BullSequana Edge

Server Hardware Console Reference Guide

86 A1 05FS 08 - July 2022

Atos

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

July 2022

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

Table of Contents

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.

Prerequistes

- 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**

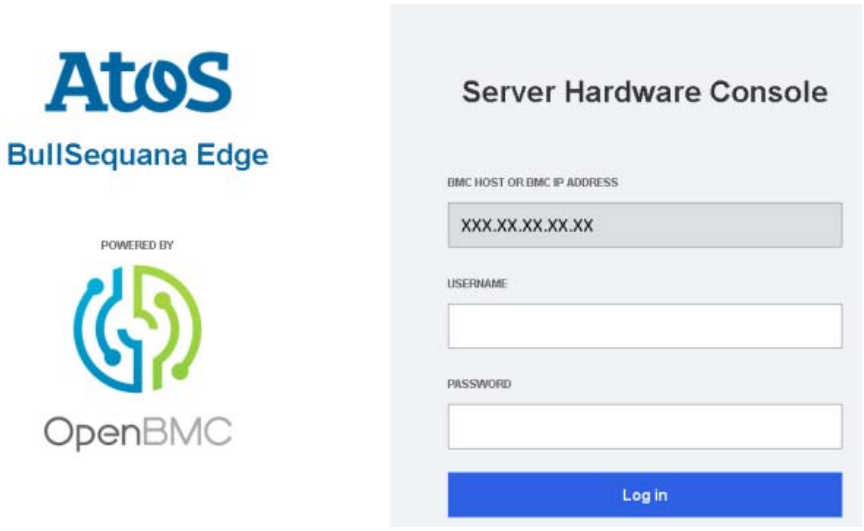
   Enter the host name or IP address into the address bar.

   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.



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

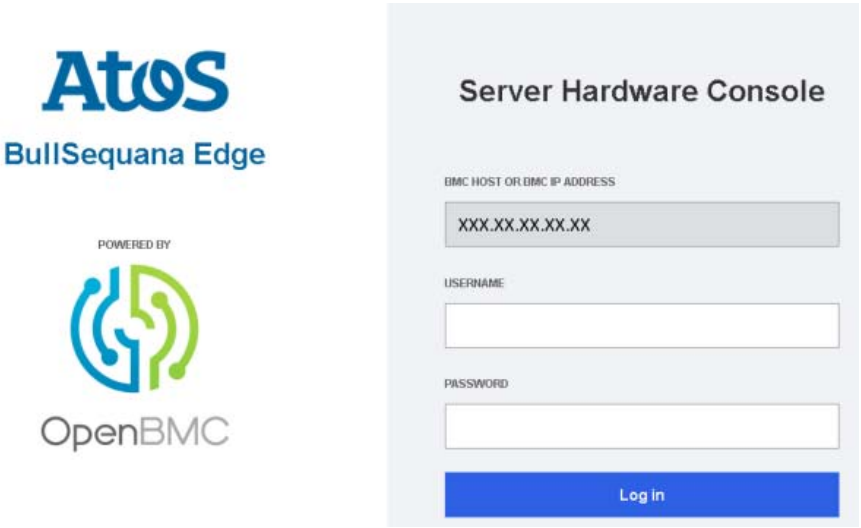
Prerequistes

- 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.



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	Factory default: root
Password	Factory default: At0s!Edge

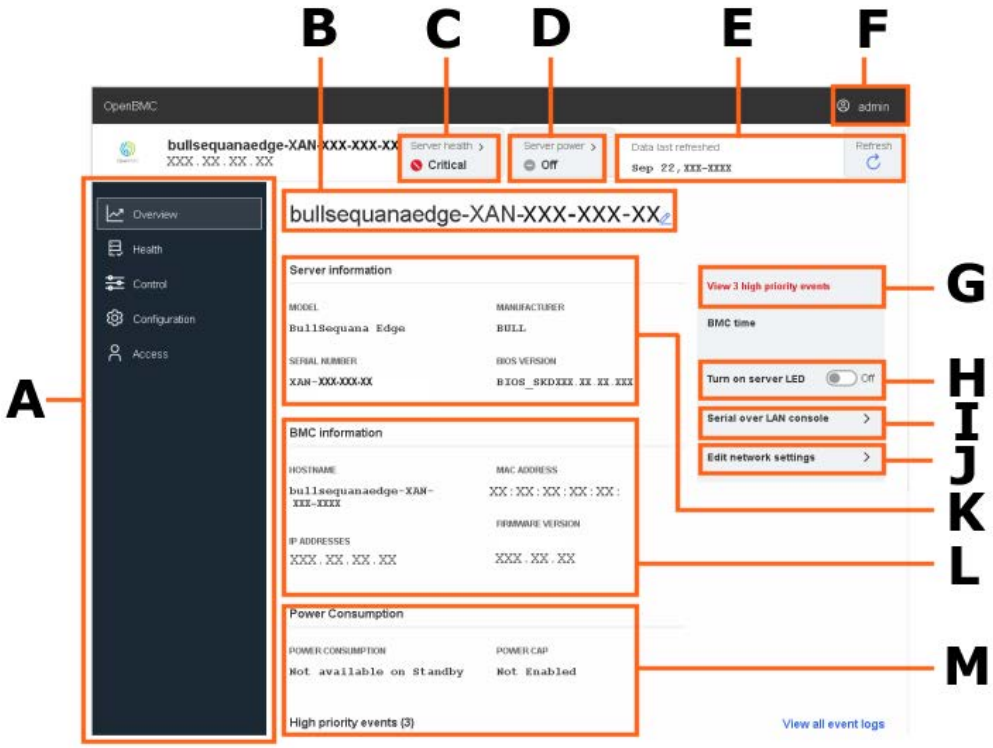
2. **Complete the Username and Password fields and click Log in**

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 **Edit** to change the host name
C	Summary of the server health status with a link to the **System Logs** page
D	Server power status with a link to the **Server power operations** 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:

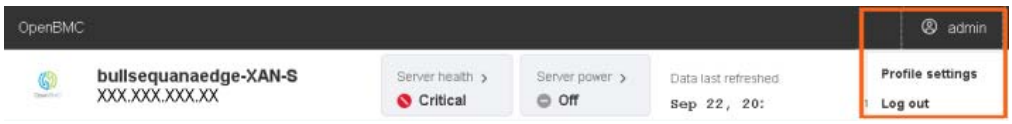
- Provide an overview of the server
- Monitor the health of the server
- Manage the server
- Configure the server
- Configure access and user settings for the server

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

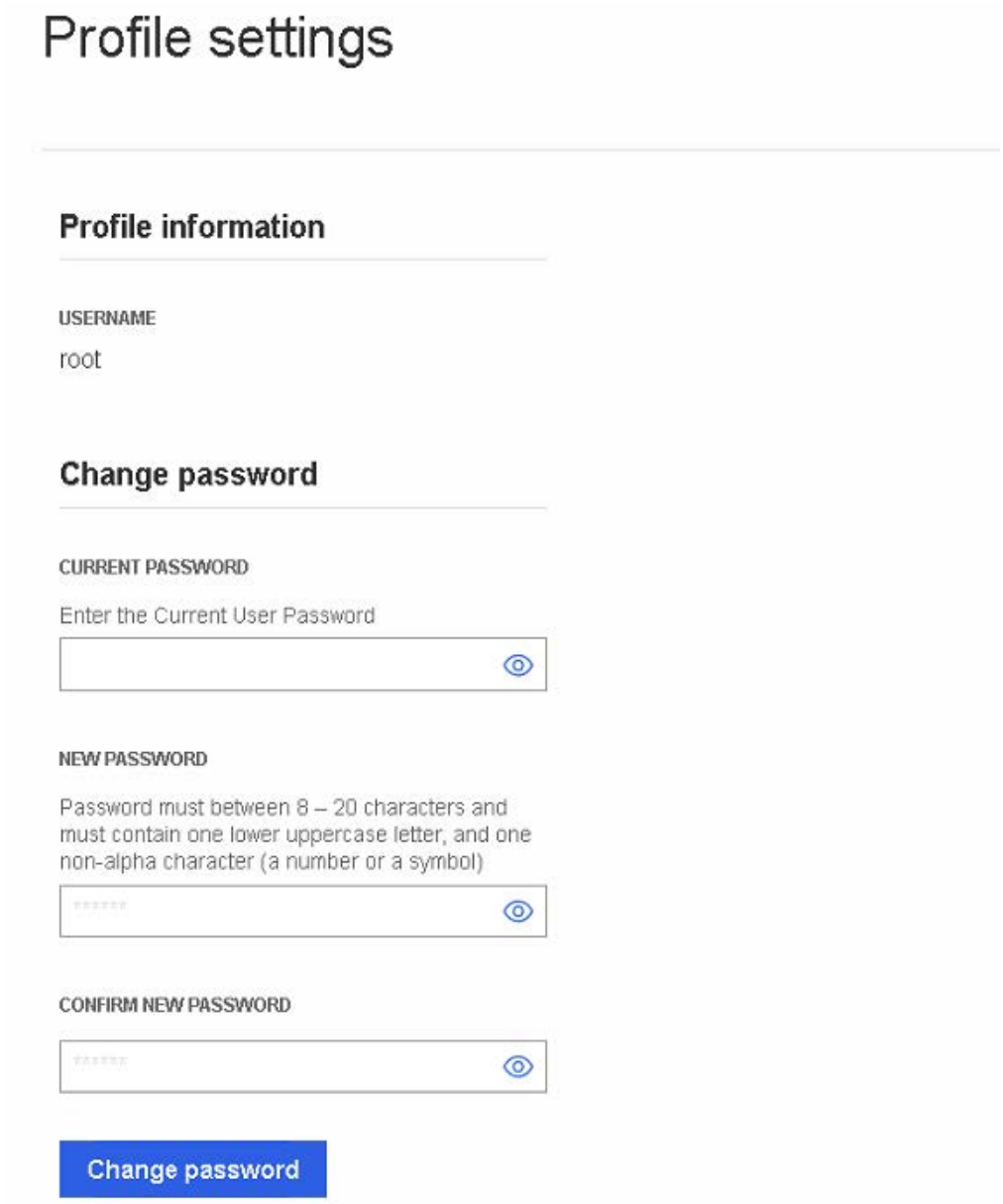
1.6. Changing the default password

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.

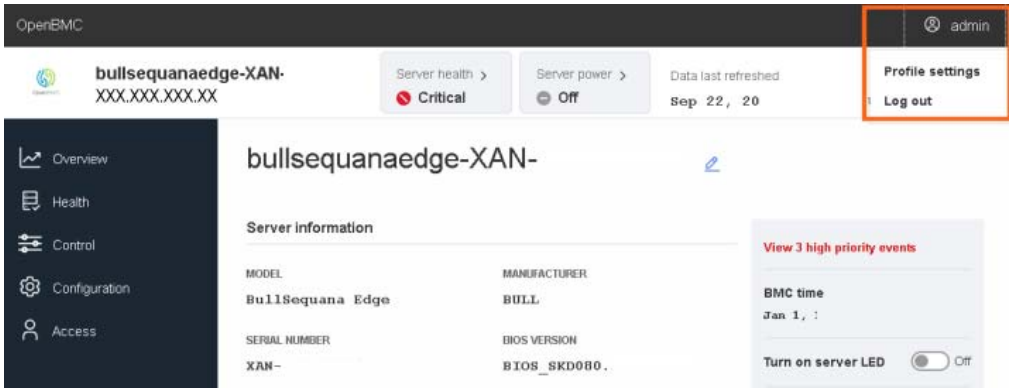


3. Enter the current password.
4. Enter and confirm the new password. Click **Change password**.

Note The password must be between eight and twenty characters long and be a mixture of upper case letters, lower case letters, numbers and special characters. It must be different from the user name.

1.7. Stopping the Server Hardware Console (SHC)

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



Chapter 2. Monitoring the server

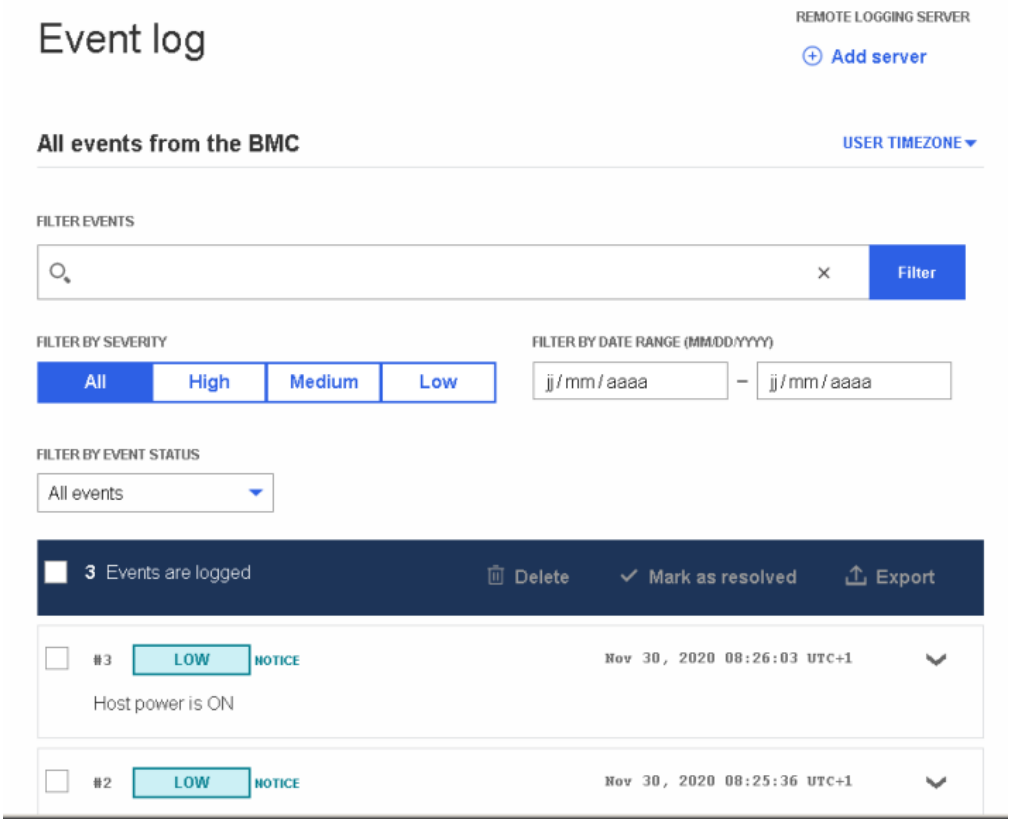
2.1. Checking event logs

Prerequisites

The server power status is Running

Procedure

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



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

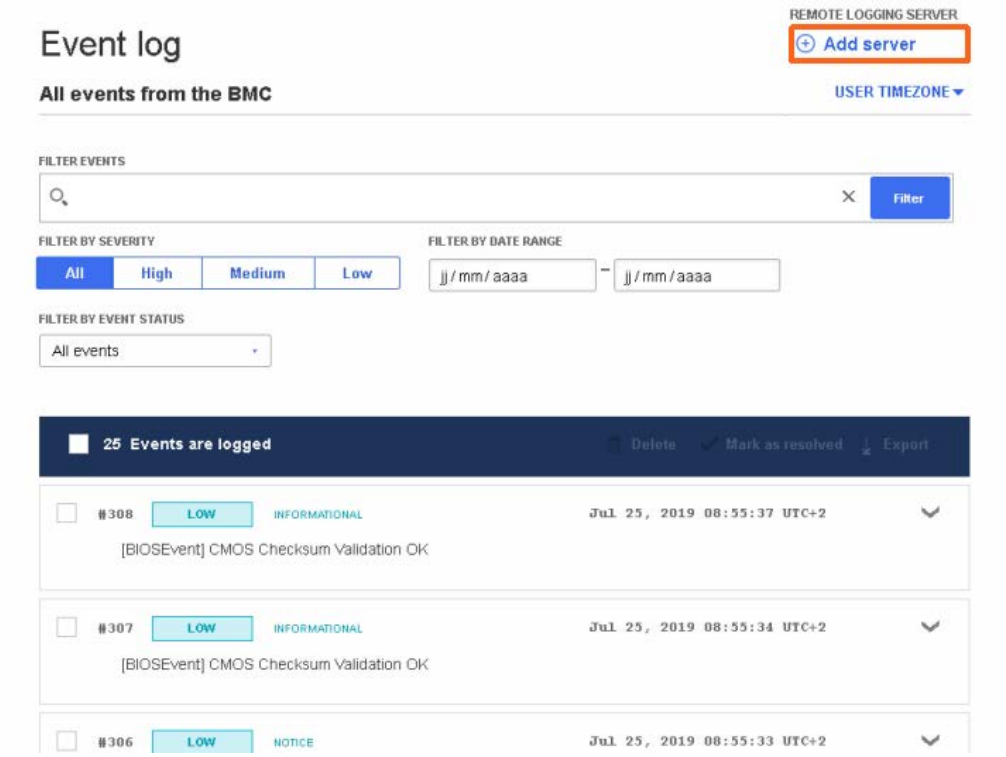
2.2. Adding a remote BMC log server

Prerequisites

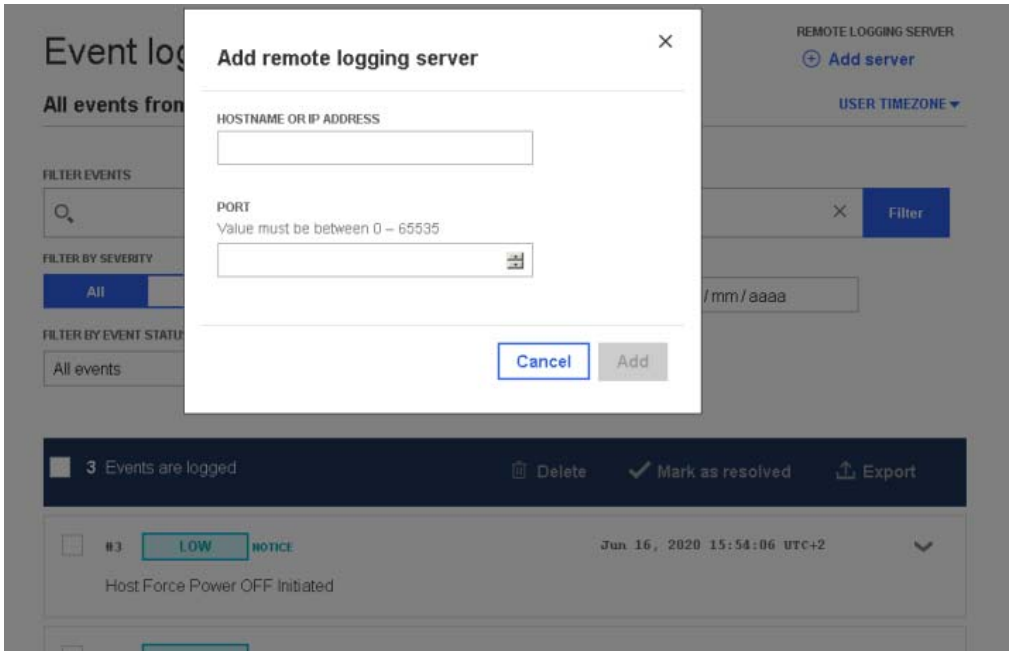
The server power status is Running

Procedure

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



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



4. Click **Add**.

2.3. Editing a remote BMC log server

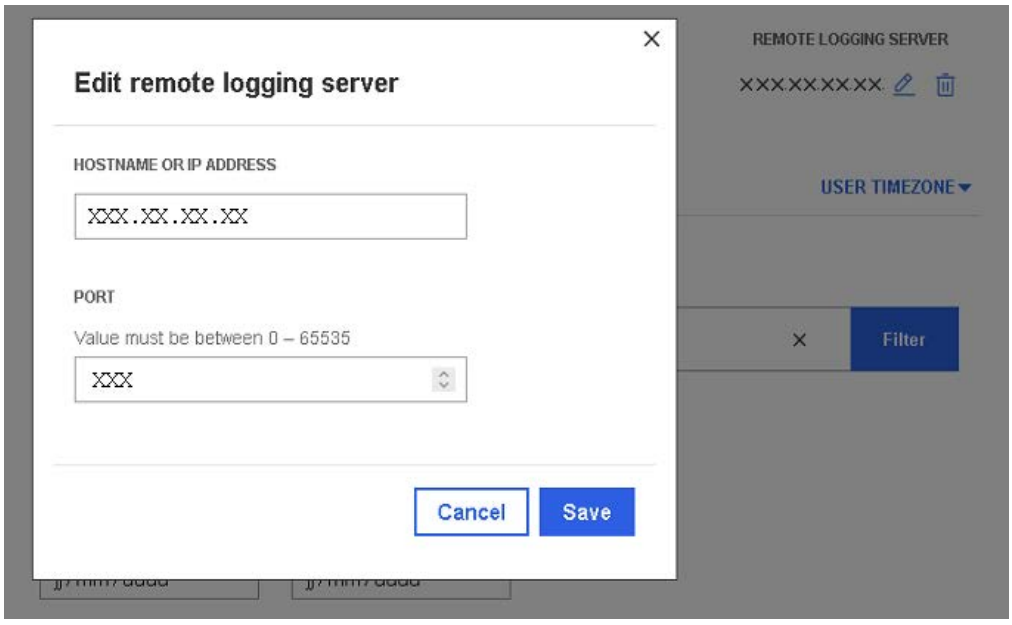
Prerequisites

The server power status is Running

Procedure

1. From the **Health** tab, click **Event log**. The **Event log** page opens.
2. Click the Edit button next to the server IP address.

