

EVIDEN

BullSequana EX & AI

SHC 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 2024, part of Eviden group. Eviden is a registered trademark of Eviden SAS. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Bull SAS.

Trademarks and Acknowledgments

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

November 2024

**Eviden
30 bis rue du Nid de Pie
49000 Angers
FRANCE**

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

Table of contents

Preface	p-1
Intended Readers	p-1
Chapter 1. Getting started	1-1
1.1. Overview	1-1
1.2. Connecting to the Server Hardware Console (SHC)	1-2
1.3. The Overview page	1-3
1.4. SHC features	1-5
1.5. Changing the user password	1-7
Chapter 2. Monitoring the system	2-1
2.1. Checking hardware information	2-1
2.2. Checking event logs	2-4
2.3. Checking the sensors	2-5
2.4. Collecting Logs	2-6
Chapter 3. Controlling the system	3-1
3.1. Managing server power operations	3-1
3.1.1. Power management features overview	3-1
3.1.2. Checking Power State	3-3
3.1.3. Setting boot options	3-4
3.1.4. Powering on the server	3-6
3.1.5. Rebooting or shutting down the server	3-7
3.2. Connecting to the Keyboard, Video, Mouse (KVM)	3-8
3.3. Connecting to the Serial Over LAN (SOL) console	3-9
3.4. Creating a virtual media session	3-10
3.5. Configuring the power restore policy	3-11
3.6. Enabling or disabling the server identification LED	3-12
3.7. Resetting settings to default values	3-13
3.8. Managing power usage	3-16
3.9. Rebooting the BMC	3-16
Chapter 4. Configuring the management controller	4-1
4.1. Setting the date and time	4-1
4.2. Managing firmware versions	4-3
4.3. Configuring network settings	4-4
4.4. Configuring Rsyslog	4-7

4.5.	Configuring KVM settings	4-8
4.6.	Configuring Global settings	4-9
Chapter 5.	Managing users	5-1
5.1.	Managing client sessions	5-1
5.2.	Configuring LDAP	5-2
5.3.	Managing local users	5-4
5.3.1.	Viewing a user list	5-4
5.3.2.	Viewing privilege roles	5-5
5.3.3.	Setting the account policy	5-7
5.3.4.	Creating a new user account	5-8
5.4.	Managing SSL certificates	5-10
5.4.1.	Viewing SSL certificates	5-10
5.4.2.	Adding a certificate	5-10
5.4.3.	Generating a Certificate Signing Request (CSR)	5-11
5.4.4.	Deleting a certificate	5-13
5.4.5.	Updating a certificate automatically	5-14

Preface

This guide explains how to use the SHC to manage the server.

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

Intended Readers

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

Chapter 1. Getting started

1.1. Overview

The Server Hardware Console (SHC) for BullSequana EX & AI servers 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)

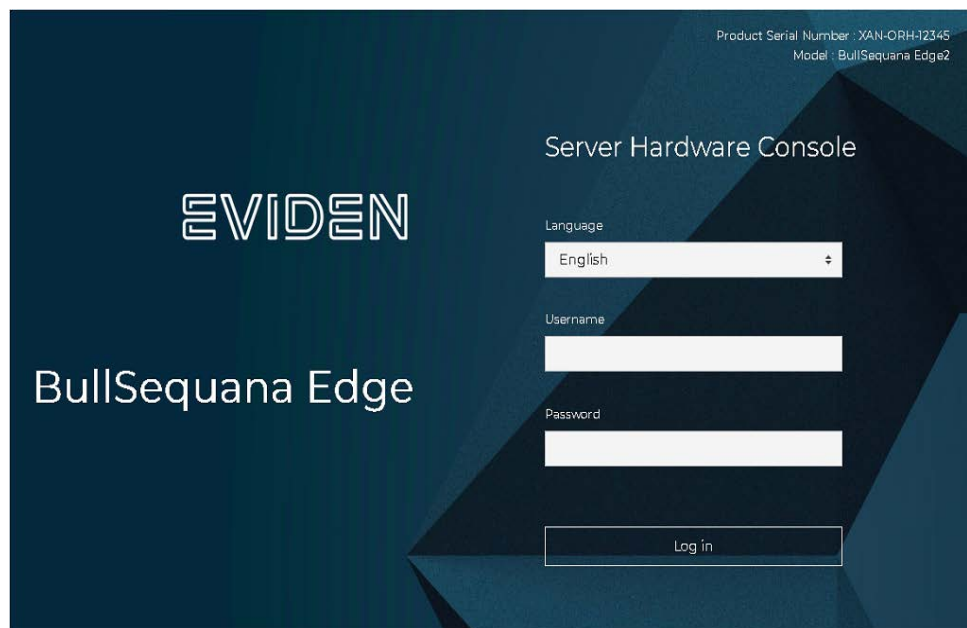
Prerequisites

- A laptop is connected to the server via the LAN
- An IP address is available for the server
- Chrome or Firefox web browsers are recommended
- Setting the language of the web browser to English is recommended

Procedure

Note The connection to the SHC must be made using the https protocol.

1. Open a web browser on the laptop.
2. Enter the server IP address into the address bar, using the https secure protocol.
3. Ignore all security messages displayed, including advanced messages. The SHC authentication page opens.



