Dell EMC PowerSwitch Z9432F-ON BMC User Guide

February 2021

February 2021
Rev. A00

Copyright

Contents

1

About this guide

This guide provides information for using the Dell EMC baseboard management controller (BMC).

CAUTION: To avoid electrostatic discharge (ESD) damage, wear grounding wrist straps when handling this equipment.

NOTE: Only trained and qualified personnel can install this equipment. Read this guide before you install and power on this equipment. This equipment contains two power cables. Disconnect both power cables before servicing.

NOTE: This equipment contains optical transceivers, which comply with the limits of Class 1 laser radiation.

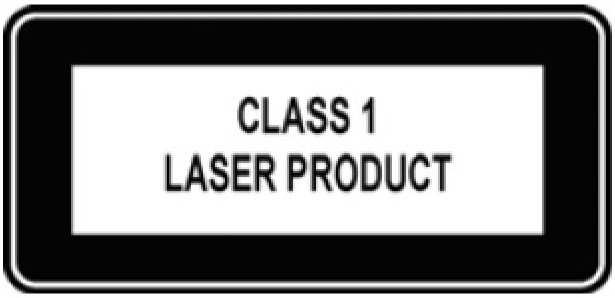


Figure 1. Class 1 laser product tag

NOTE: When no cable is connected, visible and invisible laser radiation may be emitted from the aperture of the optical transceiver ports. Avoid exposure to laser radiation. Do not stare into open apertures.

Language

NOTE: This guide may contain language that is not consistent with the current guidelines. Dell EMC plans to update the guide over subsequent releases to revise the language accordingly.

Topics:

- Information symbols
- Document revision history

Information symbols

This book uses the following information symbols:

NOTE: The **Note** icon signals important operational information.

CAUTION: The Caution icon signals information about situations that could result in equipment damage or loss of data.

WARNING: The Warning icon signals information about hardware handling that could result in injury.

WARNING: The ESD Warning icon requires that you take electrostatic precautions when handling the device.

Document revision history

Table 1. Revision history

Revision	Date	Description
A00	2021-02	Initial release

2

Hardware and software support

For the most current BMC update information, see the *Dell EMC PowerSwitch Z9432F-ON Release Notes*.

For more information about the intelligent platform management interface (IPMI), see the IPMI resources that are hosted by Intel at https://www.intel.com/content/www/us/en/servers/ipmi/ipmi-technical-resources.html.

ⓘ **NOTE:** The BMC out-of-band (OOB) network or LAN is not enabled for Trade Agreement Act-qualified (TAA) switches. The BMC OOB is enabled for non-TAA-qualified switches.

Required drivers

In Linux, the baseboard management controller (BMC) uses the `ipmitool` open-source tool during testing. To configure or get data from the BMC, `ipmitool` sends `ipmi` commands to the BMC. You must have the IPMI driver that is installed to use `ipmitool`.

To access `ipmitools`, go to https://sourceforge.net, search for `ipmitools`, and then select the **See Project** button.

ⓘ **NOTE:** Although there are newer versions available, the `ipmitool` and driver versions that are used during testing the BMC are:

- Linux version: 4.9.30
- `ipmitool` version: 1.8.18
- `ipmi` driver that the `ipmitool` uses is built with kernel 4.9.30.

BMC access

Access BMC through the network interface from a remote machine. Use `ipmitool` for host and remote access.

- LAN interface—`ipmitool` is the standard tool to access BMC over the network. A dummy static IP address is preprogrammed in the BMC. You can change this dummy static IP address of the network interface using `ipmitool` from the microprocessor console:
    - `# ipmitool lan set 1 ipaddr <x.x.x.x>`

3

BMC web user interface

You can access BMC functionality using the pages that are described here.

- TAA-qualified switches do not have the BMC web user interface available.
- Non-TAA-qualified switches do have the BMC web user interface available.

Topics:

Login

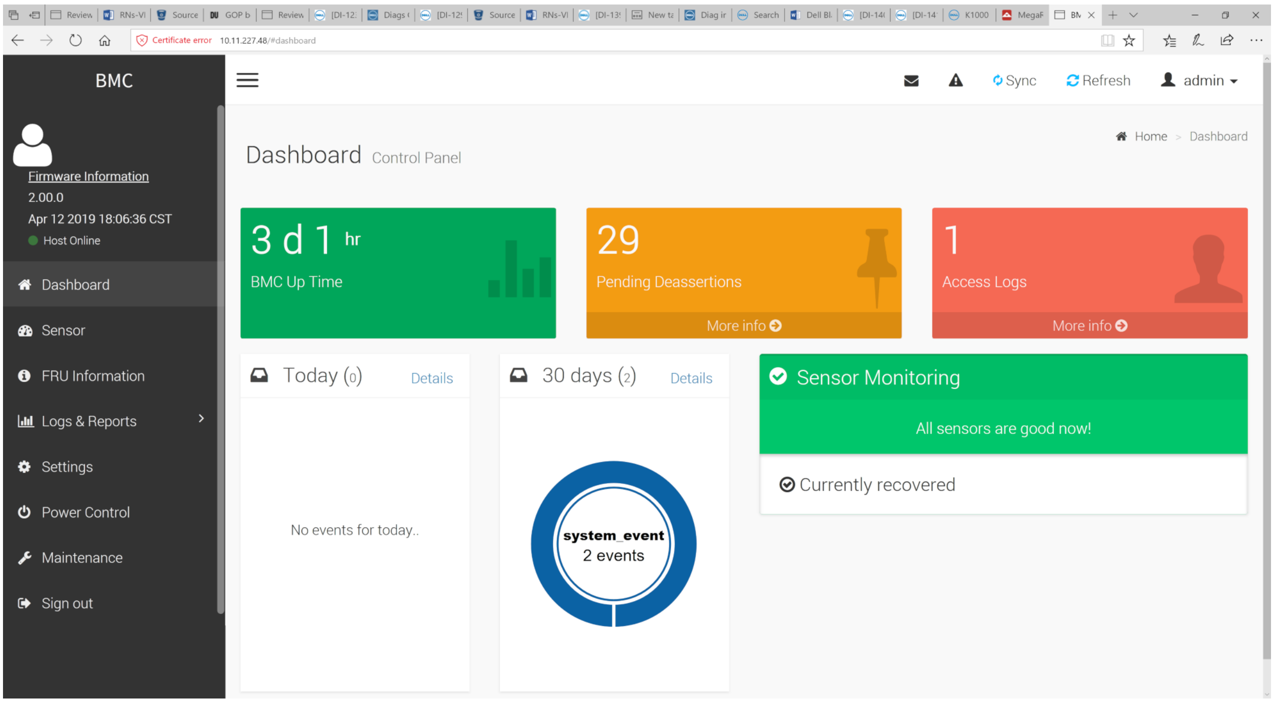
To log in to the BMC user interface, enter the user Username and Password.

- Username: `admin`
- Password (upper case): `<`*`SERVICE TAG`*`>!`

Dashboard

BMC dashboard control panel

The BMC dashboard displays current and historic BMC information. The left panel of the BMC dashboard allows you to go to each user interface section.



Firmware Information
2.00.0
Apr 12 2019 18:06:36 CST
Host Online

Dashboard Control Panel

3 d 1 hr
BMC Up Time

29
Pending Deassertions

1
Access Logs

Today (0)

No events for today..

30 days (2)

system_event
2 events

Sensor Monitoring

All sensors are good now!

Currently recovered

FRU information

Field replacement units (FRU) page

The FRU panel contains the following sections:

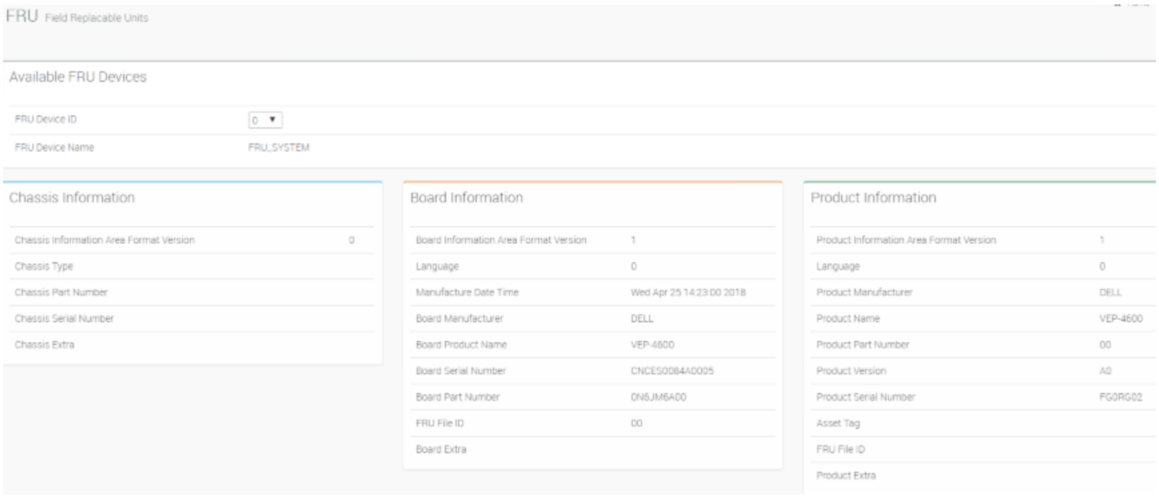
- Available FRU devices
- Chassis information
- Board information
- Product information

FRU Device ID

Select a FRU Device ID from the drop-down lists to view the details of the selected device.

FRU Device Name

The device name of the selected FRU device displays.



FRU Field Replacable Units

Available FRU Devices

FRU Device ID	0 ▼
FRU Device Name	FRU_SYSTEM

Chassis Information

Chassis Information Area Format Version	0
Chassis Type	
Chassis Part Number	
Chassis Serial Number	
Chassis Extra	

Board Information

Board Information Area Format Version	1
Language	0
Manufacture Date Time	Wed Apr 25 14:23:00 2018
Board Manufacturer	DELL
Board Product Name	VEP-4600
Board Serial Number	CNCES0084A0005
Board Part Number	0N6JM6A00
FRU File ID	00
Board Extra	

Product Information

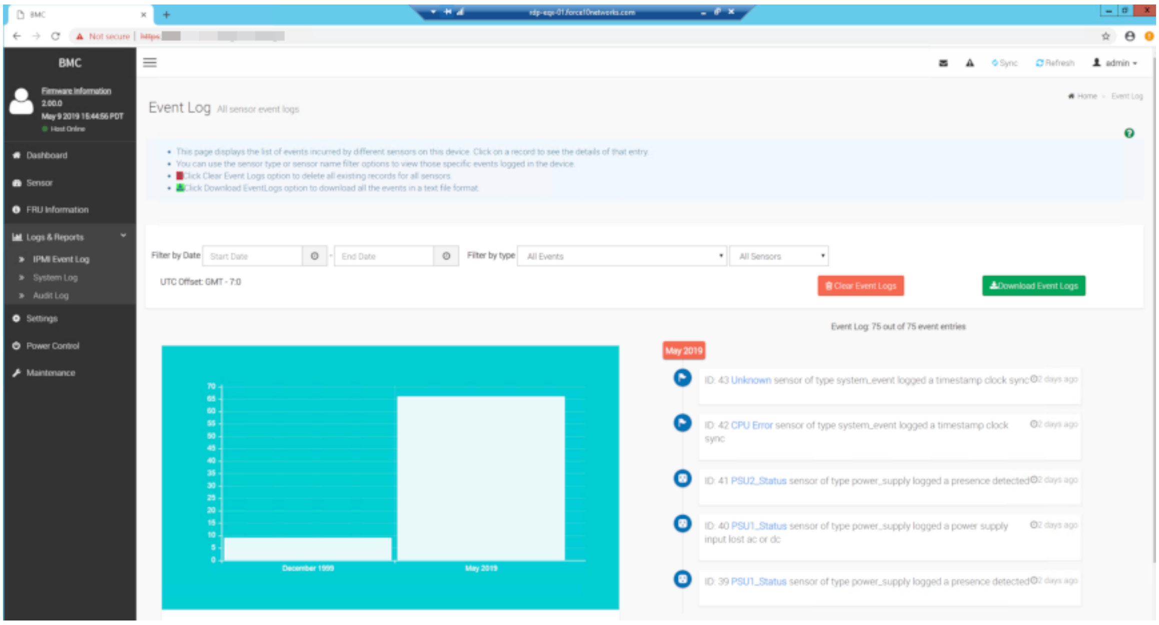
Product Information Area Format Version	1
Language	0
Product Manufacturer	DELL
Product Name	VEP-4600
Product Part Number	00
Product Version	A0
Product Serial Number	FG0RG02
Asset Tag	
FRU File ID	
Product Extra	

Logs and Reports

The Logs and Reports page contains IPMI event log, System log, and Audit log sections.

IPMI event log

- This page displays the list of events the different sensors incur on this device. Click a record to view the details of that entry.
- Use the `sensor type` or `sensor name` filter options to view specific events logged in the device.
- Click the `Clear Event Logs` option to delete all existing records for all sensors.
- Click the `Download EventLogs` option to download all the events in a text file format.



Event Log All sensor event logs

- This page displays the list of events incurred by different sensors on this device. Click on a record to see the details of that entry.
- You can use the sensor type or sensor name filter options to view those specific events logged in the device.
- Click Clear Event Logs option to delete all existing records for all sensors.
- Click Download EventLogs option to download all the events in a text file format.

UTC Offset: GMT - 7:0

Event Log: 75 out of 75 event entries

ID: 43 Unknown sensor of type system_event logged a timestamp clock sync 2 days ago

ID: 42 CPU Error sensor of type system_event logged a timestamp clock sync 2 days ago

ID: 41 PSU2_Status sensor of type power_supply logged a presence detected 2 days ago

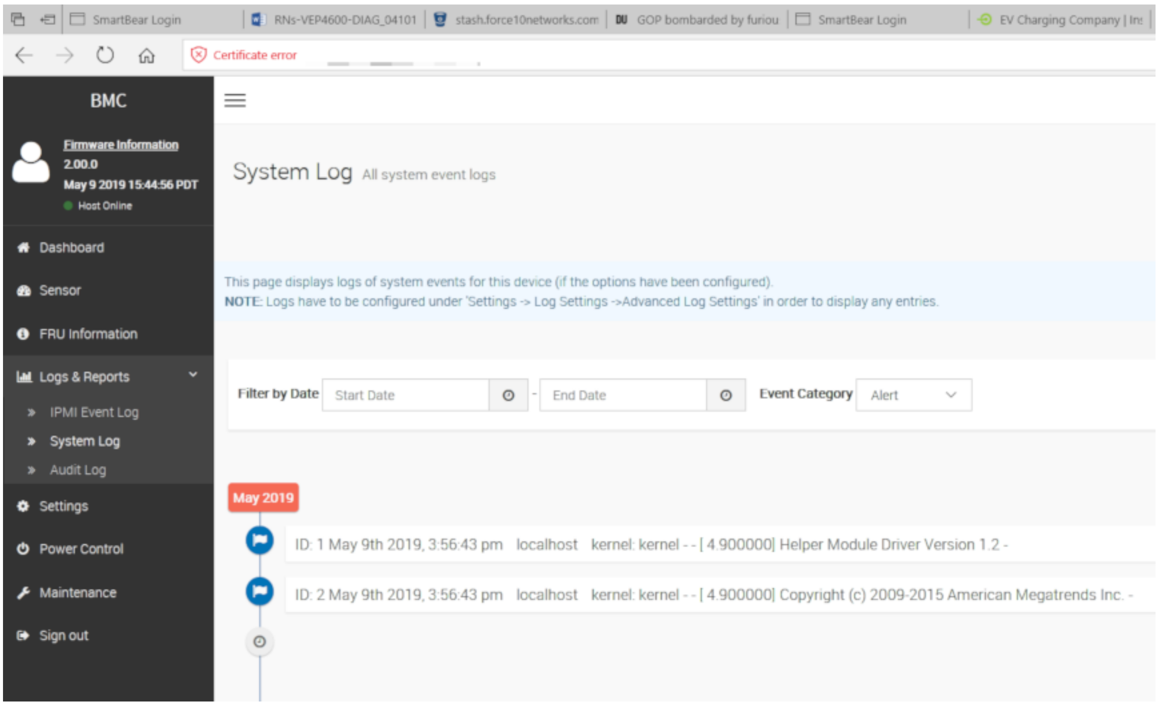
ID: 40 PSU1_Status sensor of type power_supply logged a power supply input lost ac or dc 2 days ago

ID: 39 PSU1_Status sensor of type power_supply logged a presence detected 2 days ago

System log

If you configure the options, this page displays logs of system events for this device.

NOTE: To display system events, configured the options under `Settings > Log Settings > Advanced Log Settings`.



System Log All system event logs

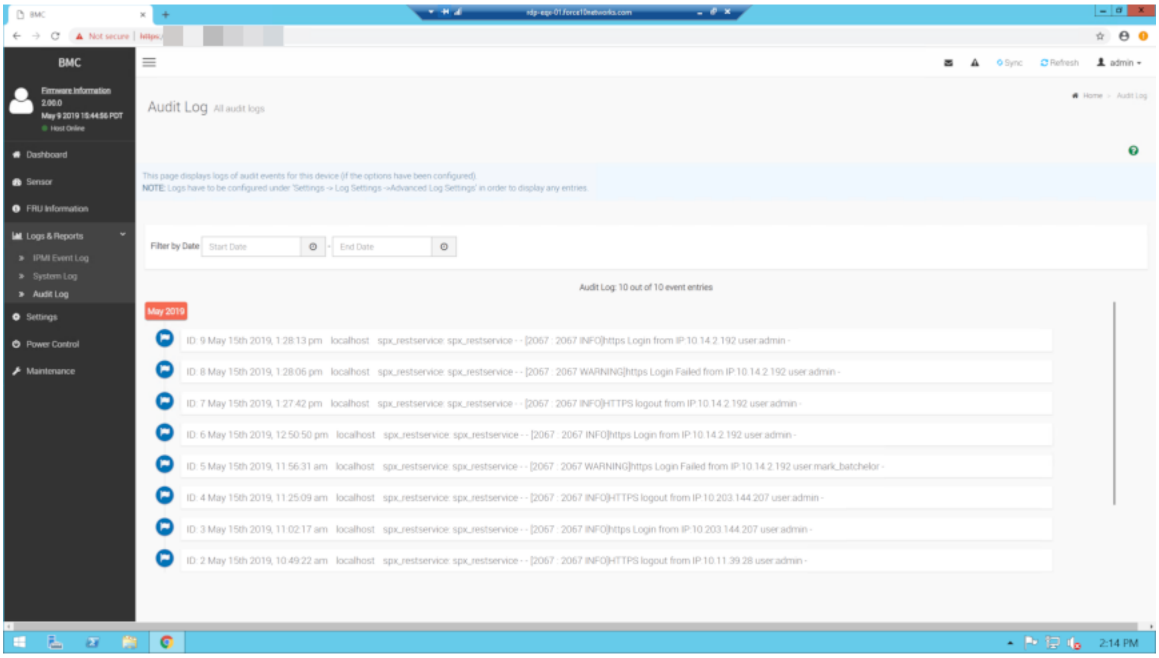
This page displays logs of system events for this device (if the options have been configured).
NOTE: Logs have to be configured under 'Settings -> Log Settings ->Advanced Log Settings' in order to display any entries.

```
ID: 1 May 9th 2019, 3:56:43 pm   localhost   kernel: kernel - - [ 4.900000] Helper Module Driver Version 1.2 -
ID: 2 May 9th 2019, 3:56:43 pm   localhost   kernel: kernel - - [ 4.900000] Copyright (c) 2009-2015 American Megatrends Inc. -
```

Audit log

If you configure the options, this page displays logs of system events for this device.

NOTE: To display the audit logs, configure the logs under `Settings > Log Settings > Advanced Log Settings`.



Audit Log All audit logs

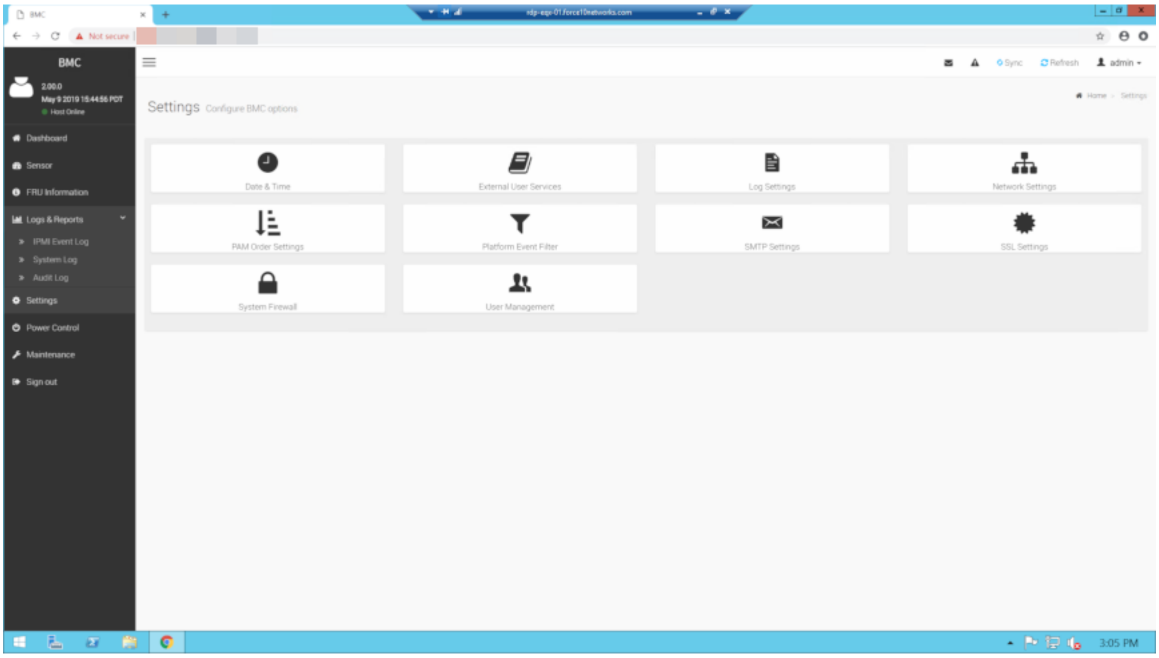
This page displays logs of audit events for this device (if the options have been configured).
NOTE: Logs have to be configured under 'Settings -> Log Settings ->Advanced Log Settings' in order to display any entries.

Audit Log: 10 out of 10 event entries

```
ID: 9 May 15th 2019, 1:28:13 pm   localhost   spx_restservice: spx_restservice - - [2067 : 2067 INFO]https Login from IP:10.14.2.192 user:admin -
ID: 8 May 15th 2019, 1:28:06 pm   localhost   spx_restservice: spx_restservice - - [2067 : 2067 WARNING]https Login Failed from IP:10.14.2.192 user:admin -
ID: 7 May 15th 2019, 1:27:42 pm   localhost   spx_restservice: spx_restservice - - [2067 : 2067 INFO]HTTPS logout from IP:10.14.2.192 user:admin -
ID: 6 May 15th 2019, 12:50:50 pm   localhost   spx_restservice: spx_restservice - - [2067 : 2067 INFO]https Login from IP:10.14.2.192 user:admin -
ID: 5 May 15th 2019, 11:56:31 am   localhost   spx_restservice: spx_restservice - - [2067 : 2067 WARNING]https Login Failed from IP:10.14.2.192 user:mark_batchelor -
ID: 4 May 15th 2019, 11:25:09 am   localhost   spx_restservice: spx_restservice - - [2067 : 2067 INFO]HTTPS logout from IP:10.203.144.207 user:admin -
ID: 3 May 15th 2019, 11:02:17 am   localhost   spx_restservice: spx_restservice - - [2067 : 2067 INFO]https Login from IP:10.203.144.207 user:admin -
ID: 2 May 15th 2019, 10:49:22 am   localhost   spx_restservice: spx_restservice - - [2067 : 2067 INFO]HTTPS logout from IP:10.11.39.28 user:admin -
```

Settings

From the Settings section, you can view, delete, and change your settings.

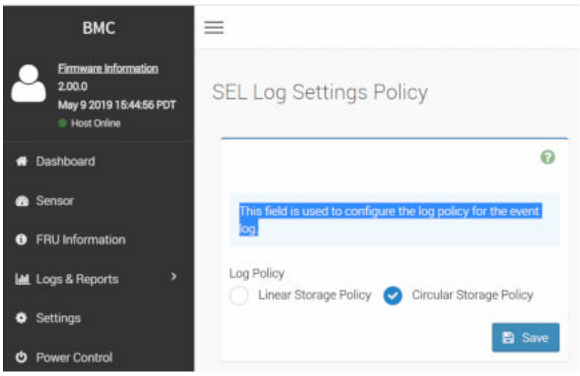


Date and time

If you select the time zone from the group of manual offset—for example, GMT/ETC timezones, the map selection displays. The timezone settings reflect only after you save the settings.

SEL Log settings

Configure the event log policy in the SEL log settings section.

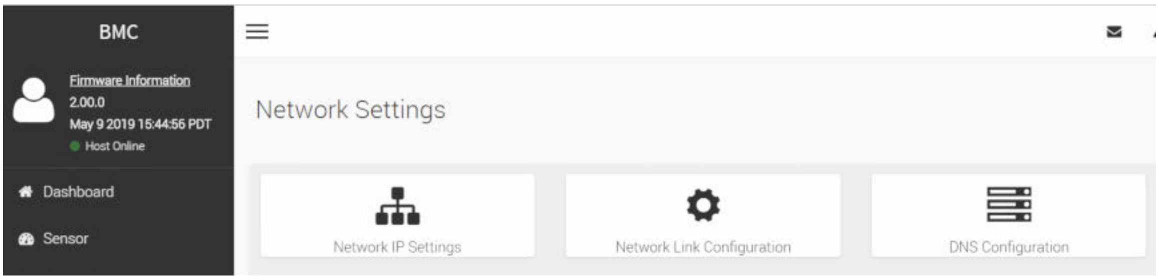


This field is used to configure the log policy for the event log

Log Policy
○ Linear Storage Policy ● Circular Storage Policy

Network settings

Use the Network settings section to configure the network IP address, link configuration, and DNS.