3. Edit the host name, IP address and Port as required.



4. Click **Save.**

2.4. Removing a remote BMC log server

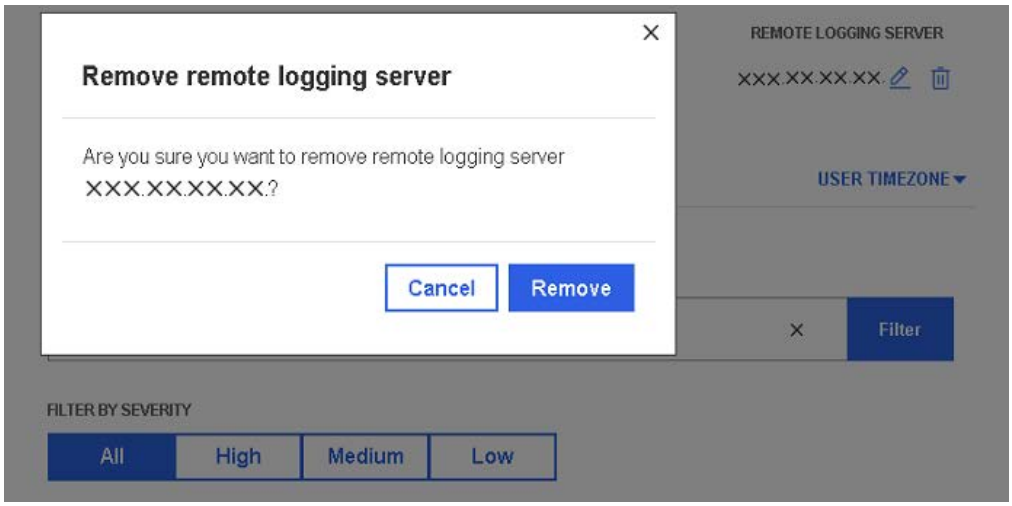
Prerequisites

The server power status is Running

Procedure

1. From the **Health** tab, click **Event log**. The **Event log** page opens.
2. Click the Delete icon next to the server IP address.

3. Click **Remove** in the pop up window to remove the server.



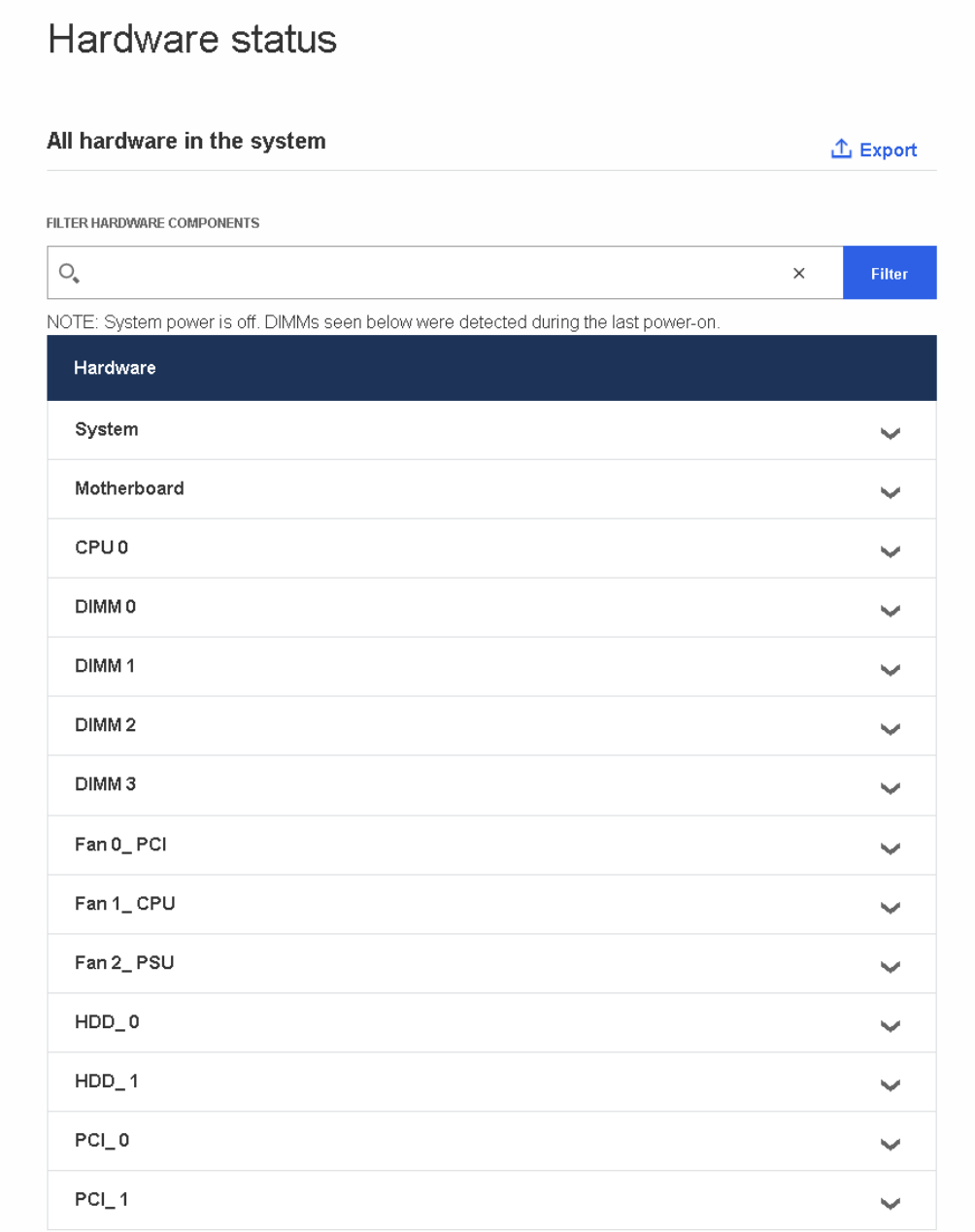
2.5. Checking the hardware status

Prerequisites

The server power status is Running

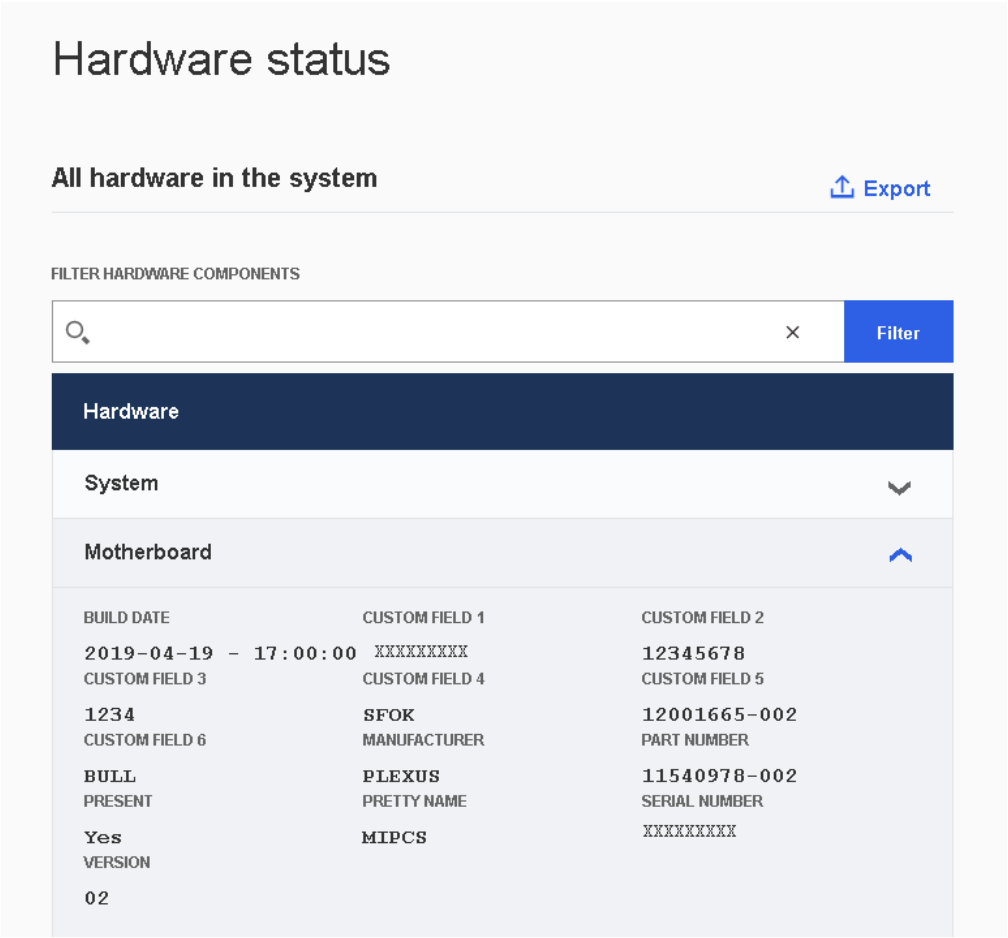
Procedure

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



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

4. 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.



5. **Export** the hardware details, as required.

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

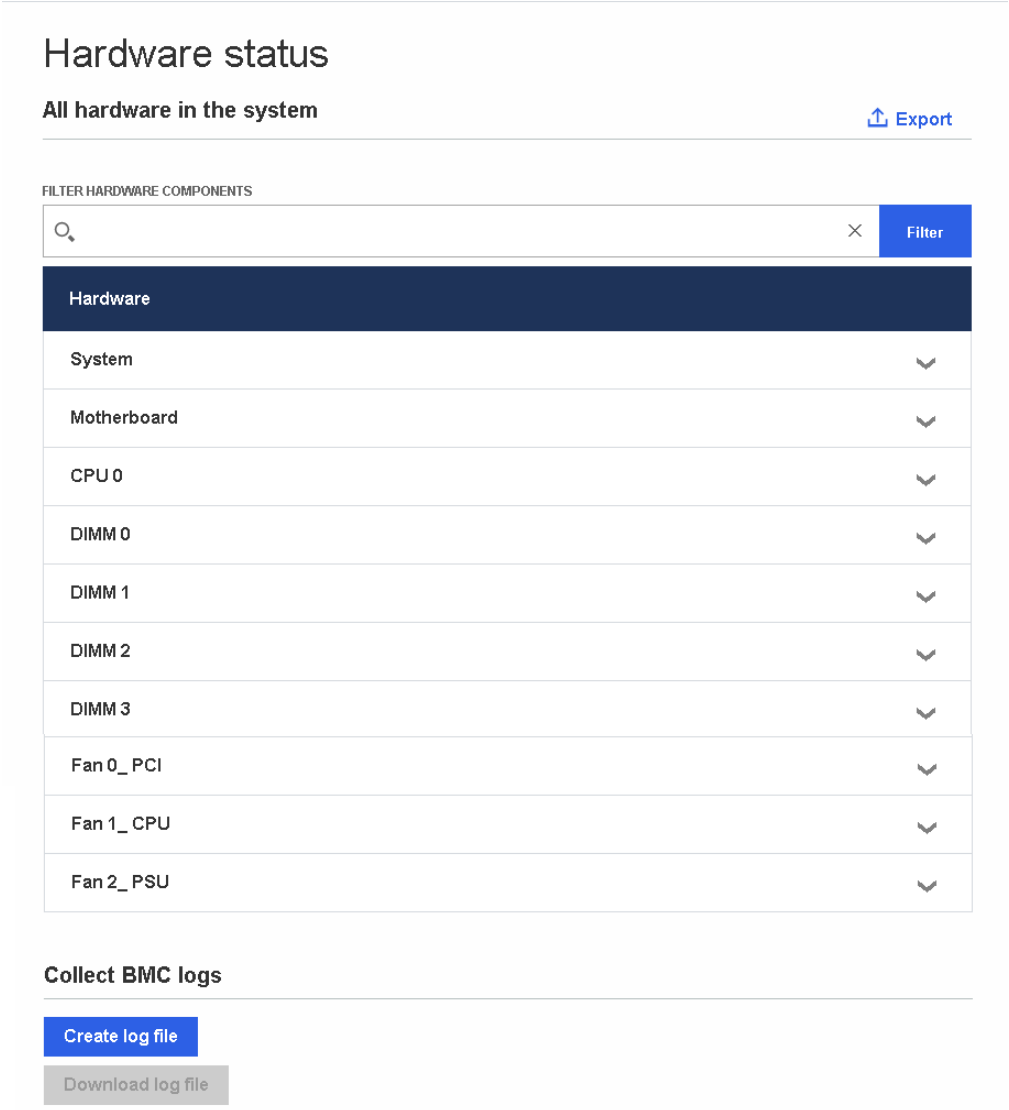
2.6. Collecting BMC logs

Prerequisites

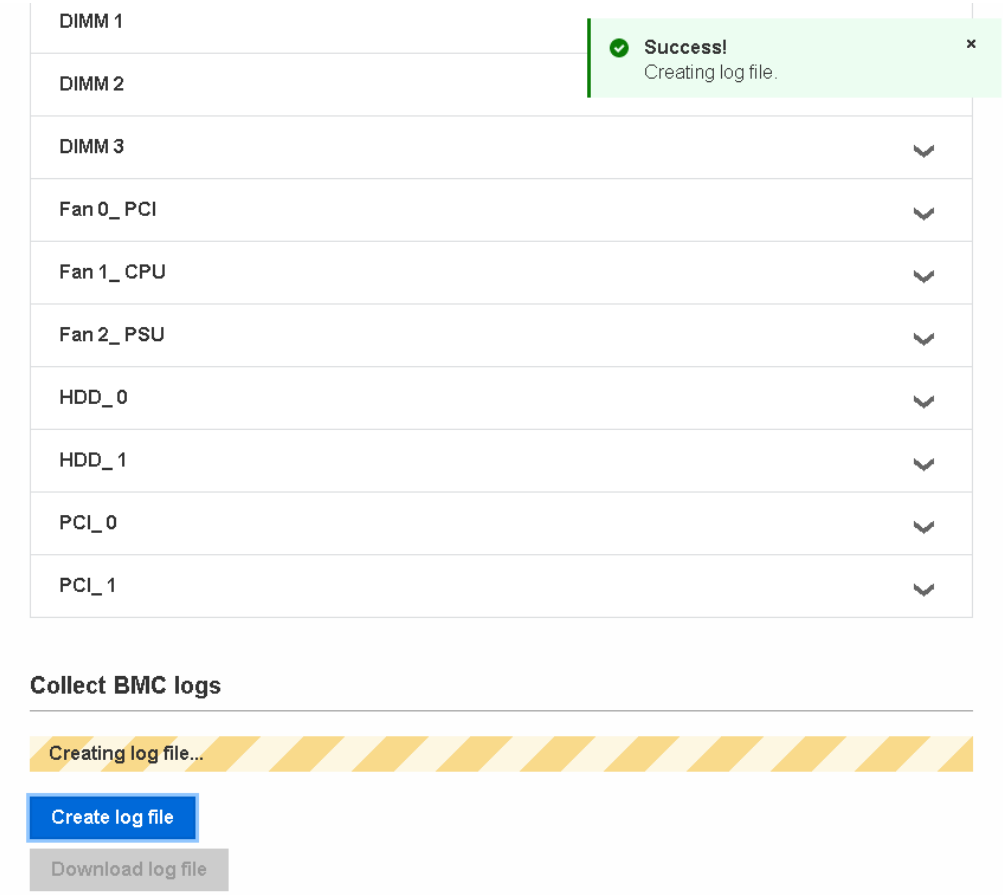
The server power status is Running

Procedure

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

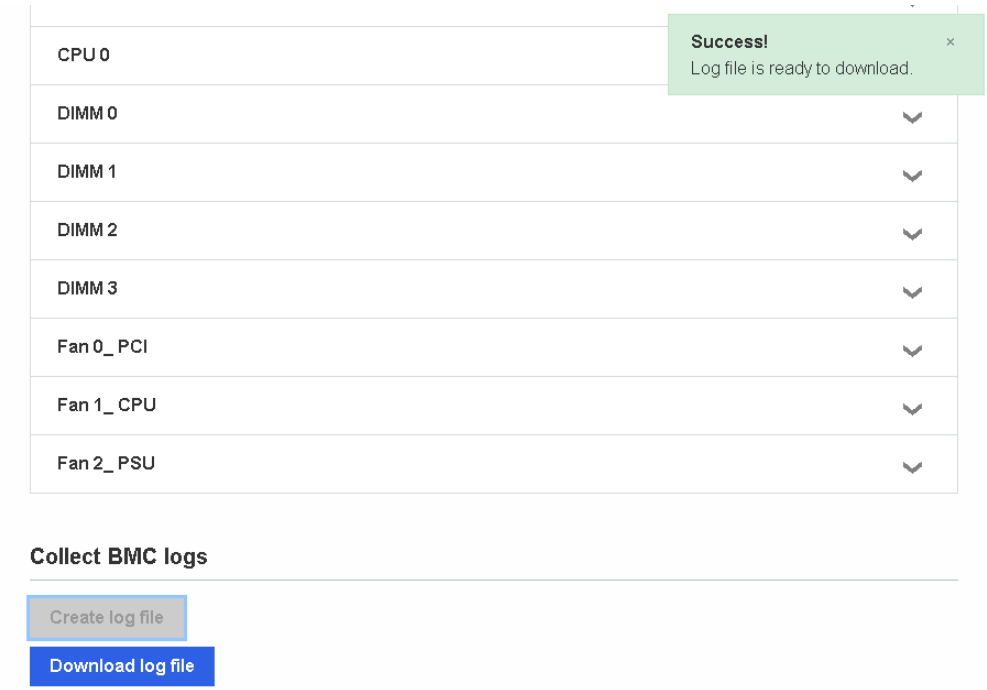


2. Click **Create log file**.



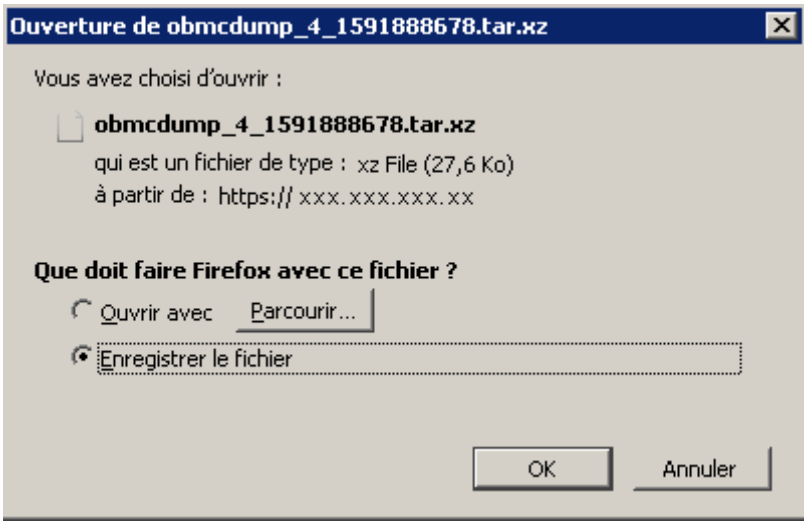
Note This operation may take a long time to complete.

