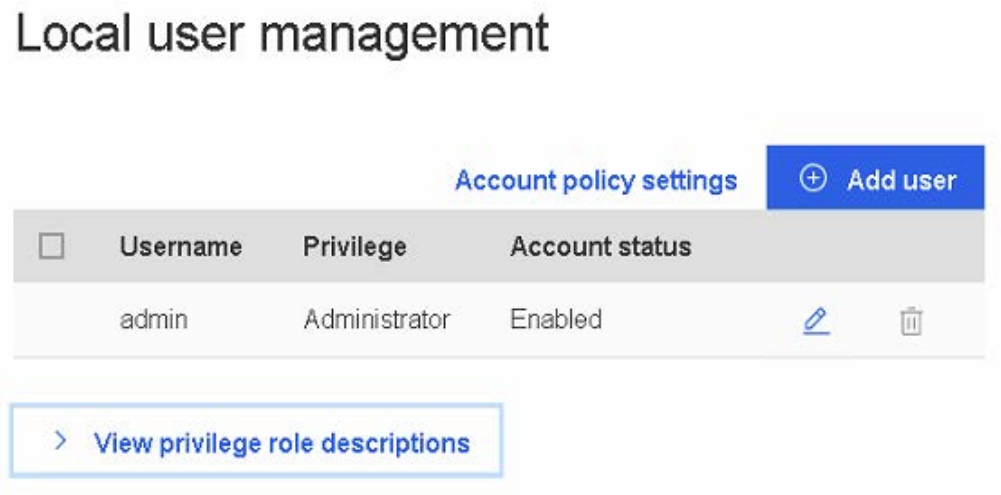
| Account policy settings    |  |
|----------------------------|--|
| Max failed login attempts  | The number of failed login attempts allowed. The value must be set between 0 (default) and 65535 |
| Automatic after timeout    | Automatic unlock after the period set in the Timeout duration parameter                          |
| Timeout duration (seconds) | Period in seconds during which the user account remains locked. The minimum setting is 1 second  |
| Manual                     | A locked user account stays locked until it is unlocked manually                                 |

3. Complete the fields as required.
4. Click **Save**.

## 5.2.4. Creating a new user account

### Procedure

1. From the **Access** tab, click **Local users**. The **Local user management** page opens.



2. Click **Add user** tab. The **Add user** page opens.

Add user

ACCOUNT STATUS

☒ Enabled

☐ Disabled

USER PASSWORD

Password must between 8 – 20 characters

USERNAME

Cannot start with a number  
No special characters except underscore

CONFIRM USER PASSWORD

PRIVILEGE

Select an option

Cancel

Add user

| Add user                |   |
|-------------------------|---|
| Account status enabled  | When selected, the user account is active and the user is able to log on. This is the default status  |
| Account status disabled | When selected, the user's account is unavailable  |
| Username                | Name the user uses to log on <ul style="list-style-type: none"><li>Names cannot start with a number</li><li>Special characters are not allowed except underscores</li></ul>   |
| Privilege               | Use the drop-down list to select the role to assign to the user   |
| User password           | The password the user will user to log on <ul style="list-style-type: none"><li>Minimum password length: 8 characters</li><li>Maximum password length: 20 characters</li><li>The password must be different from the user name</li><li>The password must not be the word 'password'</li></ul> |
| Confirm user password   |   |

3. Complete the fields as required.





4. Click **Add user**. The user is created.

## 5.2.5. Modifying a user account

### Procedure

1. From the **Access** tab, click **Local users**. The **Local user management** page opens.

### Local user management

|                          |          |               |                | Account policy settings   |   | + Add user |
|--------------------------|----------|---------------|----------------|---|---|------------|
| <input type="checkbox"/> | Username | Privilege     | Account status |   |   |            |
|                          | admin    | Administrator | Enabled        |  |  |            |
| <input type="checkbox"/> | Test     | Administrator | Enabled        |  |  |            |

> [View privilege role descriptions](#)

2. Click the **Edit** button of the required user. The **Modify user** page opens.

×

Modify user

ACCOUNT STATUS

☒ Enabled  
☐ Disabled

CURRENT PASSWORD

Enter the current user password

USERNAME

Cannot start with a number  
No special characters except underscore

USER PASSWORD

Password must between 8 – 20 characters

PRIVILEGE

CONFIRM USER PASSWORD

Cancel

Save



3. Modify one (or more) of the following fields depending on the requirements:
  - Account status
  - Username
  - Privilege
4. Enter the current password.
5. Enter and confirm the new password.