4. Complete the Username and Password fields and click **Log in**.

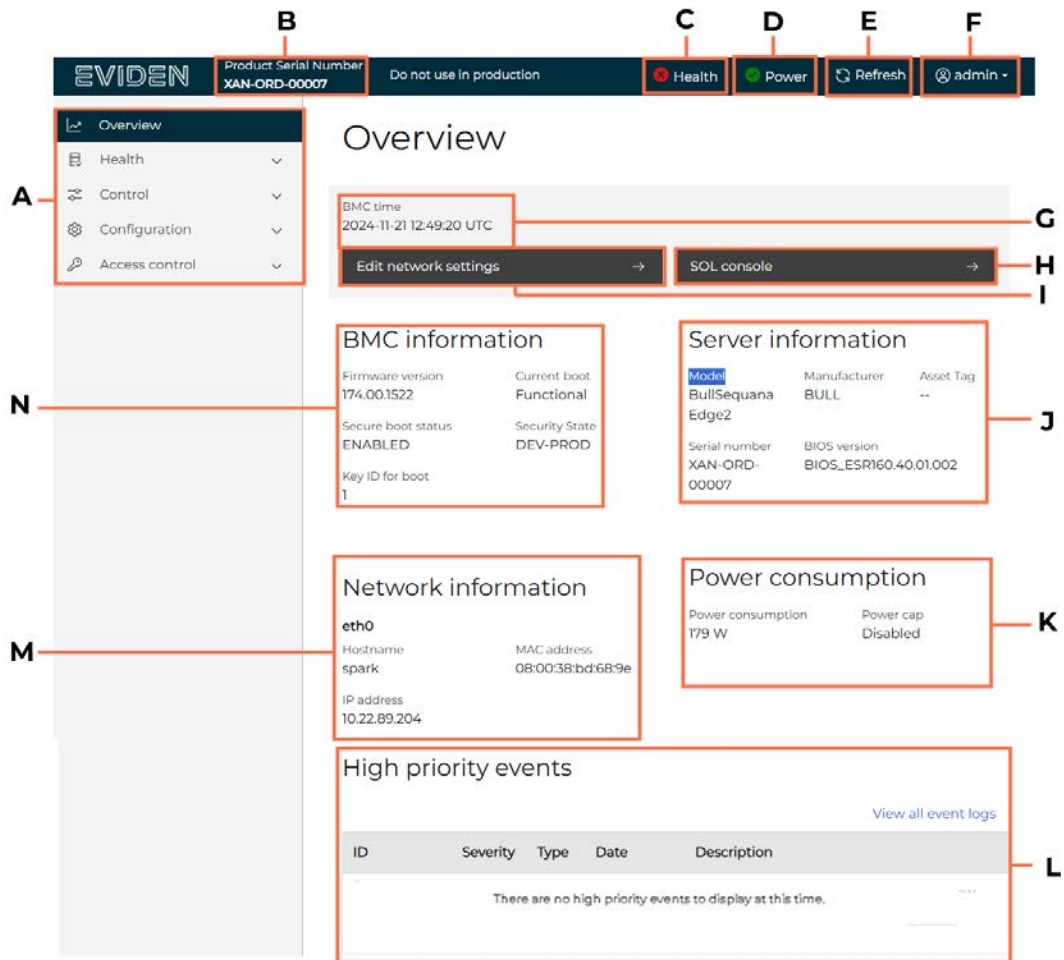
The Overview page opens

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

1.3. The Overview page

This page provides a summary of system details and their status. It also includes links to server management and configuration features.

Note Some operations, for example, editing network settings, can be performed both from the shortcut (I) on the 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 server
B	Product serial number of the server
C	Summary of the server health status with a link to the System Logs
D	Server power status with a link to the Server power operations page.
E	Refresh button for the Overview page. The date and time of the last refresh is shown in the BMC time section.
F	admin button with links to user profile settings and the log out button.

Mark	Description
G	BMC time showing the time and date for the information displayed on the Overview page.
H	Link to the Serial over LAN (SoL) console page
I	Link to the Network Settings page
J	Server details
K	Power consumption and power cap details
L	View high priority event logs. Critical events only are shown. To see all the event logs click View all event logs
M	Summary of network information
N	Summary of BMC information

1.4. 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
	Network information
	High priority event logs
Health	Hardware information
	Event log
	Sensors
	Log Collect
Control	Server power operation
	KVM
	SOL console
	Virtual Media
	Power restore policy
	Server ID LED
	Reset to default
	Manage power usage
	Reboot BMC
Configuration	Date and time settings
	Firmware
	Network settings
	Rsyslog
	KVM settings
	Global settings

Tab	Item
Access control	Client sessions
	LDAP
	Local user management
	SSL certificates

1.5. Changing the user password

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

1. From the user profile button, click **Profile settings**.



The **Profile settings** page opens.

Profile settings

Profile information

Username
admin
Privilege
Administrator

Change password

New password

Password must be between 8 – 20 characters ... ⓘ

Confirm new password

Timezone display preference

Select how time is displayed throughout the application

Timezone

- Default (UTC)
 Browser offset (CEST UTC+2)

Save settings

2. Enter and confirm the new password.
 - The password must be between 8 and 20 characters long
 - The password must be a mixture of upper case letters, lower case letters, numbers and special characters
 - The password must be different from the user name
3. Click **Save settings**.

Note According to the localisation the timezone can also be changed, for example in France UTC+2 would be used.

Chapter 2. Monitoring the system

2.1. Checking hardware information

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

Hardware information

System [↓ Get Identity Card](#) **B**

ID	Health	Part number	Serial number
<input checked="" type="checkbox"/> system	✔ OK	--	XAN-ORD-00007

A

Boards

Q Search 5 items

ID	Health	Part number	Serial number
∨ ORIUGRB	✔ OK	12002008	--
∨ ORM2BRB	✔ OK	12002023	--
∨ ORNBB	✔ OK	12002014	--
∨ ORPDB	✔ OK	111276858-001	P00000CCC
∨ motherboard	✔ OK	11861150-005	P0234404W

PCIe devices

Q Search 13 items

ID	Manufacturer	Device Name
∨ Pcie_internal_pcie25	Micron Technology Inc	7450 PRO NVMe SSD 800GB M.2
∨ Pcie_internal_pcie27	Micron Technology Inc	7450 PRO NVMe SSD 800GB M.2
∨ Pcie_internal_pcie29	Micron Technology Inc	7450 PRO NVMe SSD 800GB M.2

DIMM slot

Q Search	0 items		
ID	Health	Part number	Serial number
No items available			

Power supplies

ID	Health	Part number	Serial number
PSU1	OK	--	1358132NAA221000023

Processors

Q Search	1 items		
ID	Health	Part number	Serial number
CPU0	OK	PK8071305490600	6959905531

Storage

Q Search	8 items		
ID	Health	Part number	Serial number
NBB_M2_DISK0	Ok	--	2320416A8E1D
NBB_M2_DISK6	Ok	--	2320416A8E85
NBB_M2_DISK7	Ok	--	2320416A8F70

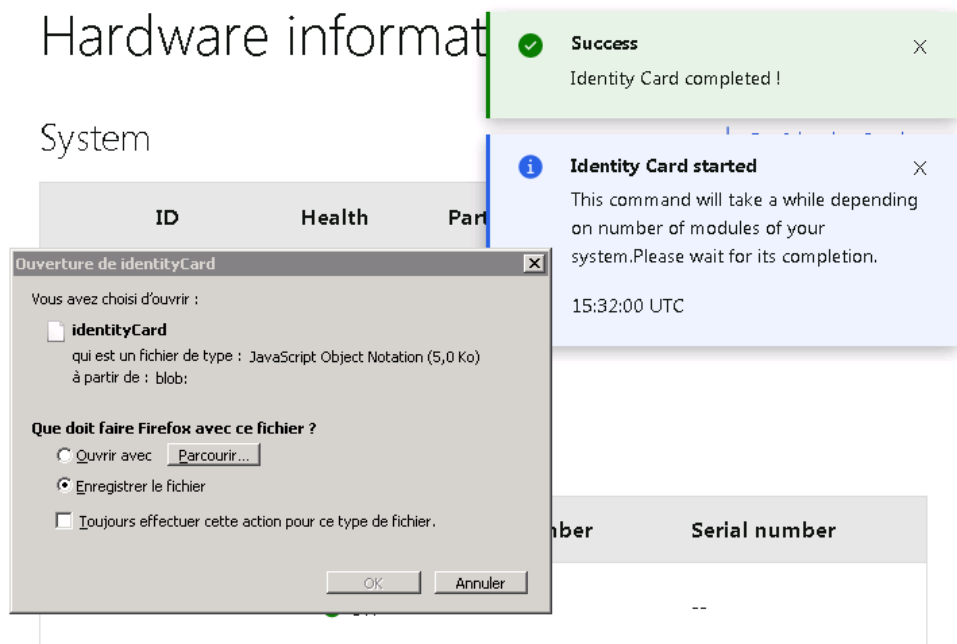
BMC manager

ID	Health	Part number	Serial number
bmc	OK	--	--

2. Click the downward pointing arrow (A) to expand the information details for a component.

Note The Part number and Model parameters are not available for M.2 NVMe disks.