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



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

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



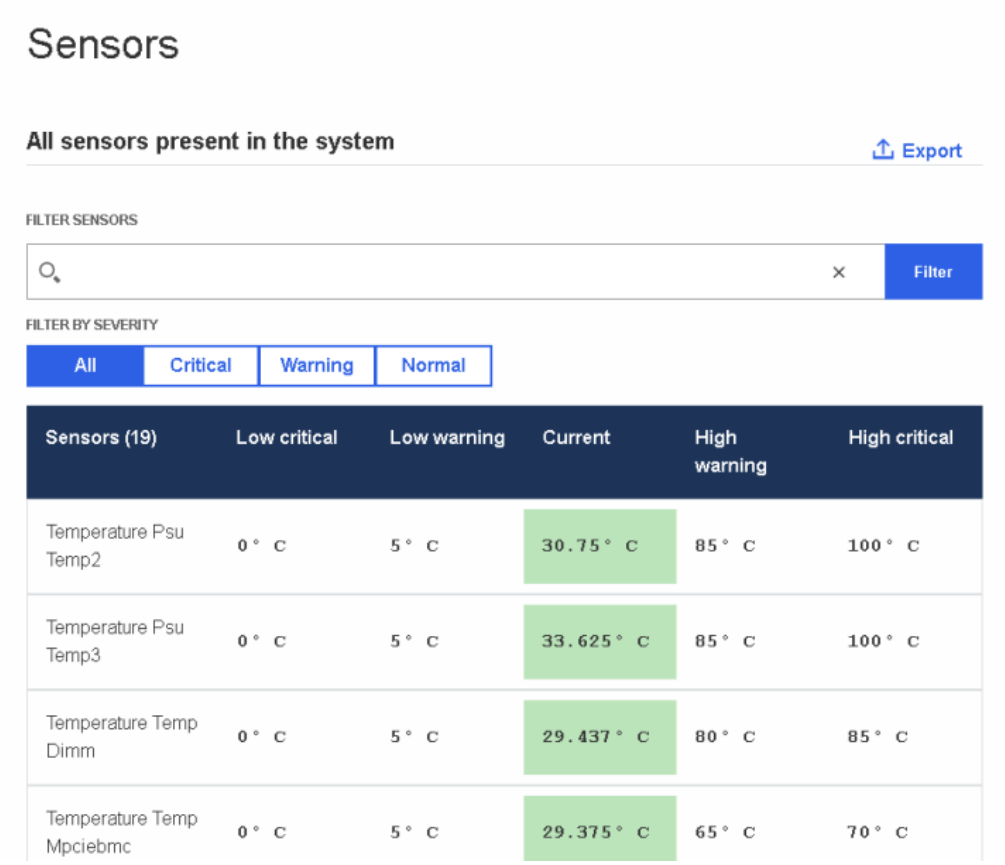
2.7. Checking the sensors

Prerequisites

The server power status is Running

Procedure

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



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

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.

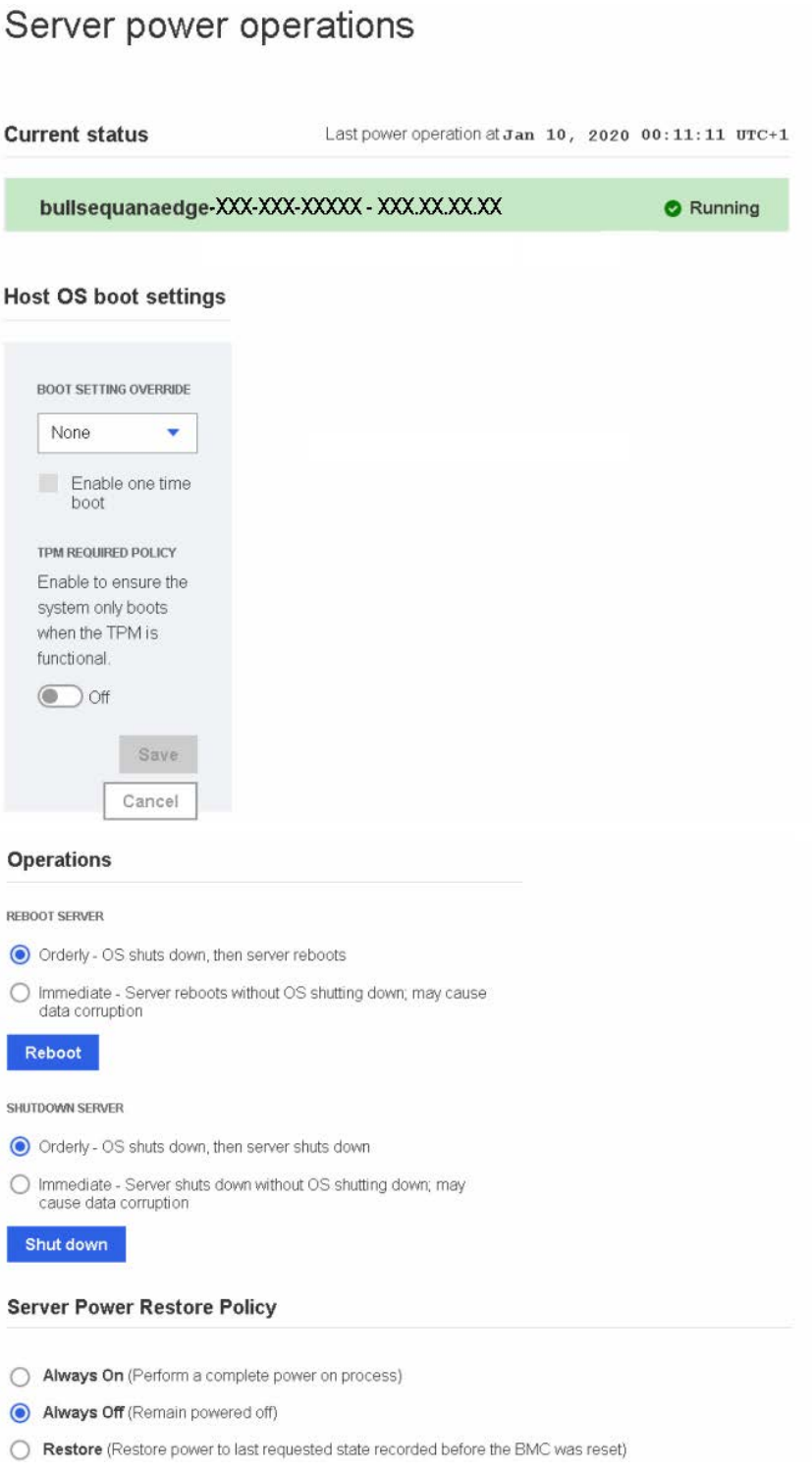
Note The sensor states are exported as .json data files.

Chapter 3. Controlling the server

3.1. Checking the power status

Procedure

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



Current Status	
Last power operation	Date and time of last power operation
Host name	The host name of the server
Power status	• Unreachable • Off • Running
Host OS boot settings	
Boot Setting Override	• None • Pxe - Boots from a PXE server • Hdd - Boots from a hard disk • Cd - Boots from a CD • 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
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 power status is Off. Powers on the server
Reboot server	Only active / visible when the server power status is Running • 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**. Reboot button - reboots the server applying the reboot option selected
Shutdown server	Only active / visible when the server power status is Running • 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**. Shut down button - shuts down the server applying the shut down option selected

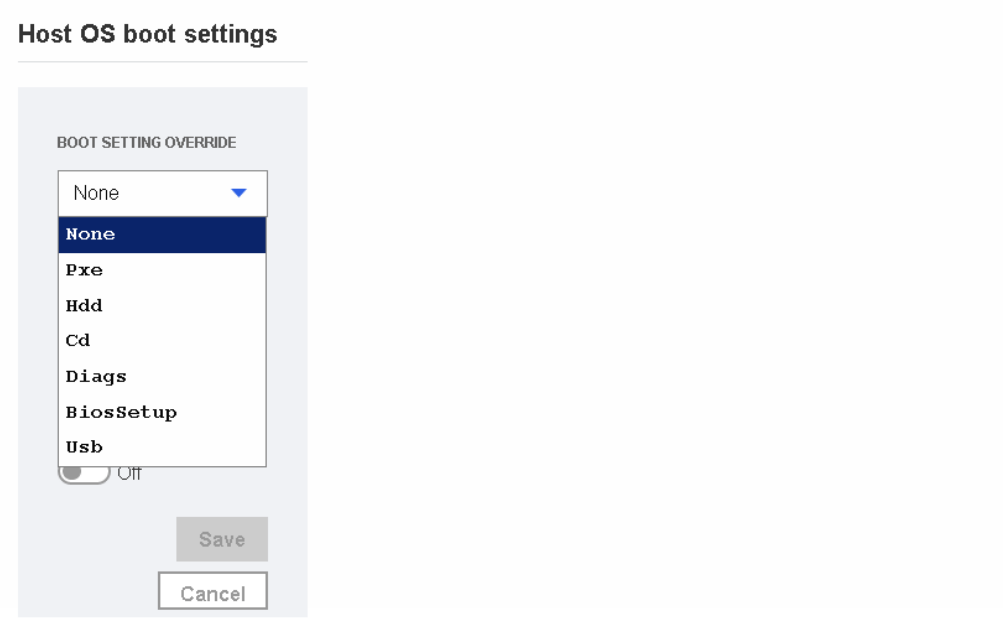
System Power Restore Policy	
Power Restore Policy	**Description**
Always On	Returns the server to the Running power status with the BMC ON and the OS launched.
Always Off	Returns the server to the Off power status with the BMC ON but the OS is not launched.
Restore	Returns the server to the power status already in place before the reboot.

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

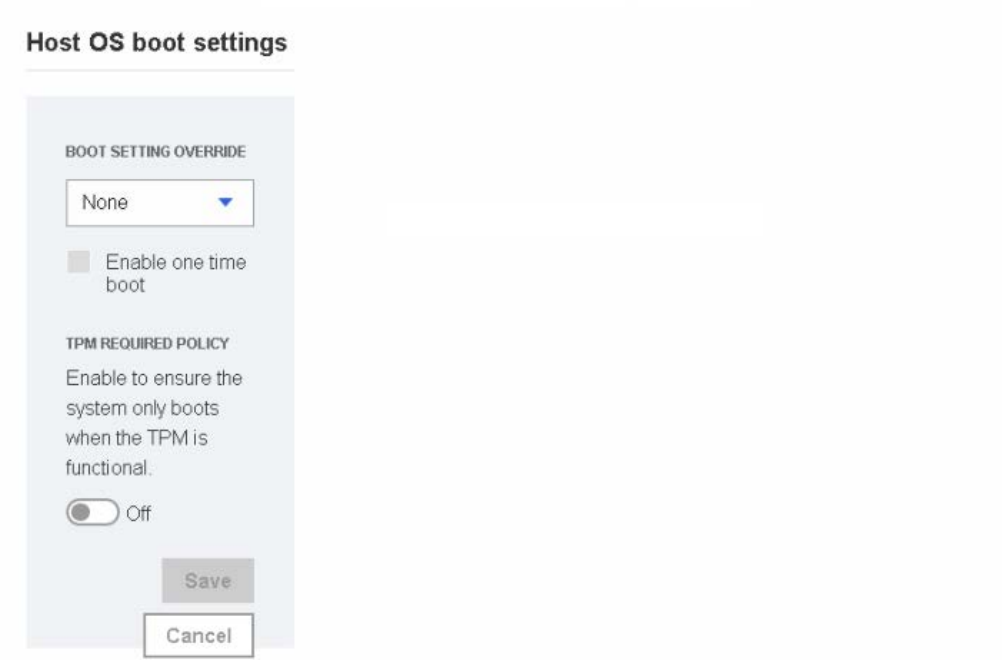
3.2. Setting boot options for host OS

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.



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



4. Click **Save**.

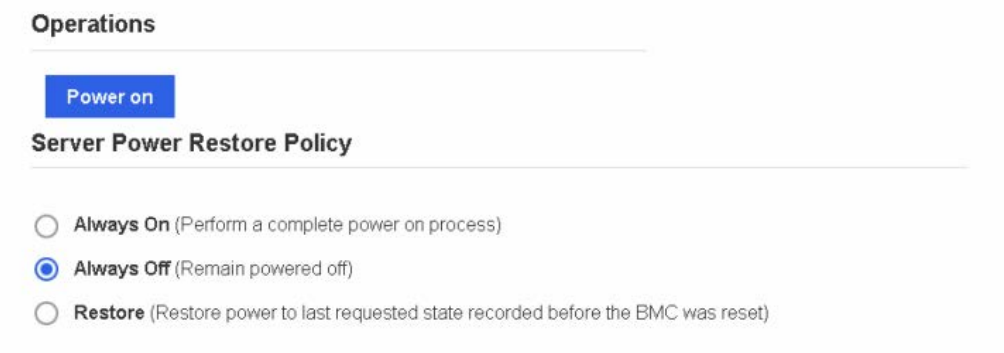
3.3. Powering on the server

Prerequisites

The server power status is Off

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.



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.

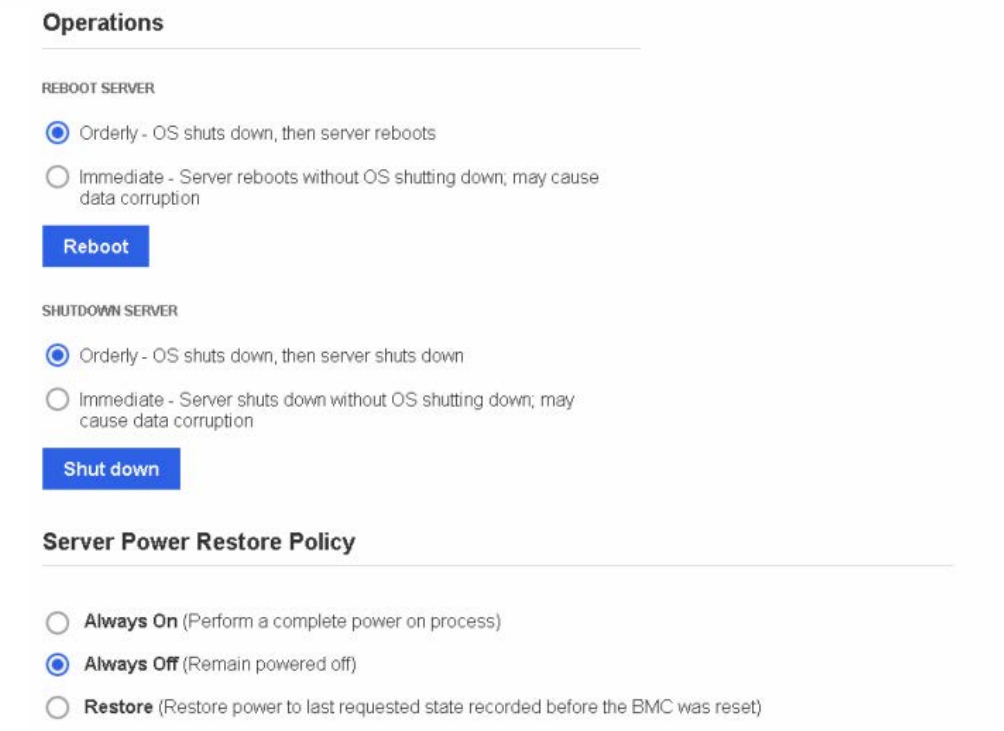
See	The Getting Started Guide or the Management Console User's Guide for more information.

Prerequisites

The server power status is Running

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.

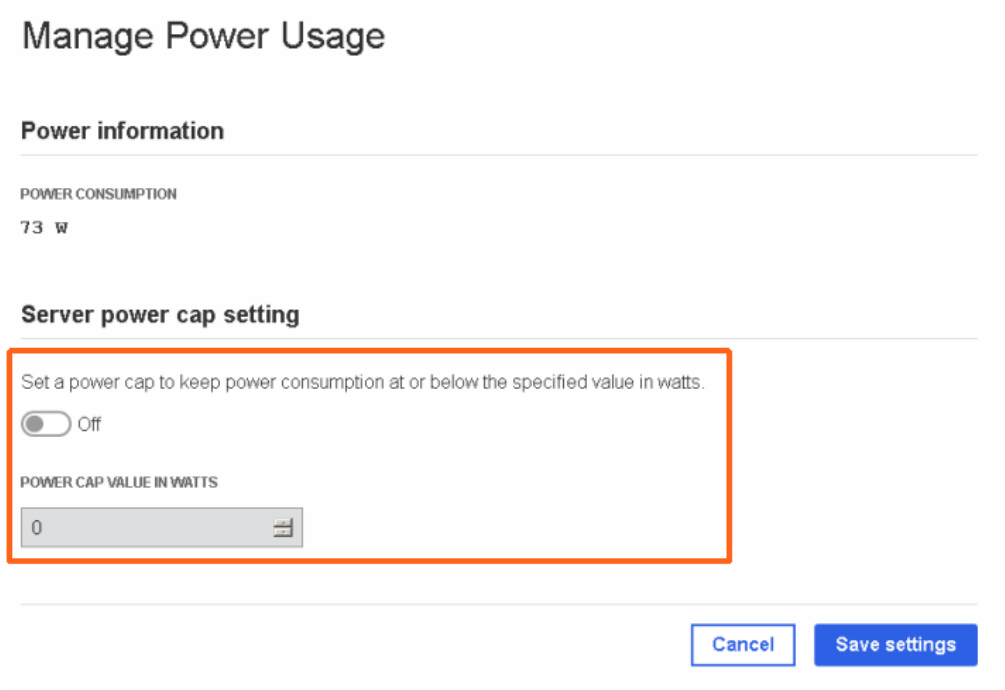


3. Select the power restore policy required.
4. Click **Reboot** or **Shut down**.

3.5. Managing power usage

Procedure

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



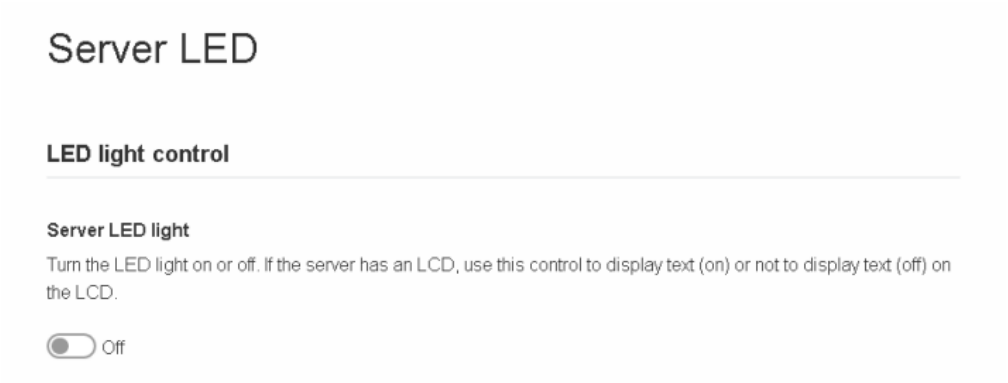
2. To set a power cap:
   a. Enable the **Server power cap setting.**
   b. Set the power cap value in the **Power Cap Value in Watts** box.
3. Click **Save settings**.

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.



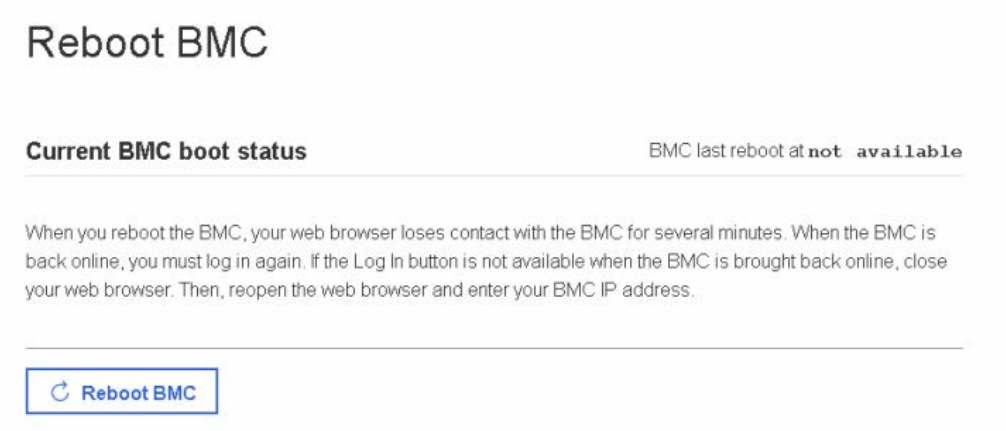
2. Turn the server identification LED off / on.