Network IP settings

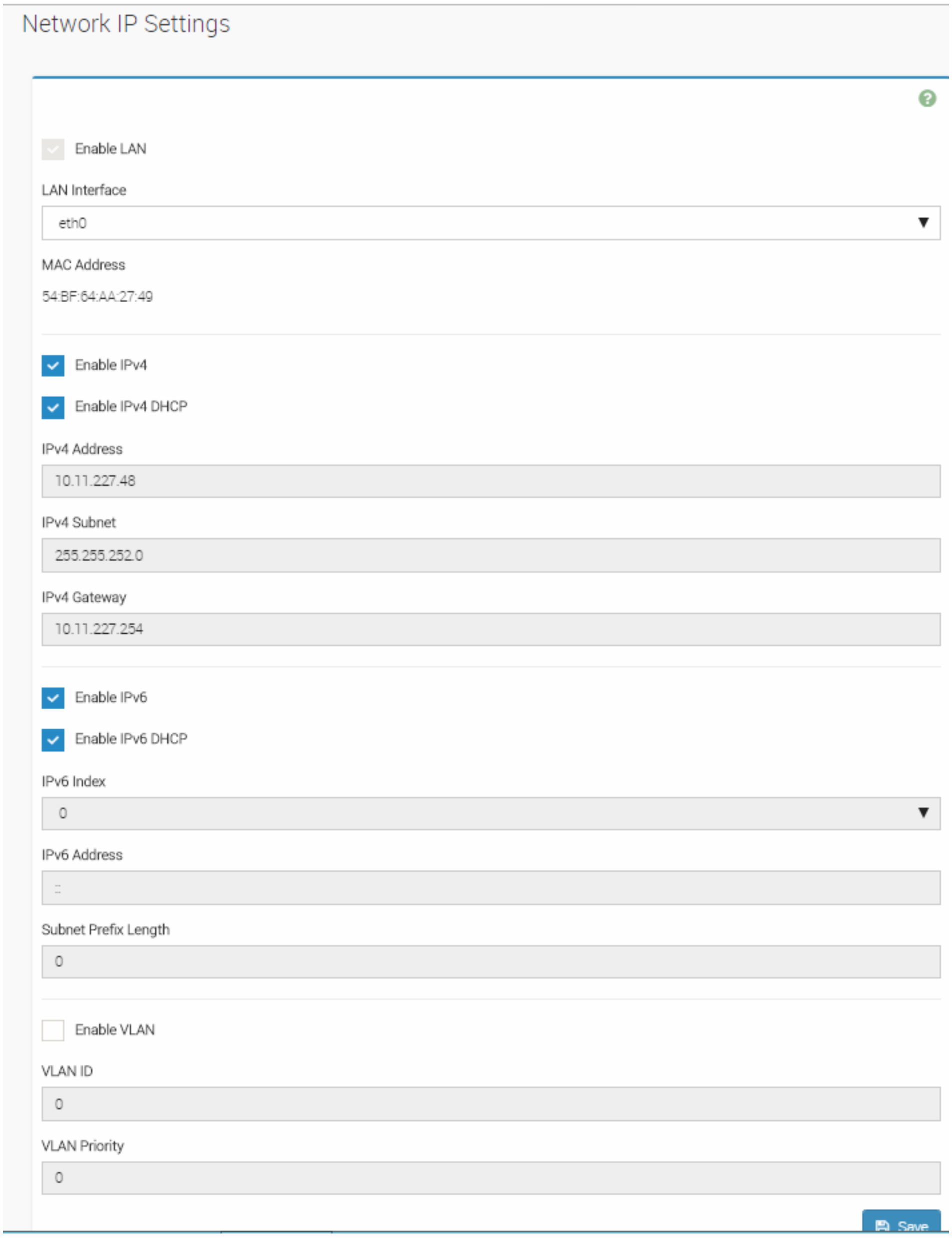
The Network IP settings sections allow you to view and set the following:

Table 2. Network IP settings

Setting	Description
Enable LAN	Check this option to enable LAN support for the selected interface.
LAN interface	Select the LAN interface to configure.
MAC address	This read-only field displays the MAC address of the selected interface.
Enable IPV4	Check this option to enable IPv4 support for the selected interface.
Enable IPv4 DHCP	Check this option to enable IPv4 DHCP support to dynamically configure IPv4 address using DHCP.
Ipv4 Address	If you disable DHCP, specify a static subnet mask to configure for the selected interface. ● IP address—consists of four sets of numbers that are separated by dots, for example, `xxx.xxx.xxx.xxx`. ● Each set range is 0-255. ● First number must not be 0.
IPv4 Subnet	If you disable DHCP, specify a static default gateway to configure for the selected interface. ● IP address—consists of four sets of numbers that are separated by dots, for example, `xxx.xxx.xxx.xxx`. ● Each set range is 0-255. ● First number must not be 0.
Enable IPv6	Check this option to enable IPv6 support for the selected interface.
Enable IPv6 DHCP	Check this option to enable IPv6 DHCP to dynamically configure IPv6 address using DHCPv6.
IPv6 Index	Choose the Ipv6 index.
Ipv6 Address	Specify a static IPv6 address to configure for the selected interface.
Subnet Prefix Length	Specify a static IPv6 address to configure for the selected interface. The range is 0-128.
Enable VLAN	Check this option to enable VLAN support for the selected interface.
VLAN ID	Specify the Identification for VLAN configuration. The range is 1-4094. ⓘ **NOTE:** You cannot change the VLAN ID without resetting the VLAN configuration. VLAN IDs 0 and 4095 are reserved VLAN IDs.
VLAN Priority	Specify the priority for the VLAN configuration. The range is 0-7.

Table 2. Network IP settings (continued)

Setting	Description
	ⓘ **NOTE:** The highest priority for the VLAN is 7.



Network IP Settings

☑ Enable LAN

LAN Interface: eth0

MAC Address: 54:BF:64:AA:27:49

☑ Enable IPv4

☑ Enable IPv4 DHCP

IPv4 Address: 10.11.227.48

IPv4 Subnet: 255.255.252.0

IPv4 Gateway: 10.11.227.254

☑ Enable IPv6

☑ Enable IPv6 DHCP

IPv6 Index: 0

IPv6 Address: ::

Subnet Prefix Length: 0

□ Enable VLAN

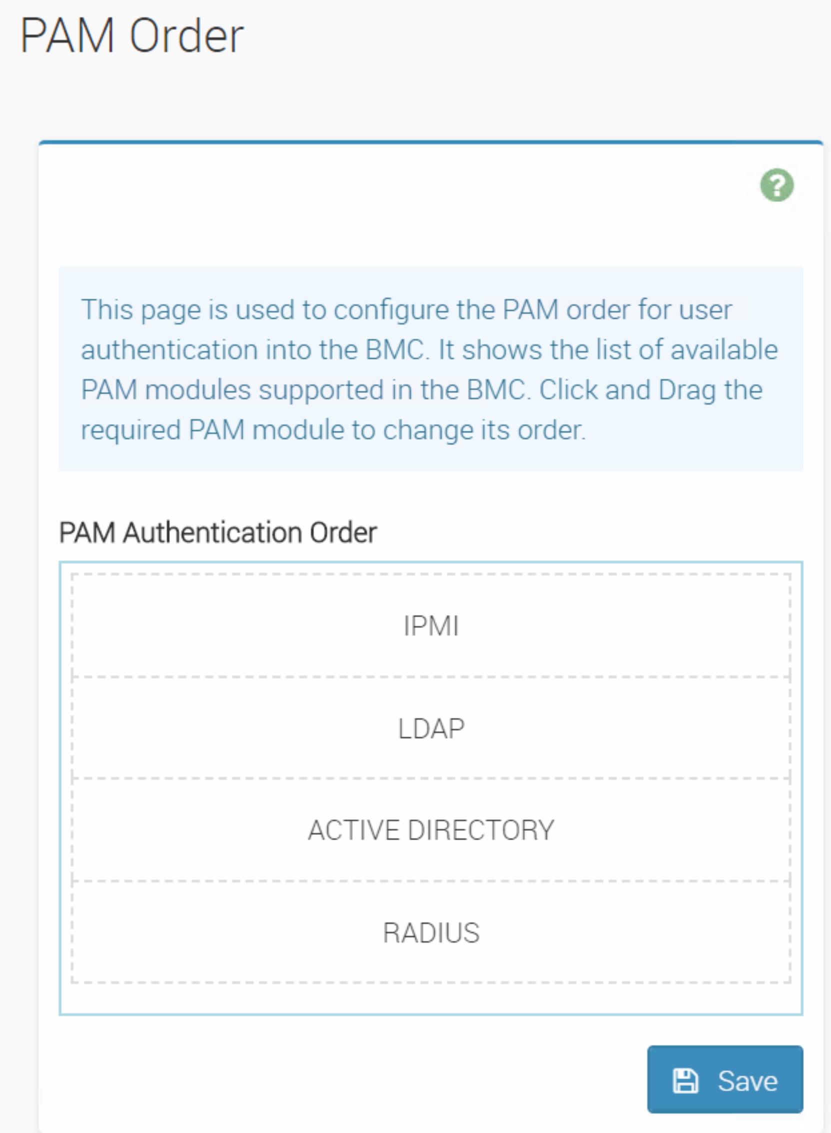
VLAN ID: 0

VLAN Priority: 0

PAM order settings

Configure the PAM order for user authentication in the BMC. PAM order shows the list of available PAM modules that are supported in the BMC.

To change the order, click and drag the PAM module.



PAM Order

This page is used to configure the PAM order for user authentication into the BMC. It shows the list of available PAM modules supported in the BMC. Click and Drag the required PAM module to change its order.

PAM Authentication Order

IPMI

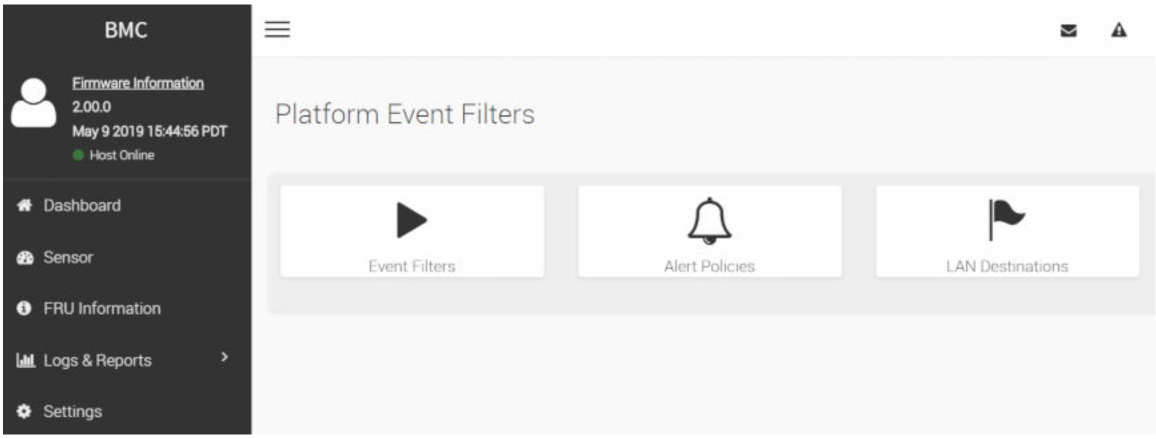
LDAP

ACTIVE DIRECTORY

RADIUS

Platform event filters

Use the platform event filters section to view, configure, or delete event filters.

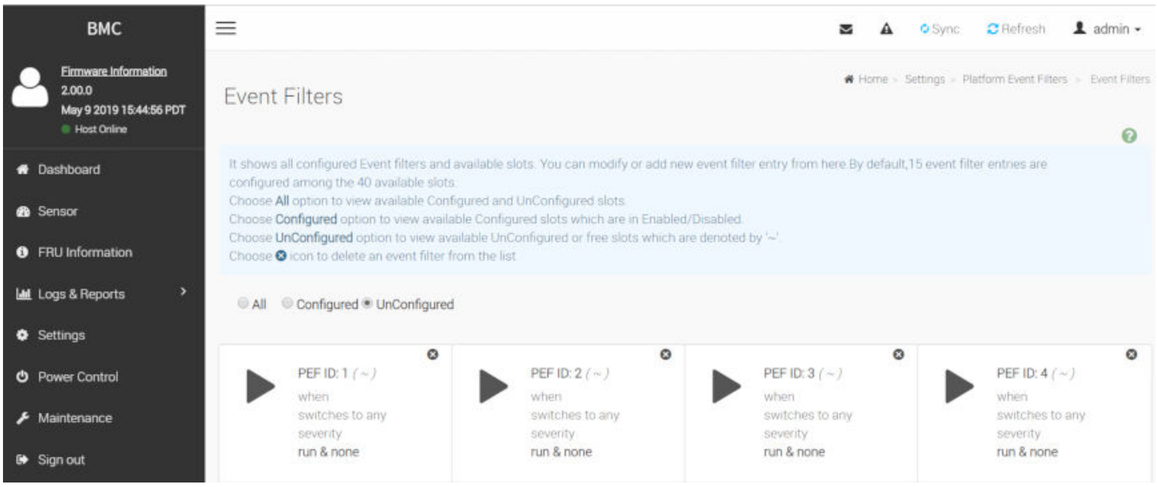


Event filters

This section displays the configured Event filters and available slots. You can modify or add a new event filter entry. By default, 15 event filter entries are configured among the 40 available slots.

Event filter options include `All`, `Configured`, `Unconfigured`, and `X`.

- Choose the `All` option to view the available configured and unconfigured slots.
- Choose the `Configured` option to view the available configured slots that are in an Enabled or Disable state.
- Choose the `Unconfigured` option to view the available unconfigured or free slots. These slots are denoted by the tilde (~) symbol.
- Choose the `X` icon to delete an event filter from the list.



Event Filters

It shows all configured Event filters and available slots. You can modify or add new event filter entry from here By default,15 event filter entries are configured among the 40 available slots.
Choose **All** option to view available Configured and UnConfigured slots.
Choose **Configured** option to view available Configured slots which are in Enabled/Disabled.
Choose **UnConfigured** option to view available UnConfigured or free slots which are denoted by '~'.
Choose icon to delete an event filter from the list

○ All ○ Configured ● UnConfigured

PEF ID: 1 (~)
when
switches to any
severity
run & none

PEF ID: 2 (~)
when
switches to any
severity
run & none

PEF ID: 3 (~)
when
switches to any
severity
run & none

PEF ID: 4 (~)
when
switches to any
severity
run & none

Alert policy settings

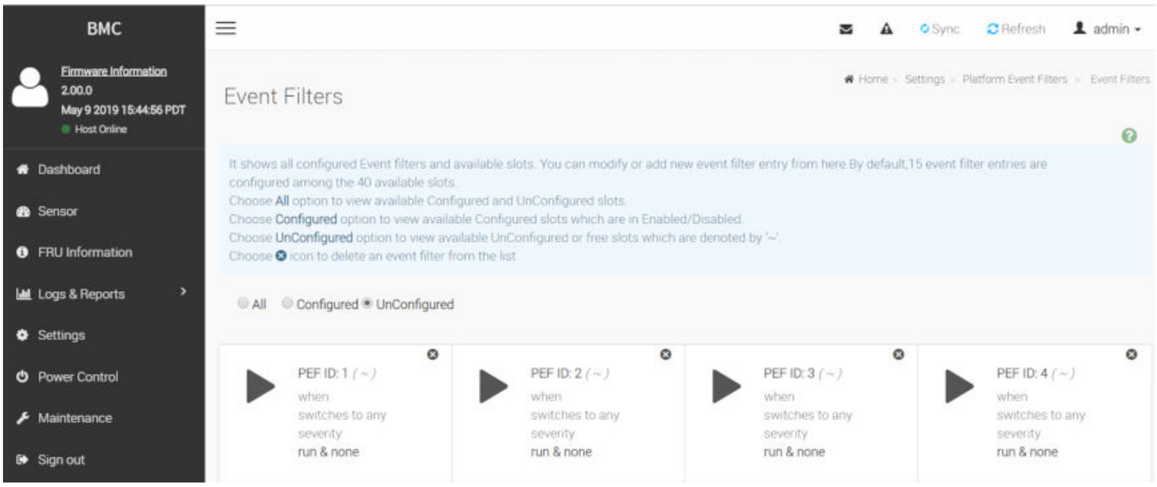
The Alert policy settings section offers the following setting options:

Table 3. Alter policies settings

Setting	Description
Policy Group Number	Select a policy number from the drop-down menu that was configured in the Event filter table.
Enable this alert	Check the `Enable` option to enable the policy settings.
Policy action	Choose from the drop-down menu a Policy set value: ● Always send an alert to this destination. ● If alert to previous destination was successful, do not send alert to this destination. Go to the next entry in this policy set. ● If alert to previous destination was successful, do not send alert to this destination. Do not process any more entries in this policy set. ● If alert to previous destination was successful, do not send alert to this destination. Go to the next entry in this policy set that is to a different channel. ● If alert to previous destination was successful, do not send alert to this destination. Go to the next entry in this policy set that is to a different destination type.
LAN Channel	Choose a particular destination from the configured destination drop-down menu list.
Destination Selector	Select a destination from the drop-down menu. **NOTE:** To configure the LAN destination, go to Configuration > PEF > LAN Destination.
Event Specific Alert String	Check the box to specify an event-specific Alert String.

Table 3. Alter policies settings (continued)

Setting	Description
Alert String Key	Select a set of values from the drop-down menu, all linked to strings kept in the PEF configuration parameters, to specify which string to send for this Alert Policy entry.



Event Filters

It shows all configured Event filters and available slots. You can modify or add new event filter entry from here By default,15 event filter entries are configured among the 40 available slots.
Choose **All** option to view available Configured and UnConfigured slots.
Choose **Configured** option to view available Configured slots which are in Enabled/Disabled.
Choose **UnConfigured** option to view available UnConfigured or free slots which are denoted by '~'.
Choose ⊗ icon to delete an event filter from the list

○ All ○ Configured ● UnConfigured

PEF ID: 1 (~)
when
switches to any
severity
run & none

PEF ID: 2 (~)
when
switches to any
severity
run & none

PEF ID: 3 (~)
when
switches to any
severity
run & none

PEF ID: 4 (~)
when
switches to any
severity
run & none

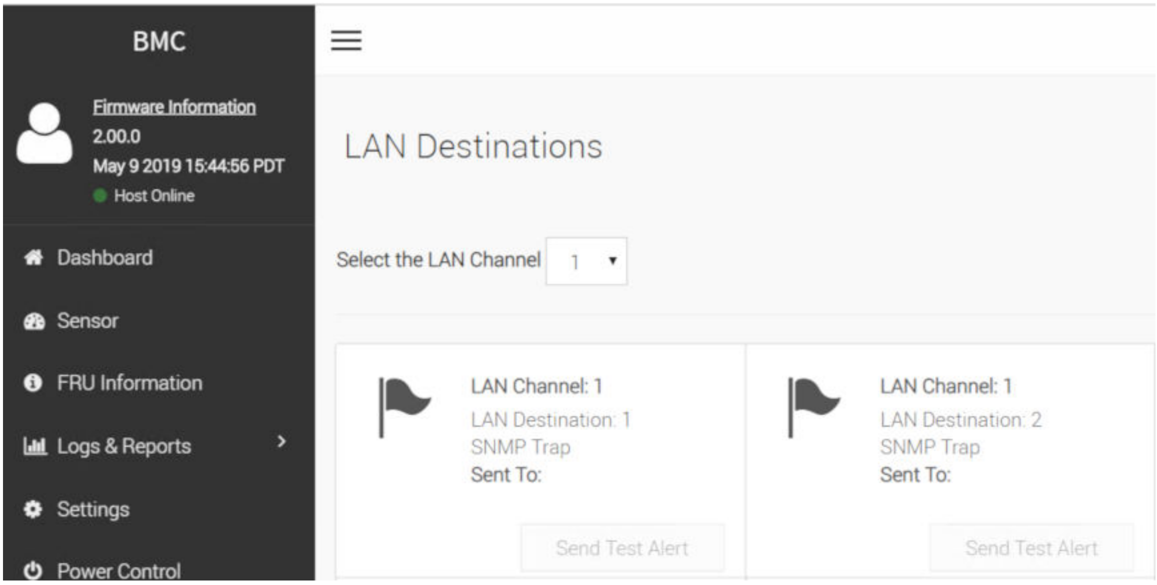
LAN destinations

Displays configured LAN destinations and the available slots. You can modify or add a new LAN destination entry from this page. A maximum of 15 slots are available.

Click the `X` icon to delete the LAN destination entry from the list.

1. Select the LAN Channel. Select the LAN Channel from the list to configure.
2. Send a Test Alert:.Select a configured slot and click **Send Test Alert** to send sample the alert to the configured destination.

    NOTE: You can only send a test alert when you enable the SMTP configuration. Enable SMTP support under `Settings > SMTP`. Ensure that the SMTP server address and port numbers are configured properly.



LAN Destinations

Select the LAN Channel 1

LAN Channel: 1
LAN Destination: 1
SNMP Trap
Sent To:

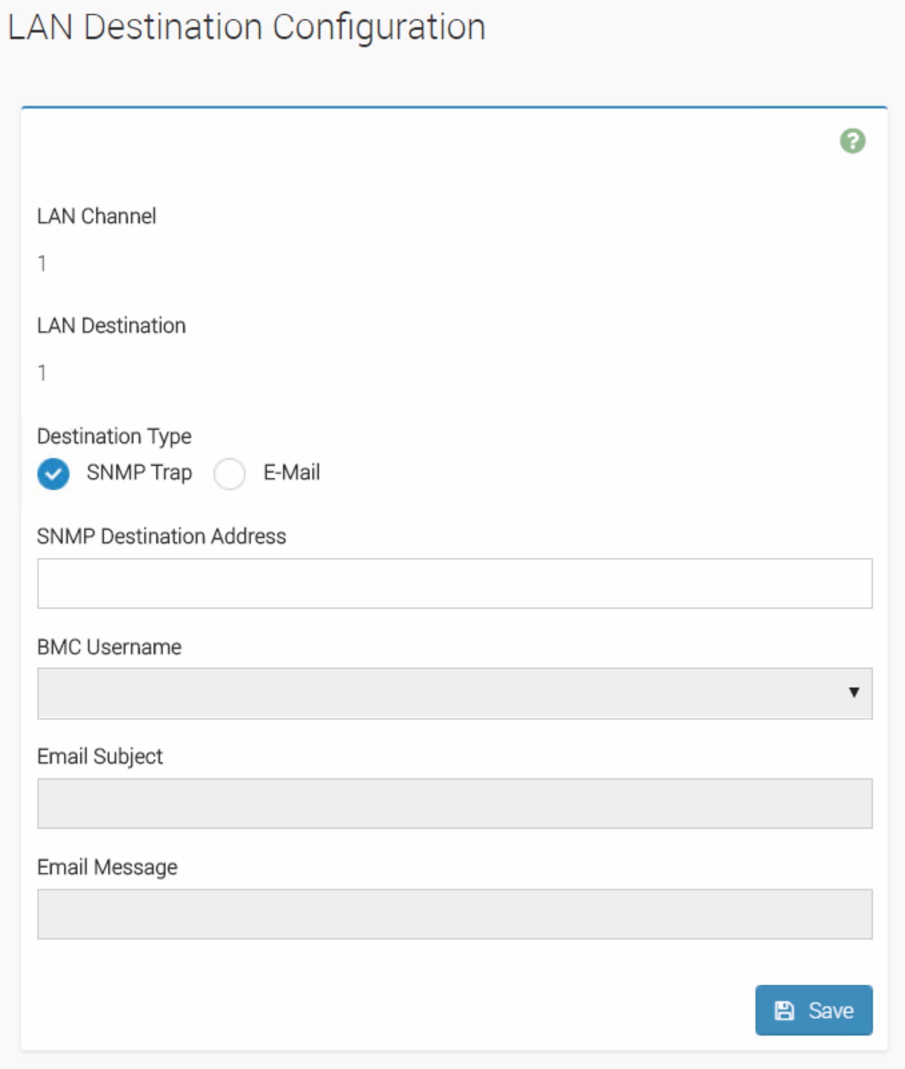
LAN Channel: 1
LAN Destination: 2
SNMP Trap
Sent To:

Table 4. LAN Destination Settings

Settings	Description
LAN Channel	Displays the read-only LAN channel number of the selected slot.

Table 4. LAN Destination Settings (continued)

Settings	Description
Destination Type	The destination types are SNMP Trap and E-Mail.
SNMP Destination Address	If destination type is SNMP Trap. Then give the IP address of the system that receives the alert. Destination address supports the IPv4 and IPv6 address formats.
BMC Username	If the Destination type is `Email Alert`, choose the user to whom the email messages alert is sent. ⓘ **NOTE:** Configure the email address for the user under `Settings > Users Management`.
Email Subject	You must configure these fields if you choose `Email Alert` as the destination type. An email messages messages is sent to the configured email address of the user if there is any severity events with a subject that is specified in subject field and contains the message field content as the email body.
Email Message	You must configure these fields if you choose `Email Alert` as the destination type. An email messages messages is sent to the configured email address of the user if there is any severity events with a subject that is specified in subject field and contains the message field content as the email body. ⓘ **NOTE:** These fields do not apply for `AMI-Format` email messages users.



LAN Destination Configuration

LAN Channel

1

LAN Destination

1

Destination Type

● SNMP Trap ○ E-Mail

SNMP Destination Address

BMC Username

Email Subject

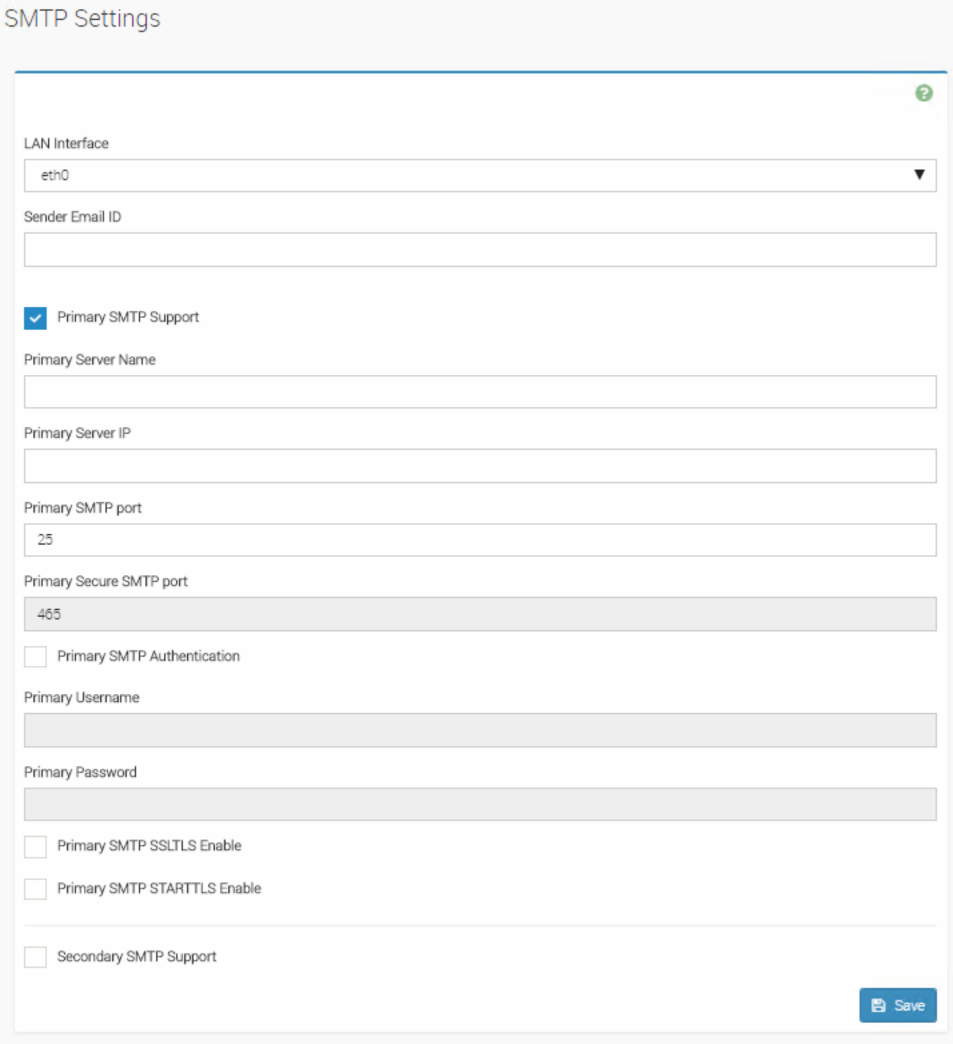
Email Message

SMTP settings

Use the SMTP settings section to configure the SMTP.