3. Click **Get Identity Card (B)** to obtain the hardware information as an identity card in the .json format.



2.2. Checking event logs

Displaying event logs

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

The screenshot shows the 'Event logs' interface. At the top right is a 'Delete all event logs' button (C). Below it is a search bar (A) with 'Search logs' and '2294 items'. Underneath are date range filters (B) for 'From date' and 'To date', both showing 'YYYY-MM-DD'. A 'Filter' button (D) is on the right. The main table (E) has columns for ID, Severity, Date, and Description. Three log entries are visible: 1686047387 (OK), 1686047345 (OK), and 1686047344 (Warning). Each entry has an export icon (E).

Mark	Description
A	Alphabetical search
B	Date range search
C	Log deletion
D	Severity filter
E	Export of log to a json file

Filtering event logs

Enter one or more search criteria in the alphabetical search (A), date range (B) and severity (D) fields to filter the event logs displayed.

Exporting event logs

Click the arrow (E) to export an event log to a json file.

Deleting event logs

Click (C) to delete all event logs.

2.3. Checking the sensors

Displaying sensors

From the **Health** tab, click **Sensors**. The **Sensors** page opens.

Sensors

A 6 of 21 items

B Status Filter

C Sensor type Filter

<input type="checkbox"/>	Sensor type	Name	Status	Lower critical	Lower warning	Current value	Upper warning	Upper critical
<input type="checkbox"/>	Fan	Fan0 DIMM R	OK	5600 RPM	8000 RPM	8206 RPM	40000 RPM	41800 RPM
<input type="checkbox"/>	Fan	Fan1 CPU	OK	5600 RPM	8000 RPM	8252 RPM	40000 RPM	41800 RPM
<input type="checkbox"/>	Fan	Fan2 CPU	OK	5600 RPM	8000 RPM	8183 RPM	40000 RPM	41800 RPM
<input type="checkbox"/>	Fan	Fan3 DIMM L	OK	5600 RPM	8000 RPM	8104 RPM	40000 RPM	41800 RPM
<input type="checkbox"/>	Fan	Fan4 GPU	OK	5600 RPM	8000 RPM	8115 RPM	40000 RPM	41800 RPM
<input type="checkbox"/>	Fan	Fan5 GPU	OK	5600 RPM	8000 RPM	8241 RPM	40000 RPM	41800 RPM

Mark	Description
A	Alphabetical search
B	Status filter
C	Sensor type filter

Filtering sensors

Enter one or more search criteria in the alphabetical search (A), date range (B) and severity (C) fields to filter the sensors displayed.

2.4. Collecting Logs

A log file is a collection of the logs for the connected server.

Displaying logs

From the **Health** tab, click **Log Collect**. The **Log Collect** page opens.

Mark	Description
A	Log file creation
B	Alphabetical search
C	Data range search
D	Log file download
E	Log file deletion

Filtering logs

Enter the search item (B) and / or the date range (C) to filter the log files displayed.

Collecting logs

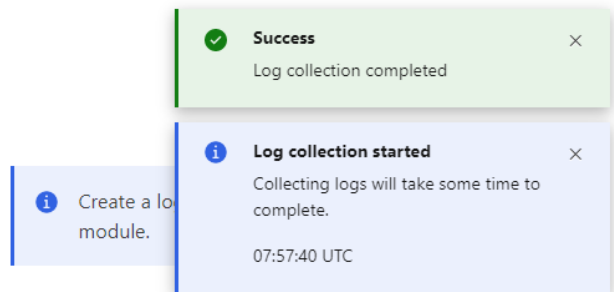
Note Due to space restrictions, it is advisable to delete the existing logs before perform a new log collect.

Click **Get logs** (A) to create a new log collection.

Log Collect

Initiate log

Get logs



Exporting event logs

Click the arrow (D) to download a log file.

Deleting event logs

Click (E) to delete the log file.

Chapter 3. Controlling the system

3.1. Managing server power operations

3.1.1. Power management features overview

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

Server power operations

Current status

Host status

Not available

Last power operation

2023-06-08 08:32:26 UTC

Last memory size

448 GiB

Host OS boot settings

Boot settings override

None

Instance 0

Enable one time boot

TPM required policy

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

Enabled

Save

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

Current Status	
Host status	<ul style="list-style-type: none"> ▪ On ▪ Off ▪ Not available
Last power operation	Date and time of last power operation
Last memory size	Memory size detected by the BIOS during last boot
Host OS boot settings	
Boot Setting Override	<ul style="list-style-type: none"> ▪ None ▪ Pxe - Boots from a PXE server ▪ Hdd - Boots from a hard disk ▪ Diags - Boots from the diagnostic partition ▪ BiosSetup - Boots from the BIOS menu ▪ Usb - Boots from a USB key
Enable one time boot	Select to apply the boot setting once
Enable button for TPM Required Policy	Ensures the system will only boot if the TPM is fully functional. This feature can be enabled or disabled with the Enabled button
Save button	Saves the Host OS boot settings
Operations	
Power on button	Only visible when the server power status is Off Powers on the server
Reboot server	<p>Only visible when the server power status is Running</p> <ul style="list-style-type: none"> ▪ Orderly - Shuts down the operating system before the server reboots ▪ Immediate - Server reboots immediately without the operating system shutting down. N.B. Risk of data loss and corruption <p>Reboot button - Reboots the server applying the reboot option selected</p>
Shutdown server	<p>Only visible when the server power status is Running</p> <ul style="list-style-type: none"> ▪ Orderly - Shuts down the operating system before the server shuts down ▪ Immediate - Server shuts down immediately without the operating system shutting down. N.B. Risk of data loss and corruption <p>Shut down button - Shuts down the server applying the shut down option selected</p>

3.1.2. Checking Power State

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

Server power operations

Current status

Host status

Off

Last power operation

1970-01-01 00:00:00 UTC

Last memory size

240 GiB

Current Status	
Host status	<ul style="list-style-type: none">▪ On▪ Off▪ Not available
Last power operation	Date and time of last power operation