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.



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

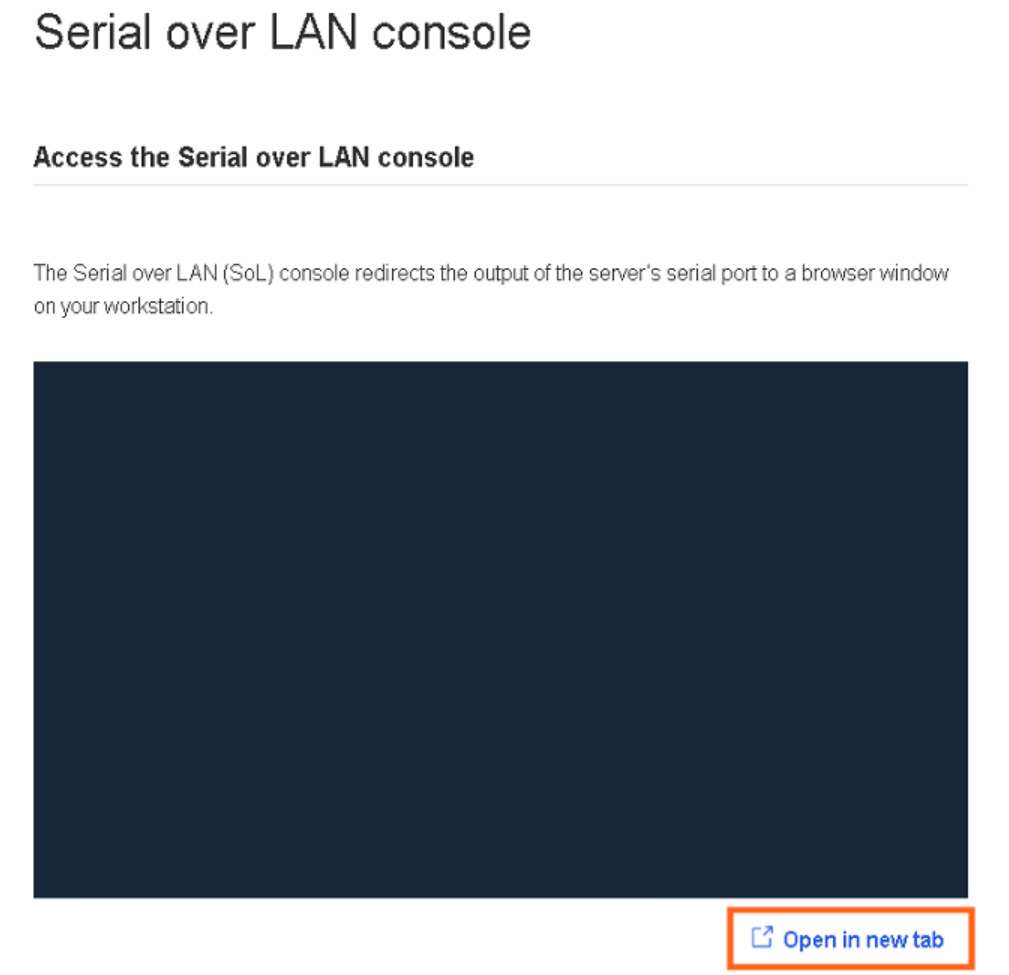
Note When the BMC is rebooted the browser loses contact with the BMC for several minutes. The log in procedure must be performed when the BMC is back online. If the log in button is not available, close the browser, reopen it and enter the BMC IP address.

Important **The date and time will be lost following a BMC reboot if they have been set manually. It is recommended to use NTP to set the date and time to preserve the settings when the BMC is rebooted.**

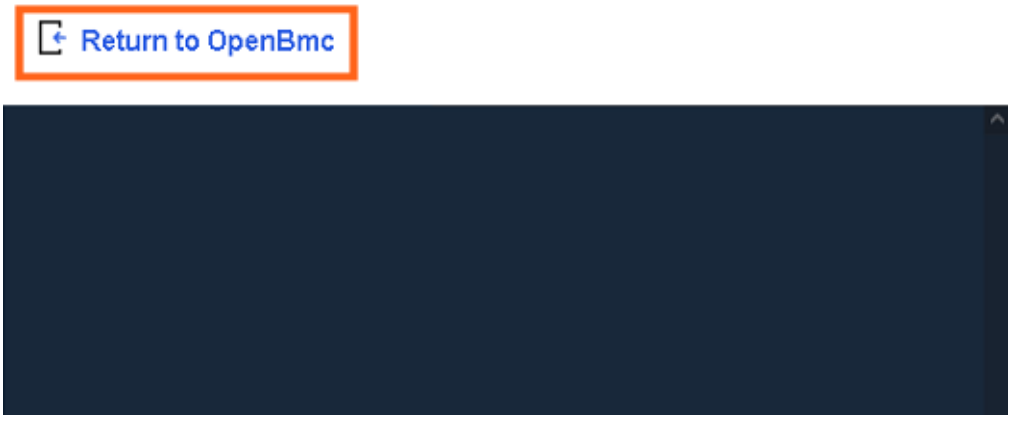
3.8. Connecting to the Serial over LAN (SoL) console

Procedure

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



2. If required, click the **Open in new tab** link to open the console in a new window.
3. Click **Return to OpenBmc** to go back to the the main window.

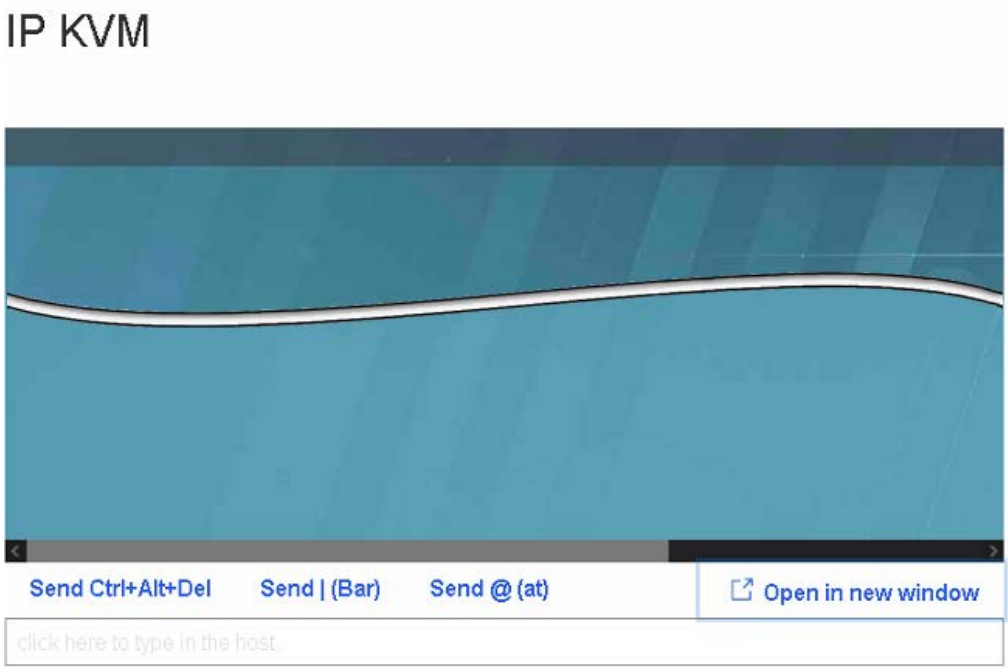


3.9. Connecting to the Keyboard Video Mouse (KVM)

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 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.**

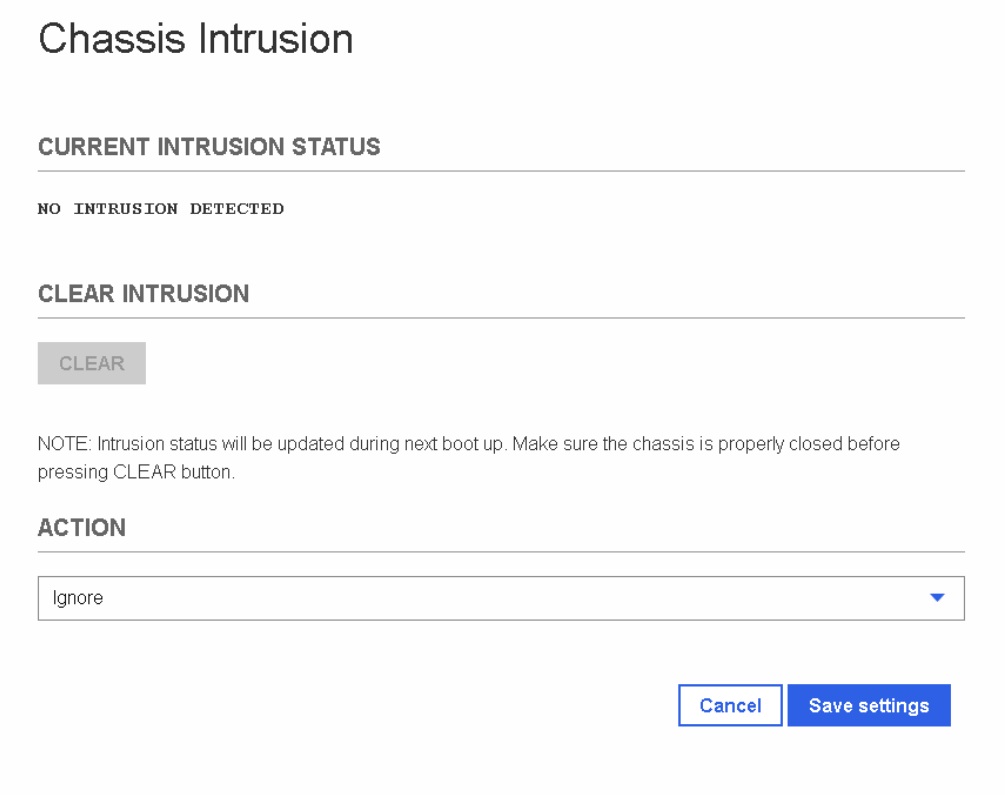
3.10. Managing intrusions

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.

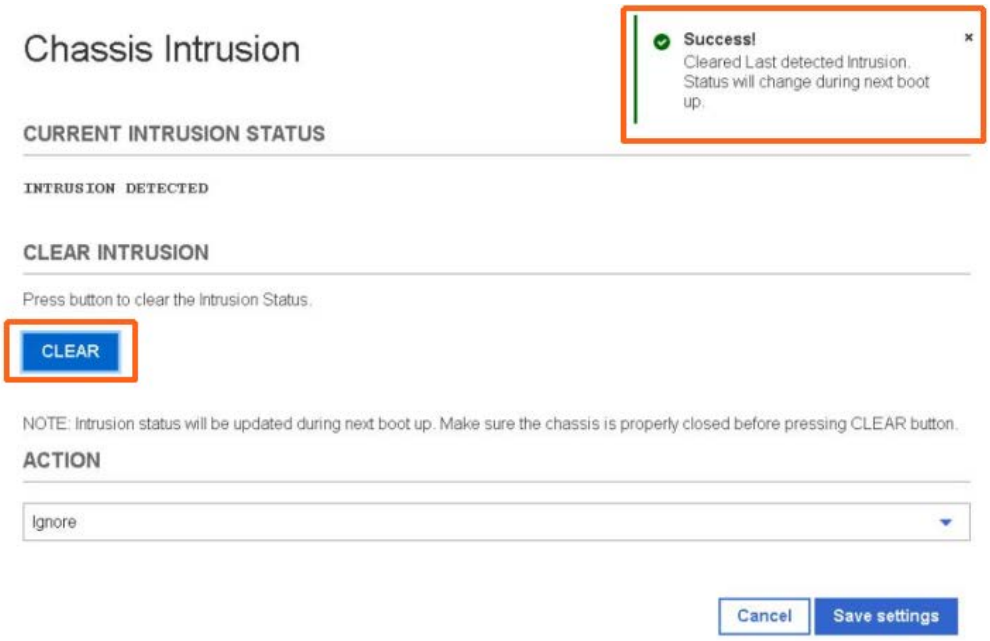


2. All intrusions detected are listed under **Current Intrusion Status.**

3.10.2. Clearing intrusions detected

Procedure

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



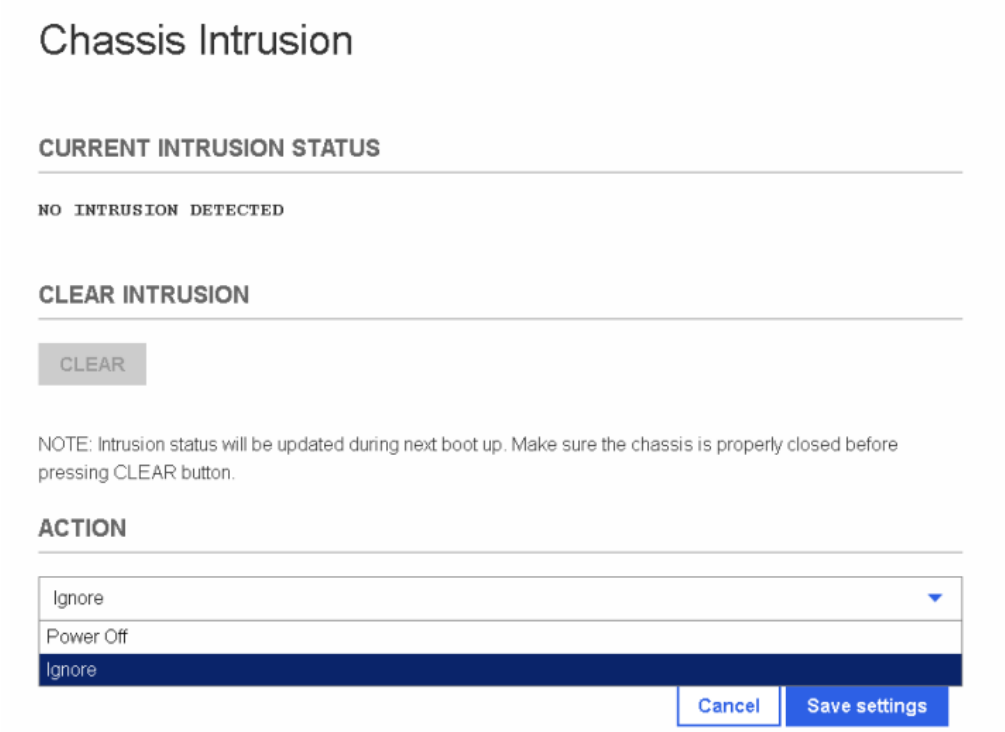
2. Click **CLEAR** to remove any actions detected from the list.
3. Wait until the Success message appears.

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.



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

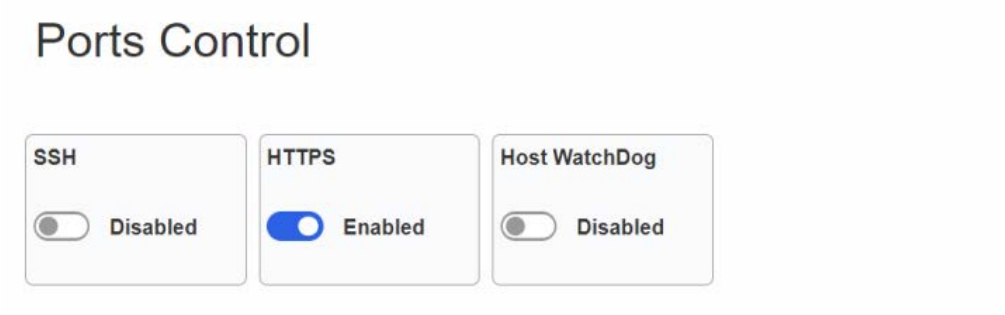
Important	**If the Power Off action is set, the server will not start until the intrusion is removed from the Current Intrusion Status list.**

3. Click **Save settings**.

3.11. Enabling port security controls

Procedure

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



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

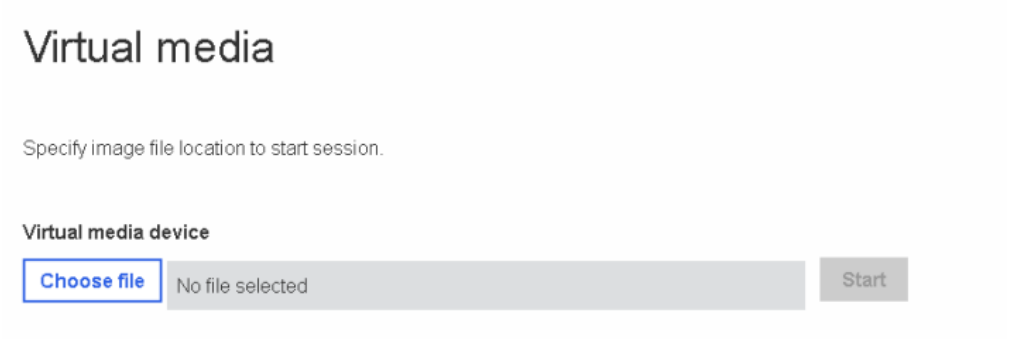
Notes
- If SSH is disabled, the BMC via SSH will not respond until it is enabled.
- If HTTPS is disabled, neither the SHC via HTTPS nor the REST commands will respond.

Important **At least one of the ports HTTPS or SSH must be enabled to keep contact with the BMC.**
If all ports are disabled, it is no longer possible to access the BMC. It is recommended to reset the BMC using the firmware recovery button. The HTTPS port will be enabled again.

3.12. Creating a virtual media session

Procedure

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



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

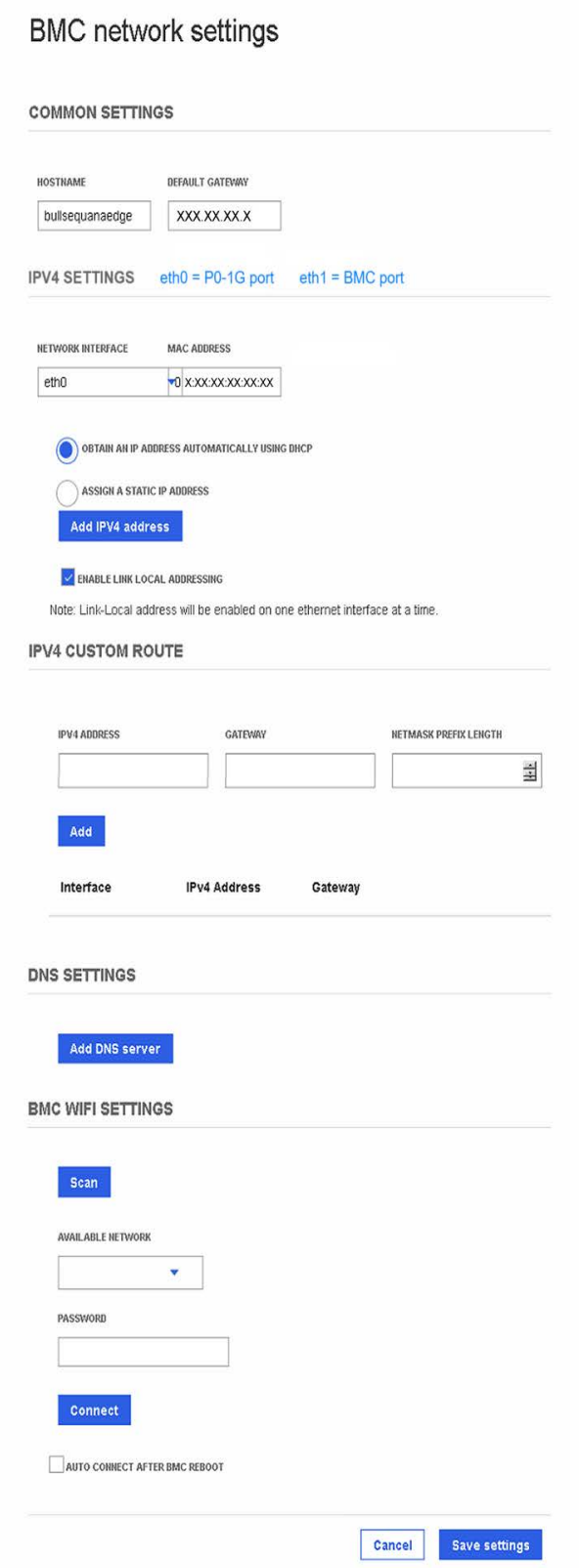
Prerequisites

- 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.