---

**Note** The password must be between eight and twenty characters long. The password must be different from the user name and not be the word 'password'.

---

6. Click **Save**. User account details are changed.

## 5.2.6. Deleting a user account

### 5.2.6.1. Deleting a single user account

#### Procedure

1. From the **Access** tab, click **Local users**. The **Local user management** page opens.

### Local user management

|                          |          |               |                | <a href="#">Account policy settings</a> |                   | <a href="#">+ Add user</a> |
|--------------------------|----------|---------------|----------------|---|-------------------|----------------------------|
| <input type="checkbox"/> | Username | Privilege     | Account status |   |                   |                            |
| <input type="checkbox"/> | Test1    | Operator      | Enabled        | <a href="#">✎</a>                       | <a href="#">🗑</a> |                            |
|                          | admin    | Administrator | Enabled        | <a href="#">✎</a>                       | <a href="#">🗑</a> |                            |
| <input type="checkbox"/> | Test3    | Operator      | Enabled        | <a href="#">✎</a>                       | <a href="#">🗑</a> |                            |
| <input type="checkbox"/> | Test     | Operator      | Enabled        | <a href="#">✎</a>                       | <a href="#">🗑</a> |                            |









[> View privilege role descriptions](#)

2. Click the remove button of the required user.
3. Click **Remove** in the confirmation dialog box to remove the user.

### 5.2.6.2. Deleting several user accounts

1. From the **Access** tab, click **Local users**. The **Local user management** page opens.
2. Select the required users. A new menu bar appears.

Local user management

| 2 selected                          |          | Remove        | Enable         | Disable   | Cancel   |
|-------------------------------------|----------|---------------|----------------|---|--|
| <input type="checkbox"/>            | Username | Privilege     | Account status |   |  |
| <input checked="" type="checkbox"/> | Test1    | Operator      | Enabled        |  |  |
|                                     | admin    | Administrator | Enabled        |  |  |
| <input checked="" type="checkbox"/> | Test3    | Operator      | Enabled        |  |  |
| <input type="checkbox"/>            | Test     | Operator      | Enabled        |  |  |

[View privilege role descriptions](#)









3. Click **Remove** in the menu bar.
4. Click **Remove** in the confirmation dialog box to remove the users.

### 5.2.7. Disabling/enabling user accounts

#### Procedure

1. From the **Access** tab, click **Local users**. The **Local user management** page opens.
2. Select the required user(s). A new menu bar appears.

Local user management

| 2 selected                          |          | Remove        | Enable         | Disable   | Cancel  |
|-------------------------------------|----------|---------------|----------------|---|---|
| <input type="checkbox"/>            | Username | Privilege     | Account status |   |   |
| <input checked="" type="checkbox"/> | Test1    | Operator      | Enabled        |  |  |
|                                     | admin    | Administrator | Enabled        |  |  |
| <input checked="" type="checkbox"/> | Test3    | Operator      | Enabled        |  |  |
| <input type="checkbox"/>            | Test     | Operator      | Enabled        |  |  |

[View privilege role descriptions](#)

3. To disable the account(s), click **Disable** in the menu bar; to enable the account(s), click **Enable** in the menu bar.





## 5.2.8. Manually unlocking a user account

### Procedure

1. From the **Access** tab, click **Local users**. The **Local user management** page opens.

Local user management


Account policy settings [+ Add user](#)

| <input type="checkbox"/> | Username | Privilege     | Account status |   |   |
|--------------------------|----------|---------------|----------------|---|---|
|                          | admin    | Administrator | Enabled        |  |  |
| <input type="checkbox"/> | Test     | Administrator | Locked         |  |  |

[View privilege role descriptions](#)

2. Click the Edit button to edit the locked user account.

Modify user ×

 Account locked [Unlock](#)