3.1.3. Setting boot options

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

Host OS boot settings

Boot settings override

None

None

Pxe

Hdd

Diags

BiosSetup

Usb

Enabled

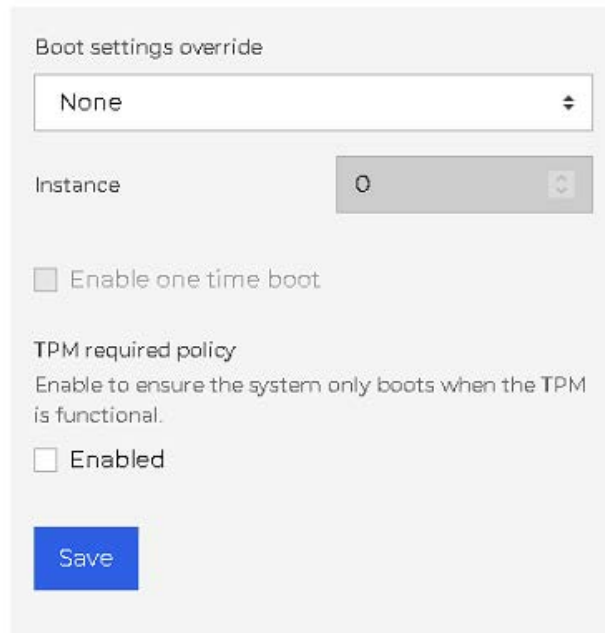
Save

Host OS boot settings	
Boot Setting Override	<ul style="list-style-type: none">▪ None▪ Pxe - Boots from a PXE server▪ Hdd - Boots from a hard disk▪ Diags - Boots from the diagnostic partition▪ BiosSetup - Boots from the BIOS menu▪ Usb - Boots from a USB key

3. If required, click **Enable one time boot** to apply the boot setting once.

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

Host OS boot settings



The screenshot shows a dialog box titled "Host OS boot settings" with a light gray background. At the top, it says "Boot settings override" above a dropdown menu currently set to "None". Below that is an "Instance" field with a numeric input set to "0". There is an unchecked checkbox for "Enable one time boot". Under the heading "TPM required policy", there is a sub-heading "Enable to ensure the system only boots when the TPM is functional." and an unchecked checkbox for "Enabled". At the bottom left is a blue "Save" button.

5. Click **Save**.

3.1.4. Powering on the server

1. From the **Control** tab, click **Server power operations**. The **Server power operations** page opens.
2. In the **Operations** section, click **Power on**.

Server power operations

Current status

Host status
Not available

Last power operation
2023-06-08 08:32:26 UTC

Last memory size
448 GiB

Host OS boot settings

Boot settings override

None

Instance 0

Enable one time boot

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

Enabled

Save

Operations

Power on

A message is displayed.

Operations

i There are no options to display while a power operation is in progress. When complete, power operations will be displayed here.

Note After initiating the power on of the system, there is a 30 second delay before the update of the host power status to avoid sensor fluctuation. It is therefore necessary to wait 30 seconds before refreshing the Server power operations page of the Server Hardware Console (SHC) to see the updated power status after a power on.

3.1.5. Rebooting or shutting down the server

1. From the **Control** tab, click **Server power operations**. The **Server power operations** page opens.
2. In the **Operations** section, select the mode and click **Reboot** or **Shutdown**.

Server power operations

Current status

Host status
Not available

Last power operation
2023-06-08 08:32:26 UTC

Last memory size
448 GiB

Host OS boot settings

Boot settings override

None

Instance 0

Enable one time boot

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

Enabled

Save

Operations

Reboot server

- Orderly - OS shuts down, then server reboots
- Immediate - Server reboots without OS shutting down; may cause data corruption

Reboot

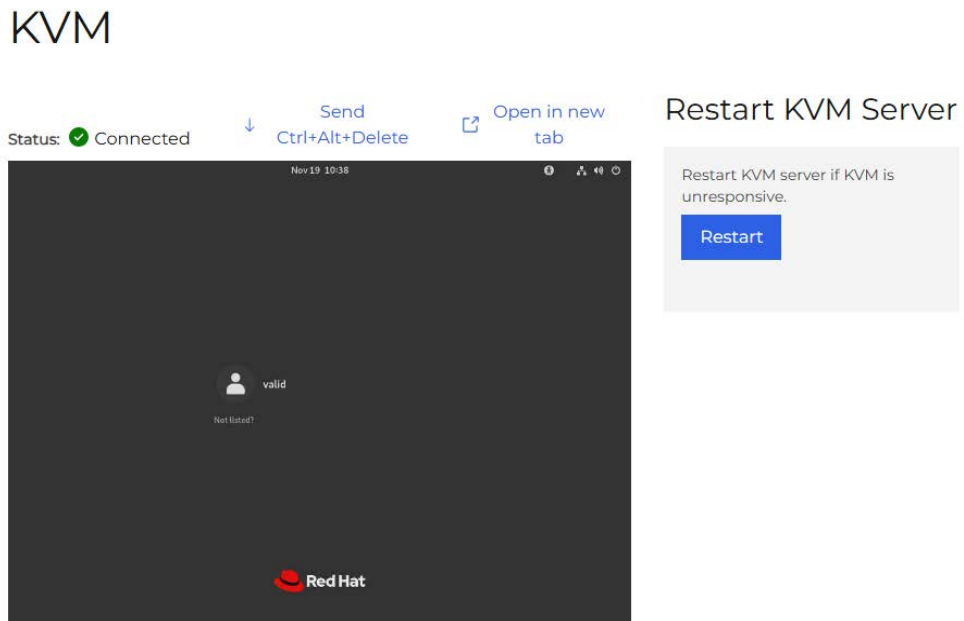
Shutdown server

- Orderly - OS shuts down, then server shuts down
- Immediate - Server shuts down without OS shutting down; may cause data corruption

Shut down

3.2. Connecting to the Keyboard, Video, Mouse (KVM)

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



If the KVM is unresponsive, click **Restart** to restart KVM server.

Note The KVM keyboard layout can be configured with the **KVM settings** feature.

3.3. Connecting to the Serial Over LAN (SOL) console

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

Serial over LAN (SOL) console

SOL console redirects the server's serial port output to this window.

Status:  Connected

 [Open in new tab](#)

```
Starting Performance Metrics Collector Daemon...
Starting System Logging Service...
[ OK ] Reached target Remote File Systems (Pre).
[ OK ] Reached target Remote File Systems.
Starting Virtualization daemon...
Starting Permit User Sessions...
[ OK ] Started Notify NFS peers of a restart.
[ OK ] Started System Logging Service.
[ OK ] Started Permit User Sessions.
[ OK ] Started Job spooling tools.
Starting Hold until boot process finishes up...
Starting GNOME Display Manager...
[ OK ] Started Command Scheduler.
[ OK ] Started GNOME Display Manager.
[ 66.057178] bridge: filtering via arp/ip/ip6tables is no longer available by default. Update your scripts to load br_netfilter if you need this.
.

Red Hat Enterprise Linux 8.6 (Ootpa)
Kernel 4.18.0-372.9.1.el8.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

localhost login: |
```

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

Note To access the BIOS settings click on the SOL screen and press the ESC key at the same time.

3.4. Creating a virtual media session

Note Only users with Administrator privilege have access to this feature.

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

Virtual media

Virtual image redirection

Virtual media device

Add file

Start

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

3.5. Configuring the power restore policy

The power restore policy determines how the system starts after a power disturbance.

1. From the **Control** tab, click **Power restore policy**. The **Power restore policy** page opens.

Power restore policy

Configure power policy to determine how the system starts after a power disturbance.