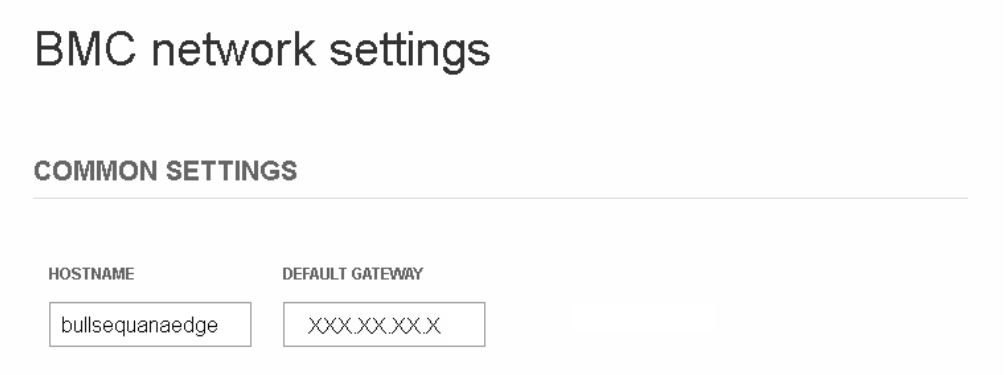


Common settings	
Hostname	The server hostname
Default gateway	Default gateway IP address
IPV4 settings	
Network interface	Select the option required: • Eth1 • Eth2
MAC address	The server MAC address
Obtain an IP address automatically using DHCP	When enabled, network IP address is retrieved from a DHCP 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.
IPV4 custom route	
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
DNS settings	
DNS server 1	DNS server IP address
Remove	Click to remove the DNS server
Add DNS server button	Click to add a DNS server
BMC WIFI settings	
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
Buttons	
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.



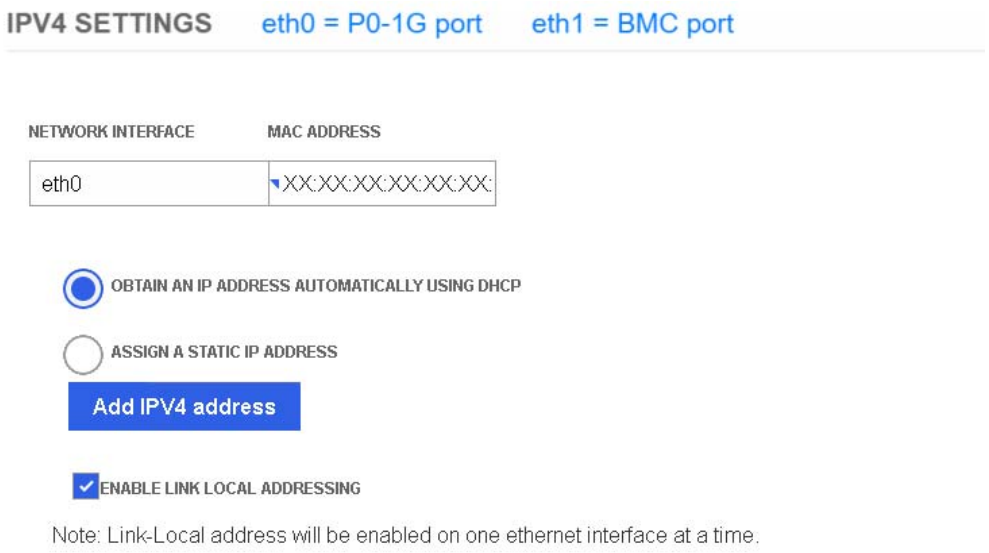
Note The default gateway for the BMC is configured automatically.

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.**



5. Click **Save settings.**

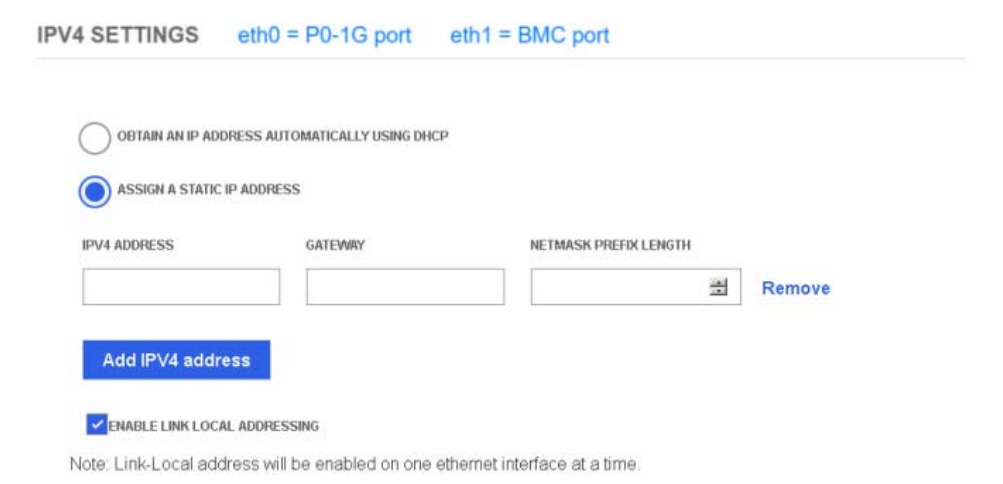
4.1.4. Assigning a static IP address

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**.



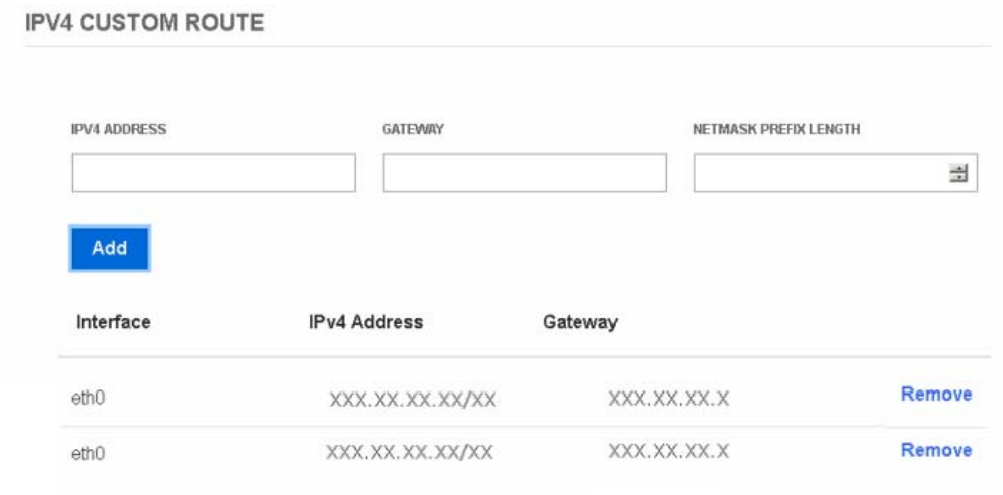
4. Click **Remove** to remove the existing IP address, if one exists.
5. Enter the network parameters for the static IP address.
6. Click **Add IPV4 address** if additional addresses are to be configured.
7. Click **Save settings.**

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.

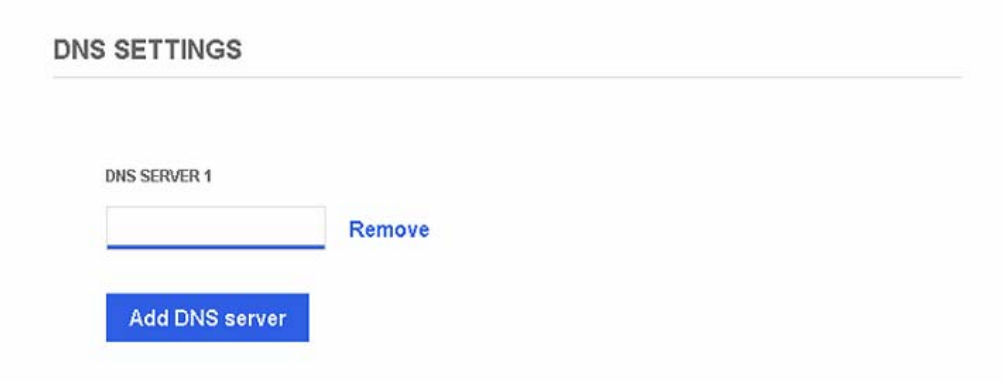


3. Click **Add**.
4. If required, click **Remove** to delete existing custom routes.

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



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

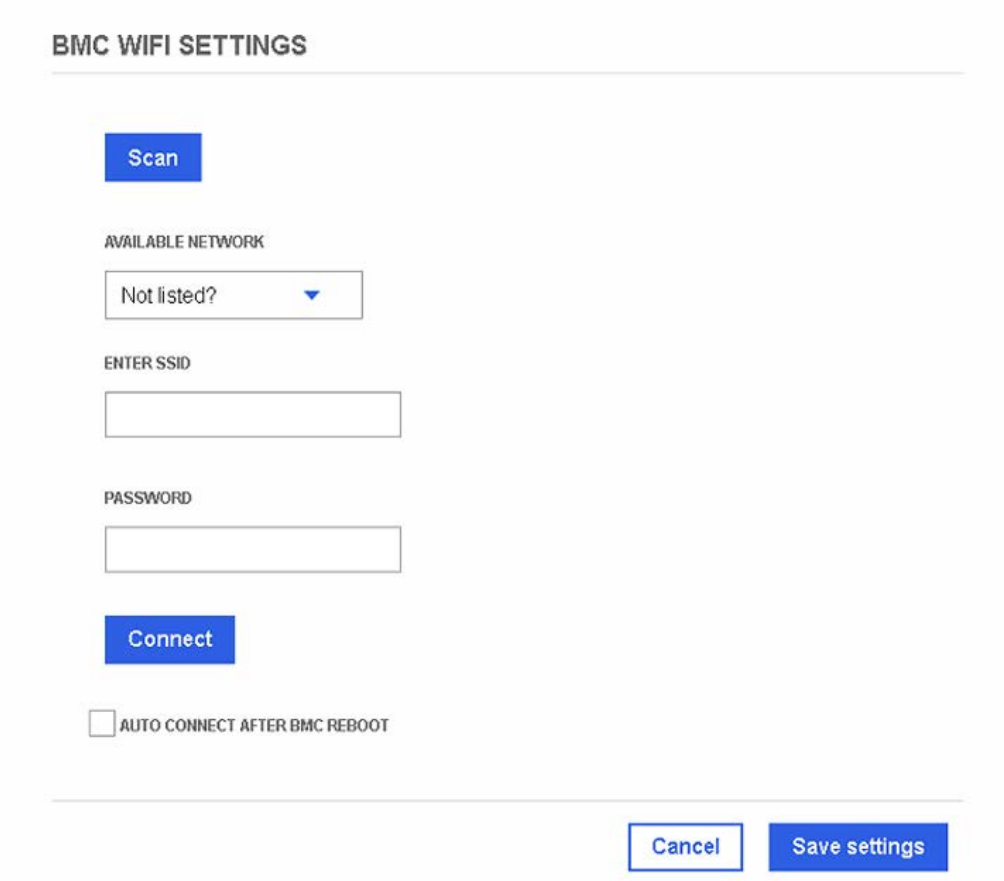
4.1.7. Configuring WIFI settings

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**.



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.

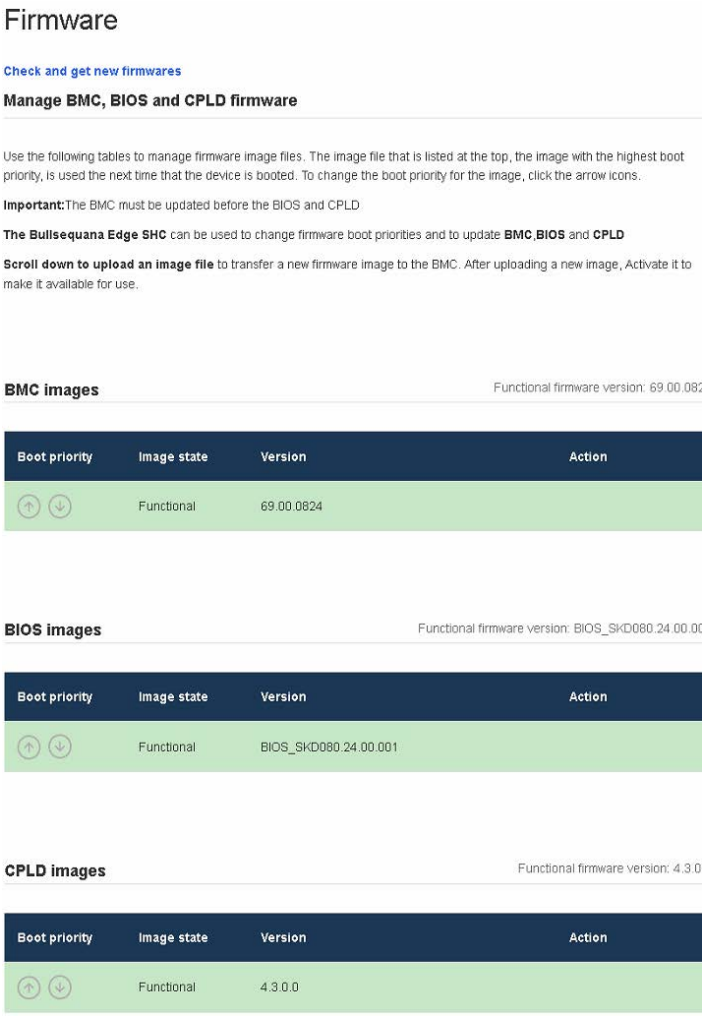
4.2.1. Checking firmware versions

Prerequisites

The server power status is Running

Procedure

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



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

4.2.2. Checking the firmware is up-to-date

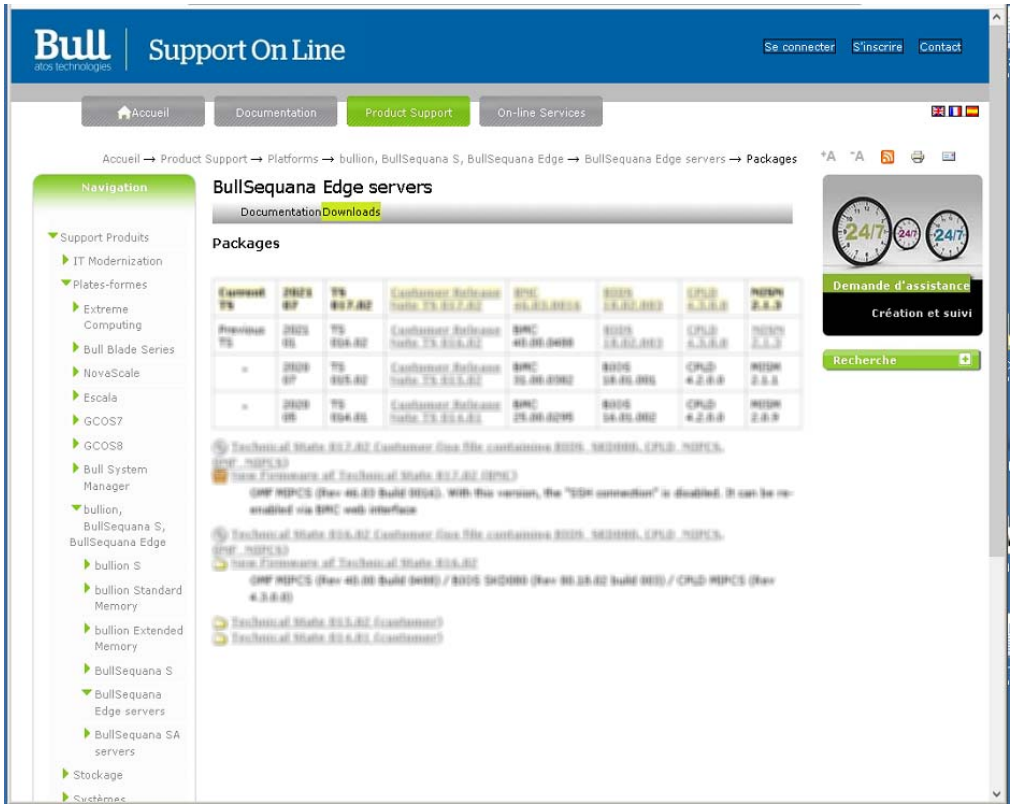
Prerequisites

- A laptop computer with the Chrome or Firefox browser installed
- Connection to the internet
- The server power status is Running

Procedure

1. From the **Configuration** tab, click **Firmware**. The **Firmware** page opens.
2. Click **Check and get new firmware**.

The support web site opens with the latest firmware list.



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

4.2.3. Updating the BMC firmware

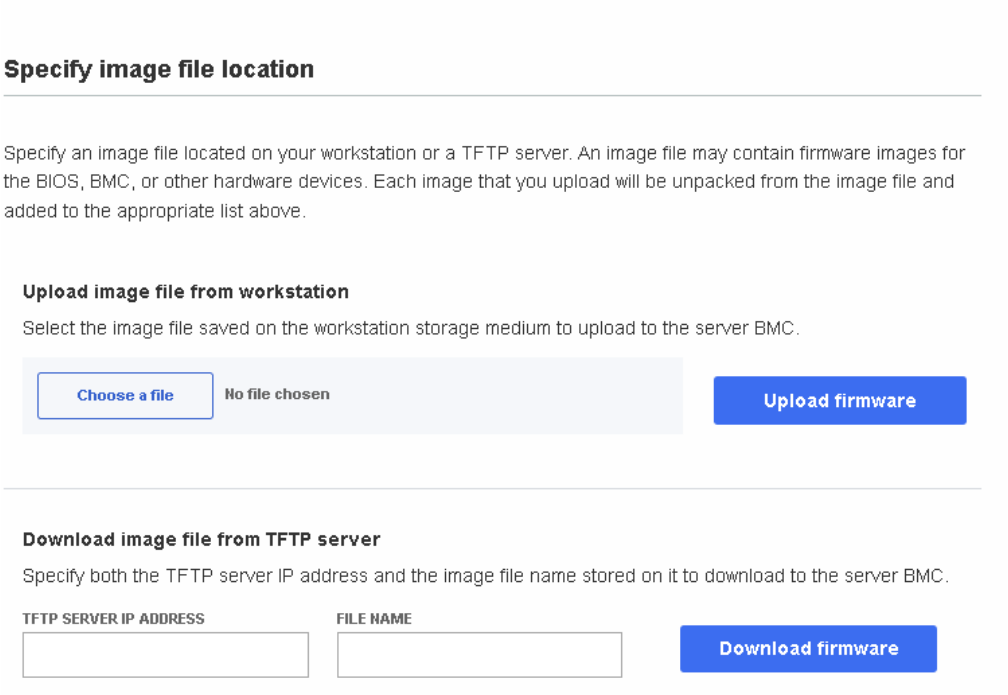
Prerequisites

The server power status is Off or Running

Procedure

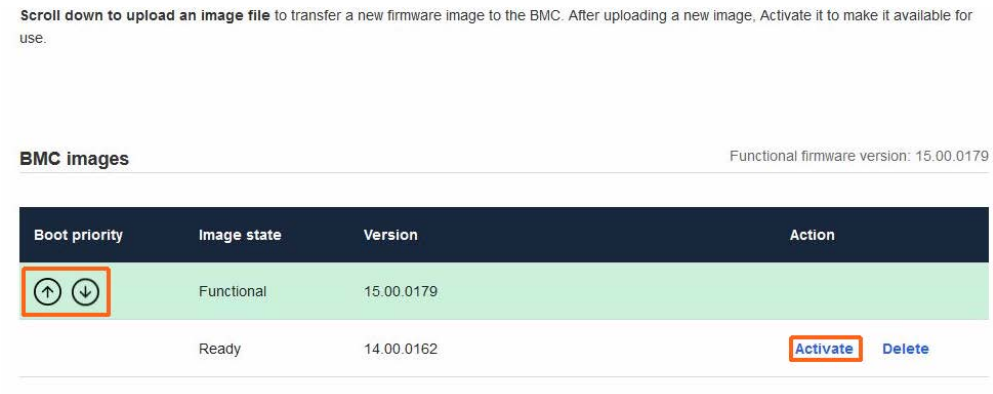
1. **Check the server power status**

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.