ACCOUNT STATUS

☒ Enabled

☐ Disabled

USER PASSWORD

Password must between 8 – 20 characters


\*\*\*\*\* 

USERNAME


Cannot start with a number  
No special characters except underscore

Test

CONFIRM USER PASSWORD

\*\*\*\*\* 

PRIVILEGE

Administrator 

[Cancel](#) [Save](#)

3. Click **Unlock**.
4. Click **Save**.

### 5.3. User roles and privileges

For each user account, a profile is created that includes the user name, the password and a role. Different sets of privileges are available for each user role.

| Privilege                                    | User Role |          |           |           |
|--|-----------|----------|-----------|-----------|
|  | Admin     | Operator | Read Only | No Access |
| Configure components managed by this service | X         |          |           |           |
| Configure manager resources                  | X         |          |           |           |
| Update password for current user             | X         |          |           |           |
| Configure users and their accounts           | X         |          |           |           |
| Log in to the service and read resources     | X         | X        | X         |           |
| IPMI access point                            | X         | X        | X         |           |
| Redfish access point                         | X         | X        | X         |           |
| SSH access point                             | X         |          |           |           |
| Web UI access point                          | X         | X        | X         |           |

---

**See**    [Section 5.2. Managing users, on page 5-3](#)

---

## 5.4. Managing SSL certificates



### 5.4.1. Viewing certificate list



#### Procedure

From the **Access** tab, click **SSL certificates**. The **SSL certificates** page opens.

#### SSL certificates

[+ Add new certificate](#) [+ Generate CSR](#)

| Certificate       | Issued by | Issued to | Valid from   | Valid until  | Actions   |
|-------------------|-----------|-----------|--------------|--------------|---|
| HTTPS Certificate | testhost  | testhost  | Sep 30, 2020 | Sep 28, 2030 |   |

| SSL certificates  |  |
|---|--|
| Certificate   | Certificate name                         |
| Issued by   | Certificate details                      |
| Issued to   |  |
| Valid from  | Validity period                          |
| Valid until   |  |
| Actions   |  |
|  | Update button to replace the certificate |
|  | Remove button to delete the certificate  |

## 5.4.2. Adding a certificate

### Procedure

1. From the **Access** tab, click **SSL certificates**. The **SSL certificates** page opens.

#### SSL certificates

| <div><a href="#">+ Add new certificate</a> <a href="#">+ Generate CSR</a></div> |           |           |              |              |   |
|---|-----------|-----------|--------------|--------------|---|
| Certificate   | Issued by | Issued to | Valid from   | Valid until  | Actions   |
| HTTPS Certificate   | testhost  | testhost  | Sep 30, 2020 | Sep 28, 2030 |   |

2. Click the **Add new certificate** tab. The **Add new certificate** page opens.

Add new certificate

CERTIFICATE TYPE

Select an option

CERTIFICATE FILE

Choose file

No file selected

Cancel

Save

3. Use the drop-down list to select a certificate type. There are two possible options:

- LDAP Certificate
- CA Certificate

4. Click **Choose file** and select a certificate file.

---

**Note** The certificate file must be a .pem file.

---

5. Click **Save**.




### 5.4.3. Deleting a certificate

#### Procedure

1. From the **Access** tab, click **SSL certificates**. The **SSL certificates** page opens.

#### SSL certificates

[+ Add new certificate](#) [+ Generate CSR](#)

| Certificate       | Issued by | Issued to | Valid from   | Valid until  | Actions   |
|-------------------|-----------|-----------|--------------|--------------|---|
| HTTPS Certificate | testhost  | testhost  | Sep 30, 2020 | Sep 28, 2030 |   |
| CA Certificate    |           |           | Aug 12, 2020 | Aug 13, 2030 |   |

2. Click the remove button of the required certificate.
3. Click **Remove** in the confirmation dialog box to remove the certificate.