Power restore policies

- Always on - The system always powers on when power is applied.
- Always off - The system always remains powered off when power is applied.
- Restore - The system returns to its last on or off power state when power is applied.

Save settings

2. Select the policy.

Power restore policy	Description
Always On	The system always powers on when power is applied
Always Off	The system always remains powered off when power is applied
Last state	The system returns to its last power state when power is applied

3. Click **Save Settings**.

3.6. Enabling or disabling the server identification LED

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

Server ID LED

LED light control

Server indicator LED

Off

2. Turn the server indicator LED on to identify the server.

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

3.7. Resetting settings to default values

Important The server must be off before resetting the setting values as indicated below.

Note Only users with SupportUser privilege have access to this feature.

1. From the **Control** tab, click **Reset to default**. The **Reset to default** page opens.

Reset to default

These functions do not perform a secure delete of any sensitive data.

Reset options

Reset BIOS settings

Reset BMC settings

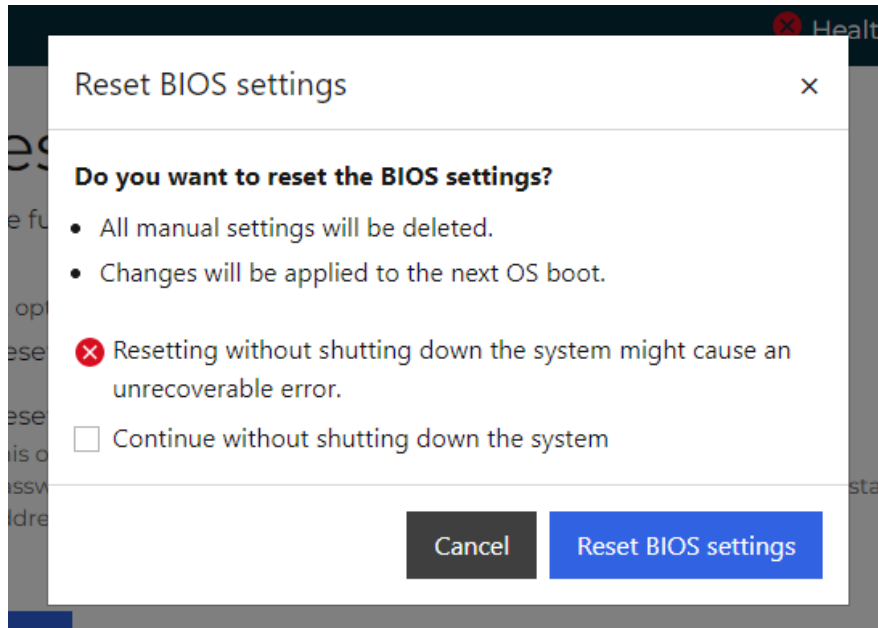
This option resets BMC settings, including: all BMC account data, all changed passwords, all policies, LDAP configurations, partition configuration, network static addresses, and time of day.

Reset

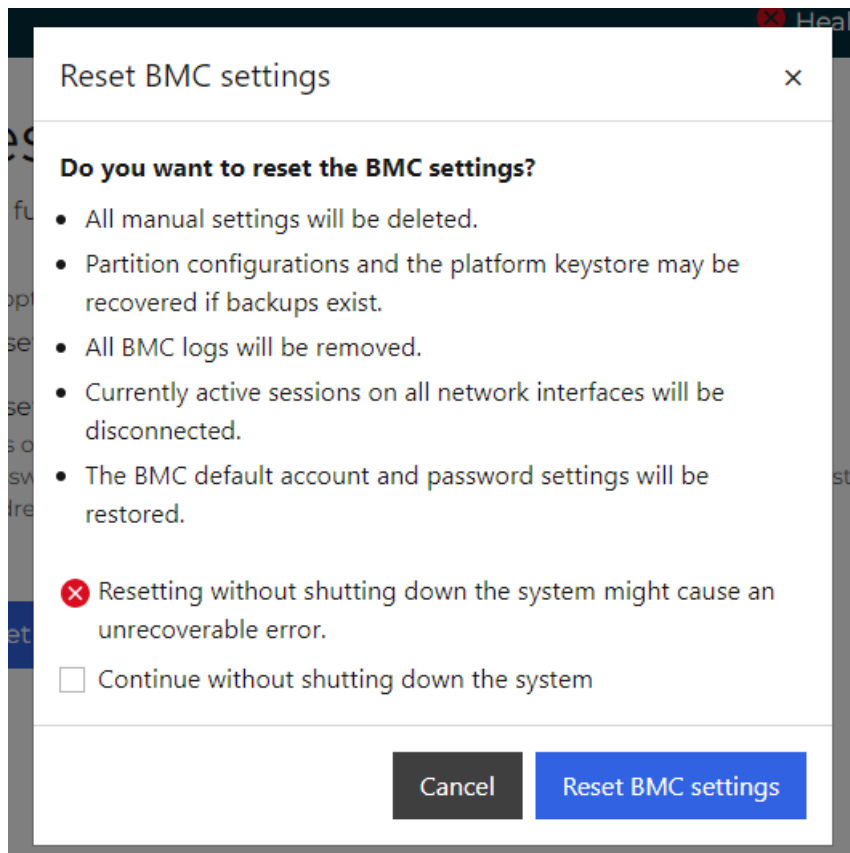
2. Select the components to reset and click **Reset**.

- Carefully read the caution points.

Reset BIOS settings



Reset BMC settings



4. Check the option **Continue without shutting down the system** if needed to go on.
5. Click **Reset BIOS settings** or **Reset BMC settings** depending on the function performed.
6. Use the SupportUser default account to connect to the SHC after the **Reset of the BMC settings**.

SHC login	
Username	Default: supportuser
Password	Default: support@eviden

3.8. Managing power usage

Note Only users with Administrator privilege have access to this feature.

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

Manage power usage

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

Current power consumption
Not available

Power cap setting

Apply power cap

Power cap value (in watts)

Value must be between 1 and 1000

Save

2. To set a power cap:
 - a. Select **Apply power cap**.
 - b. Set the power cap value in the **Power Cap Value (in watts)** box.
3. Click **Save**.

Note The power consumption and power cap value are indicated on the Overview page.

3.9. Rebooting the BMC

Note Only users with Administrator privilege have access to this feature.

1. From the **Control** tab, click **Reboot BMC**. The **Reboot BMC** page opens.

Reboot BMC

Last BMC reboot
2023-06-07 15:07:20 UTC

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

Reboot BMC(s)

2. Click the **Reboot BMC** button and confirm.

A success message is displayed.

Reboot BMC



Chapter 4. Configuring the management controller

4.1. Setting the date and time

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

Date and time settings

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

Date
2022-01-11

24-hour time
08:11:25 UTC

Configure settings

Manual

Date
YYYY-MM-DD

24-hour time (UTC)
HH:MM

2022-01-11

08:11

NTP

Server 1

Server 2

Server 3

Save settings

2. Select the date and time configuration:
 - Manual
 - Network Time Protocol (NTP) servers

Note It is recommended to configure an NTP server. Time and date settings configured manually will be lost when the BMC is reset.