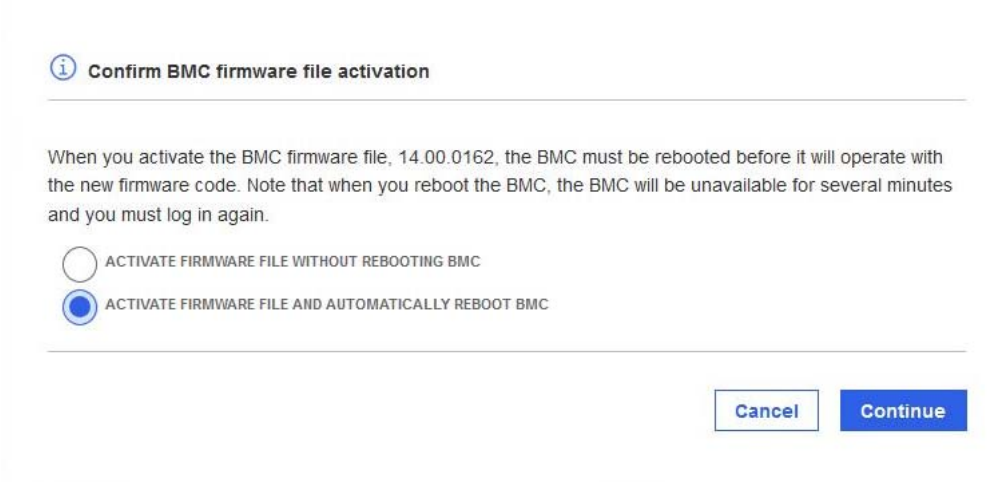


3. Activate the BMC image

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



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



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.**

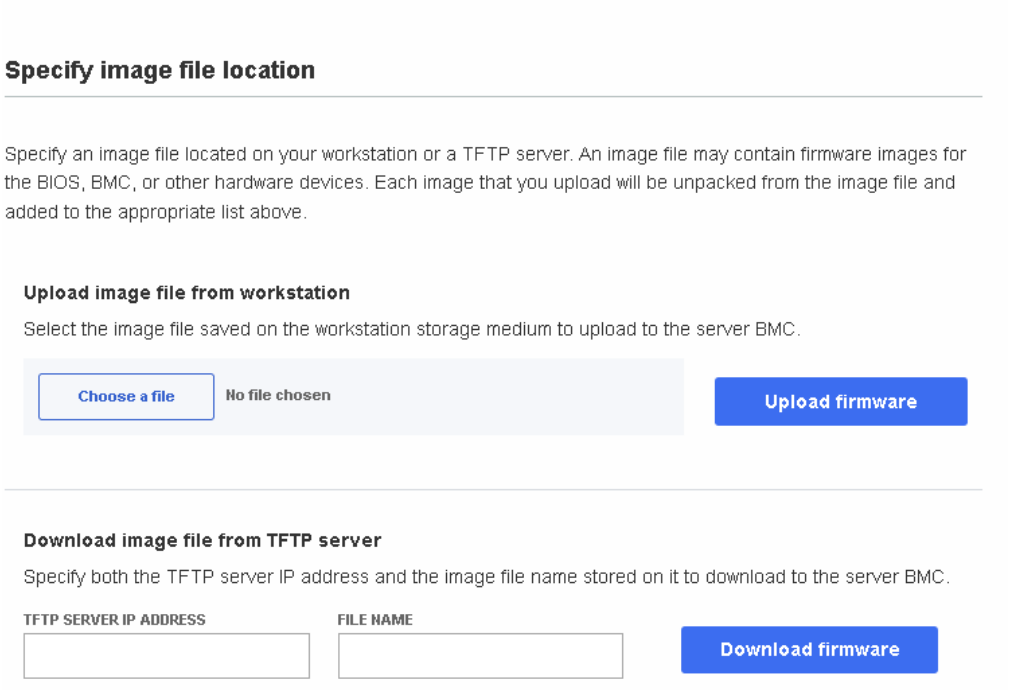
Prerequisites

The server power status is Off

Procedure

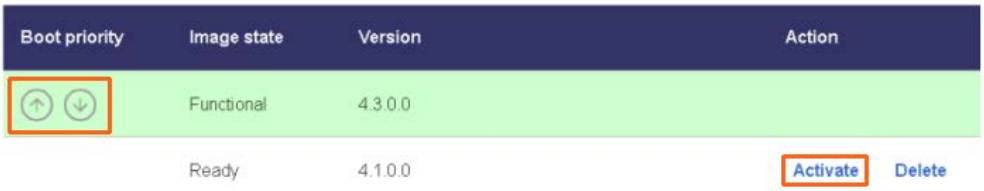
1. **Check the server power status**

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.



3. Activate the firmware

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

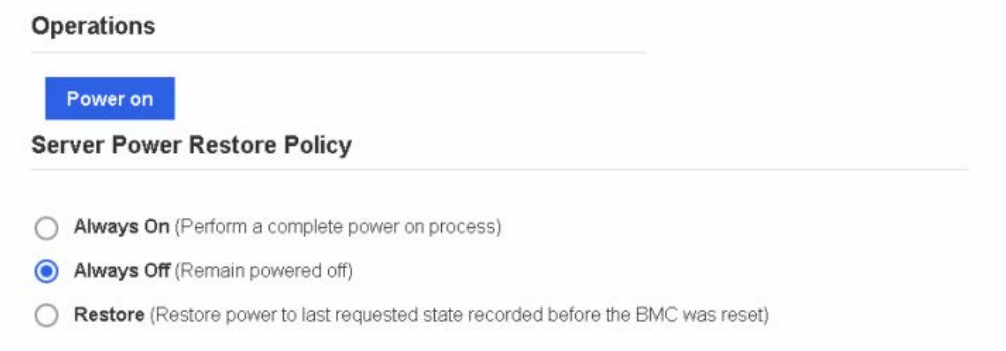


4. Wait two to three minutes and then refresh the page

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.

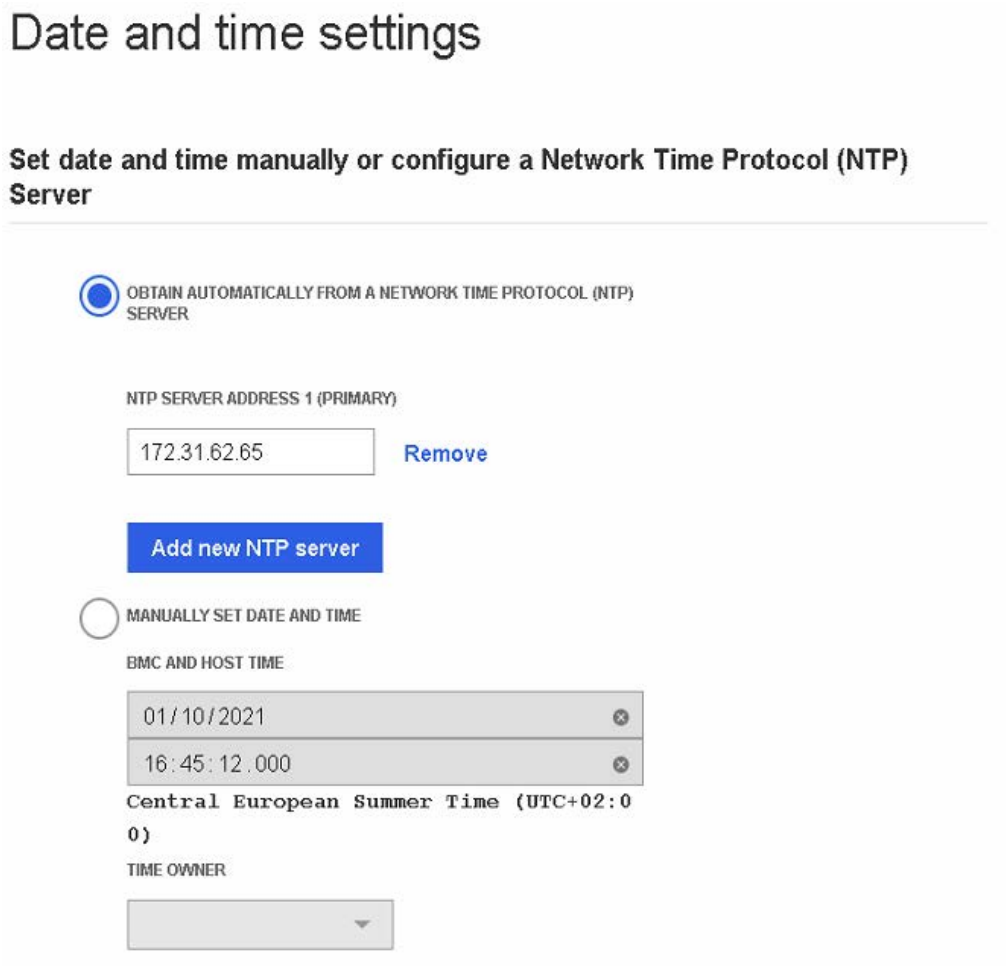


2. In the **Operations** section, click **Power on**.

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.



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**.

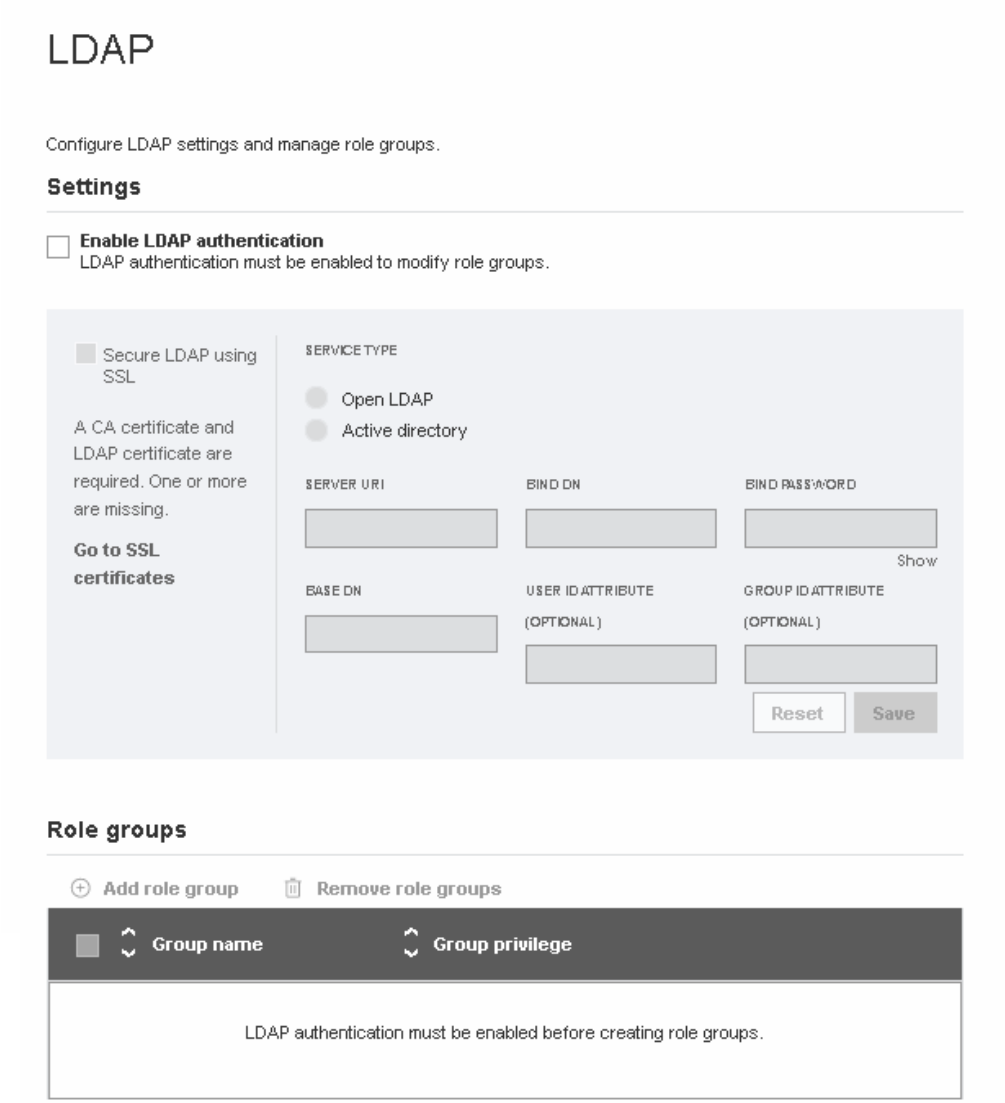
Important	**It is recommended to use the NTP server to set the date and time. If the date and time are set manually, the settings will be lost following a BMC reboot.**

3. Click **Save settings.**

Chapter 5. Managing Access

5.1. LDAP settings

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



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 **SSL certificates** page. The link is active when LDAP authentication is enabled
Service type	Selects the LDAP service type: • Open LDAP • Microsoft Active Directory
Server URI	ldap://<LDAP Server IP>

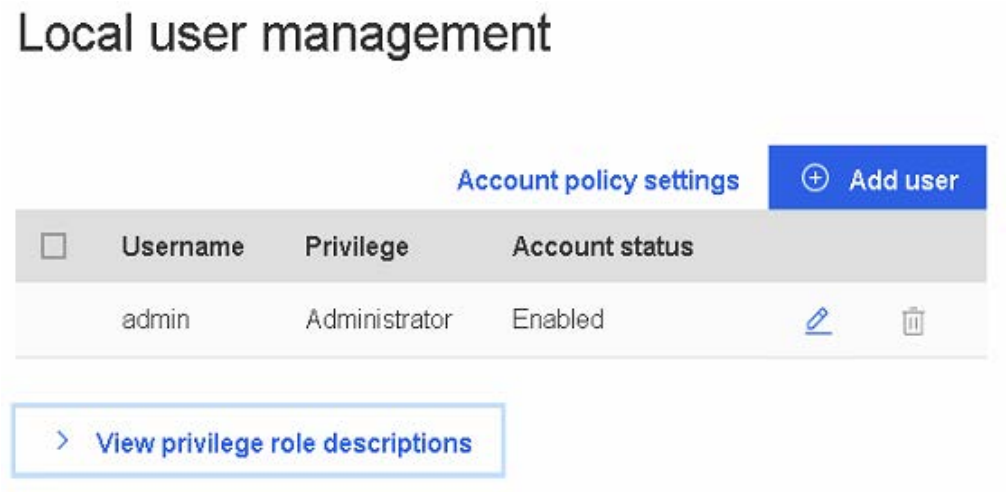
Settings	
Bind DN	Bind Distinguished Name
Bind password	Bind user password
Base DN	Base Distinguished Name. The point from which a server will start searching for users.
User ID attribute	The log in attribute that uniquely identifies a single user record.
Group ID attribute	The log in attribute that uniquely identifies a group user record.
Reset button	Clears the fields
Save 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

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.

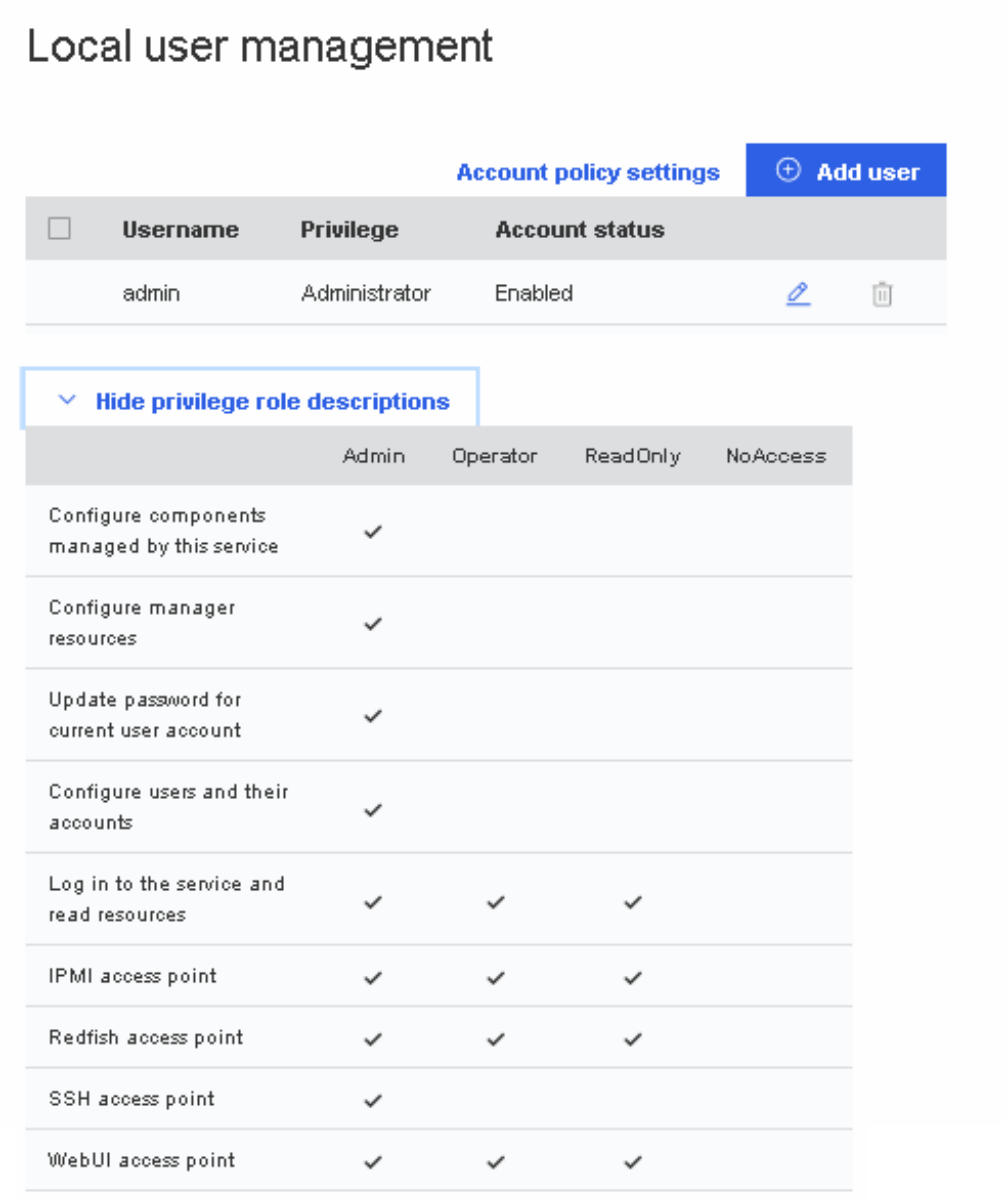


Local user management	
Username	Name the user uses to log on
Privilege	Role assigned to the user
Account status	When enabled, the user account is active and the user is able to log on. When disabled, the user's account is unavailable: the user's account is maintained but it is no longer possible to log 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

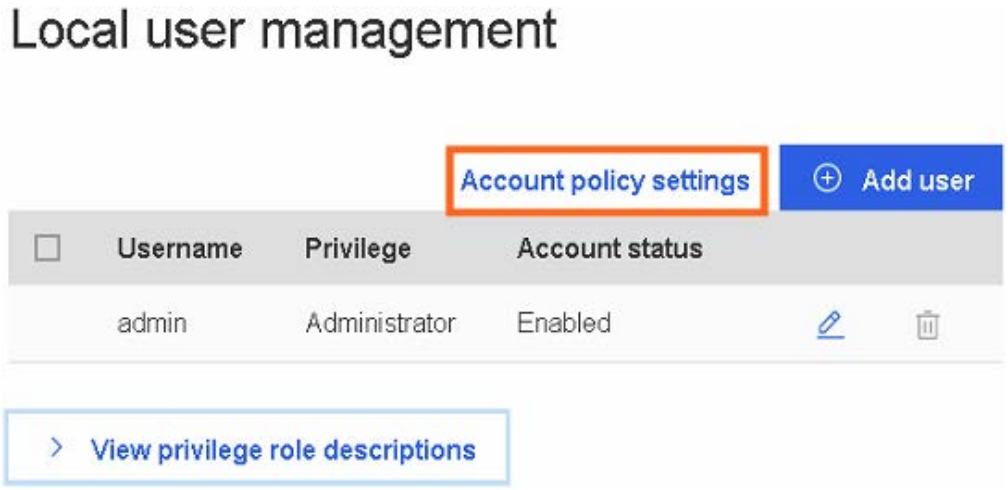
1. From the **Access** tab, click **Local users**. The **Local user management** page opens.
2. Click **View privilege role descriptions** to display the roles.