Table 5. SMTP settings

Settings	Description
LAN Interface	Select the LAN interface to configure.
Sender Email ID	Enter the Sender Email ID on the SMTP server. The maximum Email ID is 64 bytes, which includes the username and domain name.
Primary SMTP Support	Check this option to enable SMTP support for the BMC.
Primary Server Name	Enter the Machine Name of the SMTP Server. This field is for information purpose only. ● The machine name is a maximum 25 alpha-numeric characters. Space and special characters are not allowed.
Primary Server IP	Enter the Server Address for the SMTP Server. This field is mandatory. ● The IP Address is four numbers that are separated by dots, for example `xxx.xxx. xxx.xxx`. ● Each Number range is from 0-255. First Number must not be 0. Server address supports IPv4 and IPV6 address format and hostname format.
Primary SMTP port	Specify the SMTP port, from 1-65535. This field is mandatory. ● The default port is 25.
Primary Secure SMTP port	Specify the SMTP Secure port, from 1-65535. ● The default port is 465.
Primary SMTP Authentication	Check `Enable` to enable SMTP Authentication. SMTP Server Authentication supported types are: ● CRAM-MD5 ● LOGIN ● PLAIN
Primary Username	Enter the username to access SMTP Accounts. ● The User Name is 4-64 alpha-numeric characters, dot(.), hyphen(-), and underscore(_). Other special characters are not allowed. ● The User Name must start with an alphabet.
Primary password	Enter the password for the SMTP User Account. ● Password must have a minimum of four characters. ● The password maximum is 64 characters. ● White space is not allowed.
Primary SMTP SSLTLS Enable	Check `Enable` to enable the SMTP SSLTLS protocol.
Primary SMTP STARTTLS Enable	Check `Enable` to enable the SMTP STARTTLS protocol.
Secondary SMTP Support	Check this option to enable Secondary SMTP support for the BMC.



SMTP Settings

LAN Interface: eth0

Sender Email ID

☑ Primary SMTP Support

Primary Server Name

Primary Server IP

Primary SMTP port: 25

Primary Secure SMTP port: 465

□ Primary SMTP Authentication

Primary Username

Primary Password

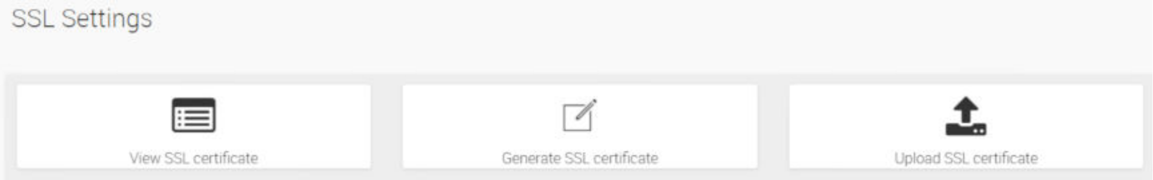
□ Primary SMTP SSLTLS Enable

□ Primary SMTP STARTTLS Enable

□ Secondary SMTP Support

SSL settings

The SSL settings page allows you to view, generate, or upload SSL Certificates.



SSL Settings

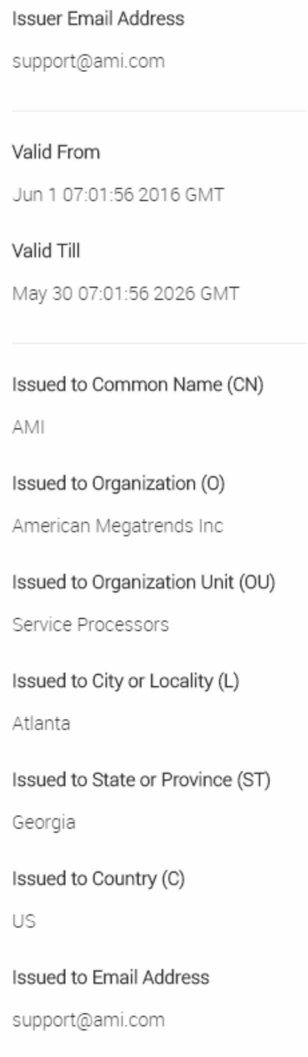
View SSL Certificate

Table 6. View SSL Certificate settings

Settings	Descriptions
Current Certificate Information	Displays basic information about the uploaded SSL Certificate with the following fields: ● Version-Serial number ● Signature Algorithm ● Public Key
Issued from	Contains the following information about the Certificate Issuer:

Table 6. View SSL Certificate settings (continued)

Settings	Descriptions
	● Common Name (CN) ● Organization (O) ● Organization Unit (OU) ● City or Locality (L) ● State or Province (ST) ● Country (C) ● Email Address
Validity Information	Displays the validity period of the uploaded Certificate. ● Valid From ● Valid To
Issued to	Displays the information to whom the Certificate is issued: ● Common Name (CN) ● Organization (O) ● Organization Unit (OU) ● City or Locality (L) ● State or Province (ST) ● Country (C) ● Email Address



Issuer Email Address

support@ami.com

Valid From

Jun 1 07:01:56 2016 GMT

Valid Till

May 30 07:01:56 2026 GMT

Issued to Common Name (CN)

AMI

Issued to Organization (O)

American Megatrends Inc

Issued to Organization Unit (OU)

Service Processors

Issued to City or Locality (L)

Atlanta

Issued to State or Province (ST)

Georgia

Issued to Country (C)

US

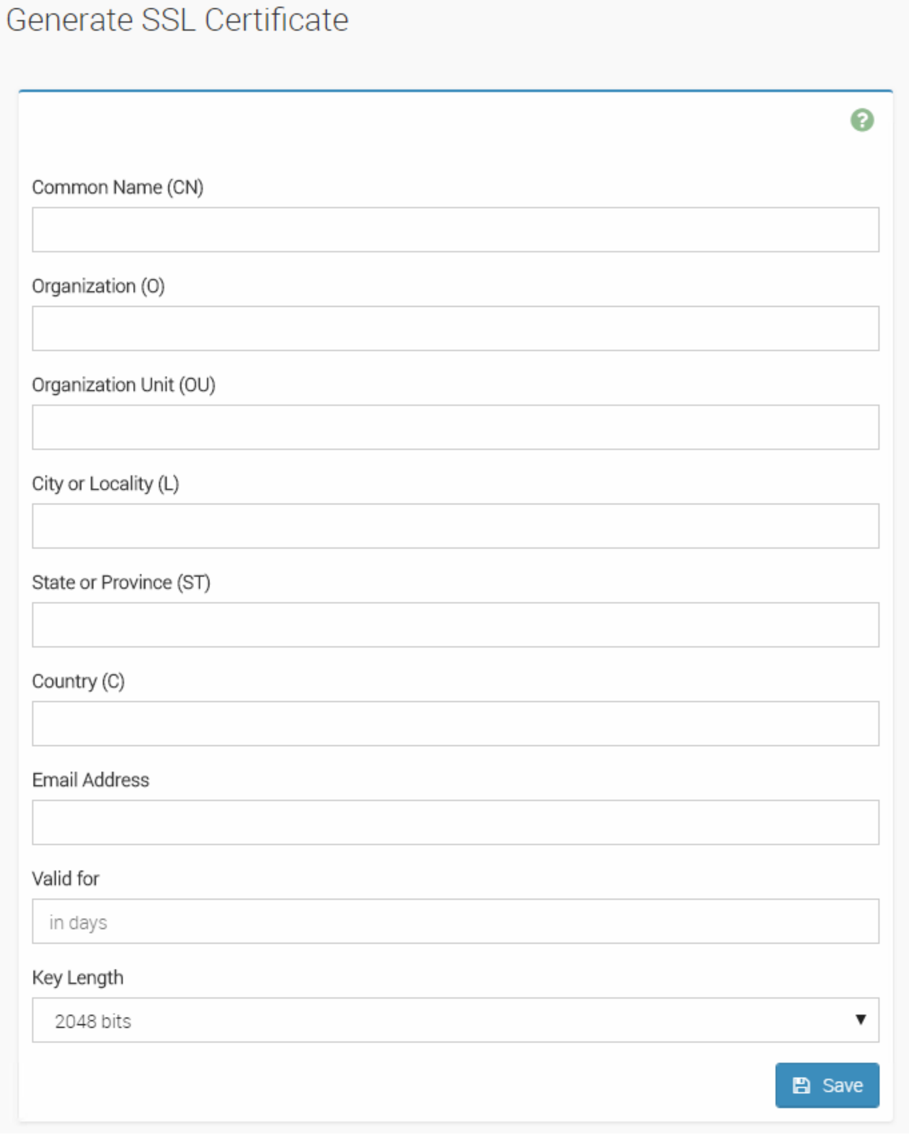
Issued to Email Address

support@ami.com

Generate SSL certificate

Table 7. Generate SSL Certificate settings

Settings	Descriptions
Common Name (CN)	Common name for the generated Certificate: ● The maximum length is 64 alpha-numeric characters. ● Special characters # and $ are not allowed.
Organization (O)	Organization name for the Certificate: ● The maximum length is 64 alpha-numeric characters. ● Special characters # and $ are not allowed.
Organization Unit (OU)	Over all organization section unit name for the Certificate: ● The maximum length is 64 alpha-numeric characters. ● Special characters # and $ are not allowed.
City or Locality (L)	City or locality for the Certificate: ● The maximum length is128 alpha-numeric characters. ● Special characters # and $ are not allowed.
State or Province (ST)	State or province for the Certificate: ● The maximum length is128 alpha-numeric characters. ● Special characters # and $ are not allowed.
Country (C)	Country code for the Certificate. This field is mandatory. ● Only two characters are allowed. ● Special characters are not allowed.
Email Address	Email address of the organization. This field is mandatory.
Valid for	Number of days the certificate is valid, from 1-3650 days.
Key Length	Choose the key length bit value of the Certificate.



Generate SSL Certificate

Common Name (CN)

Organization (O)

Organization Unit (OU)

City or Locality (L)

State or Province (ST)

Country (C)

Email Address

Valid for

in days

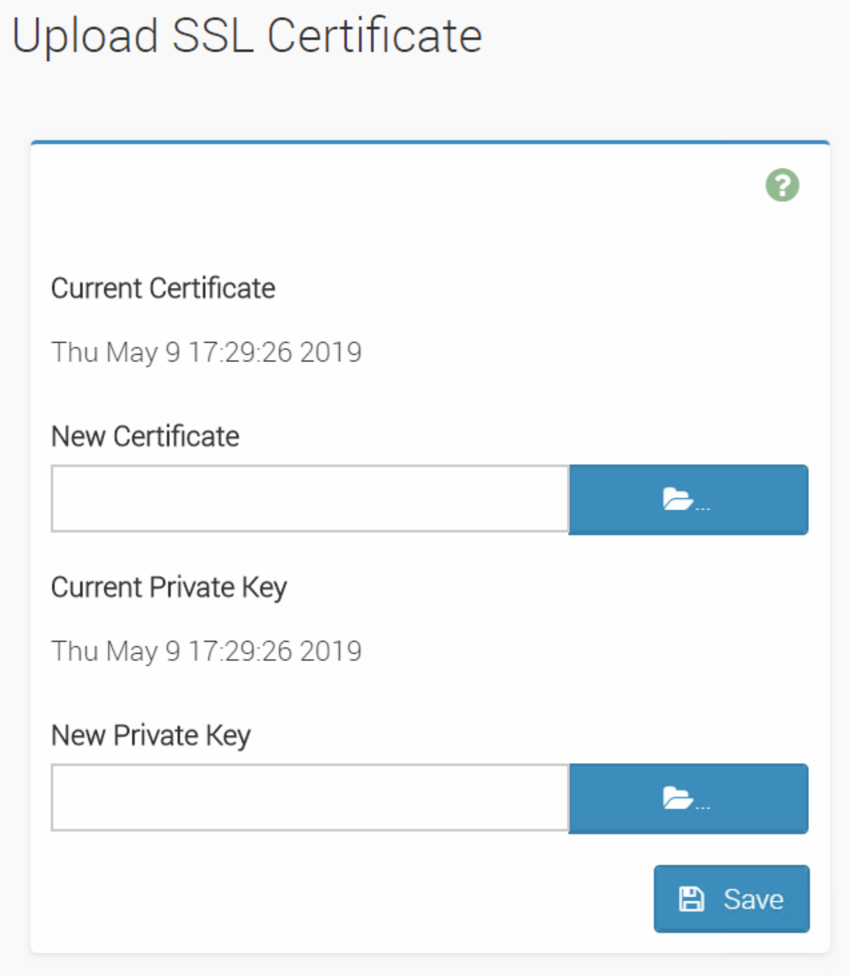
Key Length

2048 bits

Upload SSL Certificate

Table 8. Upload SSL Certificate settings

Settings	Descriptions
Current certificate	The read-only information of the current Certificate and uploaded date and time displays.
New certificate	Go to the Certificate file. The Certificate file is a pem type.
Current private key	The read-only information of the current private key and uploaded date and time displays.
New private key	Go to the private key file.


Upload SSL Certificate

Current Certificate

Thu May 9 17:29:26 2019

New Certificate

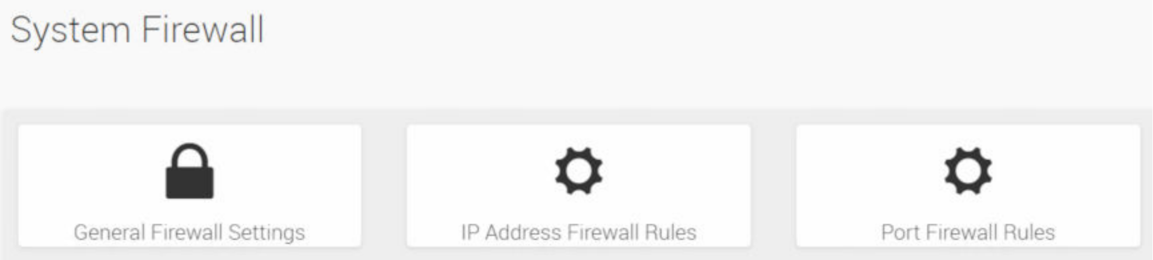
Current Private Key

Thu May 9 17:29:26 2019

New Private Key

System firewall

This page allows you to configure the system firewall order for user authentication into the BMC. The page lists the available system firewall modules that are supported in the BMC.



General firewall settings

The general firewall settings include the existing firewall settings and an option to add firewall settings.

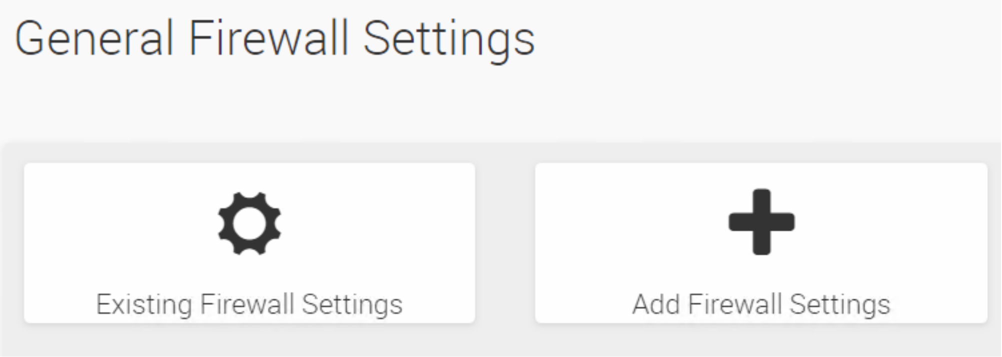
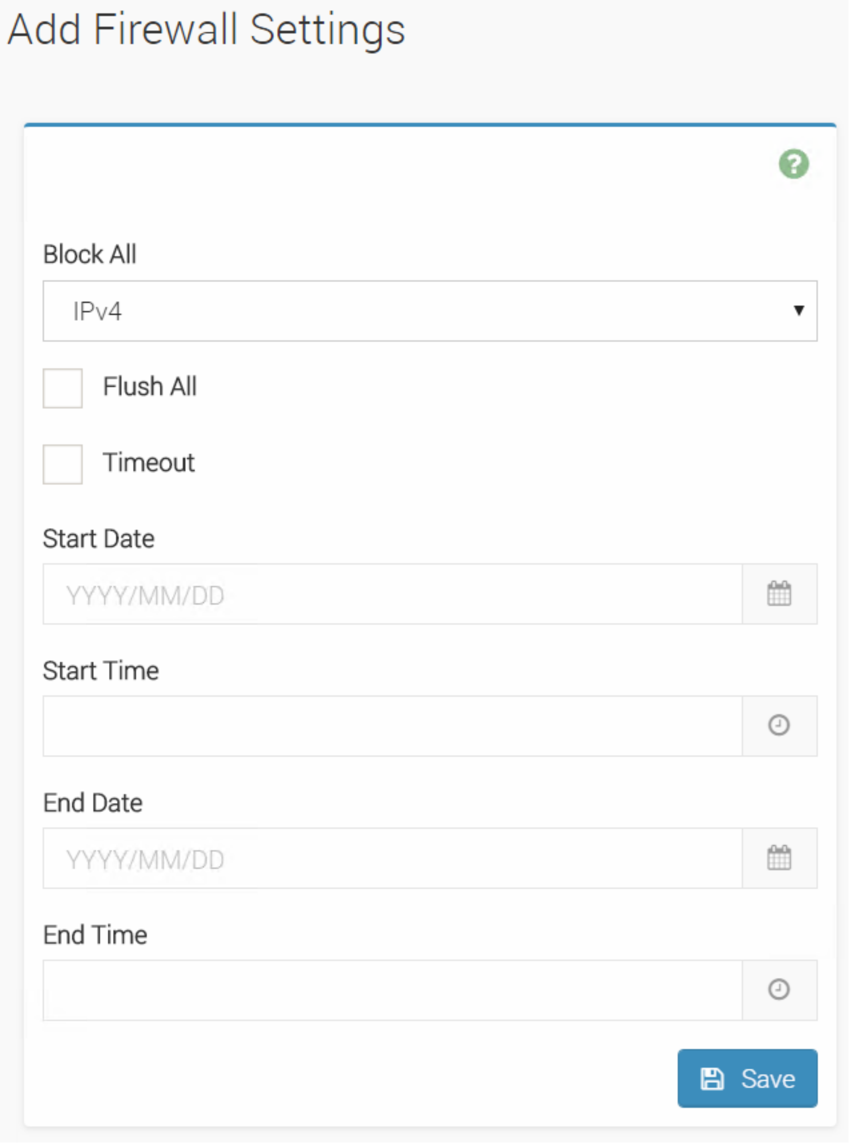


Table 9. General firewall settings

Setting	Description
Existing firewall settings	Displays a list of the general firewall configurations. ● Click X to delete an item from the list. ● You must be at least an Operator to view the page. To add or delete a firewall, user must be an Administrator.
Add firewall settings	● Block all—This option blocks all incoming IPs and ports. ● Flush all—This option flushes all system firewall rules. ● Timeout—This option enables or disables firewall rules with timeout. ● Start Date—The respective firewall rule effect start from this date. ● Start Time—The respective firewall rule effect start from this time. ● End Date—The respective firewall rule effect ends at this date. ● End Time—The respective firewall rule effect ends at this time.



Add Firewall Settings

Block All

IPv4 ▾

□ Flush All

□ Timeout

Start Date

YYYY/MM/DD

Start Time

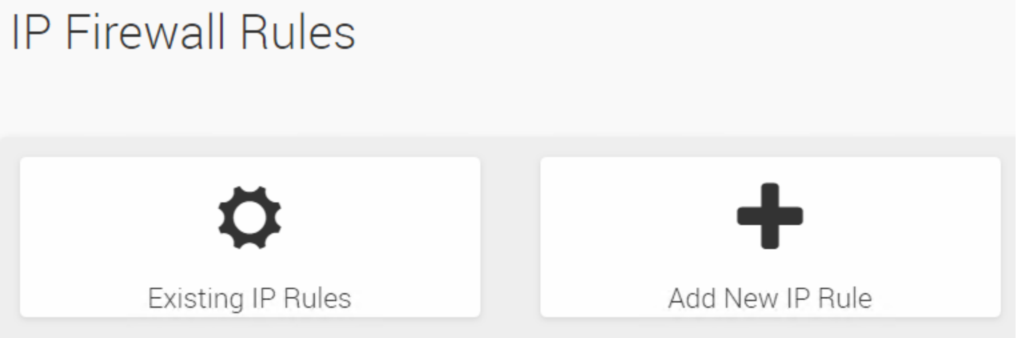
End Date

YYYY/MM/DD

End Time

IP address firewall rules

The IP address firewall rules settings include the existing IP rules settings and an option to add new IP rule settings.



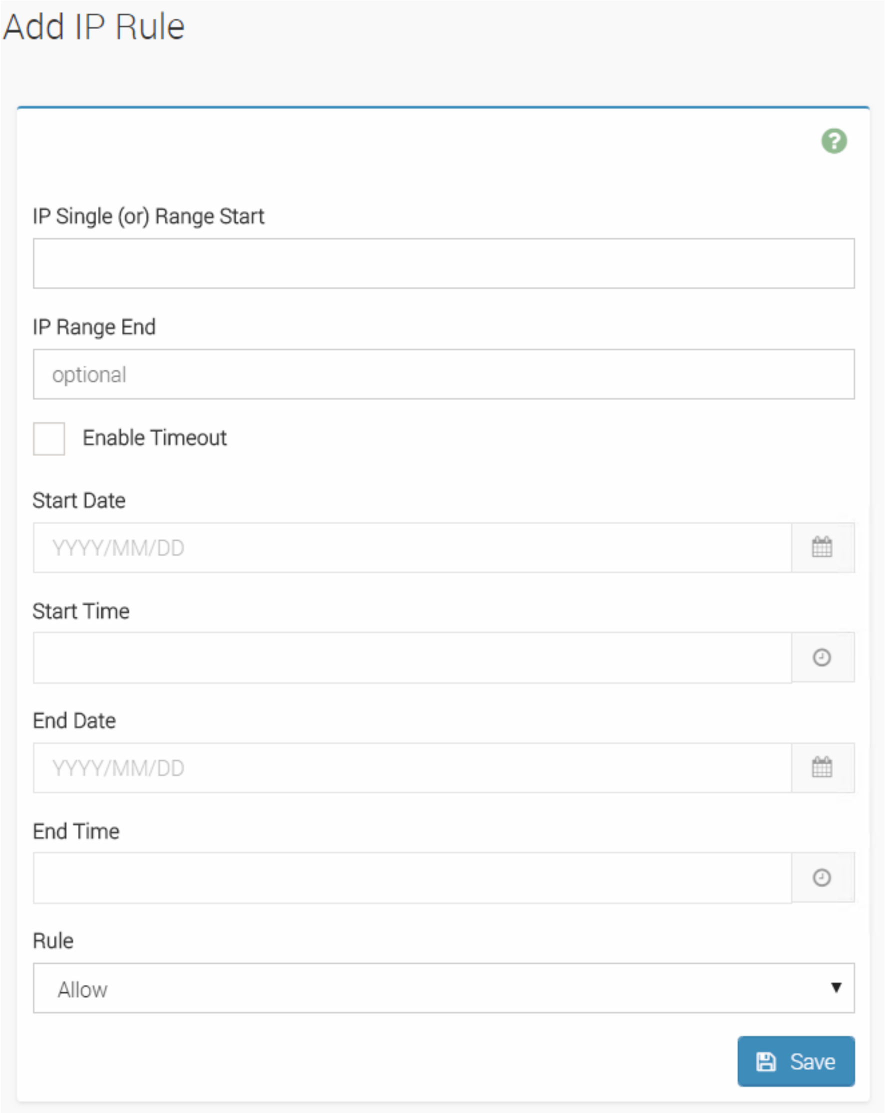
IP Firewall Rules

Table 10. IP address firewall rule settings

Setting	Description
Existing IP address rule settings	Displays a list of the existing IP firewall rules. ● Click `X` to delete an item from the list.

Table 10. IP address firewall rule settings (continued)

Setting	Description
	- You must be at least an Operator to view the page. To add or delete a firewall, user must be an Administrator.
Add IP address rule settings	- IP Single (or) Range Start—Configure the IP address or range of IP addresses. An IP address supports IPv4 address format only: ○ IPv4 address is four numbers that are separated by dots, for example, `xxx.xxx.xxx.xxx`. ○ The range is from 0-255. ○ The first number must not be 0. - IP Range End—Configured the IP address or range of IP addresses. An IP address supports IPv4 address format only: ○ IPv4 address is four numbers that are separated by dots, for example, `xxx.xxx.xxx.xxx`. ○ The range is from 0-255. ○ The first number must not be 0. - Enable Timeout—This option enables or disables firewall rules with timeout. - Start Date—The respective firewall rule effect start from this date. - Start Time—The respective firewall rule effect start from this time. - End Date—The respective firewall rule effect ends at this date. - End Time—The respective firewall rule effect ends at this time.



Add IP Rule

IP Single (or) Range Start

IP Range End

optional

□ Enable Timeout

Start Date

YYYY/MM/DD

Start Time

End Date

YYYY/MM/DD

End Time

Rule

Allow

Port firewall rules

The port firewall rules settings include the existing port rules settings and an option to add new port rule settings.

