VEP4600 BMC User Guide

May 2019

DELLEMC

Notes, cautions, and warnings

① | **NOTE: A NOTE indicates important information that helps you make better use of your product.**

⚠ | **CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

⚠ | **WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**

2019 - 05

Rev. A04

Contents

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.**

⚠ **WARNING: Only trained and qualified personnel can install this equipment. Read this guide before you install and power up this equipment. This equipment contains two power cords. Disconnect both power cords before servicing.**

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

CLASS 1
LASER PRODUCT

Figure 1. Class 1 laser product tag

⚠ **WARNING: 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.**

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

Revision	Date	Description
A00	2018-05	Initial release
A01	2018-08	Updated the *Hardware and software support*, *BMC access*, *LAN configuration*, *LAN destinations*, *Add and delete users*, *Reserve SEL command*, *Default configuration restore*, *Access system health sensors*, and *Access FRU data* sections. Added the *ipmiutil package* chapter.
A02	2019-01	WIFI/LTE firmware updates.
A03	2019-02	Firmware requirements, Remote power cycle system.
A04	2019-05	BMC web GUI.

Hardware and software support

For the most current BMC update information, see the *VEP4600 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.

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>`

BMC web GUI

GUI interface for BMC functionality.

The intuitive BMC web browser base GUI permits users to access BMC functionality with the following menus:

- Sensor
- FRU Information
- Logs & Reports
- Settings
- Power Control
- Maintenance
- Sign Out
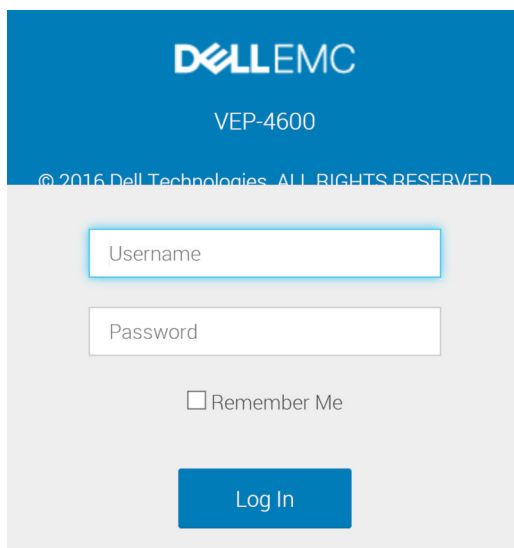
Topics:

- Login
- Dashboard
- FRU information
- Logs & Reports
- Settings
- Power control
- Maintenance