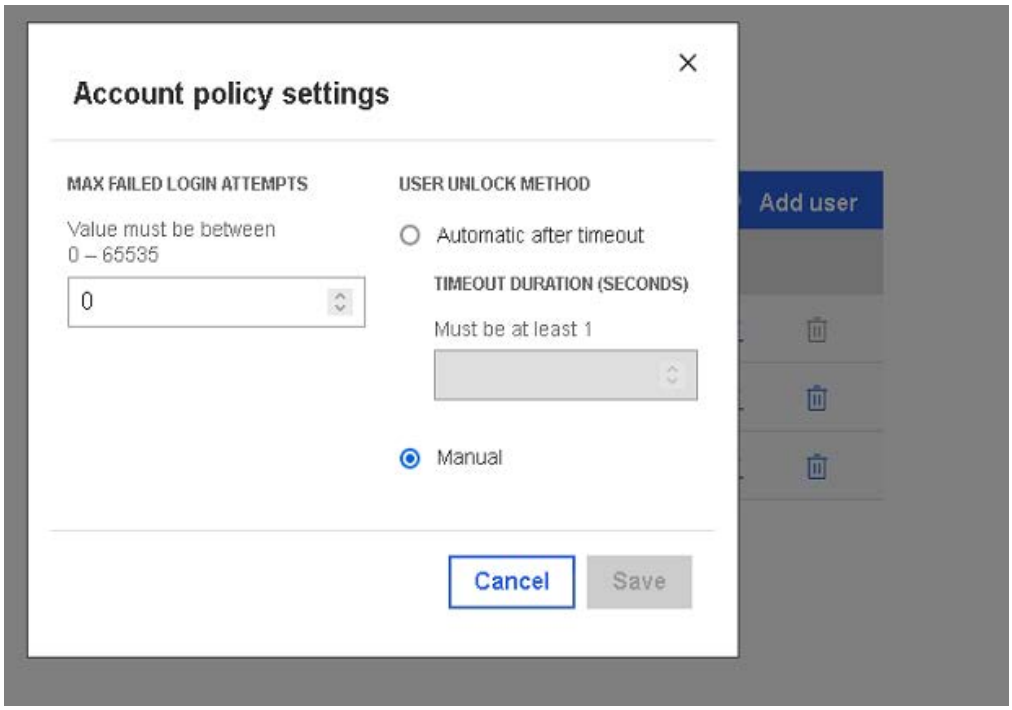
5.2.3. Setting the account policy

Procedure

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



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



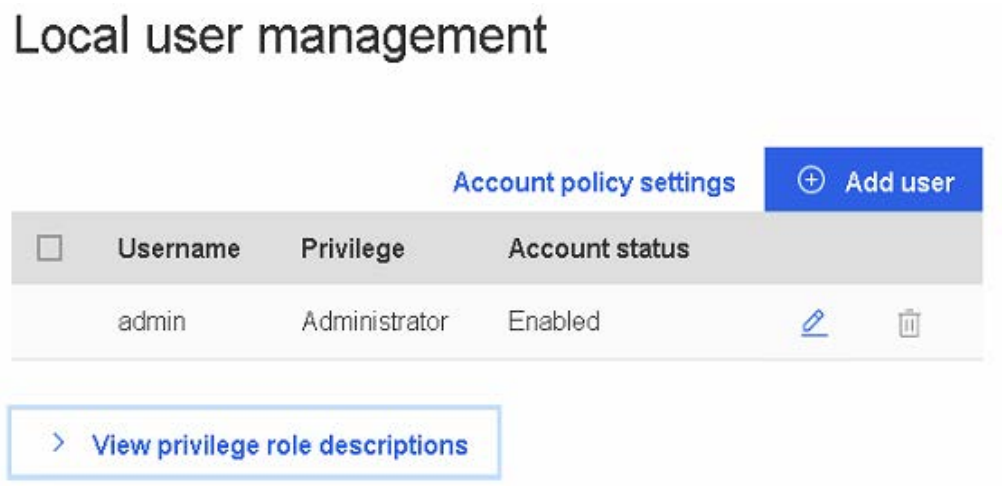
Account policy settings	
Max failed login attempts	The number of failed login attempts allowed. The value must be set between 0 (default) and 65535
Automatic after timeout	Automatic unlock after the period set in the Timeout duration parameter
Timeout duration (seconds)	Period in seconds during which 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**.

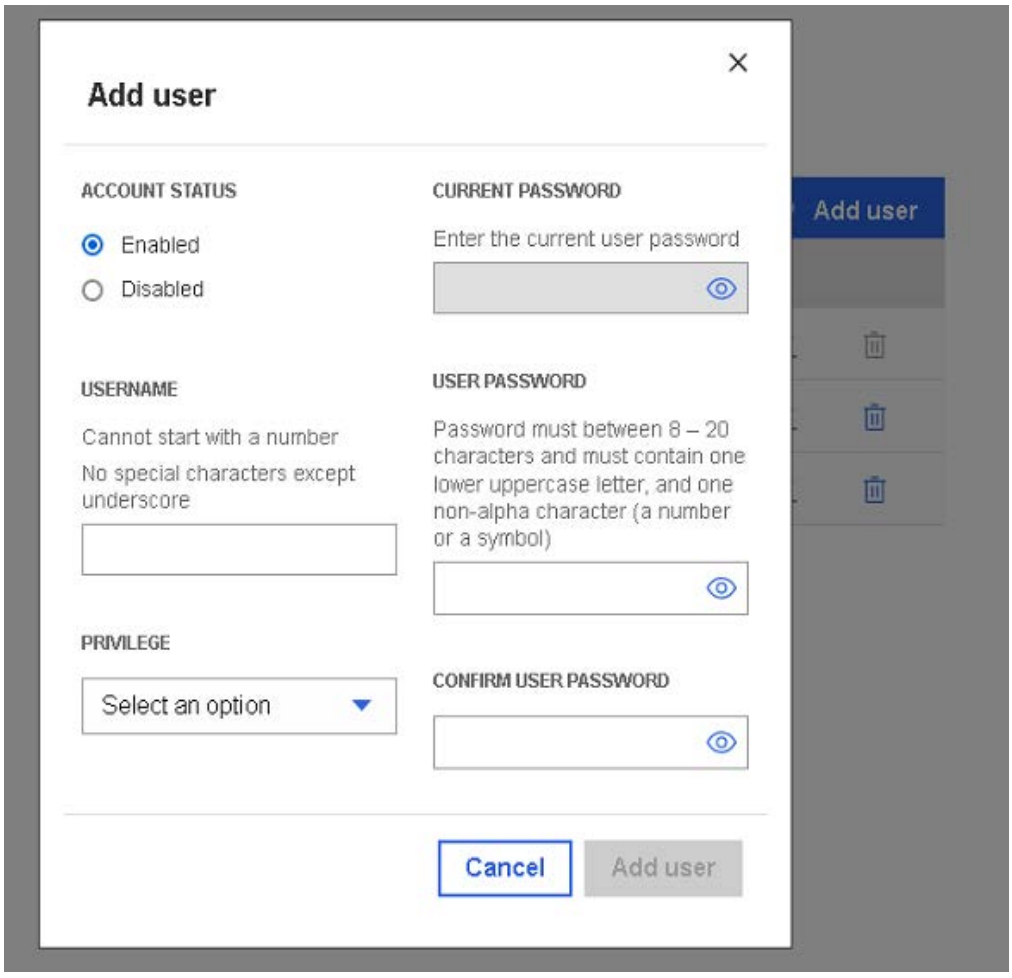
5.2.4. Creating a new user account

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.



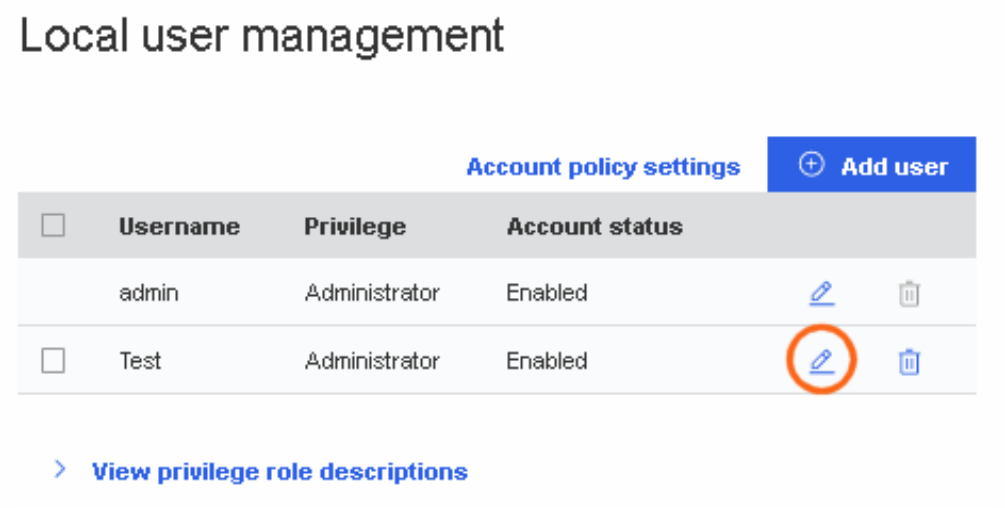
Add user	
Account status enabled	When selected, the user account is active and the user is able to log on. This is the default status
Account status disabled	When selected, the user's account is unavailable
Username	Name the user uses to log on • Names cannot start with a number • Special characters 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 user to log on • The password must be between 8 and 20 characters long
Confirm user password	• 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.

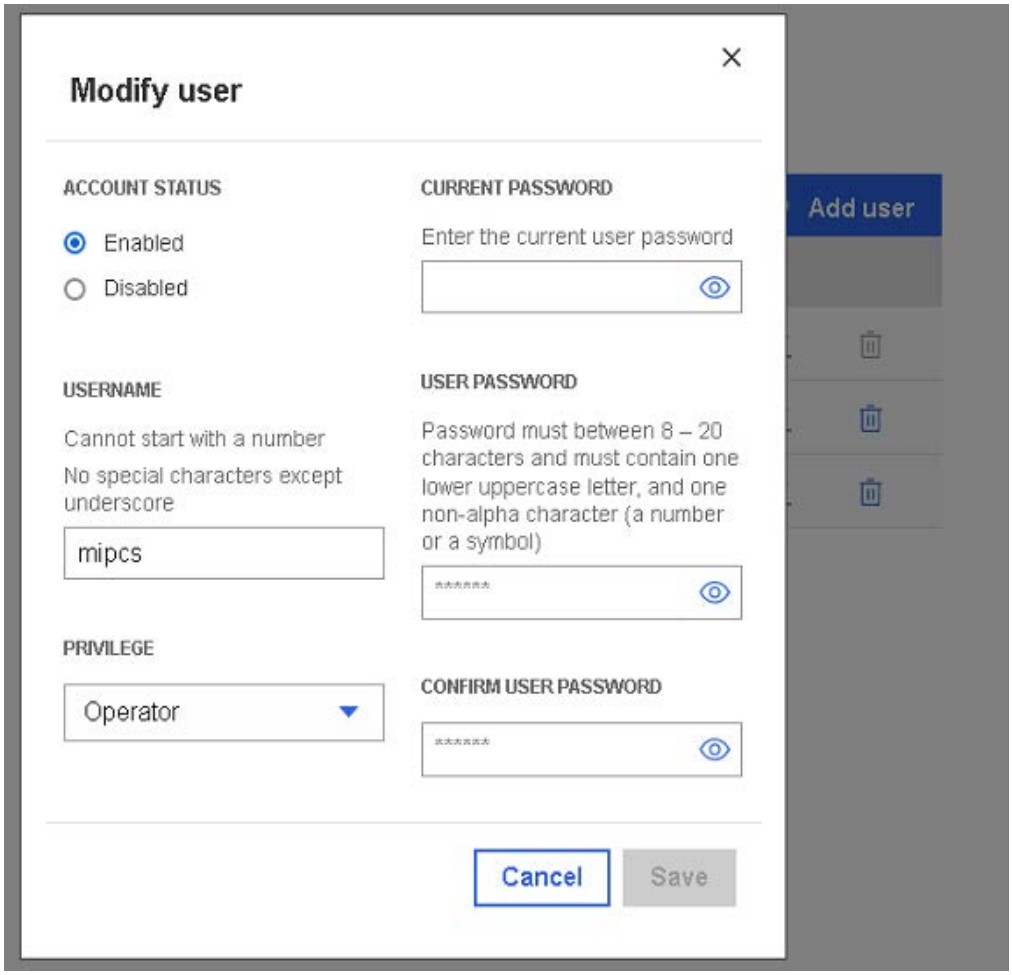
5.2.5. Modifying a user account

Procedure

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



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



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 and be a mixture of upper case letters, lower case letters, numbers and special characters. It must be different from the user name.

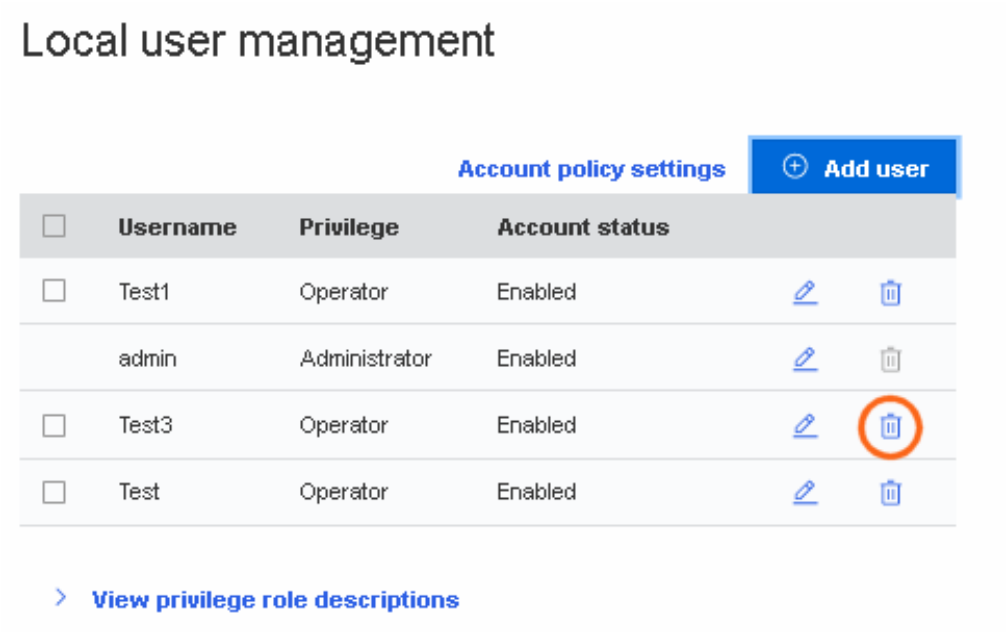
6. Click **Save**. User account details are changed.

5.2.6. Deleting a user account

5.2.6.1. Deleting a single user account

Procedure

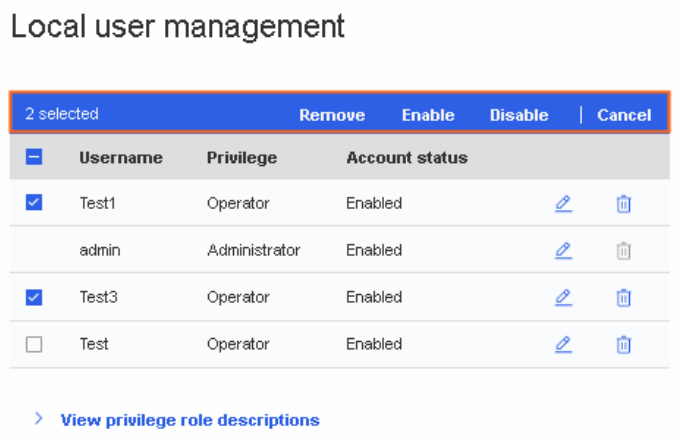
1. From the **Access** tab, click **Local users**. The **Local user management** page opens.



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.

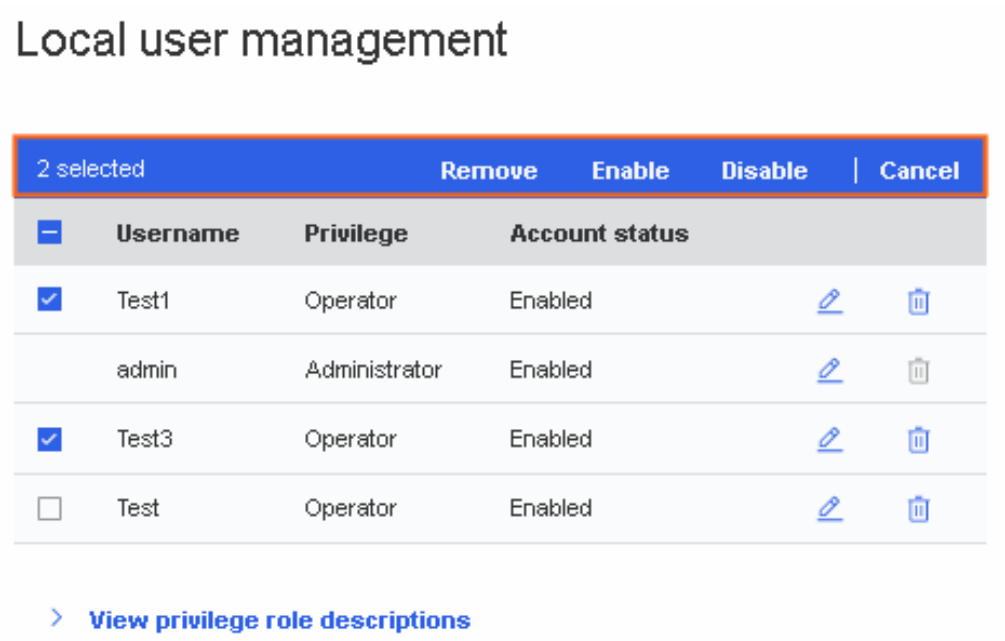


3. Click **Remove** in the menu bar.
4. Click **Remove** in the confirmation dialog box to remove the users.

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.

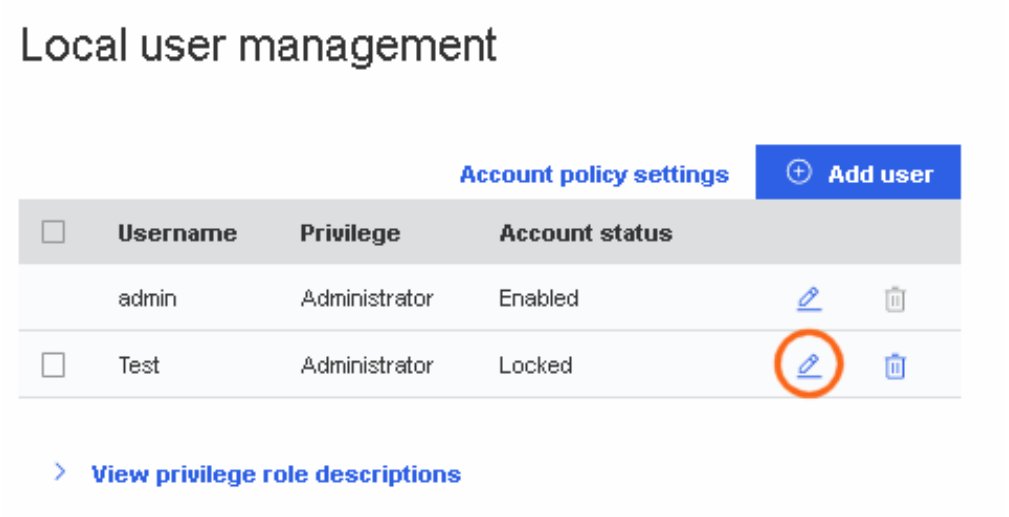


3. To disable the account(s), click **Disable** in the menu bar; to enable the account(s), click **Enable** in the menu bar.