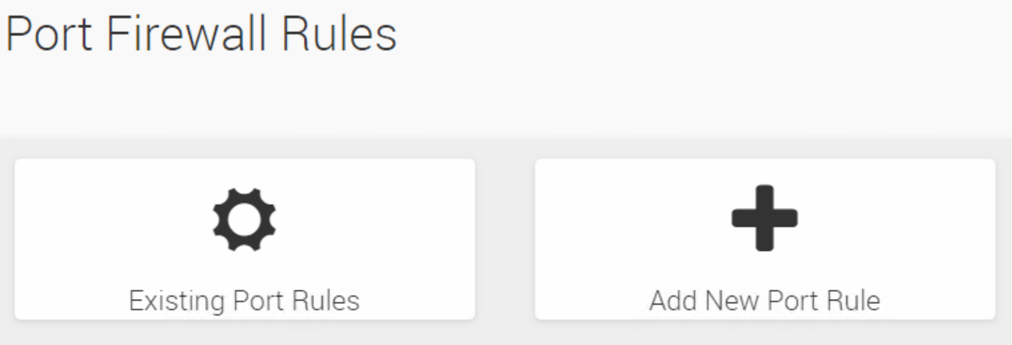
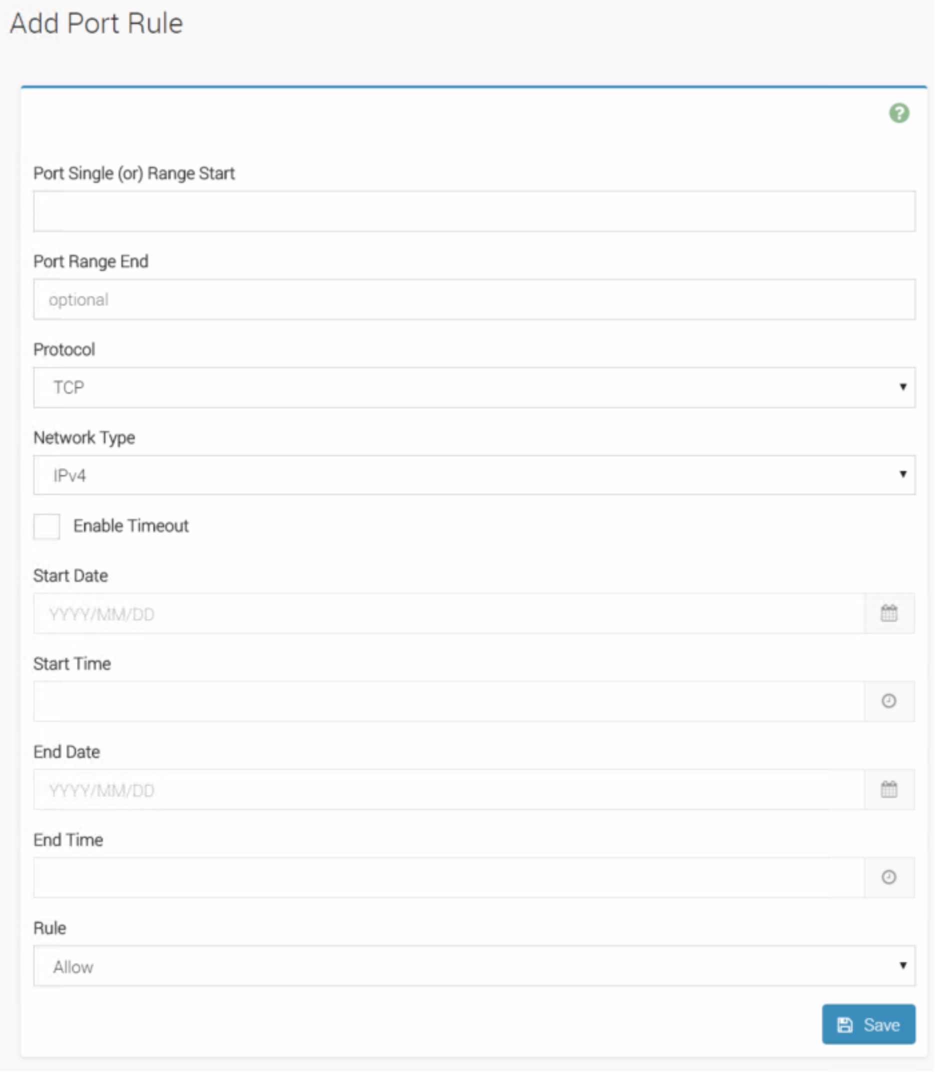

Port Firewall Rules

Table 11. IP address firewall rule settings

Setting	Description
Existing port rule settings	Displays a list of the existing port firewall rules. ● Click X to delete an item from the list. ● You must be at least an Operator to view the page. To add or delete a firewall, user must be an Administrator.
Add port rule settings	● Port Single (or) Range Start—Configure the port address or range of port addresses. A port address supports IPv4 address format only: ○ IPv4 address is four numbers that are separated by dots, for example, `xxx.xxx.xxx.xxx`. ○ The range is from 0-65535. ○ Port 80 is blocked for TCP or UDP protocols. ● Port Range End—Configured the port address or range of port addresses. An IP address supports IPv4 address format only: ○ IPv4 address is four numbers that are separated by dots, for example, `xxx.xxx.xxx.xxx`. ○ The range is from 0-65535. ○ Port 80 is blocked for TCP or UDP protocols. ● Enable Timeout—This option enables or disables firewall rules with timeout. ● Start Date—The respective firewall rule effect start from this date. ● Start Time—The respective firewall rule effect start from this time. ● End Date—The respective firewall rule effect ends at this date. ● End Time—The respective firewall rule effect ends at this time.



Add Port Rule

Port Single (or) Range Start

Port Range End

optional

Protocol

TCP

Network Type

IPv4

□ Enable Timeout

Start Date

YYYY/MM/DD

Start Time

End Date

YYYY/MM/DD

End Time

Rule

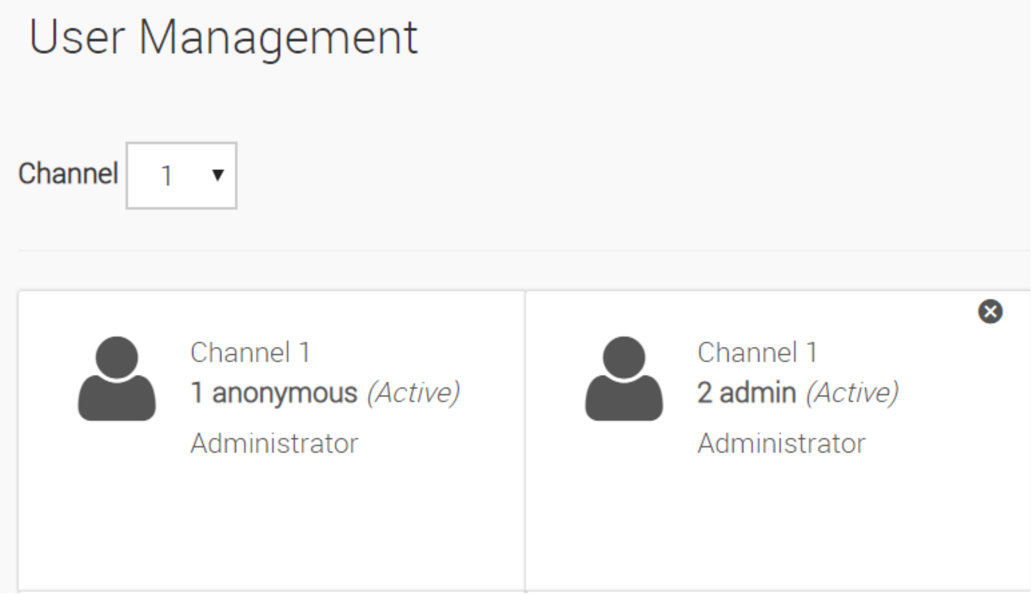
Allow

User management

Use this page to configure the user management order for authentication into the BMC. The page displays a list of available user management modules that are supported in the BMC. A maximum of 10 slots are available and include the default password (upper case): `<SERVICE TAG>!` and anonymous.

NOTE: Dell Technologies recommends that you modify the anonymous user privilege and password as a security measure.

To Add, Edit, or Delete a user, click the icon. To view the page, you must have Operator privileges. To modify or add a user, you must have Administrator privileges.



User Management

Channel 1 ▾

Channel 1
1 anonymous *(Active)*
Administrator

Channel 1
2 admin *(Active)*
Administrator

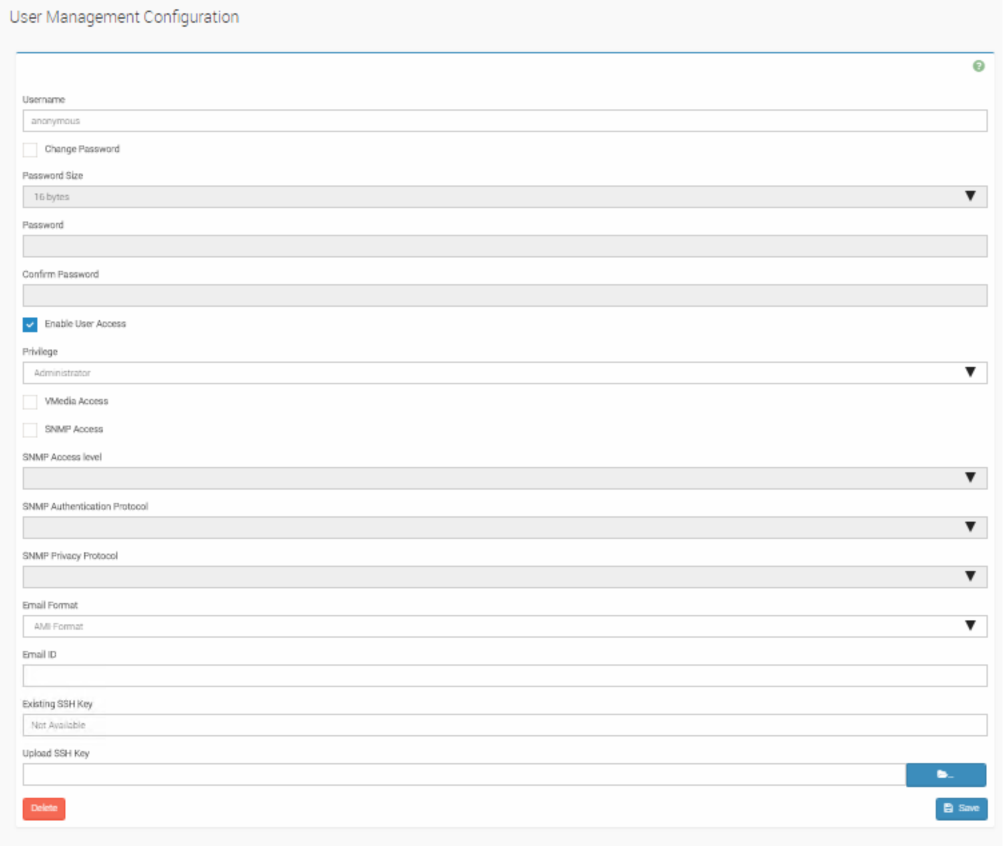
User management configuration

Table 12. User management configuration settings

Setting	Description
Username	Enter the name of the new user: ● For the IPv4 IP address, it consists of four sets of numbers that are separated by dots, for example, `xxx.xxx.xxx.xxx`. ● The range is 0–255. ● The first number must not be 0.
Change Password	Select this option to change the password.
Password Size	Select the size of the password.
Password	Enter a strong password that consists of at least one upper case letter, alphanumeric, and special characters. ⓘ **NOTE:** The password is mandatory if you enable SNMP Access. The password must have a minimum of eight characters when SNMP status is enabled.
Enable User Access	Check the box to enable user access. After enabling the user access, the IPMI messaging privilege is assigned to the user. ⓘ **NOTE:** Dell Technologies recommends that you enable IPMI messaging for the user to choose the User Access option, while creating the user through IPMI.
Privilege	Select the privilege level that is assigned to this user when the user accesses BMC through network interface. The network privilege levels are: ● User ● Administrator ● Operator ● None
SNMP Access	Check the box to enable SNMP access for the user.
SNMP Authentication Protocol	Choose an authentication protocol for the SNMP settings. The password field is mandatory if you change the authentication protocol.
SNMP Privacy Protocol	Choose the Encryption algorithm to use for the SNMP settings.
Email Format	Check this option to enable IPv6 DHCP to dynamically configure an IPv6 address using DHCPv6.

Table 12. User management configuration settings (continued)

Setting	Description
	● AMI-Format: The subject of this mail format is `Alert from (your Hostname)`. The mail content shows sensor information, for example: Sensor type and Description. ● Fixed Subject-Format: This format displays the message according to user settings. Set the subject and message for the email alert.
Email ID	Enter the email ID for the user. If the user forgets the password, a new password is mailed to the configured email ID. ⓘ **NOTE:** Configure the SMTP server to send the email. The maximum email ID size is 64 bytes which includes username and domain name.
Existing SSH Key	The uploaded SSH key read-only information displays.
Upload SSH Key	Use the **Browse** button to go to the public SSH key file. The SSH key file is of the pub type.



User Management Configuration

Username: anonymous

□ Change Password

Password Size: 16 bytes

Password:

Confirm Password:

☑ Enable User Access

Privilege: Administrator

□ VMedia Access

□ SNMP Access

SNMP Access level:

SNMP Authentication Protocol:

SNMP Privacy Protocol:

Email Format: AMI Format

Email ID:

Existing SSH Key: Not Available

Upload SSH Key:

Power control

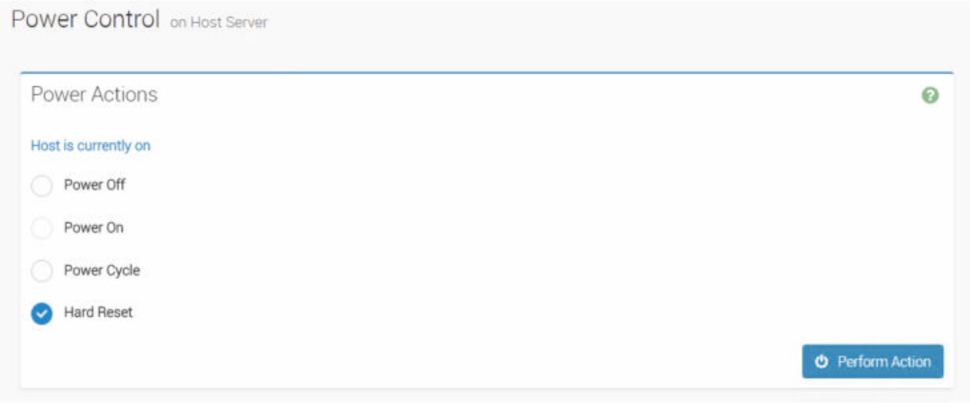
Use the Power control section to power off, power off, power cycle, or hard reset the server.

Table 13. Power control settings

Setting	Description
Power off	Select this option to immediately power off the server.
Power on	Select this option to power on the server.
Power Cycle	Select this option to first power off, and then reboot the system; a cold boot.

Table 13. Power control settings (continued)

Setting	Description
Hard reset	Select this option to reboot the system without powering off; a warm boot. Also select this option to initiate an operating system shutdown before the shutdown.



Power Control on Host Server

Power Actions

Host is currently on

○ Power Off

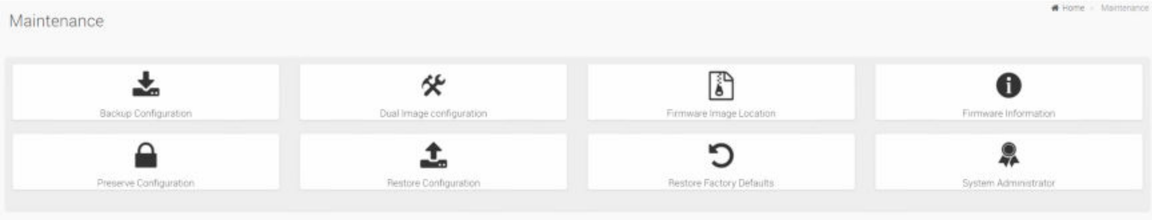
○ Power On

○ Power Cycle

● Hard Reset

Maintenance

Use the Maintenance section to update, backup, preserve, and restore your system.

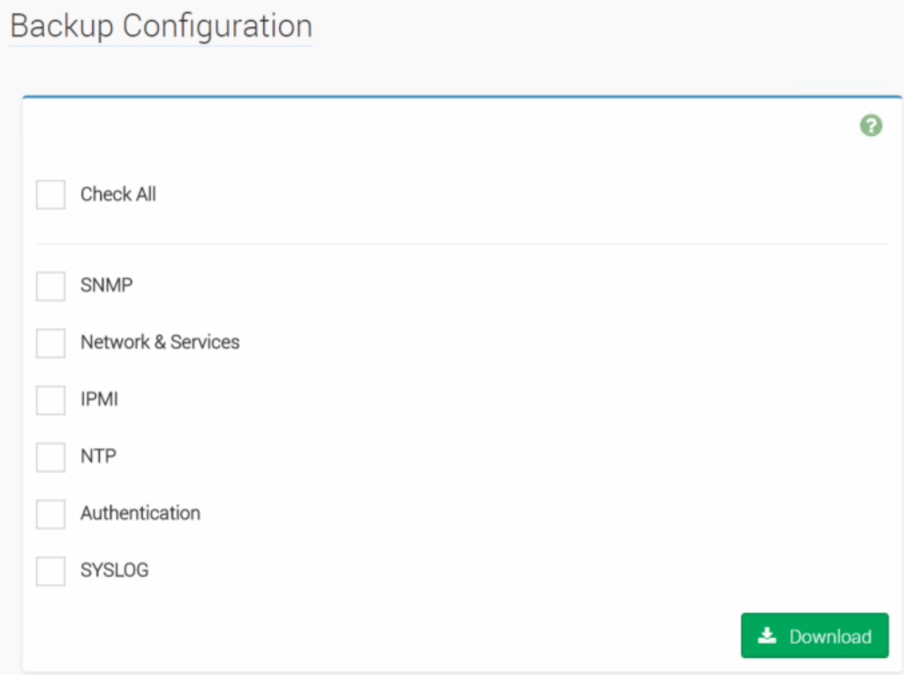


Maintenance

Backup configuration

Check the configuration to back up. Use the downloaded backup configuration to restore the configuration.

NOTE: Network configurations are interrelated to IPMI. By default, IPMI configurations are selected automatically when you select `Network and Services` to back up.



Backup Configuration

□ Check All

□ SNMP

□ Network & Services

□ IPMI

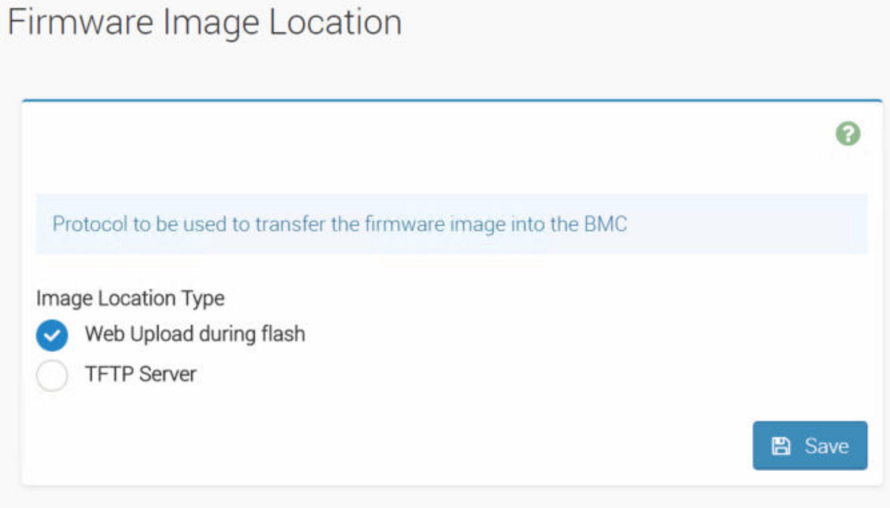
□ NTP

□ Authentication

□ SYSLOG

Firmware image location

The protocol to transfer the firmware image into the BMC.



Firmware Image Location

Protocol to be used to transfer the firmware image into the BMC

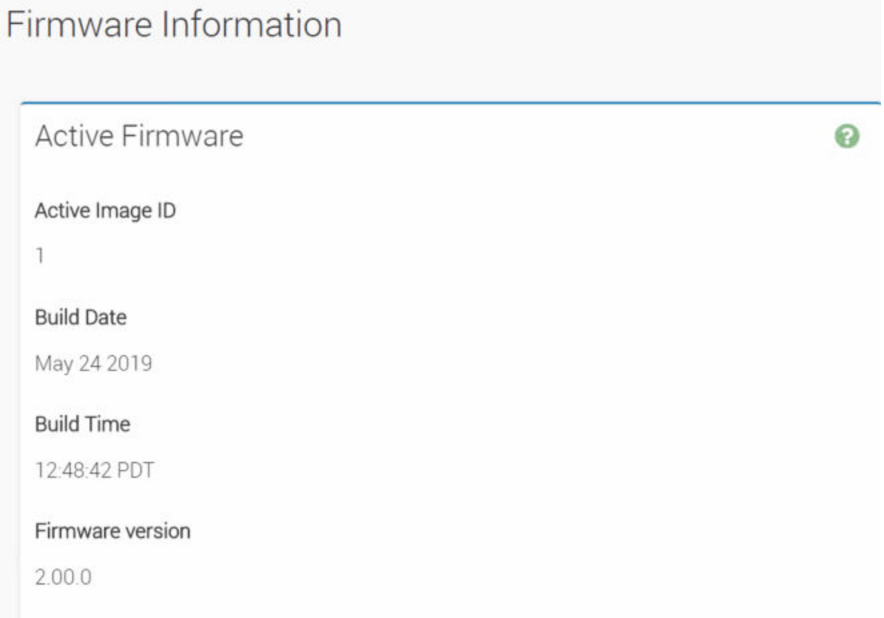
Image Location Type

● Web Upload during flash

○ TFTP Server

Table 14. Firmware information options

Options	Description
Active firmware	Describes the BMC active image ID.
Active image ID	Describes the build date of the active BMC image.
Build Time	Describes the build time of the active BMC image.
Firmware version	Describes the firmware version of the active BMC image.


Firmware Information

Active Firmware

Active Image ID

1

Build Date

May 24 2019

Build Time

12:48:42 PDT

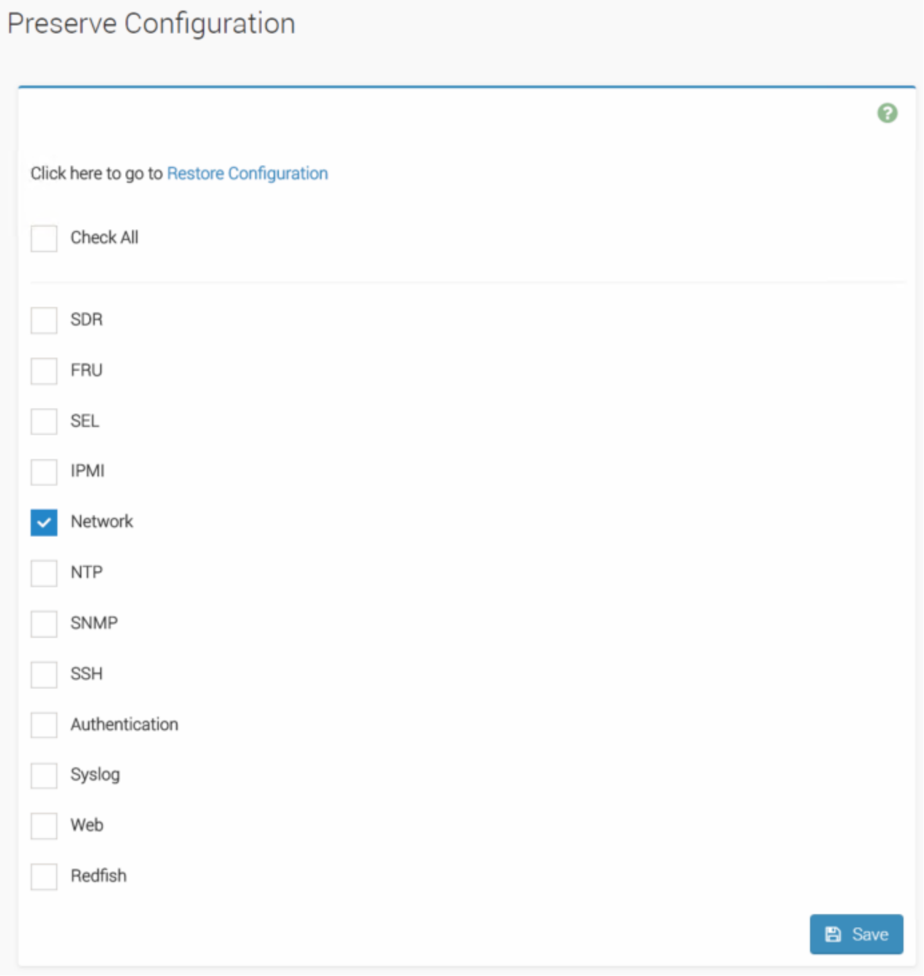
Firmware version

2.00.0

Preserve configuration

Table 15. Preserve configuration options

Options	Description
Restore Configuration	Check the configuration to preserve while the restore configuration is done.
Check All	Select this option to check all the configurations. Check or clear the check box to preserve or overwrite the configuration for your system.



Preserve Configuration

Click here to go to Restore Configuration

□ Check All

□ SDR

□ FRU

□ SEL

□ IPMI

☑ Network

□ NTP

□ SNMP

□ SSH

□ Authentication

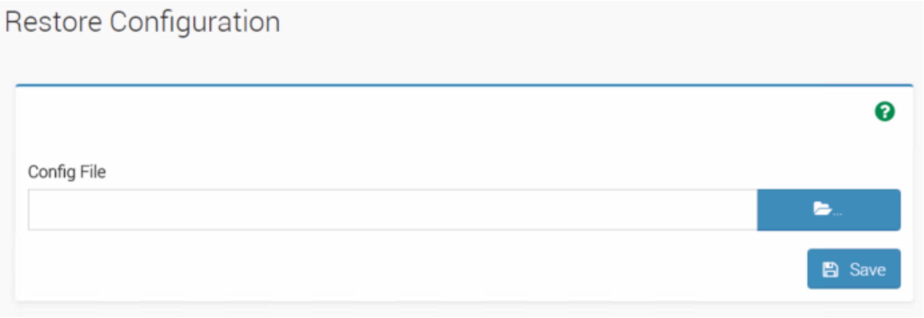
□ Syslog

□ Web

□ Redfish

Restore configuration

Use the **Browse** button to go to the configuration file to restore.