### 5.4.4. Updating a certificate

#### Procedure

1. From the **Access** tab, click **SSL certificates**. The **SSL certificates** page opens.

#### SSL certificates

[+ Add new certificate](#) [+ Generate CSR](#)

| Certificate       | Issued by | Issued to | Valid from   | Valid until  | Actions   |
|-------------------|-----------|-----------|--------------|--------------|---|
| HTTPS Certificate | testhost  | testhost  | Sep 30, 2020 | Sep 28, 2030 |   |
| CA Certificate    |           |           | Aug 12, 2020 | Aug 13, 2030 |   |

2. Click the update button of the required certificate.

## SSL certificates

[+ Add new certificate](#) [+ Generate CSR](#)

| Certificate       | Issued by | Issued to | Valid from   | Valid until  | Actions |
|-------------------|-----------|-----------|--------------|--------------|---------|
| HTTPS Certificate | testhost  | testhost  | Sep 30, 2020 | Sep 28, 2030 |         |
| CA Certificate    |           |           | Aug 12, 2020 | Aug 13, 2030 |         |

×  No file selected

3. Click **Choose file** and select a certificate file.
4. Click **Replace**.

### 5.4.5. Generating a Certificate Signing Request (CSR)

#### Procedure

1. From the **Access** tab, click **SSL certificates**. The **SSL certificates** page opens.

## SSL certificates

[+ Add new certificate](#) [+ Generate CSR](#)

| Certificate       | Issued by | Issued to | Valid from   | Valid until  | Actions |
|-------------------|-----------|-----------|--------------|--------------|---------|
| HTTPS Certificate | testhost  | testhost  | Sep 30, 2020 | Sep 28, 2030 |         |



- Click the **Generate CSR** tab. The **Generate CSR** page opens.

X

### Generate a Certificate Signing Request (CSR)

---

**GENERAL**

CERTIFICATE TYPE ^

Select an option ▼

COUNTRY ^

STATE ^

CITY ^

COMPANY NAME ^

COMPANY UNIT ^

COMMON NAME ^

CHALLENGE PASSWORD

CONTACT PERSON

EMAIL ADDRESS

ALTERNATE NAME ^

[+ Add another alternate name](#)

**PRIVATE KEY**

KEY PAIR ALGORITHM ^

Select an option ▼

Cancel

Generate CSR

| General            |   |
|--------------------|---|
| Certificate type   | Use the drop-down list to select the option required: <ul style="list-style-type: none"> <li>HTTPS certificate</li> <li>LDAP certificate</li> </ul>                                       |
| Country            | Use the drop-down list to select the country  |
| State              | Name of the state   |
| City               | Name of the city  |
| Company name       | Name of the company   |
| Company unit       | Generally the name of the department (within the company) using the system (example: Research and Development)  |
| Common name        | "Fully Qualified Domain Name" (FQDN) (example: hostName.DomainName.Top-LevelDomain).  |
| Challenge password | Depending on the certification authority, it may be necessary to define a password to authorize changes being made later to the certificate (For example: revocation of the certificate). |
| Contact person     | Generally the administrator's name  |
| Email address      | Generally the administrator's email address   |
| Alternate name     | Subject alternative name  |

| General                    |  |
|----------------------------|--|
| Add another alternate name | Click to add another Alternate name field  |
| Private key                |  |
| Key pair algorithm         | Use the drop-down list to select the option required: <ul style="list-style-type: none"> <li>• EC</li> <li>• RSA</li> </ul>  |
| Key curve ID               | This field is displayed when the EC option is selected. Use the drop-down list to select the option required: <ul style="list-style-type: none"> <li>• None</li> <li>• prime256v1</li> <li>• secp521r1</li> <li>• secp384r1</li> </ul> |
| Key bit length             | This field is displayed when the RSA option is selected. Length of the generated key in bits. Use the drop-down list to select 2048 bits   |

3. Complete the fields as required.
4. Click **Generate CSR**. A new page opens.

×

Certificate Signing Request (CSR)

-----BEGIN CERTIFICATE REQUEST-----

MIIC4zCCAcscAQEwgZ0xFTATBgNVHREMDHd3dy5hdG9zLmNybTENMAAsGA1UEBwwwE  
(...)
r2Y+t9oo3s6kzNxXHKEkVIne43oMd1I=

-----END CERTIFICATE REQUEST-----

Copy

Download

5. Click **Copy** or **Download** to save the CSR to the computer and to send it to the Certification Authority, who will check the information, and then generate and return a signed certificate.



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