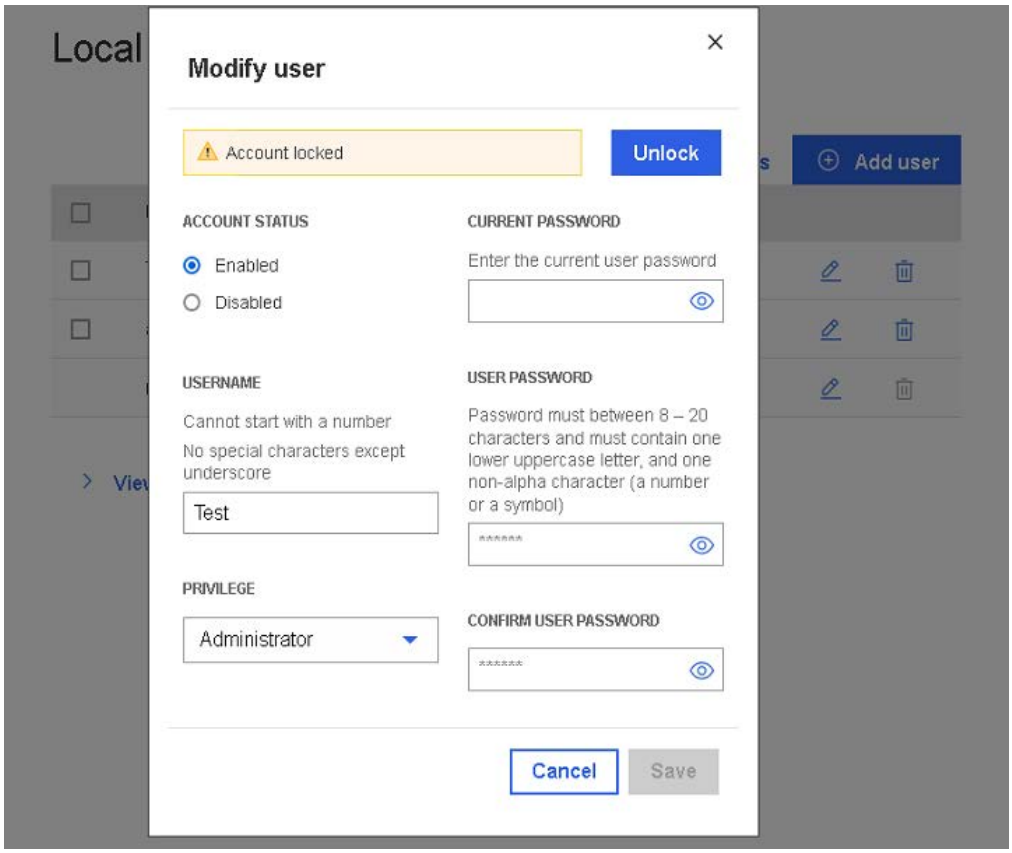
5.2.8. Manually unlocking a user account

Procedure

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



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



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	

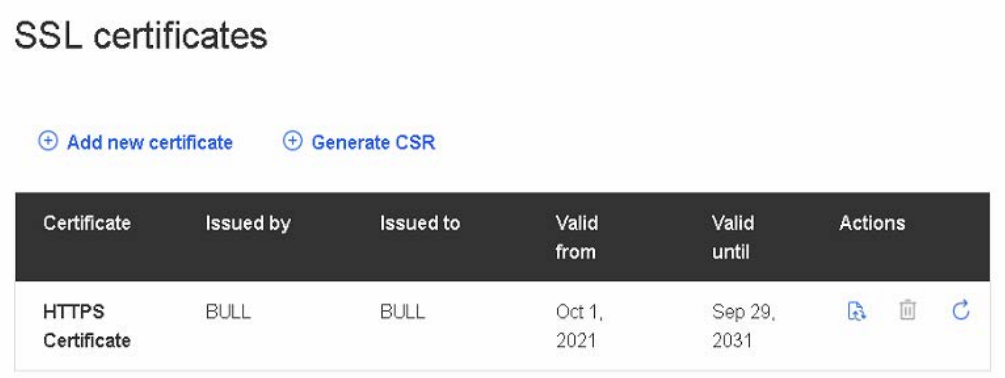
See Section 5.2. Managing users, on page 5-3

5.4. Managing SSL certificates

5.4.1. Viewing certificate list

Procedure

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

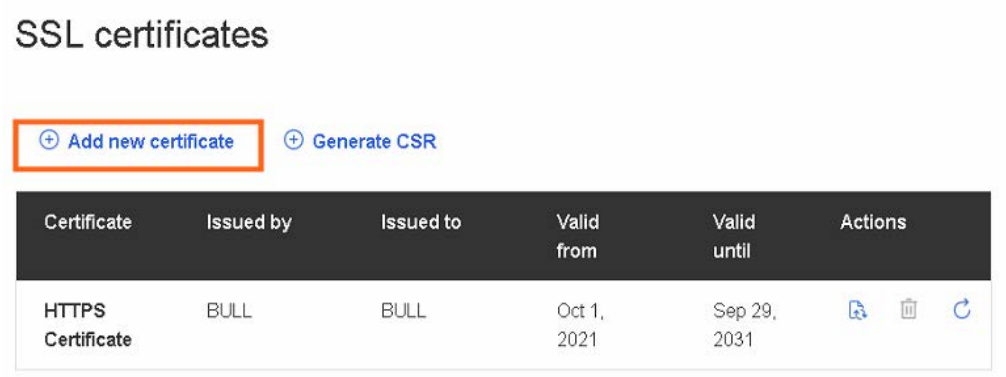


SSL certificates	
Certificate	Certificate name
Issued by	Certificate details
Issued to	
Valid from	Validity period
Valid until	
Actions	
	Update button to replace the certificate manually
	Remove button to delete the certificate
	Refresh button to check if a more up-to-date version of the certificate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

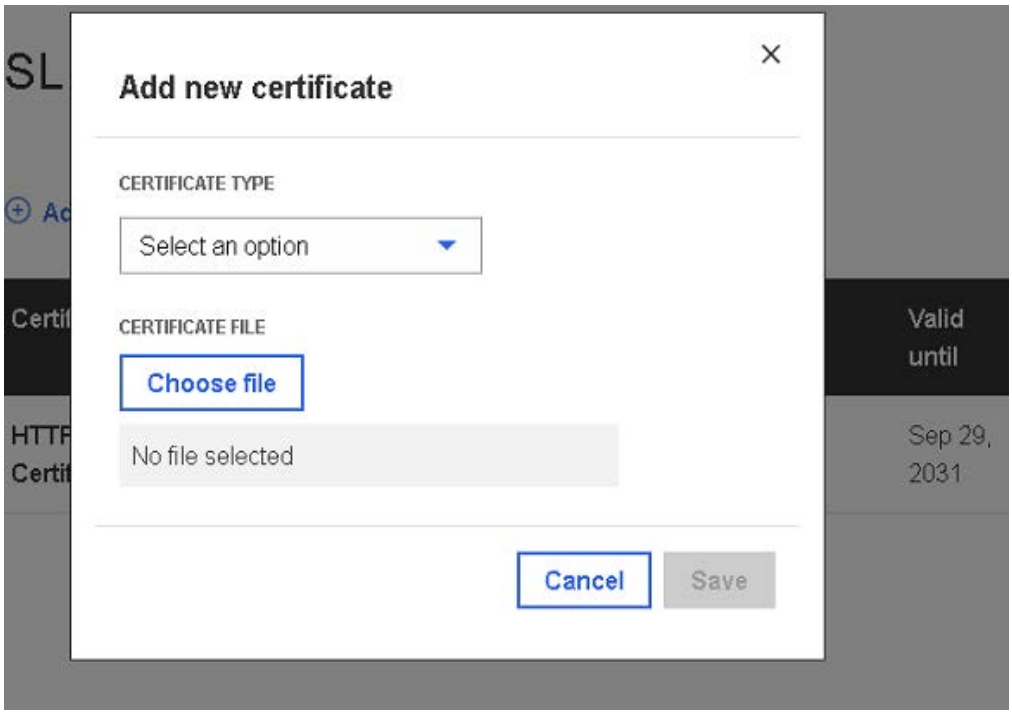
5.4.2. Adding a certificate

Procedure

1. From the **Access** 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 **Choose file** and select a certificate file.

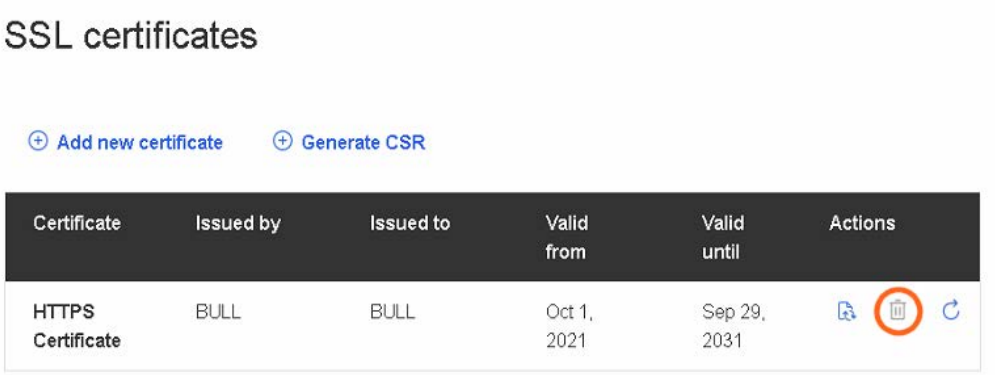
Note The certificate file must be a .pem file.

5. Click **Save**.

5.4.3. Deleting a certificate

Procedure

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

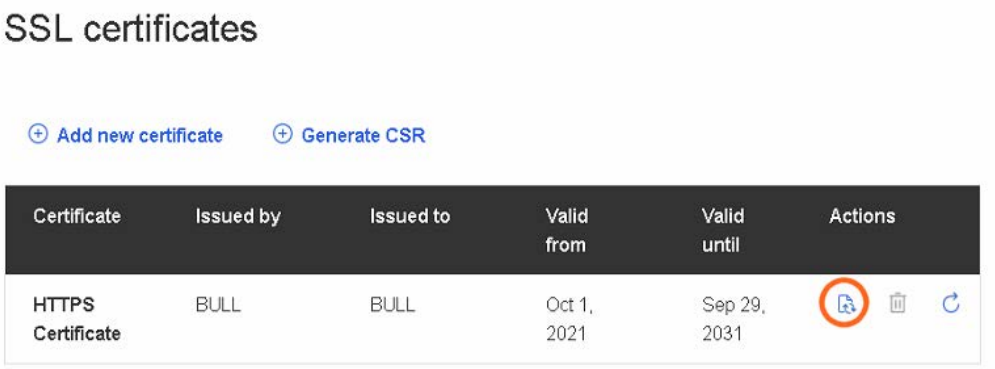


2. Click the remove button for the required certificate.
3. Click **Remove** in the confirmation dialog box to remove the certificate.

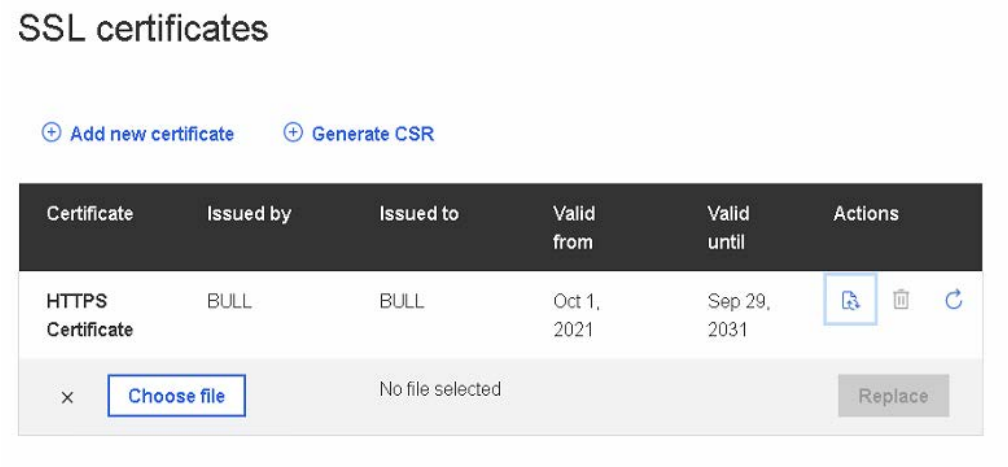
5.4.4. Updating a certificate manually

Procedure

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



2. Click the update button for the required certificate.

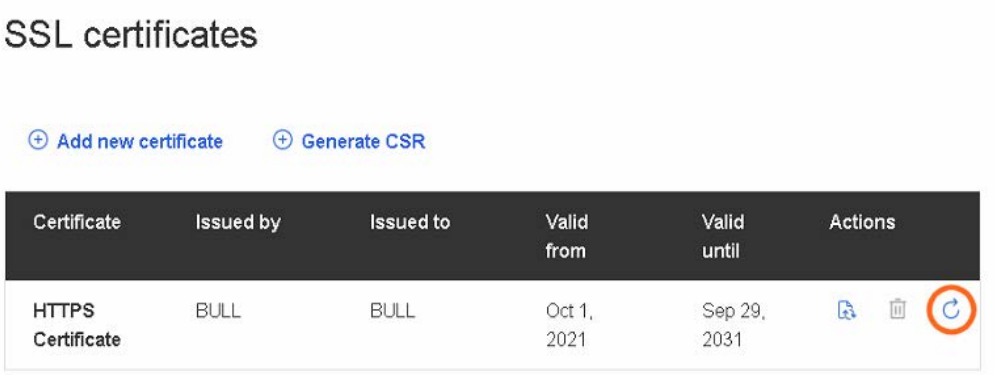


3. Click **Choose file** and select a certificate file.
4. Click **Replace**.

5.4.5. Updating a certificate automatically

Procedure

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

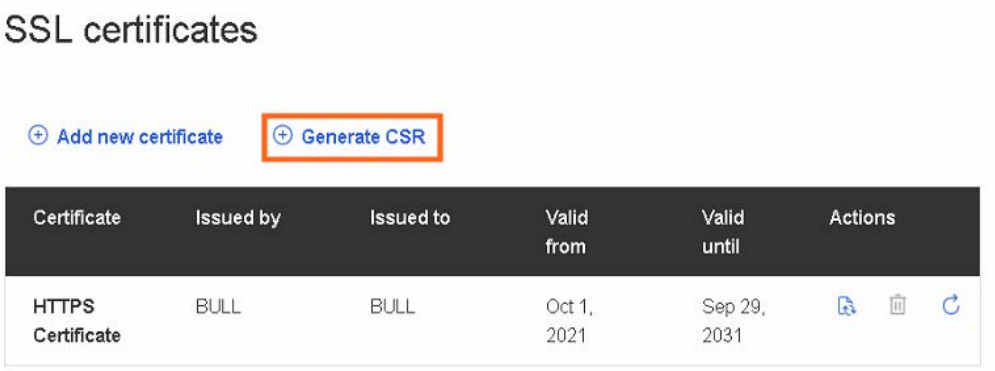


2. Click the refresh button for the required certificate.
3. The certificate will be updated if a newer version is available.

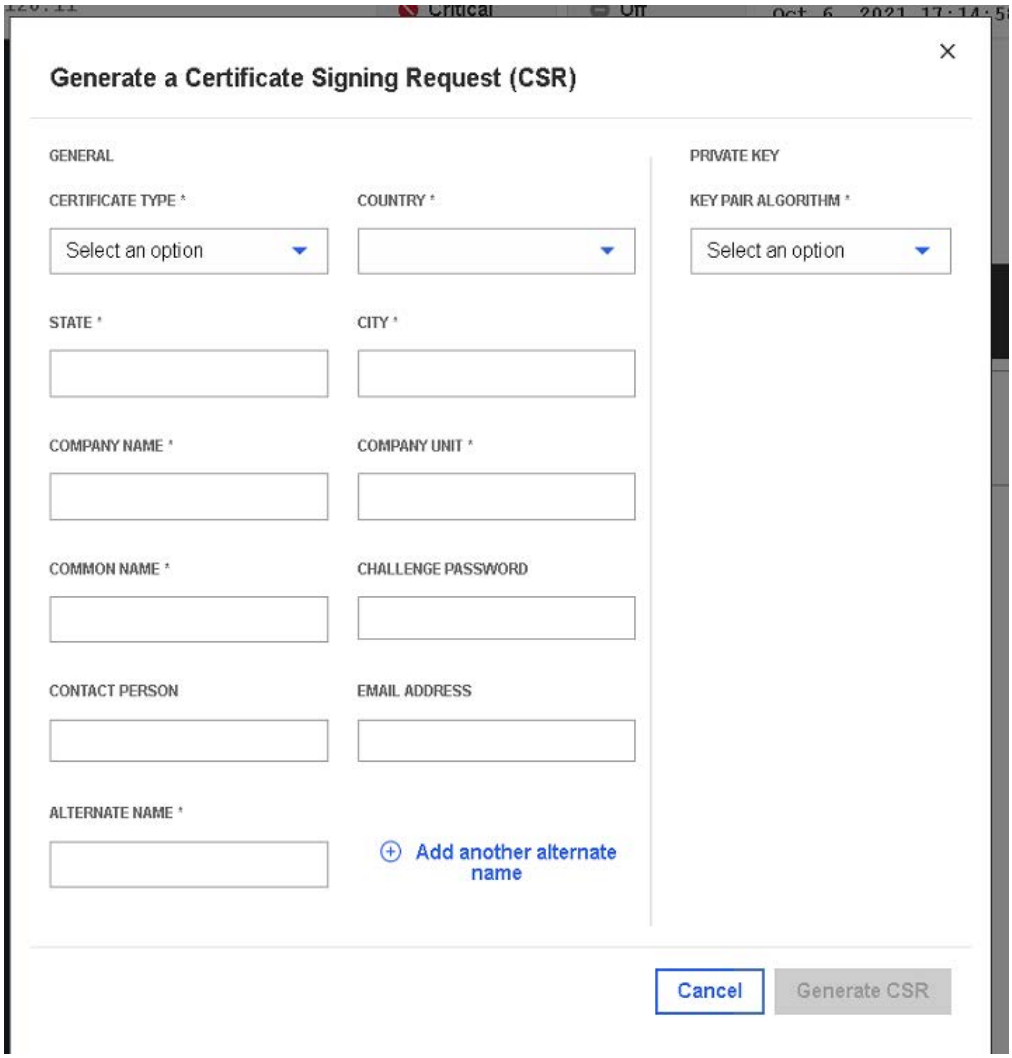
5.4.6. Generating a Certificate Signing Request (CSR)

Procedure

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



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



General	
Certificate type	Use the drop-down list to select the option required: • HTTPS certificate • LDAP certificate
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
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: • EC • RSA
Key curve ID	This field is displayed when the EC option is selected. Use the drop-down list to select the option required: • None • prime256v1 • secp521r1 • secp384r1
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.

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.

Appendix A. Restarting the BMC HTTPS server

5.5. Restarting the BMC HTTPS server

Prerequisites

- The server BMC has an IP address allocated
- A laptop connected to the BullSequana Edge server

Procedure

1. Log in as root through an SSH session on the BMC.
2. Restart the HTTPS server:

```
systemctl restart bmcweb
```

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