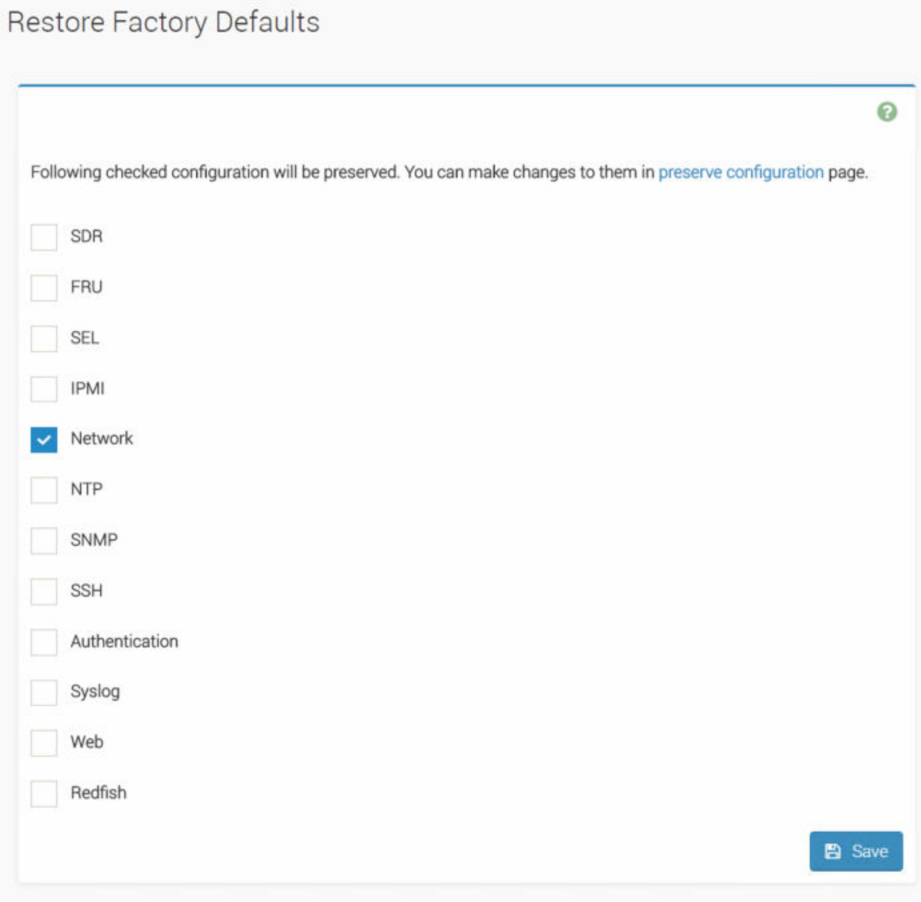


Restore Configuration

Config File

Restore factory defaults

Use the **Browse** button to go to the configuration file to restore the factory defaults.



Restore Factory Defaults

Following checked configuration will be preserved. You can make changes to them in preserve configuration page.

☐ SDR

☐ FRU

☐ SEL

☐ IPMI

☑ Network

☐ NTP

☐ SNMP

☐ SSH

☐ Authentication

☐ Syslog

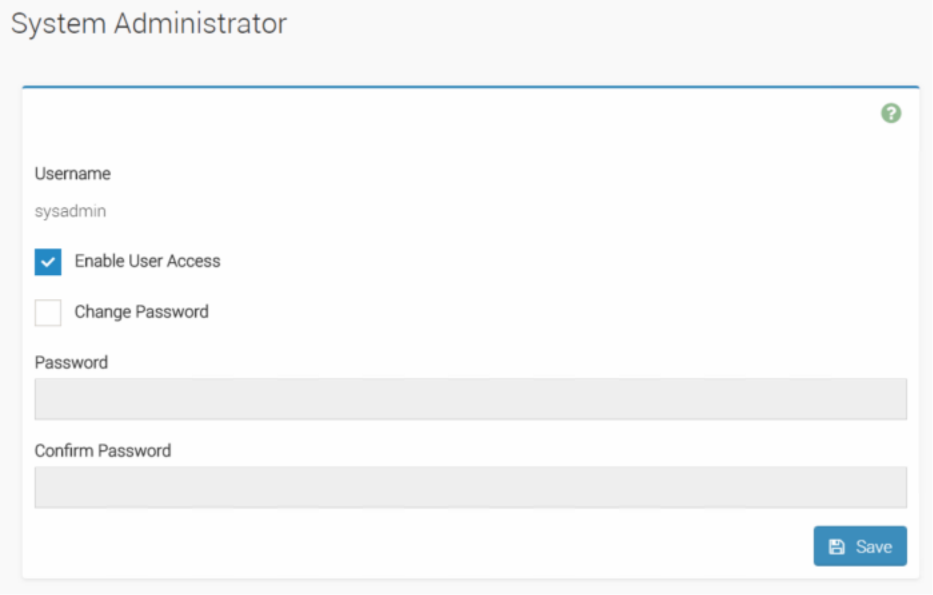
☐ Web

☐ Redfish

System administrator

Table 16. System administrator options

Options	Description
Username	Read-only username of system administrator displays.
Enable User Access	Check this option to enable user access for the system administrator.
Change Password	Check this option to change the existing password. This enables the password fields.
Password	Enter the new password. ● Password minimum is eight characters. ● Password maximum is 64 characters. ● White space is not allowed.
Confirm password	Enter the same password that you entered in the Password field. ● Password minimum is eight characters. ● Password maximum is 64 characters. ● White space is not allowed.



System Administrator

Username

sysadmin

☑ Enable User Access

□ Change Password

Password

Confirm Password

4

Configuration methods

The diagnostic operating software (DIAG OS) running on the local processor has ipmitool installed by default. You can use the ipmitool both at the switch and remotely.

Accessing BMC from the host does not require username or password. The general syntax for using ipmitool is:

NOTE: -I and -H are optional.

```
ipmitool [-c|-h|-v|-V] -I lanplus -H <hostname> [-p <port>]
[-U <username>]
[-L <privlvl>]
[-a|-E|-P|-f <password>]
[-o <oemtype>]
[-O <sel oem>]
[-C <ciphersuite>]
[-Y|[-K|-k <kg_key>]
[-y <hex_kg_key>]
[-e <esc_char>]
[-N <sec>]
[-R <count>]
< command>
```

For example, to list sensors from the host, use the following command from the host:

```
root@dellemc-diag-os:~# ipmitool sensor
PT_Mid_temp     | 31.000    | degrees C | ok    | na        | na       | na    | 78.000 | 80.000 | 85.000
NPU_Near_temp   | 29.000    | degrees C | ok    | na        | na       | na    | na     | na     | na
PT_Left_temp    | 28.000    | degrees C | ok    | na        | na       | na    | na     | na     | na
PT_Right_temp   | 30.000    | degrees C | ok    | na        | na       | na    | na     | na     | na
ILET_AF_temp    | 26.000    | degrees C | ok    | na        | na       | na    | na     | na     | na
PSU1_AF_temp    | 24.000    | degrees C | ok    | na        | na       | na    | 61.000 | 64.000 | na
PSU2_AF_temp    | 25.000    | degrees C | ok    | na        | na       | na    | na     | na     | na
PSU1_temp       | 34.000    | degrees C | ok    | na        | na       | na    | na     | na     | na
PSU2_temp       | na        | degrees C | na    | na        | na       | na    | na     | na     | na
CPU_temp        | 31.000    | degrees C | ok    | na        | na       | na    | 90.000 | 94.000 | na
FAN1_Rear_rpm   | 9120.000  | RPM       | ok    | na        | 1080.000 | na    | na     | na     | na
FAN2_Rear_rpm   | 9000.000  | RPM       | ok    | na        | 1080.000 | na    | na     | na     | na
FAN3_Rear_rpm   | 9000.000  | RPM       | ok    | na        | 1080.000 | na    | na     | na     | na
FAN4_Rear_rpm   | 9120.000  | RPM       | ok    | na        | 1080.000 | na    | na     | na     | na
FAN1_Front_rpm  | 10080.000 | RPM       | ok    | na        | 1080.000 | na    | na     | na     | na
FAN2_Front_rpm  | 10080.000 | RPM       | ok    | na        | 1080.000 | na    | na     | na     | na
FAN3_Front_rpm  | 9960.000  | RPM       | ok    | na        | 1080.000 | na    | na     | na     | na
FAN4_Front_rpm  | 10080.000 | RPM       | ok    | na        | 1080.000 | na    | na     | na     | na
PSU1_rpm        | 9000.000  | RPM       | ok    | na        | na       | na    | na     | na     | na
PSU2_rpm        | na        | RPM       | na    | na        | na       | na    | na     | na     | na
PSU_Total_watt  | 110.000   | Watts     | ok    | na        | na       | na    | na     | na     | na
PSU1_stat       | 0x0       | discrete  | 0x0180| na        | na       | na    | na     | na     | na
PSU2_stat       | 0x0       | discrete  | 0x0380| na        | na       | na    | na     | na     | na
PSU1_In_watt    | 110.000   | Watts     | ok    | na        | na       | na    | na     | na     | na
PSU1_In_volt    | 205.700   | Volts     | ok    | na        | na       | na    | na     | na     | na
PSU1_In_amp     | 0.480     | Amps      | ok    | na        | na       | na    | na     | na     | na
PSU1_Out_watt   | 90.000    | Watts     | ok    | na        | na       | na    | na     | na     | na
PSU1_Out_volt   | 12.400    | Volts     | ok    | na        | na       | na    | na     | na     | na
PSU1_Out_amp    | 7.500     | Amps      | ok    | na        | na       | na    | na     | na     | na
PSU2_In_watt    | na        | Watts     | na    | na        | na       | na    | na     | na     | na
PSU2_In_volt    | na        | Volts     | na    | na        | na       | na    | na     | na     | na
PSU2_In_amp     | na        | Amps      | na    | na        | na       | na    | na     | na     | na
PSU2_Out_watt   | na        | Watts     | na    | na        | na       | na    | na     | na     | na
PSU2_Out_volt   | na        | Volts     | na    | na        | na       | na    | na     | na     | na
PSU2_Out_amp    | na        | Amps      | na    | na        | na       | na    | na     | na     | na
ACPI_stat       | 0x0       | discrete  | 0x0180| na        | na       | na    | na     | na     | na
FAN1_prsnt      | 0x0       | discrete  | 0x0180| na        | na       | na    | na     | na     | na
FAN2_prsnt      | 0x0       | discrete  | 0x0180| na        | na       | na    | na     | na     | na
FAN3_prsnt      | 0x0       | discrete  | 0x0180| na        | na       | na    | na     | na     | na
FAN4_prsnt      | 0x0       | discrete  | 0x0180| na        | na       | na    | na     | na     | na
FAN1_Rear_stat  | 0x0       | discrete  | 0x0080| na        | na       | na    | na     | na     | na
FAN2_Rear_stat  | 0x0       | discrete  | 0x0080| na        | na       | na    | na     | na     | na
FAN3_Rear_stat  | 0x0       | discrete  | 0x0080| na        | na       | na    | na     | na     | na
FAN4_Rear_stat  | 0x0       | discrete  | 0x0080| na        | na       | na    | na     | na     | na
FAN1_Front_stat | 0x0       | discrete  | 0x0080| na        | na       | na    | na     | na     | na
FAN2_Front_stat | 0x0       | discrete  | 0x0080| na        | na       | na    | na     | na     | na
FAN3_Front_stat | 0x0       | discrete  | 0x0080| na        | na       | na    | na     | na     | na
FAN4_Front_stat | 0x0       | discrete  | 0x0080| na        | na       | na    | na     | na     | na
```

```
INTER_5.0V_volt | 4.900     | Volts     | ok    | 4.200     | 4.500     | 4.700     | 5.200     | 5.500     | 5.700
INTER_3.3V_volt | 3.300     | Volts     | ok    | 2.800     | 3.000     | 3.100     | 3.500     | 3.600     | 3.800
FPGA_1.0V_volt  | 0.990     | Volts     | ok    | 0.850     | 0.900     | 0.950     | 1.050     | 1.100     | 1.150
FPGA_1.2V_volt  | 1.190     | Volts     | ok    | 1.020     | 1.080     | 1.140     | 1.260     | 1.320     | 1.380
FPGA_1.8V_volt  | 1.780     | Volts     | ok    | 1.530     | 1.620     | 1.710     | 1.890     | 1.980     | 2.070
FPGA_3.3V_volt  | 3.200     | Volts     | ok    | 2.800     | 3.000     | 3.100     | 3.500     | 3.600     | 3.800
BMC_2.5V_volt   | 2.400     | Volts     | ok    | 2.100     | 2.200     | 2.300     | 2.600     | 2.800     | 2.900
BMC_1.15V_volt  | 1.150     | Volts     | ok    | 0.980     | 1.030     | 1.090     | 1.210     | 1.270     | 1.320
BMC_1.2V_volt   | 1.210     | Volts     | ok    | 1.020     | 1.080     | 1.140     | 1.260     | 1.320     | 1.380
SWITCH_6.8V_volt| 7.000     | Volts     | ok    | 5.800     | 6.100     | 6.400     | 7.200     | 7.500     | 7.800
SWITCH_3.3V_volt| 3.300     | Volts     | ok    | 2.800     | 3.000     | 3.100     | 3.500     | 3.600     | 3.800
SWITCH_1.8V_volt| 1.790     | Volts     | ok    | 1.530     | 1.620     | 1.710     | 1.890     | 1.980     | 2.070
USB_5.0V_volt   | 4.900     | Volts     | ok    | 4.200     | 4.500     | 4.700     | 5.200     | 5.500     | 5.700
NPU_1.2V_volt   | 1.190     | Volts     | ok    | 1.020     | 1.080     | 1.140     | 1.260     | 1.320     | 1.380
NPU_VDDCORE_volt| 0.800     | Volts     | ok    | 0.700     | 0.720     | 0.740     | 0.910     | 0.930     | 0.950
NPU_VDDANLG_volt| 0.790     | Volts     | ok    | 0.680     | 0.720     | 0.760     | 0.840     | 0.880     | 0.920
BMC_boot        | 0x0       | discrete  | 0x0180| na        | na        | na        | na        | na        | na
SEL_sensor      | 0x0       | discrete  | 0x1080| na        | na        | na        | na        | na        | na
```

The command parameters change slightly when using `ipmitool` over LAN. Enter the service tag number in uppercase.

```
root@dellemc-diag-os:~# ipmitool -U admin -P <SERVICE TAG>! -I lanplus -H 10.11.227.105 sensor
PT_Mid_temp     | 32.000    | degrees C | ok    | na        | na        | na        | 78.000    | 80.000    | 85.000
NPU_Near_temp   | 29.000    | degrees C | ok    | na        | na        | na        | na        | na        | na
PT_Left_temp    | 28.000    | degrees C | ok    | na        | na        | na        | na        | na        | na
PT_Right_temp   | 30.000    | degrees C | ok    | na        | na        | na        | na        | na        | na
ILET_AF_temp    | 26.000    | degrees C | ok    | na        | na        | na        | na        | na        | na
PSU1_AF_temp    | 24.000    | degrees C | ok    | na        | na        | na        | 61.000    | 64.000    | na
PSU2_AF_temp    | 25.000    | degrees C | ok    | na        | na        | na        | na        | na        | na
PSU1_temp       | 33.000    | degrees C | ok    | na        | na        | na        | na        | na        | na
PSU2_temp       | na        | degrees C | na    | na        | na        | na        | na        | na        | na
CPU_temp        | 31.000    | degrees C | ok    | na        | na        | na        | 90.000    | 94.000    | na
FAN1_Rear_rpm   | 9120.000  | RPM       | ok    | na        | 1080.000  | na        | na        | na        | na
FAN2_Rear_rpm   | 9000.000  | RPM       | ok    | na        | 1080.000  | na        | na        | na        | na
FAN3_Rear_rpm   | 9000.000  | RPM       | ok    | na        | 1080.000  | na        | na        | na        | na
FAN4_Rear_rpm   | 9000.000  | RPM       | ok    | na        | 1080.000  | na        | na        | na        | na
FAN1_Front_rpm  | 10080.000 | RPM       | ok    | na        | 1080.000  | na        | na        | na        | na
FAN2_Front_rpm  | 10080.000 | RPM       | ok    | na        | 1080.000  | na        | na        | na        | na
FAN3_Front_rpm  | 10080.000 | RPM       | ok    | na        | 1080.000  | na        | na        | na        | na
FAN4_Front_rpm  | 10080.000 | RPM       | ok    | na        | 1080.000  | na        | na        | na        | na
PSU1_rpm        | 9120.000  | RPM       | ok    | na        | na        | na        | na        | na        | na
PSU2_rpm        | na        | RPM       | na    | na        | na        | na        | na        | na        | na
PSU_Total_watt  | 110.000   | Watts     | ok    | na        | na        | na        | na        | na        | na
PSU1_stat       | 0x0       | discrete  | 0x0180| na        | na        | na        | na        | na        | na
PSU2_stat       | 0x0       | discrete  | 0x0380| na        | na        | na        | na        | na        | na
PSU1_In_watt    | 110.000   | Watts     | ok    | na        | na        | na        | na        | na        | na
PSU1_In_volt    | 205.700   | Volts     | ok    | na        | na        | na        | na        | na        | na
PSU1_In_amp     | 0.480     | Amps      | ok    | na        | na        | na        | na        | na        | na
PSU1_Out_watt   | 90.000    | Watts     | ok    | na        | na        | na        | na        | na        | na
PSU1_Out_volt   | 12.400    | Volts     | ok    | na        | na        | na        | na        | na        | na
PSU1_Out_amp    | 7.500     | Amps      | ok    | na        | na        | na        | na        | na        | na
PSU2_In_watt    | na        | Watts     | na    | na        | na        | na        | na        | na        | na
PSU2_In_volt    | na        | Volts     | na    | na        | na        | na        | na        | na        | na
PSU2_In_amp     | na        | Amps      | na    | na        | na        | na        | na        | na        | na
PSU2_Out_watt   | na        | Watts     | na    | na        | na        | na        | na        | na        | na
PSU2_Out_volt   | na        | Volts     | na    | na        | na        | na        | na        | na        | na
PSU2_Out_amp    | na        | Amps      | na    | na        | na        | na        | na        | na        | na
ACPI_stat       | 0x0       | discrete  | 0x0180| na        | na        | na        | na        | na        | na
FAN1_prsnt      | 0x0       | discrete  | 0x0180| na        | na        | na        | na        | na        | na
FAN2_prsnt      | 0x0       | discrete  | 0x0180| na        | na        | na        | na        | na        | na
FAN3_prsnt      | 0x0       | discrete  | 0x0180| na        | na        | na        | na        | na        | na
FAN4_prsnt      | 0x0       | discrete  | 0x0180| na        | na        | na        | na        | na        | na
FAN1_Rear_stat  | 0x0       | discrete  | 0x0080| na        | na        | na        | na        | na        | na
FAN2_Rear_stat  | 0x0       | discrete  | 0x0080| na        | na        | na        | na        | na        | na
FAN3_Rear_stat  | 0x0       | discrete  | 0x0080| na        | na        | na        | na        | na        | na
FAN4_Rear_stat  | 0x0       | discrete  | 0x0080| na        | na        | na        | na        | na        | na
FAN1_Front_stat | 0x0       | discrete  | 0x0080| na        | na        | na        | na        | na        | na
FAN2_Front_stat | 0x0       | discrete  | 0x0080| na        | na        | na        | na        | na        | na
FAN3_Front_stat | 0x0       | discrete  | 0x0080| na        | na        | na        | na        | na        | na
FAN4_Front_stat | 0x0       | discrete  | 0x0080| na        | na        | na        | na        | na        | na
INTER_5.0V_volt | 4.900     | Volts     | ok    | 4.200     | 4.500     | 4.700     | 5.200     | 5.500     | 5.700
INTER_3.3V_volt | 3.300     | Volts     | ok    | 2.800     | 3.000     | 3.100     | 3.500     | 3.600     | 3.800
FPGA_1.0V_volt  | 0.990     | Volts     | ok    | 0.850     | 0.900     | 0.950     | 1.050     | 1.100     | 1.150
FPGA_1.2V_volt  | 1.190     | Volts     | ok    | 1.020     | 1.080     | 1.140     | 1.260     | 1.320     | 1.380
FPGA_1.8V_volt  | 1.780     | Volts     | ok    | 1.530     | 1.620     | 1.710     | 1.890     | 1.980     | 2.070
FPGA_3.3V_volt  | 3.200     | Volts     | ok    | 2.800     | 3.000     | 3.100     | 3.500     | 3.600     | 3.800
BMC_2.5V_volt   | 2.400     | Volts     | ok    | 2.100     | 2.200     | 2.300     | 2.600     | 2.800     | 2.900
BMC_1.15V_volt  | 1.150     | Volts     | ok    | 0.980     | 1.030     | 1.090     | 1.210     | 1.270     | 1.320
BMC_1.2V_volt   | 1.210     | Volts     | ok    | 1.020     | 1.080     | 1.140     | 1.260     | 1.320     | 1.380
SWITCH_6.8V_volt| 7.000     | Volts     | ok    | 5.800     | 6.100     | 6.400     | 7.200     | 7.500     | 7.800
SWITCH_3.3V_volt| 3.300     | Volts     | ok    | 2.800     | 3.000     | 3.100     | 3.500     | 3.600     | 3.800
SWITCH_1.8V_volt| 1.790     | Volts     | ok    | 1.530     | 1.620     | 1.710     | 1.890     | 1.980     | 2.070
USB_5.0V_volt   | 4.900     | Volts     | ok    | 4.200     | 4.500     | 4.700     | 5.200     | 5.500     | 5.700
NPU_1.2V_volt   | 1.190     | Volts     | ok    | 1.020     | 1.080     | 1.140     | 1.260     | 1.320     | 1.380
NPU_VDDCORE_volt| 0.800     | Volts     | ok    | 0.700     | 0.720     | 0.740     | 0.910     | 0.930     | 0.950
NPU_VDDANLG_volt| 0.790     | Volts     | ok    | 0.680     | 0.720     | 0.760     | 0.840     | 0.880     | 0.920
BMC_boot        | 0x0       | discrete  | 0x0180| na        | na        | na        | na        | na        | na
SEL_sensor      | 0x0       | discrete  | 0x1080| na        | na        | na        | na        | na        | na
```

To access BMC over a LAN, use the following `ipmitool` command:

```
ipmitool [-c|-h|-v|-V] -I lanplus -H <hostname> [-p <port>]
[-U <username>]
[-L <privlvl>]
[-a|-E|-P|-f <password>]
[-o <oemtype>]
[-O <sel oem>]
[-C <ciphersuite>]
[-Y|[-K|- <kg_key>]
[-y <hex_kg_key>]
[-e <esc_char>]
[-N <sec>]
[-R <count>]
<command>
```

If needed, you can download `ipmitool` from the `https://sourceforge.net/ projects/ipmitool` website. The commands to install `ipmitool` on Ubuntu or Fedora versions are as follows:

1. Install `ipmitool` on Ubuntu versions.

   `# apt-get install ipmitool`

2. Install `ipmitool` on Fedora versions.

   `# yum install ipmitool`

Run standard IPMI commands from `ipmitool`. For the command format, see *Intelligent Platform Management Interface Specification Second Generation v2.0.pdf*. For more documentation, see *https://linux.die.net/man/1/ipmitool*.

ⓘ **NOTE:** Throughout this user guide, *Intelligent Platform Management Interface Specification Second Generation v2.0.pdf* is known as *IPMI Specification v2.0*. For more information about IPMI, see the Intel-hosted IPMI resources at https://www.intel.com/content/www/us/en/servers/ipmi/ipmi-technical-resources.html.

Topics:

- Configurations
- Date and time
- SNMP and email alerts
- Add and delete users
- Firewall
- Event log
- Default configuration restore

Configurations

LAN configurations

For network settings, see the *IPMI Specification v2.0* chapter 23.1 *Set LAN Configuration Parameters Command* and Table 23-4 *LAN Configuration Parameters*.

Besides setting IP addresses, use `ipmitool` to set the network mask, MAC address, default gateway IP and MAC addresses, and so forth.

`ipmitool` commands:

```
root@dellemc-diag-os:~#  ipmitool lan set 1

usage: lan set <channel> <command> <parameter>
LAN set command/parameter options:
ipaddr <x.x.x.x>            Set channel IP address
netmask <x.x.x.x>           Set channel IP netmask
macaddr <x:x:x:x:x:x>       Set channel MAC address
defgw ipaddr <x.x.x.x>      Set default gateway IP address
defgw macaddr <x:x:x:x:x:x> Set default gateway MAC address  bakgw
ipaddr <x.x.x.x>            Set backup gateway IP address
```

```
bakgw macaddr <x:x:x:x:x:x> Set backup gateway MAC address
password <password>         Set session password for this channel
snmp <community string>     Set SNMP public community string
user                        Enable default user for this channel
access <on|off>             Enable or disable access to this channel
alert <on|off>              Enable or disable PEF alerting for this channel
arp respond <on|off>        Enable or disable BMC ARP responding
arp generate <on|off>       Enable or disable BMC gratuitous ARP generation
arp interval <seconds>      Set gratuitous ARP generation interval
vlan id <off|<id>>          Disable or enable VLAN and set ID (1-4094)
vlan priority <priority>    Set vlan priority (0-7)
auth <level> <type,..>      Set channel authentication types
  level  = CALLBACK, USER, OPERATOR, ADMIN
  type   = NONE, MD2, MD5, PASSWORD, OEM
ipsrc <source>                 Set IP Address source
  none   = unspecified source
  static = address manually configured to be static
  dhcp   = address obtained by BMC running DHCP
  bios   = address loaded by BIOS or system software
cipher_privs XXXXXXXXXXXXXX    Set RMCP+ cipher suite privilege levels
X = Cipher Suite Unused
c = CALLBACK
u = USER
o = OPERATOR
a = ADMIN
O = OEM  bad_pass_thresh <thresh_num> <1|0> <reset_interval> <lockout_interval>
                                 Set bad password threshold
```

NOTE: Dell Technologies recommends setting LAN parameters from the host microprocessor. You can run all other `ipmitool` options from a remote machine after the BMC has the correct IP address and LAN settings. When running `ipmitool` from a remote machine, the command prefix is `ipmitool -H <ip address of BMC> -I lanplus -U <user_name> -P <password> …">`

The *`<channel>`* number is the LAN channel, which is `1` in this BMC implementation.

Dell Technologies recommends running the LAN settings command from a system-side machine rather than from a remote machine. To set a dynamic host configuration protocol (DHCP) IP address, use the following command:

```
# ipmitool lan set 1 ipsrc dhcp
```

To set a static IP address:

```
# ipmitool lan set 1 ipsrc static
# ipmitool lan set 1 ipaddr <x.x.x.x>
```

You can also add the BMC IP address from the BIOS. For more information, see the BIOS manual at www.dell.com/support.

DNS configuration

Use these commands to set and get domain name server (DNS)-related settings, for example hostname, domain setting, and DNS server settings. BMC supports only three DNS server IP addresses. These IP addresses can be either IPv4 or IPv6.