Login

Enter `Username` and `password.`
- Username: admin
- Password: admin

Dashboard

BMC dashboard control panel

Top level monitoring.
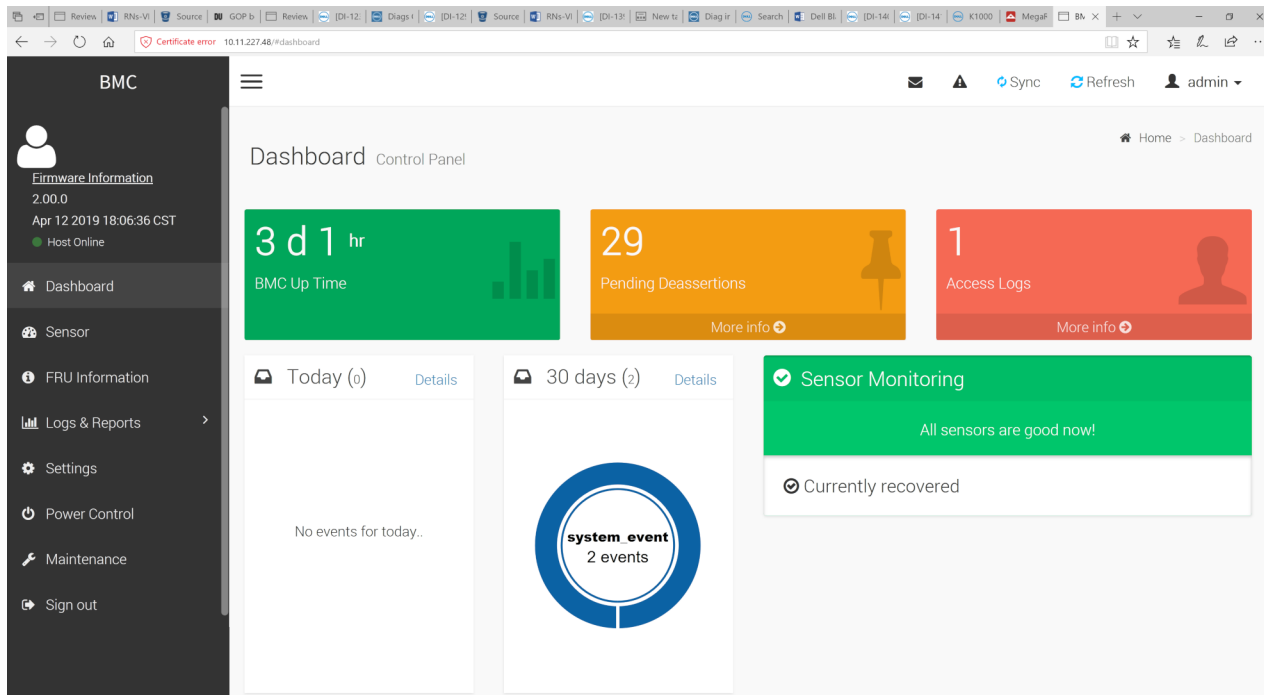
BMC dashboard control panel

FRU information

FRU (Field Replacement Units) sections

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 will be displayed.

FRU screen

Logs & Reports

Contains IPMI event log, System log, and Audit log screens.

IPMI Event Log

IPMI Event Log sections:

- 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.

System Log

System log sections:

• 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.
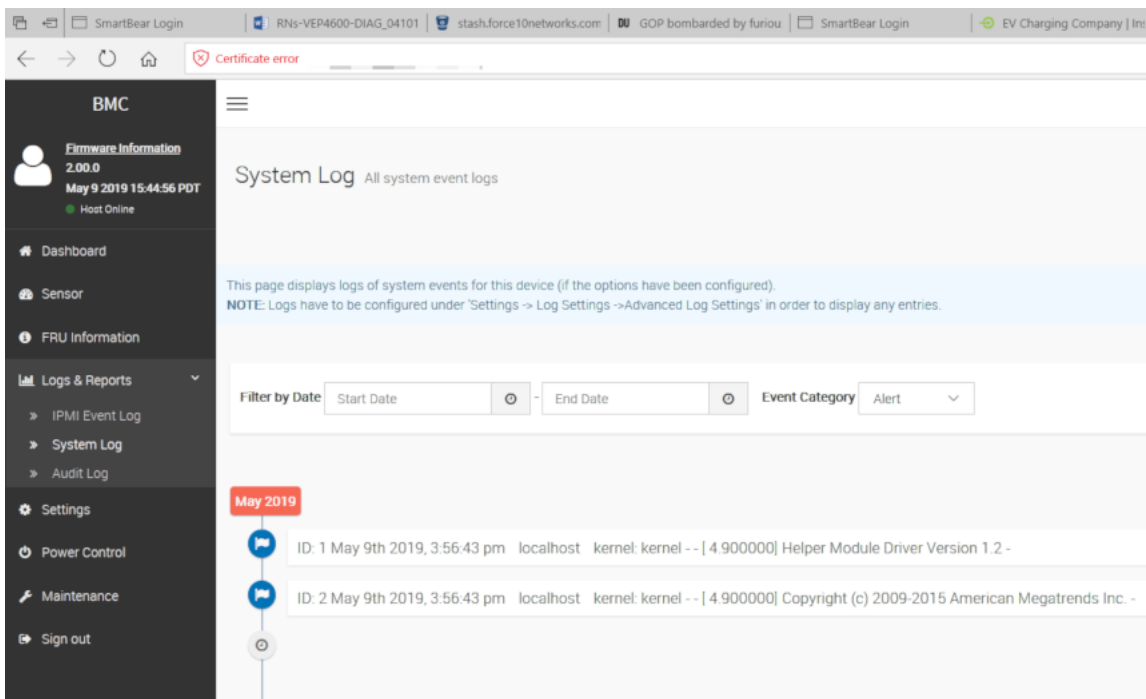
System log screen