3. Click **Save settings**.

4. Click **Profile Settings** at the top of the page. The **Profile settings** page opens.

Profile settings

Profile information

Username
admin

Privilege
Administrator

Change password

New password

Password must be between 8 – 20 characters ... 

Confirm new password

Timezone display preference

Select how time is displayed throughout the application

Timezone

- Default (UTC)
- Browser offset (CEST UTC+2)

[Save settings](#)

5. Select the timezone display:
 - Default
 - Browser offset
6. Click **Save settings**.

4.2. Managing firmware versions

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

Firmware

Firmware version

Component	Version
BIOS	BIOS_ESR160.37.01.001
BMC	160.02.0004
FPGA	1.E.0.0

Update firmware

Image file
Only .tar, .tar.gz files accepted

Add file Force Update

Firmware update may take up 10 minutes due to security features

Start update

2. To update a firmware version, click **Add file** to select the firmware version file, and click **Start update**.

Notes

- It is strongly recommended to power off the system before updating the BIOS and FPGA firmware.
 - After a BIOS firmware update, the boot option is reset to PXE. It is therefore necessary to change the boot option after the update if PXE is not desired boot option.
 - Select the **Force Update** box to reinstall the same firmware version.
-

4.3. Configuring network settings

Note The server hostname may be modified in the screen below.

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

Network settings

Configure BMC network settings

i Changing BMC network settings may result in a loss of the remote connection to the BMC. Please ensure that all the values are correct before applying changes so that you can reconnect remotely to the BMC.

Global settings

Hostname [🔗](#)
spark

Use domain name
 Disabled

Use DNS servers
 Disabled

Use NTP servers
 Disabled

eth0

Interface settings

FQDN: spark MAC address: 08:00:38:bd:68:9e

IPv4

DHCP: Enabled

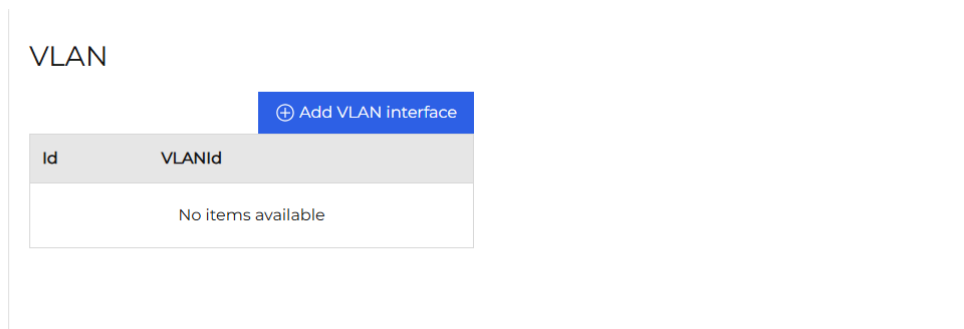
IPv4 addresses + Add static IPv4 address

IP address	Gateway	Subnet mask	Address origin	
XX.XX.XX.XX	0.0.0.0	255.255.0.0	IPv4LinkLocal	
XX.XX.XX.XX	0.0.0.0	255.255.255.0	DHCP	

Static DNS

+ Add IP address

IP address
No items available



Global settings	
Hostname	The server hostname: it must be a combination of upper case letters (A to Z), lower case letters (a to z) and numbers (0 to 9). The only authorized special character is the hyphen (-)
Use domain name	enables or not domain name usage
Use DNS servers	enables or not DNS server usage
Use NTP servers	enables or not NTP server usage
Interface settings	
FQDN	Fully Qualified Domain Name used by the DNS server
Mac address	The server MAC address
IPv4	
DHCP	When enabled, the server IP address is retrieved from a DHCP server
IP address	Server IP address
Gateway	Gateway IP address
Subnet mask	Sub-net mask to be used
Address origin	DHCP or Static or IPv4LinkLocal
Add Static IPv4 address	Click this button to add a static IP address
Static DNS	
IP address	DNS IP address
Add IP address	Click this button to add a DNS IP address
VLAN	
VLANid	VLAN interface identifier
Add VLAN Interface	Click this button to add a VLAN interface identifier

2. Fill in Hostname.
3. Select IPV4 configuration: DHCP or Static.

4. Add a static IP address if required.
5. Add a DNS server if required.
6. Add a VLAN interface if required.
7. Click **Save settings**.

4.4. Configuring Rsyslog

1. From the **Configuration** tab, click **Rsyslog**. The **Rsyslog** page opens.

Rsyslog

Enable Syslog Forwarding

IP address

Port

[Save settings](#)

Rsyslog	
Enable Syslog Forwarding	When selected, this option allows events to be sent by the syslog protocol on a Linux platform, in order to centralize all the events
IP address	Syslog server IP address
Port	Syslog server listening port

2. Select **Enable Syslog Forwarding** and complete the fields as required.
3. Click **Save settings**.

4.5. Configuring KVM settings

1. From the **Configuration** tab, click **KVM settings**. The **KVM settings** page opens.

KVM settings

Default keyboard layout

Save settings

2. Select the keyboard layout language from the drop-down list.
3. Click **Save settings**.

4.6. Configuring Global settings

1. From the **Configuration** tab, click **Global settings**. The **Global settings** page opens.

Global settings

Platform Name

Managed Server Name

Save settings

2. Complete the required fields.
3. Click **Save settings**.

Chapter 5. Managing users

5.1. Managing client sessions

1. From the **Access control** tab, click **Client session**. The **Client sessions** page opens.

Client sessions

Search sessions 4 items

<input type="checkbox"/>	Client ID	Username	IP address	
<input type="checkbox"/>	0Uusq9L9wh	admin	XX.XX.XX.XX	Disconnect
<input type="checkbox"/>	3m69dprWbM	oper	XX.XX.XX.XX	Disconnect
<input type="checkbox"/>	gnuR9f84uC	usertest_1	XX.XX.XX.XX	Disconnect
<input type="checkbox"/>	O8d4bbcD1k	usertest_2	XX.XX.XX.XX	Disconnect

20 Items per page < 1 >

2. To disconnect the user, click **Disconnect**.

5.2. Configuring LDAP

1. From the **Access control** tab, click **LDAP**, the **LDAP** page opens.

LDAP

Configure LDAP settings and manage role groups

Settings

LDAP authentication

Enable

<p>Secure LDAP using SSL</p> <p>A CA certificate and an LDAP certificate are required to enable secure LDAP</p> <p><input type="checkbox"/> Enable</p> <p>CA Certificate valid until</p> <p>--</p> <p>LDAP Certificate valid until</p> <p>--</p> <p>Manage SSL certificates</p>	<p>Service type</p> <p><input checked="" type="radio"/> OpenLDAP</p> <p><input type="radio"/> Active Directory</p>	<p>Server URI [ⓘ]</p> <p>ldap://</p>	<p>Bind DN</p>	<p>Bind password</p>
		<p>Base DN</p>	<p>User ID attribute - optional</p>	<p>Group ID attribute - optional</p>

Save settings

Role groups

i LDAP authentication must be enabled to modify role groups.