To set DNS configuration details, use the DNS configuration command. The DNS configuration is buffered and applies only after you set a DNS Restart—`parameter #7`.

Date and time

BIOS sets the date and time during boot up. Use the `iseltime` tool that is part of the `ipmiutil` package. Use the `ipmiutil` command only on the local processor.

Install the `ipmiutil` package using the `iseltime` command.

To override the date and time that is used in the system event log (SEL) log, use the following command:

```
root@dellemc-diag-os:~# ipmitool sel time get
08/01/2018 15:10:46
root@dellemc-diag-os:~# ipmitool sel time set
usage: sel time set "mm/dd/yyyy hh:mm:ss"
root@dellemc-diag-os:~#
```

For `ipmiutil/iseltime`, download and install the binaries and documentation from https://ipmiutil.sourceforge.net. Also, various Linux distributions have binary packages prebuilt and available for download.

SNMP and email alerts

Event filters

To set the platform event filters, use the `raw` command format. To configure an entry in the filter table:

```
root@dellemc-diag-os:~# ipmitool raw 0x04 0x12 0x6 0x2 0xc0 0x1 0x2 0x2 0xff 0xff 0xff 0xff 0xff 0x01 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
Byte 3  (0x60) - event filter table cmd
Byte 4(0x2) - filter number
Byte 5(0xc0) - filter config(enable)
Byte 6(0x1) - action(alert)
Byte 7(0x2) - policy number
Byte 8(0x2)  - event severity(information)
Byte 9(0xff) - slave address
Byte 10  (0xff) - channel number(any)
Byte 11(0xff)  - sensor number(any)
Byte 12(0x01) - event trigger(threshold)
```

The entry 2 is changed after the command, as shown:

```
root@dellemc-diag-os:~#
root@dellemc-diag-os:~#  ipmitool pef filter list
1 | disabled, configurable
2 | enabled, pre-configured | Any | Any | Information | OEM | Any | Alert | 2
3 | disabled, configurable
4 | disabled, configurable
5 | disabled, configurable
6 | disabled, configurable
7 | disabled, configurable
8 | disabled, configurable
9 | disabled, configurable
10 | disabled, configurable
11 | disabled, configurable
12 | disabled, configurable
13 | disabled, configurable
14 | disabled, configurable
15 | disabled, configurable
16 | disabled, configurable
17 | disabled, configurable
18 | disabled, configurable
19 | disabled, configurable
20 | disabled, configurable
21 | disabled, configurable
22 | disabled, configurable
23 | disabled, configurable
24 | disabled, configurable
25 | disabled, configurable
26 | disabled, configurable
27 | disabled, configurable
28 | disabled, configurable
29 | disabled, configurable
30 | disabled, configurable
31 | disabled, configurable
32 | disabled, configurable
```

```
33 | disabled, configurable
34 | disabled, configurable
35 | disabled, configurable
36 | disabled, configurable
37 | disabled, configurable
38 | disabled, configurable
39 | disabled, configurable
40 | disabled, configurable
```

For more information, see the *IPMI Specification v2.0* chapter 17.7 *Event Filter Table* and chapter 30.3 *Set PEF Configuration Parameters Command*.

Alert policies and destinations

For more information, see the *IPMI Specification v2.0* chapter 17.11 *Alert Policy Table* and chapter 30.3 *Set PEF Configuration Parameters Command (parameter 9)*.

LAN destinations

BMC supports SNMP alert destinations. These destinations are SNMP traps. When you set a LAN destination for alerts, the BMC sends an SNMP trap to the set a destination whenever BMC detects alert conditions. You can set up the SNMP management application on the destination to receive these SNMP traps; however, setting up the SNMP management station is beyond the scope of this document.

To view alert destinations, use the `ipmitool lan alert print` command.

```
root@dellemc-diag-os:~#  ipmitool lan alert print
Alert Destination        : 0
Alert Acknowledge        : Unacknowledged
Destination Type         : PET Trap
Retry Interval           : 0
Number of Retries        : 0
Alert Gateway            : Default
Alert IP Address         : 0.0.0.0
Alert MAC Address        : 00:00:00:00:00:00
Alert Destination        : 1
Alert Acknowledge        : Unacknowledged
Destination Type         : PET Trap
Retry Interval           : 0
Number of Retries        : 0
Alert Gateway            : Default
Alert IP Address         : 0.0.0.0
Alert MAC Address        : 00:00:00:00:00:00
Alert Destination        : 2
Alert Acknowledge        : Unacknowledged
Destination Type         : PET Trap
Retry Interval           : 0
Number of Retries        : 0
Alert Gateway            : Default
Alert IP Address         : 0.0.0.0
Alert MAC Address        : 00:00:00:00:00:00
.
.
.
Alert Destination        : 15
Alert Acknowledge        : Unacknowledged
Destination Type         : PET Trap
Retry Interval           : 0
Number of Retries        : 0
Alert Gateway            : Default
Alert IP Address         : 0.0.0.0
Alert MAC Address        : 00:00:00:00:00:00
```

You can configure up to 15 destinations. To configure destination 1 to send an alert to a machine with IP address 10.11.227.180:

```
root@dellemc-diag-os:~#  ipmitool lan alert set 1 1 ipaddr 10.11.227.105
Setting LAN Alert 1 IP Address to 10.11.227.105
```

The following output using the `ipmitool lan alert print` command shows that the configuration was successful:

```
root@dellemc-diag-os:~# ipmitool lan alert print 1 1
Alert Destination        : 1
Alert Acknowledge        : Unacknowledged
Destination Type         : PET Trap
Retry Interval           : 0
Number of Retries        : 0
Alert Gateway            : Default
Alert IP Address         : 10.11.227.105
Alert MAC Address        : 00:00:00:00:00:00
```

Alert policy setup

To set up the alert policy, you must use the `ipmitool raw` command.

To view the current policy table, use the `ipmitool pef policy list` command.

```
root@dellemc-diag-os:~# ipmitool pef policy list
1 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
2 | 2 | enabled | Match-always | 1 | 802.3 LAN | PET | AMI | 0 | 0 | 10.11.227.105 | 00:00:00:00:00:00
3 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
4 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
5 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
6 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
7 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
8 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
9 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
10 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
.
.
.
57 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
58 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
59 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
60 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
```

There are 60 entries available for a policy table. The following example shows setting a policy entry. For a detailed description of the table entries, see the *IPMI Specification v2.0 Alert policy table entry*.

```
root@dellemc-diag-os:~# ipmitool raw 0x4 0x12 0x9 0x2 0x28 0x11 0x00

root@dellemc-diag-os:~# ipmitool pef policy list
1 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
2 | 2 | enabled | Match-always | 1 | 802.3 LAN | PET | AMI | 0 | 0 | 10.11.227.105 | 00:00:00:00:00:00
3 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
4 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
5 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
6 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
7 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
8 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
9 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
10 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
.
.
.
57 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
58 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
59 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
60 | 0 | disabled | Match-always | 0 | IPMB (I2C) | 0
```

Add and delete users

The following describes adding and deleting users:

There are 10 entries for a user list.

1. Add a new user by modifying one of the empty entries in the user list using the following command. This creates a user with no access. Enter the service tag number in upper case.

```
$ ./ipmitool -H xx.xx.xxx.xx -I lanplus -U admin -P <SERVICE TAG>! user set name 3 <name>
$ ./ipmitool -H xx.xx.xxx.xx -I lanplus -U admin -P <SERVICE TAG>! user set password 3
Password for user 3:
Password for user 3:
Set User Password command successful (user 3)
```

2. Set the privilege level for the user in Step 1 using the following command.

```
$ ./ipmitool -H xx.xx.xxx.xx -I lanplus -U admin -P <SERVICE TAG>! user  priv 3
User Commands:
  summary      [<channel number>]
  list         [<channel number>]
  set name     <user id> <username>
  set password <user id> [<password> <16|20>]
  disable      <user id>
  enable       <user id>
  priv         <user id> <privilege level> [<channel number>]
      Privilege levels:
      * 0x1 - Callback
      * 0x2 - User
      * 0x3 - Operator
      * 0x4 - Administrator
      * 0x5 - OEM Proprietary
      * 0xF - No Access

   test         <user id> <16|20> [<password]>

$ ./ipmitool -H xx.xx.xxx.xx -I lanplus -U admin -P <SERVICE TAG>! user priv 3 2
Set Privilege Level command successful (user 3)
$ ./ipmitool -H xx.xx.xxx.xx -I lanplus -U admin -P <SERVICE TAG>! user list
ID  Name    Callin  Link Auth  IPMI Msg   Channel Priv Limit
1           false   false      true       ADMINISTRATOR
2   <SERVICE TAG>!   true    true       true       ADMINISTRATOR
3   <name>  true    true       true       USER
4           true    false      false      NO ACCESS
5           true    false      false      NO ACCESS
6           true    false      false      NO ACCESS
7           true    false      false      NO ACCESS
8           true    false      false      NO ACCESS
9           true    false      false      NO ACCESS
10          true    false      false      NO ACCESS
```

   a. You can individually enable channels for a certain privilege level access. For example, to place the LAN channel accessible for "USER" level access, use the following command.

```
$ ./ipmitool -H xx.xx.xxx.xxx -I lanplus -U admin -P <SERVICE TAG>! channel setaccess 1 3 callin=off link=off
ipmi=on privilege=1
Set User Access (channel 1 id 3) successful.
$ ./ipmitool -H xx.xx.xxx.xxx -I lanplus -L USER -U <name> -P <password> fru
Get Device ID command failed: 0xd4 Insufficient privilege level
FRU Device Description : Builtin FRU Device (ID 0)
Get Device ID command failed: Insufficient privilege level
$ ./ipmitool -H xx.xx.xxx.xxx -I lanplus -U admin -P <SERVICE TAG>! channel setaccess 1 3 callin=off link=off
ipmi=on privilege=2
Set User Access (channel 1 id 3) successful.
$ ./ipmitool -H xx.xx.xxx.xx -I lanplus -L USER -U <name> -P <password> fru
FRU Device Description : Builtin FRU Device (ID 0)
 Board Mfg Date        : Mon Feb 12 08:00:00 2018
 Board Mfg             : Dell
 Board Product         : <platform>
 Board Serial          : CNCES0082C0002
 Board Part Number     : 0G1T60X01
 Product Manufacturer  : Dell
 Product Name          : <platform>
 Product Version       : 00
 Product Serial        : X1
 Product Asset Tag     : D4SSG02
```

```
FRU Device Description : FRU_PSU1 (ID 1)
 Unknown FRU header version 0x00

FRU Device Description : FRU_PSU2 (ID 2)
 Board Mfg Date        : Fri Jan 12 18:47:00 2018
 Board Mfg             : DELL
 Board Product         : PWR SPLY,495W,RDNT,DELTA
 Board Serial          : CNDED0081G01GL
 Board Part Number     : 0GRTNKA02

FRU Device Description : FRU_FAN1 (ID 3)
 Unknown FRU header version 0x00

FRU Device Description : FRU_FAN2 (ID 4)
 Board Mfg Date        : Mon Feb 12 08:01:00 2018
 Board Mfg             : Dell
 Board Product         : <platform>
 Board Serial          : CNCES008260036
 Board Part Number     : 07CRC9X01
 Product Manufacturer  : Dell
 Product Name          : <platform>
 Product Version       :
 Product Serial        :
 Product Asset Tag     : D4SSG02
```

For more information, see the *IPMI Specification v2.0* chapter 22.26 *Set User Access Command*, 22.28 *Set User Name Command*, and 22.30 *Set User Password Command*.

- Request data byte 1—[7]
  - 0b-Do not change the following bits in this byte
  - 1b-Enable changing bits in this byte
- Request data byte 1—[6] User restricted to callback
  - 0b-User Privilege Limit is determined by the User Privilege Limit parameter for both callback and non-callback connections.
  - 1b-User Privilege Limit is determined by the User Privilege Limit parameter for callback connections, but is restricted to Callback level for non-callback connections. A user can only initiate a callback when he/she 'calls in' to the BMC, but after the callback connect is made, the user could potentially establish a session as an Operator.
- Request data byte 1—[5] User link authentication enable/disable. This is used to enable/disable a user's name and password information for link authentication. Link authentication itself is a global setting for the channel and is enabled/disabled via the serial or moden configuration parameters.
  - 0b-disable user for link authentication
  - 1b-enable user for link authentication
- Request data byte 1—User IPMI Messaging enable/disable. This is used to enable/disable a user's name and password information for IPMI messaging. In this case, *IPMI Messaging* means the ability to execute generic IPMI commands that are not associated with a particular payload type. For example, if you disable IPMI Messaging for a user, but that user is enabled for activating the SOL payload type, IPMI commands associated with SOL and session management, such as *Get SOL Configuration parameters* and *Close Session* are available, but generic IPMI commadns such as *Get SEL Time* are not.
  - 0b-disable user for link authentication
  - 1b-enable user for link authentication
- Request data byte 2—User ID
  - [7:6] reserved
  - [5:0] User ID. 00000b = reserved
- Request data byte 3—User limits
  - [7:6] reserved
  - [3:0] User Privilege Limit. This determines the maximum privilege level that the user can to switch to on the specified channel.
    - 0h-reserved
    - 1h-Callback
    - 2h-User
    - 3h-Operator
    - 4h-Adminstrator
    - 5h-OEM Proprietary
    - Fh-NO ACCESS

- Request data byte (4)—User Session Limit. Optional—Sets how many simultaneous sessions are activated with the username associated with the user. If not supported, the username activates as many simultaneous sessions as the implementation supports. If an attempt is made to set a non-zero value, a CCh "invalid data field" error returns.
    - [7:4]-Reserved
    - [3:0]-User simultaneous session limit. 1=based. oh=only limited by the implementations support for simultaneous sessions.
- Response data byte 1—Completion code

  ⓘ **NOTE:** If the user access level is set higher than the privilege limit for a given channel, the implementation does not return an error completion code. If required, It is up to the software to check the channel privilege limits set using the `Set Channel Access` command and provide notification of any mismatch.

Set User Name Command

- Request date byte 1—User ID
    - [7:6]-reserved
    - [5:0]-User ID. 000000b-reserved. User ID 1 is permanently associated with User 1, the null user name.
- Request date byte 2:17—User Name String in ASCII, 16 bytes maximum. Strings with fewer then 16 characters terminate with a null (00h) character. The 00h character is padded to 16 bytes. When the string is read back using the `Get User Name` command, those bytes return as 0s.
- Response data byte 1—Completion code

Set User Password Command

- Request data byte 1—User ID. For IPMI v20, the BMC supports 20-byte passwords (keys) for all user IDs that have configurable passwords. The BMC maintains an internal tag indicating if the password is set as a 16-byte or 20-byte password. Use a 16-byte password in algorithms that require a 20-byte password. The 16-byte password is padded with 0s to create 20-bytes. If an attempt is made to test a password that is stored as a 20-byte password as a 16-byte password, and vice versa, the `test password` operation returns a `test failed` error completion code. You cannot use a password stored as a 20-byte password to establish an IPMI v1.5 session. You must set the password as a 16-byte password to configure the same password for both IPMI v20 and IPMI v1.5 access. The password is padded with 0s as necessary. Use the test password operation to determine if a password is stored as 16-bytes or 20-bytes.
- Request data byte 2—
    - [7:2] Reserved
    - [1:0] Operation
        - 00b-disable user
        - 01b-enable user-10b-set password
        - 11b-test password. This compares the password data give in the request with the presently stored password and returns an OK completion code if it matches. Otherwise, an error completion code returns.
- Request data byte 3:18—For 16-byte passwords. Password data. This is a fixed-length required filed used for setting and testing password operations. If the user enters the password as an ASCII string, it must be null (00h) terminated 00h padded if the string is shorter than 16 bytes. This field is not needed for the `disable user` or `enable user` operation. If the field is present, the BMC ignores the data.
- Request data byte 3:22—For 20-byte passwords. This is a fixed-length required filed used for setting and testing password operations. If the user enters the password as an ASCII string, it must be null (00h) terminated 00h padded if the string is shorter than 20 bytes. This field is not needed for the `disable user` or `enable user` operation. If the field is present, the BMC ignores the data.
- Response data byte 1—Completion code. Generic plus the following command-specific completion codes:
    - 80h-mandatory password test failed. Password size is correct but the password data does not match the stored value.
    - 81h-mandatory password test failed. Wrong password size.

Firewall

To set a firewall, use the `set firewall configuration` command. Use parameters 0–3 to add the iptables rules and 4–7 to remove the iptables rules.

- NetFN—0x32
- Command—0x76

- Request data Byte 1—parameter selector
- Request data Byte 2—State selector
- Request data Byte 3:N—Configuration parameter data
- Response data Byte 1—Completion code
  - 80h—Parameter not supported
  - 81h—Invalid time (start/stop time)
  - 82h—Attempt to write read-only parameter
  - 83h—Attempt to access HTTP Port 80

To set the firewall configuration state, use the following:

Table 17. Firewall set parameters

Type specific param	#	Parameter data
To set the command to DROP	00	Parameter to drop packets. Parameter 0–3 uses this state to add the rules to drop the packets based on the IP address/port number or ange of IP addresses/port numbers. Use parameter 4–7 to remove the rule.
To set the command to ACCEPT	01	Parameter to accept packets. Parameter 0–3 uses this state to add the rules to accept the packets based on the IP address/port number or ange of IP addresses/port numbers. Use parameter 4–7 to remove the rule.

To set the firewall parameters, use the following:

Table 18. Firewall parameters

Parameter	#	Parameter data
Add the IPv4 address rule	0	Data 1:4—IP address ● MS-byte first. This is an IPv4 address that is blocked or unblocked based on the state.
Add the range of IPv4 addresses rule	1	Data 1:8—IP address range ● [1:4]—Starting IP address from which IPs are blocked or unblocked based on the state. ● [5:8]—Ending IP address until IPs are blocked or unblocked based on the state. For example, if the IP address is x1.x2.x3.x4, the format is: ● 1st byte = x1 ● 2nd byte = x2 ● 3rd byte = x3 ● 4th byte = x4
Add the IPv4 port number rule	2	Data 1:—Protocol TCP/UDP ● 0 = TCP ● 1 = UDP ● 2 = both TCP and UDP ● Data 2:3—port number ● [2:3]—MX byte first. Port number blocked or unblocked based on the state.
Add the Pv4 port number range rule	3	Data 1:—Protocol TCP/UDP

Table 18. Firewall parameters (continued)

Parameter	#	Parameter data
		- 0 = TCP - 1 = UDP - 2 = both TCP and UDP - Data 2:5—port range - [2:3]—Port number from the ports blocked or unblocked based on the state. - [4:5]—Port number till ports are blocked or unblocked based on the state.
Remove the IPv4 address rule	4	Data 1:4—IP address - MS-byte first. This is the IPv4 address type that is blocked or unblocked based on state.
Remove the range of IPv4 addresses rule	5	Data 1:8—IP address range - [1:4]—Starting IP address that is blocked or unblocked based on the state. - [5:8]—Ending IP address that is blocked or unblocked based on the state. For example, if the IP address is x1.x2.x3.x4, the format is: - 1st byte = x1 - 2nd byte = x2 - 3rd byte = x3 - 4th byte = x4
Remove the IPv4 port number rule	6	Data 1:—Protocol TCP/UDP - 0 = TCP - 1 = UDP - 2 = both TCP and UDP - Data 2:3—port number - [2:3]—Port number from the ports blocked or unblocked based on the state.
Remove the IPv4 port range rule	7	Data 1:—Protocol TCP and UDP - 0 = TCP - 1 = UDP - 2 = both TCP and UDP - Data 2:5—port range - [2:3]—Port number from the ports blocked or unblocked based on the state. - [4:5]—Port number till ports are blocked or unblocked based on the state.
Flush IPv4 and IPv6 iptable	8	Flush all the rules set using iptables and ip6tables.
Drop all	9	Add iptables rules to block IPv4 and IPv6 traffic to the BMC. The state selector is not used. - Data1: Protocol - Bit 7:2—Reserved

Table 18. Firewall parameters (continued)

Parameter	#	Parameter data
		- Bit 1—IPv6 - Bit 0—IPv4
Remove drop all rule	10	Remove iptables rules to block IPv4 and IPv6 traffic to the BMC. The state selector is not used. - Data1: Protocol - Bit 7:2—Reserved - Bit 1—IPv6 - Bit 0—IPv4
Add IPv4 address with timeout rule	11	Data 1:4—IP address - MS-byte first. The IPv4 address type blocked or unblocked based on the state. - Date 5:10—Start time - [5:6]—Year - LS-byte first if little endian system. Two-byte data required to form year. - 7—month - 8—date - 9—hour - 10—minute - Date 11-16—stop time - [11:12]—Year - LS-byte first if little endian system. Two-byte data required to form year. - 13—month - 14—date - 15—hour - 16—minute
Add IPv4 range of addresses with timeout rule	12	Data 1:8—IP address - [1:4]—Starting IP address blocked or unblocked based on the state. - [5:8]—Ending IP address till IPs are blocked or unblocked based on the state. - Date 9:14—Start time - [9:10]—Year - LS-byte first if little endian system. Two-byte data required to form year. - 11—month - 12—date - 13—hour - 14—minute - Date 15-20—Stop time - [15:16]—Year - LS-byte first if little endian system. Two-byte data required to form year.
Add the IPv4 port number with timeout rule	13	Data 1—Protocol TCP and UDP - 0 = TCP - 1 = UDP - 2 = both TCP and UDP - Data 2:3—port number

Table 18. Firewall parameters (continued)

Parameter	#	Parameter data
		● [2:3]—Port number from the ports blocked or unblocked based on the state. ● Date 4:9—Start time ● [4:5]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 6—month ● 7—date ● 8—hour ● 9—minute ● Date 10-15—stop time ● [10:11]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 12—month ● 13—date ● 14—hour ● 15—minute
Add the IPv4 port range with timeout rule	14	Data 1:—Protocol TCP and UPD ● 0 = TCP ● 1 = UDP ● 2 = both TCP and UDP ● Data 2:5—port number ● [2:3]—Port number from the ports blocked or unblocked based on the state. ● [4:5]—Port number till the ports blocked or unblocked based on the state. ● Date 6:11Start time ● [6:7]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 8—month ● 9—date ● 10—hour ● 11—minute ● Date 12-17—stop time ● [12:13]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 14—month ● 15—date ● 16—hour ● 17—minute
Remove the IPv4 address with timeout rule	15	Data 1:4—IP address ● MS-byte first. The IPv4 address type blocked or unblocked based on the state. ● Date 5:10—Start time ● [5:6]—Year ● LS-byte first if little endian system. Two-byte data required to form year.

Table 18. Firewall parameters (continued)

Parameter	#	Parameter data
		• 7—month • 8—date • 9—hour • 10—minute • Date 11-16—stop time • [11:12]—Year • LS-byte first if little endian system. Two-byte data required to form year. • 13—month • 14—date • 15—hour • 16—minute
Remove the range IPv4 address with timeout rule	16	Data 1:8—IP address • [1:4]—Starting IP address blocked or unblocked based on the state. • [5:8]—Ending IP address till IPs are blocked or unblocked based on the state. • Date 9:14—Start time • [9:10]—Year • LS-byte first if little endian system. Two-byte data required to form year. • 11—month • 12—date • 13—hour • 14—minute • Date 15-20—Stop time • [15:16]—Year • LS-byte first if little endian system. Two-byte data required to form year. • 17—month • 18—date • 19—hour • 20—minute
Remove the IPv4 port number with timeout rule	17	Data 1—Protocol TCP and UDP • 0 = TCP • 1 = UDP • 2 = both TCP and UDP • Data 2:3—port number • [2:3]—Port number from the ports blocked or unblocked based on the state. • Date 4:9—Start time • [4:5]—Year • LS-byte first if little endian system. Two-byte data required to form year. • 6—month • 7—date • 8—hour • 9—minute • Date 10-15—stop time • [10:11]—Year • LS-byte first if little endian system. Two-byte data required to form year.

Table 18. Firewall parameters (continued)

Parameter	#	Parameter data
		● 12—month ● 13—date ● 14—hour ● 15—minute
Remove the IPv4 port number range with timeout rule	18	Data 1:—Protocol TCP and UPD ● 0 = TCP ● 1 = UDP ● 2 = both TCP and UDP ● Data 2:5—port number ● [2:3]—Port number from the ports blocked or unblocked based on the state. ● [4:5]—Port number till the ports blocked or unblocked based on the state. ● Date 6:11Start time ● [6:7]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 8—month ● 9—date ● 10—hour ● 11—minute ● Date 12-17—stop time ● [12:13]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 14—month ● 15—date ● 16—hour ● 17—minute
Drop all IPv4 or IPv6 with timeout rule	19	Add iptables rules to block IPv4 and IPv6 traffic to the BMC. The state selector is not used. ● Data1: Protocol ● Bit 7:2—Reserved ● Bit 1—IPv6 ● Bit 0—IPv4 ● Date 2:7—Start time ● [2:3]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 4—month ● 5—date ● 6—hour ● 7—minute ● Date 8:13—Stop time ● [8:9]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 10—month ● 11—date ● 12—hour ● 13—minute

Table 18. Firewall parameters (continued)

Parameter	#	Parameter data
Remove drop all Ipv4 or IPv6 with timeout rule	20	Add iptables rules to block IPv4 and IPv6 traffic to the BMC. The state selector is not used. ● Data1: Protocol ● Bit 7:2—Reserved ● Bit 1—IPv6 ● Bit 0—IPv4 ● Date 2:7—Start time ● [2:3]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 4—month ● 5—date ● 6—hour ● 7—minute ● Date 8:13—Stop time ● [8:9]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 10—month ● 11—date ● 12—hour ● 13—minute
Add IPv6 address with timeout rule	21	Data 1:16—IPv6 address ● MS-byte first. The IPv6 address type blocked or unblocked based on the state. ● Date 7:22—Start time ● [17:18]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 19—month ● 20—date ● 21—hour ● 22—minute ● Date 23-28—stop time ● [23:24]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 25—month ● 26—date ● 27—hour ● 28—minute
Add IPv6 address range with timeout rule	22	Data 1:16—IPv6 address range ● [1:16]—Port number from the ports blocked or unblocked based on the state. ● [17:32]—Port number till the ports blocked or unblocked based on the state. ● Date 33:38—Start time ● [33:34]—Year ● LS-byte first if little endian system. Two-byte data required to form year.

Table 18. Firewall parameters (continued)

Parameter	#	Parameter data
		• 35—month • 36—date • 37—hour • 38—minute • Date 39:44—stop time • [39:40]—Year • LS-byte first if little endian system. Two-byte data required to form year. • 41—month • 42—date • 43—hour • 44—minute
Remove the IPv6 address with timeout rule	23	Data 1:16—IPv6 address • MS-byte first. The IPv4 address type blocked or unblocked based on the state. • Date 17:22—Start time • [17:18]—Year • LS-byte first if little endian system. Two-byte data required to form year. • 19—month • 20—date • 21—hour • 22—minute • Date 23-28—stop time • [23:24]—Year • LS-byte first if little endian system. Two-byte data required to form year. • 25—month • 26—date • 27—hour • 28—minute
Remove the Ipv6 address range with timeout rule	24	Data 1:16—IPv6 address range • [1:16]—Port number from the ports blocked or unblocked based on the state. • [17:32]—Port number till the ports blocked or unblocked based on the state. • Date 33:38—Start time • [33:34]—Year • LS-byte first if little endian system. Two-byte data required to form year. • 35—month • 36—date • 37—hour • 38—minute • Date 39:44—stop time • [39:40]—Year • LS-byte first if little endian system. Two-byte data required to form year. • 41—month • 42—date • 43—hour

Table 18. Firewall parameters (continued)

Parameter	#	Parameter data
		● 44—minute
Add the IPv6 port number with timeout rule	25	Data 1—Protocol TCP and UDP ● 0 = TCP ● 1 = UDP ● 2 = both TCP and UDP ● Data 2:3—port number ● [2:3]—Port number from the ports blocked or unblocked based on the state. ● Date 4:9—Start time ● [4:5]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 6—month ● 7—date ● 8—hour ● 9—minute ● Date 10-15—stop time ● [10:11]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 12—month ● 13—date ● 14—hour ● 15—minute
Add the IPv6 port number range with timeout rule	26	Data 1—Protocol TCP and UDP ● 0 = TCP ● 1 = UDP ● 2 = both TCP and UDP ● Data 2:5—port number ● [2:3]—Port number from the ports blocked or unblocked based on the state. ● [4:5]—Year ● Date 6:11—Start time ● [6:7]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 8—month ● 9—date ● 10—hour ● 11—minute ● Date 12-17—stop time ● [12:13]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 14—month ● 15—date ● 16—hour ● 17—minute
Remove the IPv6 port number with timeout rule	27	Data 1—Protocol TCP and UDP ● 0 = TCP ● 1 = UDP

Table 18. Firewall parameters (continued)

Parameter	#	Parameter data
		● 2 = both TCP and UDP ● Data 2:3—port number ● [2:3]—Port number from the ports blocked or unblocked based on the state. ● [4:9]—Year ● Date 4:9—Start time ● [4:5]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 6—month ● 7—date ● 8—hour ● 9—minute ● Date 10-15—stop time ● [10:11]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 12—month ● 12—date ● 14—hour ● 15—minute
Remove the IPv6 port range with timeout rule	28	Data 1—Protocol TCP and UDP ● 0 = TCP ● 1 = UDP ● 2 = both TCP and UDP ● Data 2:5—port number ● [2:3]—Port number from the ports blocked or unblocked based on the state. ● [4:5]—Year ● Date 6:11—Start time ● [6:7]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 8—month ● 9—date ● 10—hour ● 11—minute ● Date 12-17—stop time ● [12:13]—Year ● LS-byte first if little endian system. Two-byte data required to form year. ● 14—month ● 15—date ● 16—hour ● 17—minute
Add the IPv6 address rule	29	Data 1:16—IPv6 address. ● MS-byte first. This is an IPv6 address that is blocked or unblocked based on state.
Add the IPv6 address range rule	30	Data 1:16—IPv6 address range

Table 18. Firewall parameters (continued)

Parameter	#	Parameter data
		● [1:16]—Starting IP address from which IPs are blocked or unblocked based on the state. ● [17.32]—Ending IP address until IPs are blocked or unblocked based on the state.
Remove the IPv6 address rule	31	Data 1:16—IPv6 address ● MS-byte first. This is an IPv6 address that is blocked or unblocked based on state.
Remove the IPv6 address range rule	32	Data 1:16—IPv6 address range ● [1:16]—Starting IP address from which IPs are blocked or unblocked based on the state. ● [17.32]—Ending IP address until IPs are blocked or unblocked based on the state.
Add the IPv6 port number rule	33	Data 1—Protocol TCP and UDP ● 0 = TCP ● 1 = UDP ● 2 = both TCP and UDP ● Data 2:3—port number ● [2:3]—Port number from the ports blocked or unblocked based on the state.
Add the IPv6 port number range rule	34	Data 1—Protocol TCP and UDP ● 0 = TCP ● 1 = UDP ● 2 = both TCP and UDP ● Data 2:5—port number ● [2:3]—Port number from the ports blocked or unblocked based on the state. ● [4:5]—Port number till the ports are blocked or u nblocked based on the state.
Remove the IPv6 port number rule	35	Data 1—Protocol TCP and UDP ● 0 = TCP ● 1 = UDP ● 2 = both TCP and UDP ● Data 2:3—port number ● [2:3]—Port number from the ports blocked or unblocked based on the state.
Remove the IPv6 port number range rule	36	Data 1—Protocol TCP and UDP ● 0 = TCP ● 1 = UDP ● 2 = both TCP and UDP ● Data 2:5—port number ● [2:3]—Port number from the ports blocked or unblocked based on the state.

Table 18. Firewall parameters (continued)

Parameter	#	Parameter data
		● [4:5]—Port number till the ports are blocked or u nblocked based on the state.

Event log

To get the IPMI event log, use the `ipmitool sel list` command.

To clear the event log, use the `ipmitool sel clear` command.

For IPMI event log settings, see the *IPMI Specification v2.0* chapter 31.4 *Reserve SEL Command* and 31.5 *Get SEL Entry Command*.

Reserve system event log (SEL) command

Use reserve SEL to set the present owner of the SEL. This reservation provides a limited amount of protection on repository access from the IPMB when you delete or incrementally read records. Use get SEL to read the SEL repository.

- Response data byte 1—Completion code
  - 81h—cannot execute the command, SEL erase in progress
- Response data byte 2—Reservation ID, LS byte 0000h reserved.
- Response data byte 3—Reservation ID, SM byte

Get SEL command

- Request data byte 1:2—Reservation IS, LS byte first. Only required for a partial get. Otherwise use 0000h.
- Request data byte 3:4—SEL record ID, LS byte first.
  - 0000h=GET FIRST ENTRY
  - FFFFh=GET LAST ENTRY
- Request data byte 5—Offset into record
- Request data byte 6—Bytes to read. FFH means read entire record.
- Response data byte 1—Completion code. Returns an error completion code if the SEL is empty.
  - 81h=cannot execute the command, SEL erase in progress.
- Response data byte 2:3—Next SEL record ID. LS byte first (returns FFFFh if the record just returned is the last record).
  - **NOTE:** FFFFh is not allowed as the record ID of an actual record. For example, the record ID in Record Data for the last record cannot be FFFFh.
- Response data byte 4:N—Record data, 16 bytes for the entire record.

Set LOG configuration command

To set the system or audit log configuration, use the `set LOG configuration` command.

- Netfn—0x32
- Command—0x68

Audit log configuration

- Request data byte 1—Cmd
  - [7:2] Reserved
  - [1:0] 01h–Audit log
- Request data byte 1—Status
  - [7:2] Reserved

  - [1:0] 01h–Disabled
  - 01h–Enable local
- Response data byte 1—00h-success
  - CCh=invalid data field
  - FFh=unspecified error
- Response data byte 1—Cmd
  - [7:2] Reserved
  - [1:0] 00h–system log
- Response data byte 2—Status
  - [7:2] Reserved
  - [1:0] 01h–Disabled
  - 01h–Enable local
- Response data byte 3-70 for REMOTE (68 bytes) or 3-7 for LOCAL (5 bytes)—ENABLED REMOTE
  - **NOTE:** These request data bytes are required only when you enable either the local or remote system log.

```
64bytes : Hostname (ASCII)
Remote syslog server
4bytes : port number
```

To set the remote server ip address to 10.0.124.22 and port to 770:

```
ipmitool -I lanplus -H xx.xx.xx.xx -U xxx -P xxx raw 0x32 0x68 0x00
0x02 0x31 0x30 0x2e 0x30 0x2e 0x31 0x32 0x34 0x2e 0x32 0x32 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x02 0x03 0x00 0x00
ENABLED LOCAL
4bytes : Size (LSB first)
size of each file to rotate (file size is from 3 to 65535 KB)
1bytes : Rotate
Number of back-up files after logrotate (maximum 1 file)
```

To set the file size to 100 bytes, use the IPMI command:

```
ipmitool -I lanplus -H xx.xx.xx.xx -U xxx -P xxx raw 0x32 0x68 0x00
0x01 0x64 0x00 0x00 0x00 0x01
```

Default configuration restore

Use configuration restore to start the configuration from scratch. For example, use configuration restore to remove the old configuration and start over if you reinstall the system or move the system to a new location.

Restore default configuration command

- NetFn—0x32
- Command—0x66
- Response byte 1—Completion code

Default settings

The following tables list the default settings after a switch restore.

Table 19. Default settings after a switch restore

Name	Setting
BMC OOB	Enabled for non-TAA and disabled for TAA

Table 19. Default settings after a switch restore (continued)

Name	Setting
BMC OOB — after restore to default	Disabled
BMC WEB	Enabled for non-TAA and disabled for TAA
BMC WEB — after restore to default	Disabled
BMC console	Enabled for non-TAA and disabled for TAA
BMC console — after restore to default	Enabled for non-TAA and disabled for TAA
BMC supports unique password	Yes
BMC OOB username/password	admin/<*SERVICE TAG*>! (Enter the service tag in upper case.)
BMC OOB username/password — after restore to default	admin/**admin** (but only valid for the IPMI commands for `mc info` and change administrator password)
BMC WEB	admin/<*SERVICE TAG*>! (Enter the service tag in upper case.)
BMC WEB — after restore to default	admin/**admin** (but WEB GUI displays a message to confirm change of the administrator password)
BMC console login username/password	sysadmin/<*SERVICE TAG*>! (Enter the service tag in upper case.)
BMC console login username/password — after restore to default	sysadmin/superuser

Set backup configuration flag

To set the backup flags for the `manage BMC confirguration` command, use the `set backup configuration flag` command.

- NetFN—0x32
- Command—0xF3
- Request data byte 1:2—Byte 1 is the value specifies to back up a configuration feature or not.
  - [7]—Reserved
  - [6]—1b: Backup SNMP. 0b: Do not backup the simple network management protocol (SNMP)
  - [5]—1b: Backup SYSLOC. 0b: Do not backup SYSLOG
  - [4]—1b: Backup KVM. 0b: Do not backup keyboard, video, and mouse (KVM)
  - [3]—1b: Backup NTP. 0b: Do not backup network time protocol (NTP)
  - [2]—1b: Backup IPMI. 0b: Do not backup IPMI
  - [1]—1b: Backup NETWORK And SERVICES. 0b: Do not backup NETWORK And SERVICES
  - [0]—1b: Backup AUTHENTICATION. 0b: Do not backup AUTHENTICATION

  ⓘ **NOTE:** Reserved bits may be updated further based on the requirement.
- Response data byte 1—Completion code
  - 0x83—Authentication feature is not enabled
  - 0x84—NTP feature is not enabled
  - 0x85—KVM feature is not enabled
  - 0x86—SNMP feature is not enabled

5

Host power control

The following are host power control commands:

- `Power Off`—the `ipmitool` powers off
- `Power On`—the `ipmitool` powers on
- `Power Cycle`—the `ipmitool` power cycles
- `Hard Reset`—the `ipmitool` power resets

6

Remote power

This section describes how to remote power cycle the BMC and DIAG OS. It also describes remote `ipmitool` power management.

Topics:

Remote BMC and DIAG OS power cycle

Run `ipmitool` from the BMC serial console command prompt. Enter the service tag number in upper case.

a. Use this command to power cycle a remote system.

```
# ipmitool -H xxx.x.x.x -U admin -P <SERVICE TAG>! power cycle
```

If BMC has a different administrator who is configured, replace the `-u` and `-p` parameters with `admin\<`*`SERVICE TAG`*`>!`.

NOTE: The username and password **must be** `admin\<`*`SERVICE TAG`*`>!`.

- `-u`—admin
- `-p`—<*SERVICE TAG*>!

```
~ # ipmitool -H xxx.x.x.x -U admin -P <SERVICE TAG>! power status
Chassis Power is on
~ # ipmitool -H xxx.x.x.x -U admin -P <SERVICE TAG>! power cycle
Chassis Power Control: Cycle
~ # POWER CYCLE CHASSIS
POWER OFF CHASSIS
POWER ON CHASSIS
[22313.320000] LPC RESET
PDK LPC Reset is invoked
Current fan number: 5
[22318.510000] LPC RESET
PDK LPC Reset is invoked
Current fan number: 5
[610 : 685 INFO]Power Consumption Mode Change Cmd:2147440117

[610 : 685 INFO]Power Consumption Mode Value Updated (0):

OEM storage.get_SEL_Timezone
[22370.210000] UsbConfigureHS(): USB Device 0 is running in High Speed
[22370.320000] HUB port 0 reset
[22370.320000] UsbConfigureHS(): USB Device 0 is running in High Speed
Starting to Read Current PostCode buffer...
Current Post Codes are ...
0x01 0x02 0x03 0x04 0x05 0x06 0x19 0xa1 0xa3 0xa3 0xa7 0xa9 0xa7 0xa7 0xa7 0xa8 0xa9
0xa9 0xaa 0xae 0xaf 0xe0 0xe1 0xe4 0xe3 0xe5 0xb0 0xb0 0xb1 0xb1 0xb4 0xb2 0xb3 0xb3
0xb3 0xb6 0xb6 0xb6 0xb6 0xb6 0xb6 0xb7 0xb7 0xbe 0xb7 0xb7 0xb7 0xb8 0xb8 0xb8 0xb8
0xb8 0xb8 0xb9 0xb9 0xba 0xb9 0xbb 0xbb 0xbb 0xbb 0xbb 0xbb 0xbb 0xbb 0xbb 0xbb 0xb7
0xbc 0xbc 0xbc 0xbc 0xbc 0xbf 0xe6 0xe7 0xe8 0xe9 0xeb 0xec 0xed 0xee 0x4f 0x61 0x9a
0x78 0x68 0x70 0x79 0xd1 0xd2 0xd4 0x91 0x92 0x94 0x94 0x94 0x94 0x94 0x94 0x94 0x94
0x94 0x94 0x94 0x94 0x94 0x94 0x95 0x96 0xef 0x92 0x92 0x92 0x99 0x91 0xd5 0x92 0x92
0x92 0x92 0x97 0x98 0x9d 0x9c 0xb4 0xb4 0xb4 0xb4 0xb4 0x92 0xa0 0xa2 0xa2 0xa2 0x99
0x92 0x92 0x92
[610 : 685 INFO]Power Consumption Mode Change Cmd:2147440116

[610 : 685 INFO]Power Consumption Mode Value Updated (1):
```

Remote `ipmitool` DIAG OS power management

Use `ipmitool` to reboot and power off from the BMC serial console command prompt.

> ⓘ **NOTE:** When building the kernel for the Z9432F-ON switch, the kernel flag `CONFIG_IPMI_POWEROFF` must be set to `n`. Having this flag that is turned on causes the kernel to send the `ipmi` command to power off the switch when the CPU is powered off. For example, pressing the push button for five seconds powers off the CPU. But pressing the push button for five seconds with the flag set to `n`, powers off the switch to Standby mode. The only way to power on the switch is to issue the `ipmi` command from a remote station to the BMC.

Enter the service tag number in upper case.

1. Run `ipmitool` from the BMC serial console command prompt.
   a. Use this command to reboot the remote system:

      ```
      ipmitool -I lanplus -H xxx.x.x.x -U admin -P <SERVICE TAG>! power reset
      ```

   b. Use this command to power off the remote system:

      ```
      ipmitool -I lanplus -H xxx.x.x.x -U admin -P <SERVICE TAG>! power off
      ```

   c. Use this command to power on the remote system:

      ```
      ipmitool -I lanplus -H xxx.x.x.x -U admin -P <SERVICE TAG>! power on
      ```

   d. Use this command to cold reboot the remote system:

      ```
      ipmitool -I lanplus -H xxx.x.x.x -U admin -P <SERVICE TAG>! power cycle
      ```

2. Boot into the BIOS settings.

   ```
   ipmitool -I lanplus -H xxx.x.x.x -U admin -P <SERVICE TAG>! chassis bootparam set
   bootflag force_bios
   ```

   ```
   ipmitool -I lanplus -H xxx.x.x.x -U admin -P <SERVICE TAG>! power reset
   ```

7

Access system health sensors

To check sensor information, use the following command:

```
root@dellemc-diag-os:~# ipmitool sensor list
```

To change the sensor threshold, see the *IPMI Specification v2.0* chapter 35.8 *Set Sensor Thresholds Command*.

- Request data byte 1—Sensor number, FFH=reserved
- Request data byte 2—
  - [7:6] - reserved. Write as 00b
  - [5] - 1b=set upper non-recoverable threshold
  - [4] - 1b=set upper critical threshold
  - [3] - 1b=set upper non-critical threshold
  - [2] - 1b=set lower non-recoverable threshold
  - [1] - 1b=set lower critical threshold
  - [0] - 1b=set lower non-critical threshold
- Request data byte 3—lower non-critical threshold. Ignored if bit 0 of byte 2 = 0
- Request data byte 4—lower critical threshold. Ignored if bit 1 of byte 2 = 0
- Request data byte 5—lower non-recoverable threshold. Ignored if bit 2 of byte 2 = 0
- Request data byte 6—upper non-critical threshold. Ignored if bit 3 of byte 2 = 0
- Request data byte 7—upper critical threshold value. Ignored if bit 4 of byte 2 = 0
- Request data byte 8—upper non-recoverable threshold value. Ignored if bit 5 of byte 2 = 0
- Response data byte 1—Completion code

ipmitool sensors

```
root@dellemc-diag-os:~#  ipmitool sensor list
PT_Mid_temp      | 32.000     | degrees C | ok     | na     | na        | na     | 78.000 | 80.000 | 85.000
NPU_Near_temp    | 29.000     | degrees C | ok     | na     | na        | na     | na     | na     | na
PT_Left_temp     | 28.000     | degrees C | ok     | na     | na        | na     | na     | na     | na
PT_Right_temp    | 30.000     | degrees C | ok     | na     | na        | na     | na     | na     | na
ILET_AF_temp     | 26.000     | degrees C | ok     | na     | na        | na     | na     | na     | na
PSU1_AF_temp     | 24.000     | degrees C | ok     | na     | na        | na     | 61.000 | 64.000 | na
PSU2_AF_temp     | 25.000     | degrees C | ok     | na     | na        | na     | na     | na     | na
PSU1_temp        | 33.000     | degrees C | ok     | na     | na        | na     | na     | na     | na
PSU2_temp        | na         | degrees C | na     | na     | na        | na     | na     | na     | na
CPU_temp         | 31.000     | degrees C | ok     | na     | na        | na     | 90.000 | 94.000 | na
FAN1_Rear_rpm    | 9120.000   | RPM       | ok     | na     | 1080.000  | na     | na     | na     | na
FAN2_Rear_rpm    | 9000.000   | RPM       | ok     | na     | 1080.000  | na     | na     | na     | na
FAN3_Rear_rpm    | 9000.000   | RPM       | ok     | na     | 1080.000  | na     | na     | na     | na
FAN4_Rear_rpm    | 9000.000   | RPM       | ok     | na     | 1080.000  | na     | na     | na     | na
FAN1_Front_rpm   | 10080.000  | RPM       | ok     | na     | 1080.000  | na     | na     | na     | na
FAN2_Front_rpm   | 10080.000  | RPM       | ok     | na     | 1080.000  | na     | na     | na     | na
FAN3_Front_rpm   | 10080.000  | RPM       | ok     | na     | 1080.000  | na     | na     | na     | na
FAN4_Front_rpm   | 10080.000  | RPM       | ok     | na     | 1080.000  | na     | na     | na     | na
PSU1_rpm         | 9000.000   | RPM       | ok     | na     | na        | na     | na     | na     | na
PSU2_rpm         | na         | RPM       | na     | na     | na        | na     | na     | na     | na
PSU_Total_watt   | 110.000    | Watts     | ok     | na     | na        | na     | na     | na     | na
PSU1_stat        | 0x0        | discrete  | 0x0180| na     | na        | na     | na     | na     | na
PSU2_stat        | 0x0        | discrete  | 0x0380| na     | na        | na     | na     | na     | na
PSU1_In_watt     | 110.000    | Watts     | ok     | na     | na        | na     | na     | na     | na
PSU1_In_volt     | 205.700    | Volts     | ok     | na     | na        | na     | na     | na     | na
PSU1_In_amp      | 0.480      | Amps      | ok     | na     | na        | na     | na     | na     | na
PSU1_Out_watt    | 90.000     | Watts     | ok     | na     | na        | na     | na     | na     | na
PSU1_Out_volt    | 12.400     | Volts     | ok     | na     | na        | na     | na     | na     | na
PSU1_Out_amp     | 7.500      | Amps      | ok     | na     | na        | na     | na     | na     | na
PSU2_In_watt     | na         | Watts     | na     | na     | na        | na     | na     | na     | na
PSU2_In_volt     | na         | Volts     | na     | na     | na        | na     | na     | na     | na
PSU2_In_amp      | na         | Amps      | na     | na     | na        | na     | na     | na     | na
PSU2_Out_watt    | na         | Watts     | na     | na     | na        | na     | na     | na     | na
PSU2_Out_volt    | na         | Volts     | na     | na     | na        | na     | na     | na     | na
PSU2_Out_amp     | na         | Amps      | na     | na     | na        | na     | na     | na     | na
ACPI_stat        | 0x0        | discrete  | 0x0180| na     | na        | na     | na     | na     | na
FAN1_prsnt       | 0x0        | discrete  | 0x0180| na     | na        | na     | na     | na     | na
FAN2_prsnt       | 0x0        | discrete  | 0x0180| na     | na        | na     | na     | na     | na
```

```
FAN3_prsnt      | 0x0       | discrete  | 0x0180| na    | na       | na    | na     | na     | na
FAN4_prsnt      | 0x0       | discrete  | 0x0180| na    | na       | na    | na     | na     | na
FAN1_Rear_stat  | 0x0       | discrete  | 0x0080| na    | na       | na    | na     | na     | na
FAN2_Rear_stat  | 0x0       | discrete  | 0x0080| na    | na       | na    | na     | na     | na
FAN3_Rear_stat  | 0x0       | discrete  | 0x0080| na    | na       | na    | na     | na     | na
FAN4_Rear_stat  | 0x0       | discrete  | 0x0080| na    | na       | na    | na     | na     | na
FAN1_Front_stat | 0x0       | discrete  | 0x0080| na    | na       | na    | na     | na     | na
FAN2_Front_stat | 0x0       | discrete  | 0x0080| na    | na       | na    | na     | na     | na
FAN3_Front_stat | 0x0       | discrete  | 0x0080| na    | na       | na    | na     | na     | na
FAN4_Front_stat | 0x0       | discrete  | 0x0080| na    | na       | na    | na     | na     | na
INTER_5.0V_volt | 4.900     | Volts     | ok    | 4.200 | 4.500    | 4.700 | 5.200  | 5.500  | 5.700
INTER_3.3V_volt | 3.300     | Volts     | ok    | 2.800 | 3.000    | 3.100 | 3.500  | 3.600  | 3.800
FPGA_1.0V_volt  | 0.990     | Volts     | ok    | 0.850 | 0.900    | 0.950 | 1.050  | 1.100  | 1.150
FPGA_1.2V_volt  | 1.190     | Volts     | ok    | 1.020 | 1.080    | 1.140 | 1.260  | 1.320  | 1.380
FPGA_1.8V_volt  | 1.780     | Volts     | ok    | 1.530 | 1.620    | 1.710 | 1.890  | 1.980  | 2.070
FPGA_3.3V_volt  | 3.200     | Volts     | ok    | 2.800 | 3.000    | 3.100 | 3.500  | 3.600  | 3.800
BMC_2.5V_volt   | 2.400     | Volts     | ok    | 2.100 | 2.200    | 2.300 | 2.600  | 2.800  | 2.900
BMC_1.15V_volt  | 1.150     | Volts     | ok    | 0.980 | 1.030    | 1.090 | 1.210  | 1.270  | 1.320
BMC_1.2V_volt   | 1.210     | Volts     | ok    | 1.020 | 1.080    | 1.140 | 1.260  | 1.320  | 1.380
SWITCH_6.8V_volt| 7.000     | Volts     | ok    | 5.800 | 6.100    | 6.400 | 7.200  | 7.500  | 7.800
SWITCH_3.3V_volt| 3.300     | Volts     | ok    | 2.800 | 3.000    | 3.100 | 3.500  | 3.600  | 3.800
SWITCH_1.8V_volt| 1.790     | Volts     | ok    | 1.530 | 1.620    | 1.710 | 1.890  | 1.980  | 2.070
USB_5.0V_volt   | 4.900     | Volts     | ok    | 4.200 | 4.500    | 4.700 | 5.200  | 5.500  | 5.700
NPU_1.2V_volt   | 1.190     | Volts     | ok    | 1.020 | 1.080    | 1.140 | 1.260  | 1.320  | 1.380
NPU_VDDCORE_volt| 0.800     | Volts     | ok    | 0.700 | 0.720    | 0.740 | 0.910  | 0.930  | 0.950
NPU_VDDANLG_volt| 0.790     | Volts     | ok    | 0.680 | 0.720    | 0.760 | 0.840  | 0.880  | 0.920
BMC boot        | 0x0       | discrete  | 0x0180| na    | na       | na    | na     | na     | na
SEL_sensor      | 0x0       | discrete  | 0x1080| na    | na       | na    | na     | na     | na
```

8

IPMI commands

ⓘ **NOTE:** All commands are subject to change as the `ipmi` commands evolve over time.