[+ Add role group](#)

<input type="checkbox"/>	Group name	Group privilege
No items available		

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

Settings	
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
Save settings button	Saves the configurations
Role groups	
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

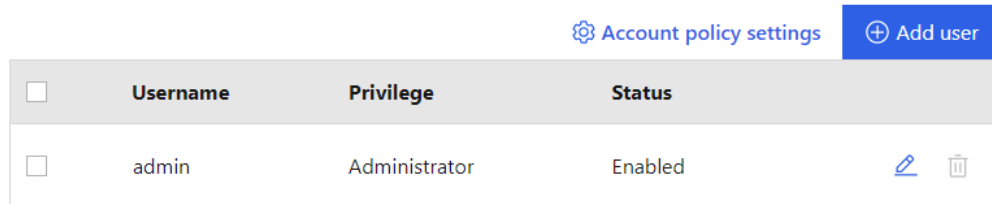
2. Set the configuration and click **Save settings**.



5.3. Managing local users

5.3.1. Viewing a user list



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

Local user management



<input type="checkbox"/>	Username	Privilege	Status	
<input type="checkbox"/>	admin	Administrator	Enabled	 

[View privilege role descriptions](#)

Local user management	
Username	Name the user uses to log on
Privilege	Role assigned to the user
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

5.3.2. Viewing privilege roles

1. From the **Access** tab, click **Local user management**. 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	Status	
<input type="checkbox"/>	test_user1	ReadOnly	Enabled	✎ 🗑️
<input type="checkbox"/>	admin	Administrator	Enabled	✎ 🗑️
<input type="checkbox"/>	supportuser	SupportUser	Enabled	✎ 🗑️
<input type="checkbox"/>	oper	Operator	Enabled	✎ 🗑️
<input type="checkbox"/>	no_user	NoAccess	Enabled	✎ 🗑️
<input type="checkbox"/>	test_user2	Administrator	Enabled	✎ 🗑️

[^ View privilege role descriptions](#)

Privilege	Administrator	SupportUser	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	✓	✓	✓	✓	

Operator users do not have access to the following SHC pages:

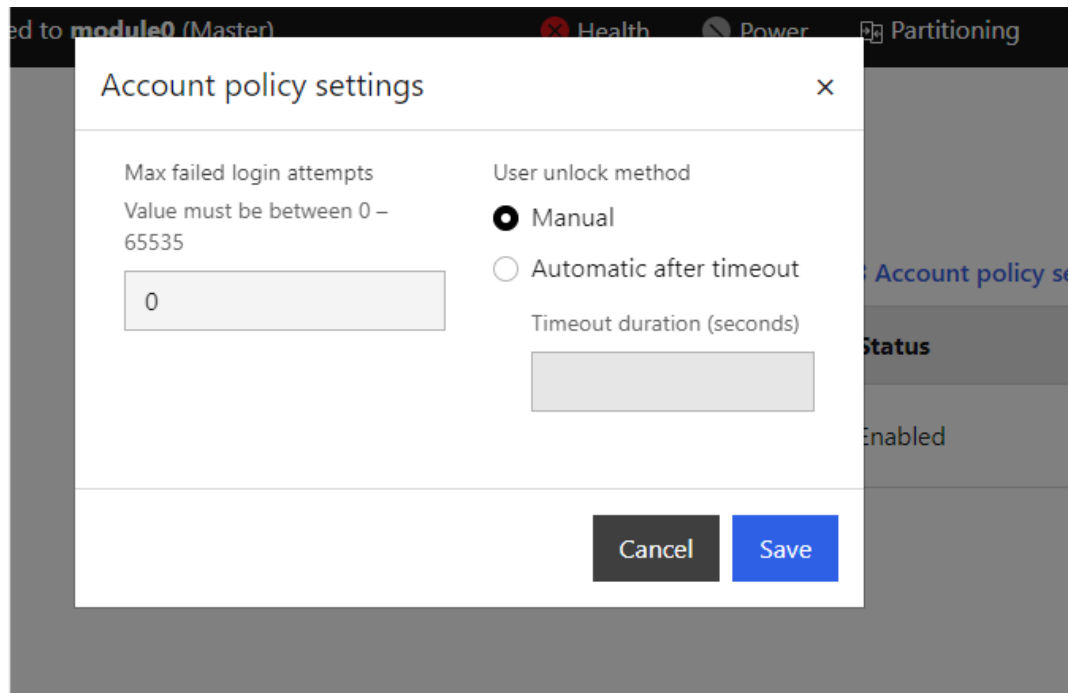
- Reset to default
- Manage power usage
- Reboot BMC
- Date and time settings
- Rsyslog
- KVM settings
- Global settings

ReadOnly users do not have access to the following SHC pages:

- KVM
- SOL console
- Reset to default
- Manage power usage
- Reboot BMC
- Date and time settings
- Rsyslog
- KVM settings
- Global settings

5.3.3. Setting the account policy

1. From the **Access** tab, click **Local user management**. The **Local user management** page opens.
2. Click the **Account policy settings** tab. The **Account policy settings** page opens.

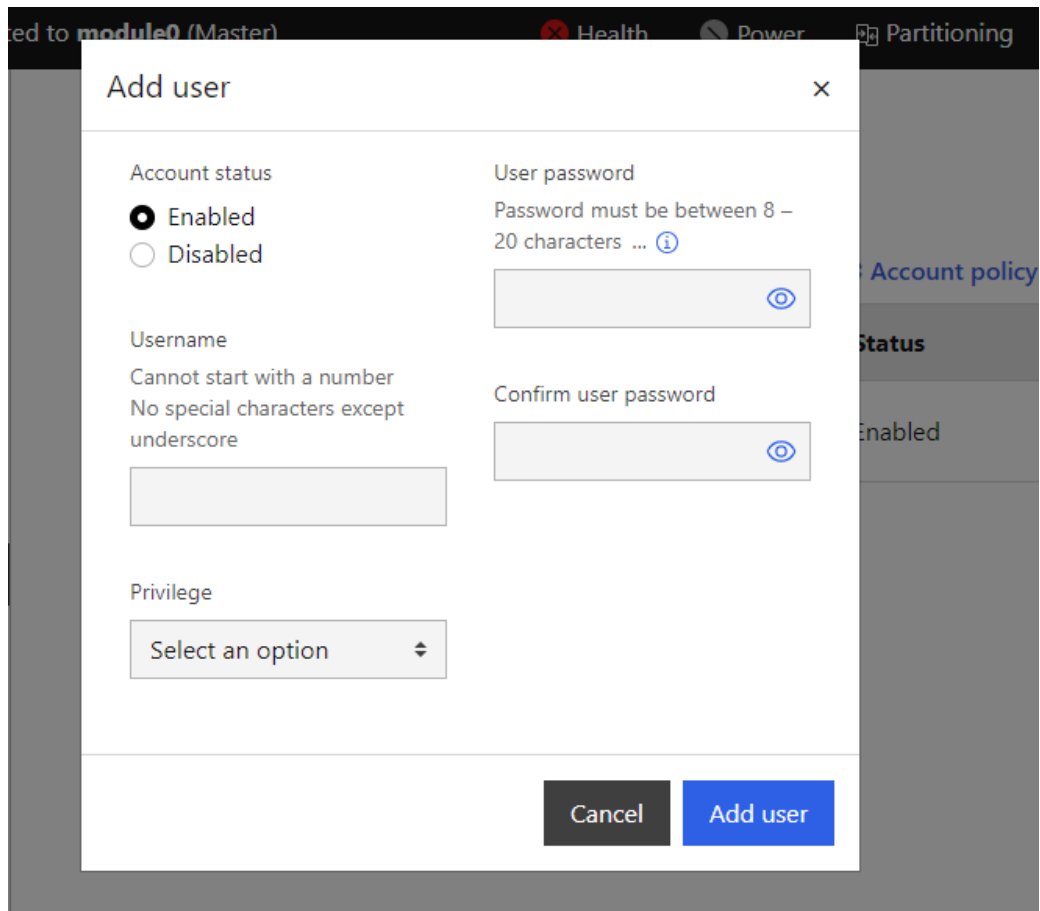


Account policy settings	
Max failed login attempts	The number of failed login attempts allowed. The value must be set between 0 (default) and 65535
Manual	A locked user account stays locked until it is unlocked manually
Automatic after timeout	Automatic unlock after the period set in the Timeout duration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

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

5.3.4. Creating a new user account

1. From the **Access** tab, click **Local user management**. The **Local user management** page opens.
2. Click **Add user** tab. The **Add user** page opens.



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"> • Names cannot start with number • Special characters are not allowed except underscores
Privilege	Use the drop-down list to select the role to assign to the user
User password	The password the user will use to log on <ul style="list-style-type: none"> ▪ The password must be between 8 and 20 characters long
Confirm user password	<ul style="list-style-type: none"> ▪ The password must be a mixture of upper case letters, lower case letters, numbers and special characters ▪ The password must be different from the user name



3. Complete the fields as required.
4. Click **Add user**. The user is created.



5.4. Managing SSL certificates

5.4.1. Viewing SSL certificates

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

SSL certificates

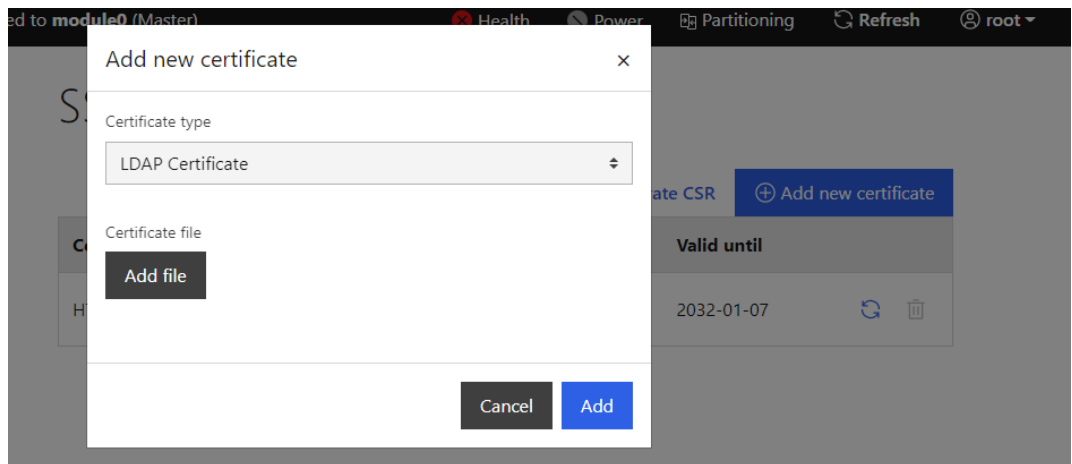
					+ Generate CSR	+ Add new certificate
Certificate	Issued by	Issued to	Valid from	Valid until		
HTTPS Certificate	BULL	BULL	2022-01-09	2032-01-07		

SSL certificates	
Certificate	Certificate name
Issued by	Certificate details
Issued to	
Valid from	Validity period
Valid until	
Actions	
	Remove button to delete the certificate
	Refresh button to check if a more up-to-date version of the certificate is available

5.4.2. Adding a certificate

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

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



3. Use the drop-down list to select a certificate type. There are two possible options:
 - LDAP Certificate
 - CA Certificate
4. Click **Add file** and select a certificate file.

Note The certificate file must be a .pem file.

5. Click **Add**.

5.4.3. Generating a Certificate Signing Request (CSR)

Important A valid SSL certificate is required to use the HTTPS protocol. By default, a temporary certificate is delivered. For optimum security, it is advised to generate and install a new certificate.

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

2. Click the **Generate CSR** tab. The CSR generating page opens.

Certificate Signing Request (CSR)	
Certificate type	Select an option: <ul style="list-style-type: none"> ▪ HTTPS Certificate ▪ LDAP Certificate
Country	Select a country
Private key - Key pair algorithm	Select: <ul style="list-style-type: none"> ▪ EC ▪ RSA
State	Name of the state
City	Name of the city
Company name	Name of the company
Company unit	Generally the name of the department

Certificate Signing Request (CSR)	
Common name	"Fully Qualified Domain Name" (FQDN) example: hostName.DomainName.Top-LevelDomain. If the Common Name differs from the network name, a security warning will pop up when the system is accessed using HTTPS
Challenge password - optional	Depending on the certification authority, it may be necessary to define a challenge password to authorize later changes to the certificate (example: revocation of the certificate). The minimum length of this password is four characters
Contact person - optional	Generally the administrator's name
Email address - optional	Generally the administrator's email address
Alternate name - optional	Multiple alternate names separated by space



3. Complete the fields. Define the key pair algorithm for the private key:
 - For RSA key pair algorithm, select the key bit length
 - For EC key pair algorithm, select the key curve ID
4. Click **Generate CSR** to generate the CSR.
5. Click **Download** to save the CSR to the computer or **Copy** to save its content into the clipboard and send it to the Certification Authority, who will check the information, and then generate and return a signed certificate.
6. When the signed certificate is received, use the **Add new certificate** tab to install the certificate.

5.4.4. Deleting a certificate

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

2. Click the remove button for the required certificate.

SSL certificates



Certificate	Issued by	Issued to	Valid from	Valid until	
HTTPS Certificate	BULL	BULL	2022-01-09	2032-01-07	 

3. Click **Remove** in the confirmation dialog box to remove the certificate.

5.4.5. Updating a certificate automatically

1. From the **Access control** tab, click **SSL certificates**. The **SSL certificates** page opens.
2. Click the refresh button for the required certificate.

SSL certificates

Certificate	Issued by	Issued to	Valid from	Valid until	
HTTPS Certificate	BULL	BULL	2022-01-09	2032-01-07	 

3. The certificate will be updated if a newer version is available.