- `ipmi raw`
- `ipmi i2c`
- `ipmi ian print`
- `ipmi ian set`
- `ipmi ian alert`
- `ipmi chassis status`
- `ipmi chassis selftest`
- `ipmi chassis power status`
- `ipmi chassis power up / on`
- `ipmi chassis power down / off`
- `ipmi chassis power cycle`
- `ipmi chassis identify`
- `ipmi chassis poh`
- `ipmi chassis restart_cause`
- `ipmi chassis policy list`
- `ipmi chassis policy always-on`
- `ipmi chassis policy previous`
- `ipmi chassis policy always-off`
- `ipmi chassis bootparam get` *`<param #>`*
- `ipmi chassis bootparam set bootparam set bootflag` *`<device>`*
  - **Legal devices are:**
  - `none` : No override
  - `force_pxe` : Force PXE boot
  - `force_disk` : Force boot from default hard-drive
  - `force_safe` : Force boot from default hard-drive, request Safe Mode
  - `force_diag` : Force boot from diagnostic partition
  - `force_cdrom` : Force boot from CD/DVD
  - `force_bios` : Force boot into BIOS setup
  - **Legal options are:**
  - `help` : Print this message
  - `PEF` : Clear valid bit on reset/power cycle caused by PEF
  - `timeout` : Automatically clear boot flag valid bit on timeout
  - `watchdog`: Clear valid bit on reset/power cycle caused by watchdog
  - `reset` : Clear valid bit on push button reset/soft reset
  - `power` : Clear valid bit on power up via power push button or wake event
  - Any Option may be prepended with `no-` to invert sense of operation
- `ipmi chassis bootdev` *`<device>`* `bios`
- `ipmi event` *`<num>`*
- `ipmi event file` *`<filename>`*
- `ipmi event event`*`<sensorid><state> [event_dir]`*
- `ipmi mc reset` *`<warm | cold>`*
- `ipmi mc guid`
- `ipmi mc info`
- `ipmi mc watchdog get`
- `ipmi mc watchdog reset`

- ipmi mc watchdog off
- ipmi mc selftest
- ipmi mc getenables
- ipmi mc getenabled *<item><option=on | off>*
- ipmi mc getsysinfo *<argument>* system_fw_version
- ipmi mc getsysinfo *<argument>* primary_os_name
- ipmi mc getsysinfo *<argument>* os_name
- ipmi mc getsysinfo *<argument>* system_nam
- ipmi mc setsysinfo *<argument>* system_fw_version
- ipmi mc setsysinfo *<argument>* primary_os_name
- ipmi mc setsysinfo *<argument>* os_name
- ipmi mc setsysinfo *<argument>* system_nam
- ipmi sdr list | elist [option] all
- ipmi sdr list | elist [option] full
- ipmi sdr list | elist [option] compact
- ipmi sdr list | elist [option] event
- ipmi sdr list | elist [option] mcloc
- ipmi sdr list | elist [option] fru
- ipmi sdr list | elist [option] generic
- ipmi sdr type [option] *<Senfor_Type>*
- ipmi sdr type [option] list
- ipmi sdr get *<Sensor_ID>*
- ipmi sdr info
- ipmi sdr entity *<Entity_ID>*[.*<Instance_ID>*]
- ipmi sdr dump *<file>*
- ipmi sensor list
- ipmi sensor thresh *<id><threshold><setting>*
- ipmi sensor get *<id>*
- ipmi sensor reading *<id>*
- ipmi fru print [fru id]
- ipmi fru read *<fru id><fru file>*
- ipmi fru write *<fru id><fru file>*
- ipmi fru fru internaluse
- ipmi sel info
- ipmi sel clear
- ipmi sel delete *<id>*
- ipmi sel list
- ipmi sel elist
- ipmi sel get
- ipmi sel add *<filename>*
- ipmi sel time get
- ipmi sel time set
- ipmi sel save *<filename>*
- ipmi sel redraw *<filename>*
- ipmi sel writeraw *<filename>*
- ipmi pef info
- ipmi pef status
- ipmi pef policy list
- ipmi pef policy enable
- ipmi pef policy disable
- ipmi pef policy create
- ipmi pef policy delete
- ipmi sol info [*<channel number>*]
- ipmi sol set *<parameter><value>*[channel]

- ipmi sol payload *<enable|disable|status>*[channel][userid]
- ipmi sol activate [*<usesolkeepalive|n)eepalive>*][instance=*<number>*]
- ipmi sol deactivate [instance=*<number>*]
- ipmi sol looptest [*<loop times>*[*<loop interval(in ms)>*[*<instance>*]]]
- ipmi user summary [*<channel number>*]
- ipmi user list [*<channel number>*]
- ipmi user set name *<user id><username>*
- ipmi user set password *<user id>*[*<password><16|20>*]
- ipmi user disable *<user id>*
- ipmi user enable *<user id>*
- ipmi user priv *<user id><privilege level>*[*<channel number>*]
- ipmi user test *<user id><16|20>*[*<password>*]
- ipmi channel authcap *<channel number><max privilege>*
- ipmi channel getaccess *<channel number>*[user id]
- ipmi channel setaccess *<channel number><user id>*[callin=on][ipmi=on|off][link=on][privilege=level]
- ipmi channel info [channel number]
- ipmi channel getciphers *<ipmi | sol>*[channel]
- ipmi session info *<active | all | id 0xnnnnnnnn | handle 0xnn>*
- ipmi dcmi discover
- ipmi dcmi power*<command>* reading
- ipmi dcmi power*<command>* get_limit
- ipmi dcmi power*<command>* set_limit
- ipmi dcmi power*<command>* activate
- ipmi dcmi power*<command>* deactivate
- ipmi dcmi sensors
- ipmi dcmi asset_tag
- ipmi dcmi set_asset_tag
- ipmi dcmi get_mc_id_string
- ipmi dcmi set_mc_id_string
- ipmi dcmi get_temp_reading
- ipmi dcmi get_conf_param
- ipmi dcmi set_conf_param
- ipmi dcmi oob_discover
- ipmi shell
- ipmi exec
- ipmi set
  - **Options are:**
  - hostname <host> : Session hostname
  - username <user> : Session username
  - password <pass> : Session password
  - privlvl <level> : Session privilege level force
  - authtype <type> : Authentication type force
  - localaddr <addr> : Local IPMB address
  - targetaddr <addr> : Remote target IPMB address
  - port <port> : Remote RMCP port
  - csv [level] : Enable output in comma-separated format
  - verbose [level] : Verbose level

9

ipmiutil package

NOTE: All commands are subject to change as the `ipmiutil` package evolves over time. For more information about the IPMI utility, use cases, and the newest list of subcommands, see the IPMI website that is hosted by Intel at https://www.intel.com/content/www/us/en/servers/ipmi/ipmi-technical-resources.html.

- `ipmiutil`—a metacommand to invoke each of the following functions:
  - `ipmiutil alarms (ialarms)`—show and set the front panel alarms, including light emitting diodes (LEDs) and relays.
  - `ipmiutil config (iconfig)`—list, save, or restore the BMC configuration parameters.
  - `ipmiutil cmd (icmd)`—send specific IPMI commands to the BMC for testing and debug purposes.
  - `ipmiutil discover (idiscover)`—discover the available IPMI LAN nodes on a subnet.
  - `ipmiutil events (ievents)`—a stand-alone utility to decode IPMI events and platform event trap (PET) data.
  - `ipmiutil firewall (ifirewall)`—discover the available IPMI LAN nodes on a subnet.
  - `ipmiutil fru (ifru)`—show decoded field replaceable units (FRU) board/product inventory data and write FRU asset tags.
  - `ifruset`—show decoded FRU inventory data and set a FRU product area.
  - `iseltime`—show and set the IPMI system event log (SEL) time according to the system time.
  - `ipmiutil fwum (ifwum)`—OEM firmware update manager extensions
  - `ipmiutil getevt (igetevent)`—receive any IPMI events and display them.
  - `ipmiutil health (ihealth)`—check and report the basic health of the IPMI BMC.
  - `ipmiutil hpm (ihpm)`—hardware platform management (HPM) firmware update manager extensions
  - `ipmiutil lan (ilan)`—show and configure the local area network (LAN) port and platform event filter (PEF) table to generate BMC LAN alerts using the firmware events.
  - `ipmiutil picmg (ipicmg)`—discover the available IPMI LAN nodes on a subnet.
  - `ipmiutil reset (ireset)`—cause the BMC to hard reset or power down the system.
  - `ipmiutil sel (isel)`—a tool to show the firmware system event log (SEL) records.
  - `ipmiutil sensor (isensor)`—show the sensor data records (SDR), readings, and thresholds.
  - `ipmiutil serial (iserial)`—a tool to show and configure the BMC serial port for various modes, for example, Terminal mode.
  - `ipmiutil sol (isol)`—start or stop an IPMI serial-over-LAN console session.
  - `ipmiutil sunoem (isunoem)`—Sun OEM functions.
  - `ipmiutil wdt (iwdt)`—show and set the watchdog timer.
  - `checksel`—cron script using `impiutil sel` to check the SEL, write new events to the OS system log, and clear the SEL if nearly full.
  - `ipmi_port`—daemon to bind the remote management control protocol (RMCP) port and sleep to prevent Linux portmap from stealing the RMCP port.
  - `ipmi_wdt`—initial script to restart the watchdog timer every 60 seconds using the cron.
  - `ipmi_asy`—initial script that runs the `ipmiutil getevt -a` command for a remote shutdown.
  - `ipmi_evt`—initial script the runs the `imput getevt -s` command for monitoring events.
  - `hpiutil/*`—parallel hardware platform interface (HPI) utilities that conform to the SA Forum Hardware Platform Interface. Also a basis of the `openhpi/clients/`
  - `bmc_panic`—a kernel patch to save information if the system panics. The command is found in the OpenIPMI driver in kernels 2.6 and greater and in the Intel IMB driver in version 28 and greater

10

Access FRU data

To check field replacement unit (FRU) data, use the following command:

```
root@dellemc-diag-os:~# ipmitool fru print
```

For more FRU information, see the *IPMI Specification v2.0* chapter 34.2 *Read FRU Data Command*.

- Request data 1—FRU device ID. FFh=reserved
- Request data 2—FRU inventory offset to read, LS byte
- Request data 3—FRU inventory offset to read, LS byte
  - Offset is in bytes or words-per-device. Access type returned in the `Get FRU Inventory Area Info` command output.
- Request data 4—Count to read. Count is '1' based.
- Response data 1—Completion code. Generic, plus the command specifics:
  - 81h=FRU device busy. The requested cannot be completed because the logical FRU device is in a state where FRU information is temporarily unavailable. This state is possibly due to a loss of arbitration if the FRU implements as a device on a shared bus.
  - Software can elect to retry the operation after a minimum of 30 milliseconds if the code returns. Dell Technologies recommends that the management controllers incorporate built-in retry mechanisms. Generic IPMI does not take advantage of this completion code.
- Response data 2—Count returned. Count is '1' based.
- Response data 3:2=N—Requested data

ipmitool FRUs

```
root@dellemc-diag-os:~#  ipmitool fru print
FRU Device Description : Builtin FRU Device (ID 0)
Board Mfg Date         : Sat May 19 06:04:00 2018
Board Mfg              : CES00
Board Product          : <platform>
Board Serial           : CN01XR4WCES0085F0002
Board Part Number      : 01XR4WX01
Product Manufacturer   : CES00
Product Name           : <platform>
Product Asset Tag      : GDNRG02
FRU Device Description : PSU1_fru (ID 1)
Board Mfg Date         : Fri Mar 30 21:30:00 2018
Board Mfg              : DELL
Board Product          : PWR SPLY,750W,AC,PS/IO,DELTA
Board Serial           : CNDED0083U00D5
Board Part Number      : 0HXWNFA00FRU
Device Description : PSU2_fru (ID 2)
Board Mfg Date         : Fri Mar 30 22:12:00 2018
Board Mfg              : DELL
Board Product          : PWR SPLY,750W,AC,PS/IO,DELTA
Board Serial           : CNDED0083U00BY
Board Part Number      : 0HXWNFA00FRU
Device Description : FAN1_fru (ID 3)
Board Mfg Date         : Mon Jan  1 00:00:00 1996
Board Serial           : CN07R5RFCES0084N0081
Board Part Number      : 07R5RFX01FRU
Device Description : FAN2_fru (ID 4)
Board Mfg Date         : Mon Jan  1 00:00:00 1996
Board Serial           : CN07R5RFCES0084N0080
Board Part Number      : 07R5RFX01FRU
Device Description : FAN3_fru (ID 5)
Board Mfg Date         : Mon Jan  1 00:00:00 1996
Board Serial           : CN07R5RFCES0084N0083
Board Part Number     : 07R5RFX01FRU
Device Description : FAN4_fru (ID 6)
Board Mfg Date        : Mon Jan  1 00:00:00 1996
Board Serial          : CN07R5RFCES0084N0082
Board Part Number     : 07R5RFX01
```

11

Dell EMC support

The Dell EMC support site provides documents and tools to help you use Dell EMC equipment and mitigate network outages. Through the support site you can obtain technical information, access software upgrades and patches, download available management software, and manage your open cases. The Dell EMC support site provides integrated, secure access to these services.

To access the Dell EMC support site, go to www.dell.com/support/. To display information in your language, scroll down to the bottom of the web page and select your country from the drop-down menu.

- To obtain product-specific information, enter the 7-character service tag, which is known as a luggage tag, or 11-digit express service code of your switch and click **Submit**.
- To view the platform service tag or express service code, pull out the luggage tag on the upper-right side of the platform or retrieve it remotely using the `ipmitool -H <bmc ip address> -I lanplus -U <user name> -P <password> fru` command.
- To receive more technical support, click **Contact Us**. On the Contact Information web page, click **Technical Support**.

To access switch documentation, go to www.dell.com/support/ and enter your switch type.

To search for drivers and downloads, go to **Drivers & Downloads** tab for your switch.

To participate in Dell EMC community blogs and forums, go to www.dell.com/community.

A

Firmware update

BMC, BIOS, and CPLD firmware update is required before you install the Z9432F-ON switch.

⚠ **CAUTION: The preferred method of updating the BMC code is through the ONIE Firmware Updater. For firmware update instructions, see the *Dell EMC PowerSwitch Firmware Updater Release Notes*. Only use the following update method if there is an issue with the Firmware Updater.**

To update the firmware from a remote machine, use the BMC LAN interface.

You can also update the firmware in the local host operating system using the USB interface. The USB interface is between the BMC and the microprocessor. When using the USB, the BMC simulates a virtual USB device, then Yafuflash sends the image to the BMC using the USB bus. Typically the update process completes in five minutes.

For more information about Yafuflash, see the *Dell EMC PowerSwitch Z9432F-ON Release Notes*.

Table 20. Firmware update

Tool	Medium	Operating system	Comments
Yafuflash	USB	Linux	Recommended—Host operating system only
Yafuflash	LAN	Windows or Linux	Internal use only

The BMC virtual USB is disabled by default. Enable the USB before you update the firmware.

Update BMC by USB interface

Enable BMC virtual USB:

```
 ipmitool raw 0x32 0xaa 0x00 (Then wait 15s)
```

Update Main BMC:

```
./Yafuflash -cd -mse 1 rom.ima
```

Update BMC by LAN interface

1. Ensure that the client Linux or Windows machine can ping the BMC IP address.
2. Open a command window.
3. Update the main BMC using the following command. Enter the service tag number in uppercase.

```
./Yafuflash -nw -ip bmc_ip -u admin -p <SERVICE TAG>! -mse 1 bmc.ima
```

Topics:

- USB-based firmware update
- BIOS access process
- Update BMC in DIAG OS
- Network interface settings
- Configure BMC network manually

USB-based firmware update

Update your BMC, BIOS, and CPLD firmware with the following commands:

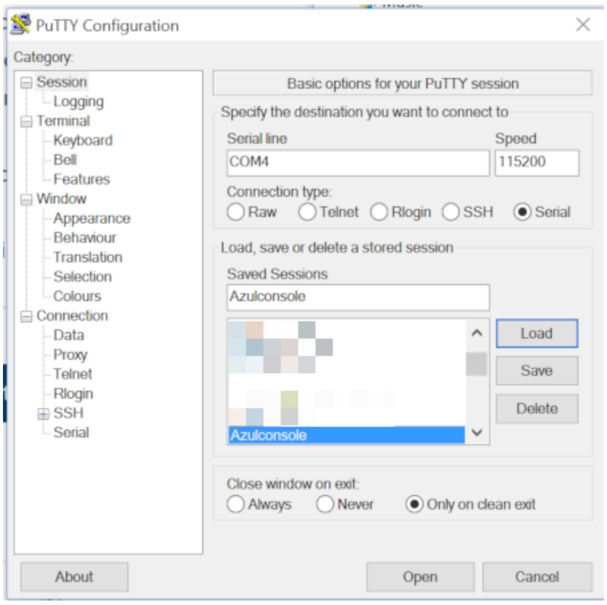
Power on the switch

Plug in the power cable to the back of the switch. The switch powers up immediately.

Create a serial console connection

To establish a console connection, use a universal serial bus (USB)-to-RS-232 connection from a USB port to the switch console port.

NOTE: The baud rate is 115200.



Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM4

Speed: 115200

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

Saved Sessions: Azulconsole

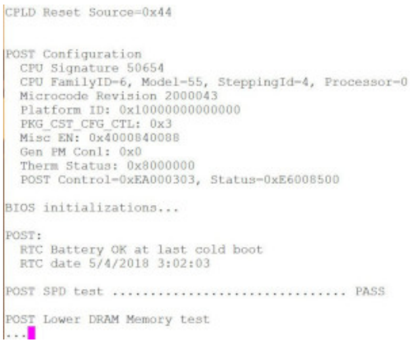
Azulconsole

Close window on exit: ○ Always ○ Never ● Only on clean exit

BIOS access process

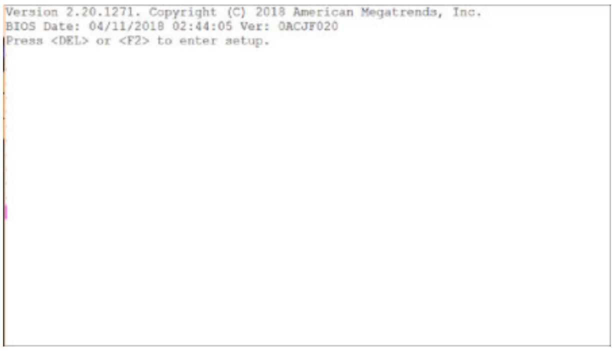
1. Press **delete** after the `POST Lower DRAM Memory test` appears on the screen. Continue pressing **delete** to progress to the `BIOS setup and configuration` screen.

   NOTE: If the `BIOS setup and configuration` screen window passes, power off and power on the platform again to restart the boot up process.



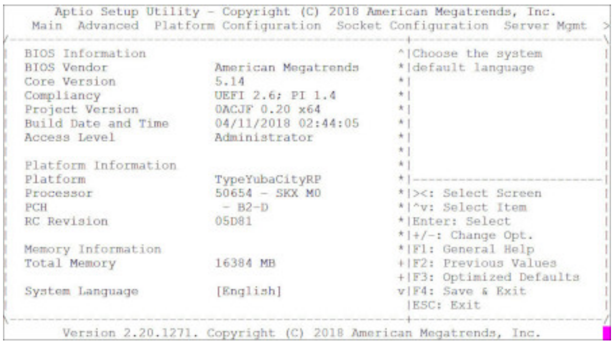
```
CPLD Reset Source=0x44


POST Configuration
  CPU Signature 50654
  CPU FamilyID=6, Model=55, SteppingId=4, Processor=0
  Microcode Revision 2000043
  Platform ID: 0x1000000000000000
  PKG_CST_CFG_CTL: 0x3
  Misc EN: 0x4000840088
  Gen PM Con1: 0x0
  Therm Status: 0x8000000
  POST Control=0xEA000303, Status=0xE6008500

BIOS initializations...

POST:
  RTC Battery OK at last cold boot
  RTC date 5/4/2018 3:02:03

POST SPD test ................................ PASS

POST Lower DRAM Memory test
...
```

Figure 2. Initial boot up screen



```
Version 2.20.1271. Copyright (C) 2018 American Megatrends, Inc.
BIOS Date: 04/11/2018 02:44:05 Ver: 0ACJF020
Press <DEL> or <F2> to enter setup.
```

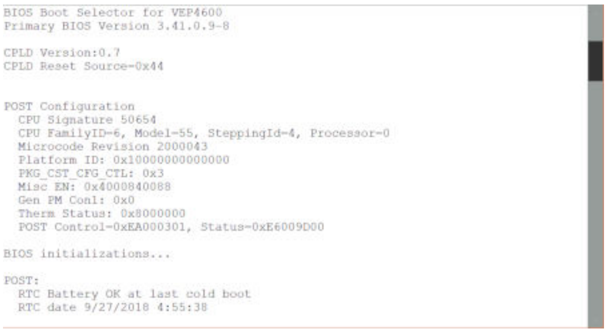
Figure 3. Boot up screen



```
      Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
   Main  Advanced  Platform Configuration  Socket Configuration  Server Mgmt  >
/-------------------------------------------------------+-----------------------------\
|  BIOS Information                                    ^|Choose the system          |
|  BIOS Vendor                 American Megatrends     *|default language           |
|  Core Version                5.14                    *|                           |
|  Compliancy                  UEFI 2.6; PI 1.4        *|                           |
|  Project Version             0ACJF 0.20 x64          *|                           |
|  Build Date and Time         04/11/2018 02:44:05     *|                           |
|  Access Level                Administrator           *|                           |
|                                                      *|                           |
|  Platform Information                                *|                           |
|  Platform                    TypeYubaCityRP          *|---------------------------|
|  Processor                   50654 - SKX M0          *|><: Select Screen          |
|  PCH                          - B2-D                 *|^v: Select Item            |
|  RC Revision                 05D81                   *|Enter: Select              |
|                                                      *|+/-: Change Opt.           |
|  Memory Information                                  *|F1: General Help           |
|  Total Memory                16384 MB                +|F2: Previous Values        |
|                                                      +|F3: Optimized Defaults     |
|  System Language             [English]               v|F4: Save & Exit            |
|                                                       |ESC: Exit                  |
\-------------------------------------------------------+-----------------------------/
        Version 2.20.1271. Copyright (C) 2018 American Megatrends, Inc.
```

Figure 4. BIOS setup and configuration screen

2. Use the scrollbar on the right side of the console window to scroll up to display the BIOS and CPLD versions.



```
BIOS Boot Selector for VEP4600
Primary BIOS Version 3.41.0.9-8

CPLD Version:0.7
CPLD Reset Source=0x44


POST Configuration
  CPU Signature 50654
  CPU FamilyID=6, Model=55, SteppingId=4, Processor=0
  Microcode Revision 2000043
  Platform ID: 0x10000000000000
  PKG_CST_CFG_CTL: 0x3
  Misc EN: 0x4000840088
  Gen PM Con1: 0x0
  Therm Status: 0x8000000
  POST Control=0xEA000301, Status=0xE6009D00

BIOS initializations...

POST:
  RTC Battery OK at last cold boot
  RTC date 9/27/2018 4:55:38
```

Figure 5. Display BIOS and CPLD versions

Update BMC in DIAG OS

Use the following DIAG OS command to update BMC:

```
updatetool -D MAIN-BMC -U -e ./<platform>-BMC-vx.xx.ima
```

NOTE: Switch to the BMC console to monitor the BMC update status. Confirm BMC updates. Reboot the system. Go to the BIOS update.

Update the BMC using the following command:

```
#updatetool -D MAIN-BMC -U - e <BMC_update_filename>
```

Replace *<BMC_update_filename>* with the file from the USB drive that is mounted.

You are prompted for confirmation. Press y and enter to continue. When the update is complete, you must power cycle the system.

```
root@dellemc-diag-os:~# updatetool -D MAIN-BMC -U -e <BMC_update_filename>
disable preserve BIOS configration
 00
Disable device protect

Disable MAIN-BMC protect operation success, wait HW reset
Write image to MAIN-BMC
INFO: Yafu INI Configuration File not found... Default options will not be applied...

Creating IPMI session via USB...Done

---------------------------------------------
YAFUFlash - Firmware Upgrade Utility (Version 4.112.0)
---------------------------------------------
(C)Copyright 2016, American Megatrends Inc.
Image To be updated is (Image-1)
===================================================
               Firmware Details
===================================================
                          RomImage    Image 1     Image 2

   ModuleName Description  Version     Version     Version
1. boot       BootLoader   0.2.000000  0.2.000000  0.2.000000
2. conf       ConfigParams 0.20.000000 0.20.000000 0.20.000000
3. root       Root         0.20.000000 0.20.000000 0.20.000000
4. osimage    Linux OS     0.20.000000 0.20.000000 0.20.000000
5. www        Web Pages    0.20.000000 0.20.000000 0.20.000000
6. testapps                0.20.000000 0.20.000000 0.20.000000
7. ast2500e                1.0.000000  1.0.000000  0.20.0
Existing Image and Current Image are Same
So,Type (Y/y) to do Full Firmware Upgrade or (N/n) to exit
Enter your Option : y

****************************************************
 WARNING!
 FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED.
 PLEASE DO NOT USE THIS FLASH TOOL FROM THE REDIRECTION CONSOLE.
****************************************************
Uploading Firmware Image : 100%... done
Skipping [boot] Module ....
Flashing [conf] Module ....
Flashing  Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [root] Module ....
Flashing  Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [osimage] Module ....
Flashing  Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [www] Module ....
Flashing  Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [testapps] Module ....
Flashing  Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [ast2500e] Module ....
Flashing  Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Resetting the firmware..........
write MAIN-BMC image success
Enable device protect

Update MAIN-BMC image success
root@dellemc-diag-os:~#
```

Network interface settings

Complete the following after the switch boots:

1. Go to the BMC console and check the network interface settings.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 54:BF:64:A9:E7:C9
          inet addr:xxx.xx.xxx.xx  Bcast:xxx.xx.xxx.xxx  Mask:255.255.255.0
          inet6 addr: fe80::56bf:64ff:fea9:e7c9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2495 errors:1 dropped:837 overruns:0 frame:1
          TX packets:442 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:494108 (482.5 KiB)  TX bytes:60152 (58.7 KiB)
          Interrupt:2
```

2. Pin the gateway to confirm that the link is up and functioning.

```
ping xxx.xx.xxx.xxx
PING xxx.xx.xxx.xxx (xxx.xx.xxx.xxx): 56 data bytes
64 bytes from xxx.xx.xxx.xxx: seq=0 ttl=255 time=10.000 ms
64 bytes from xxx.xx.xxx.xxx: seq=1 ttl=255 time=0.000 ms
64 bytes from xxx.xx.xxx.xxx: seq=2 ttl=255 time=0.000 ms
```

Configure BMC network manually

NOTE: The BMC out-of-band (OOB) network or LAN is not enabled for Trade Agreement Act-qualified (TAA) switches. The BMC OOB is enabled for non-TAA-qualified switches.

Use the following to configure the BMC network manually. Enter the service tag number in upper case.

1. Log in to the BMC-IPMI console using your sysadmin/<*SERVICE TAG*>! or superuser credentials.
2. Edit the `/etc/network/interfaces` file.

```
auto lo
iface lo inet loopback
auto  eth0
  iface eth0 inet static
  address xxx.xx.xxx.xx
netmask 255.255.255.0
broadcast xxx.xx.xxx.xxx
gateway xxx.xx.xxx.xxx
```

3. Replace the IP network info with your IP network address, then run the following command to restart network service:

```
/etc/init.d/networking restart
```

If you reboot the BMC, you may lose the network information. In this case, you must start all over again because you do not have the BIOS configured. Without the BIOS configured, each time you reboot BMC, the system fetches the information from BIOS configuration and refreshes the interfaces file.