Audit Log

Audit log sections:

• 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.
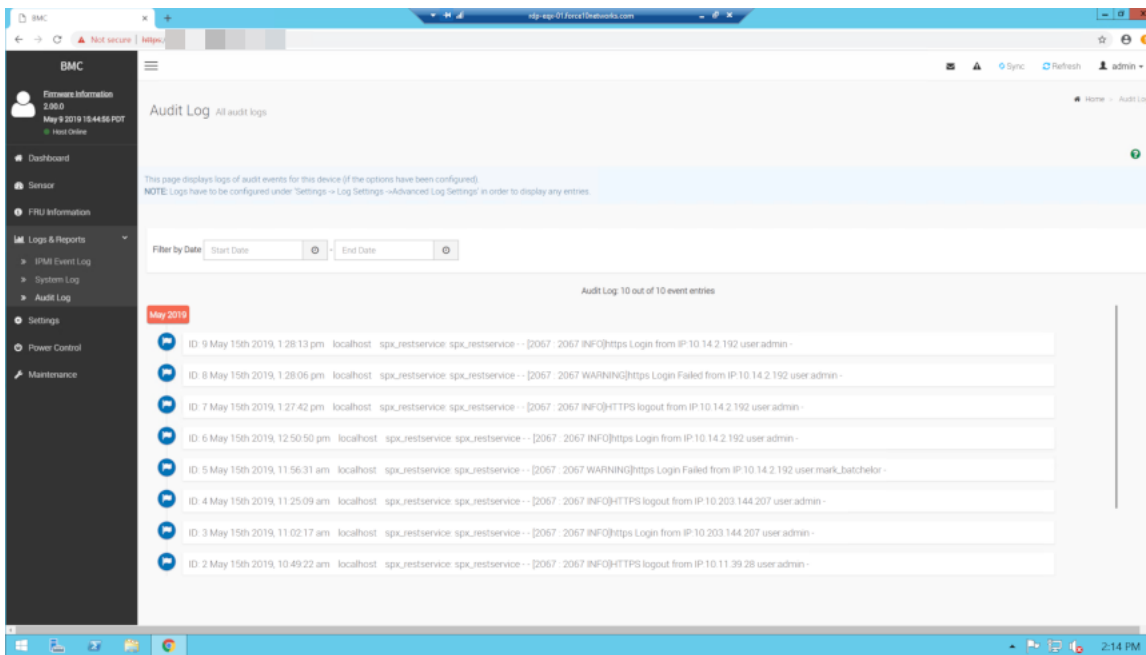
Audit log screen

Settings

The Settings screen include the following sections:

- Date & Time
- External User Services
- Log settings
- Network settings
- PAM order settings
- Platform event filter
- SMTP settings
- SSL settings
- System firewall
- User mnagement
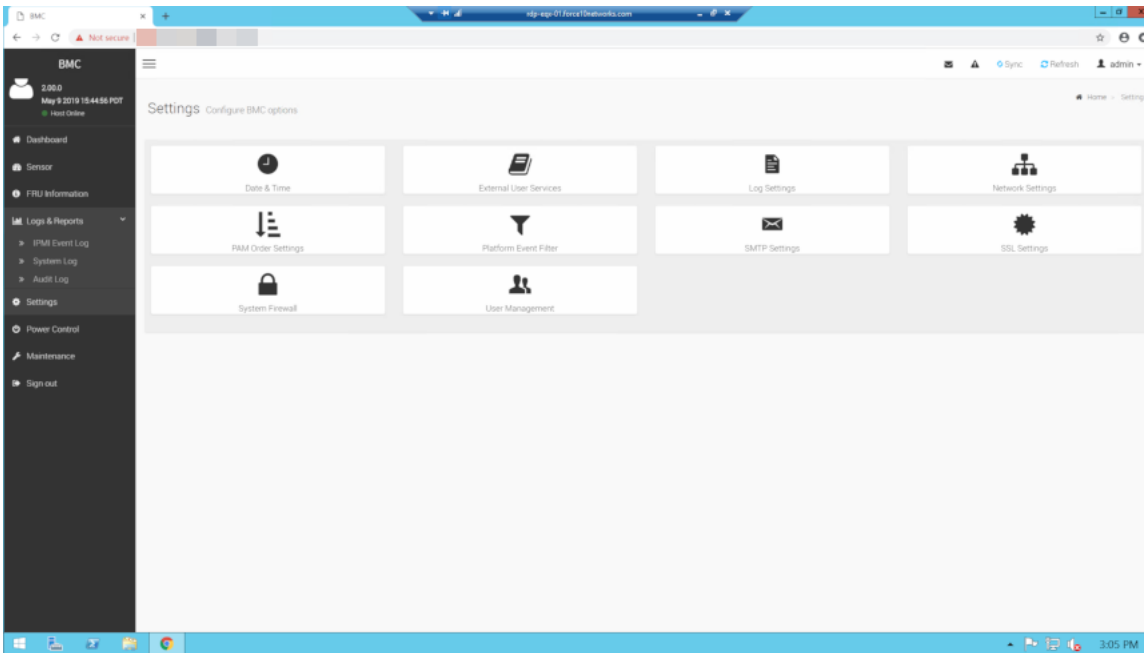
Settings screen

Date & time

Date & time sections:

· ⓘ | **NOTE: If the timezone is selected from the group of manual offset(GMT/ETC timezones), the map selection will be disabled. The TimeZone settings will be reflected only after saving the settings.**

External user services

External user services sections:

• LDAP/E-directory settings
• Active directory settings
• RADIUS settings

Setup each External user service using the options supplied.
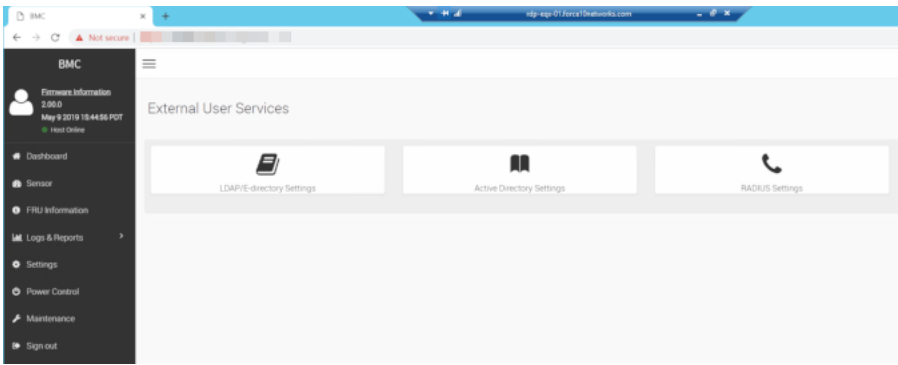
External user services screen

Log settings

Log settings sections:

- SEL Log settings policy
- Advanced log settings

Setup each Log settings section using the options supplied.
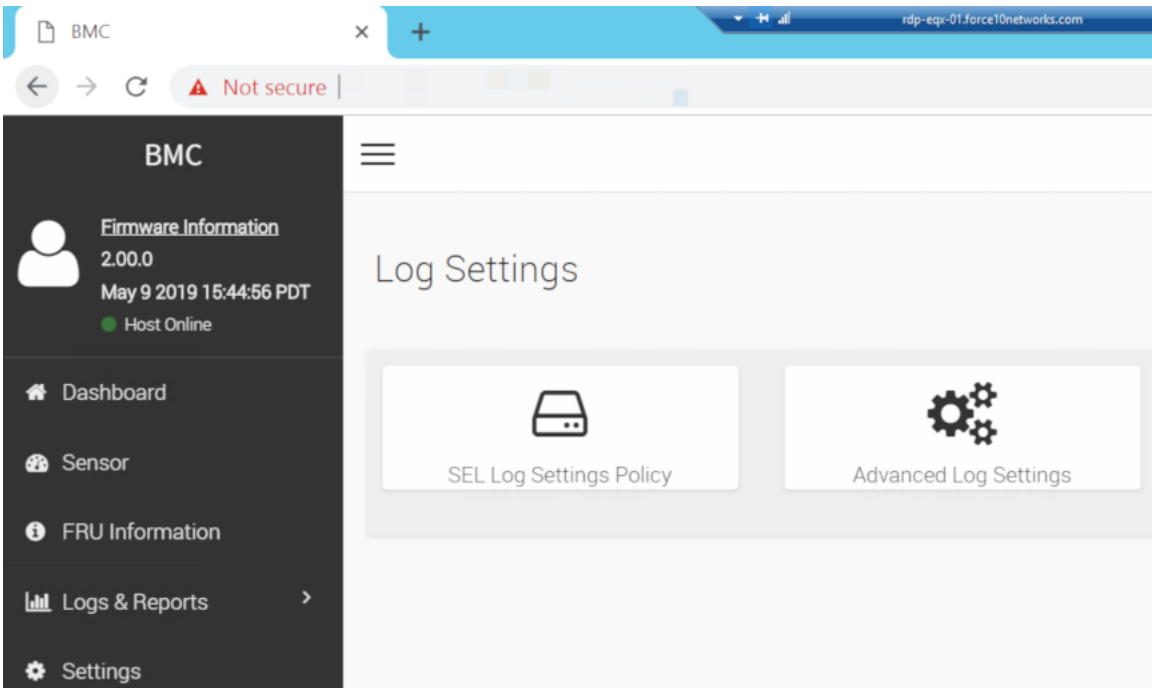
Log settings screen

SEL Log settings

SEL settings:

This field is used to configure the log policy for the event log.
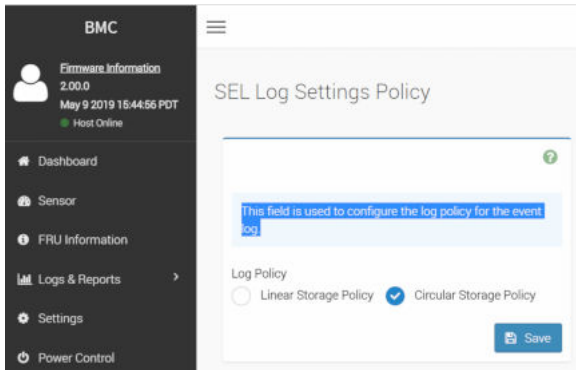
SEL log settings screen

Network settings

Network sections:

- Network IP settings
- Network link configuration
- DNS configuration

Setup each Log settings section using the options supplied.
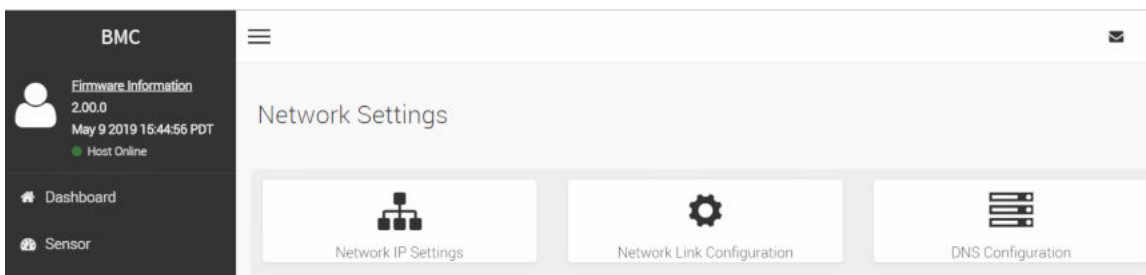
Network settings screen

Network IP settings

Enable LAN

Check this option to enable LAN support for the selected interface.

LAN interface

Select the LAN interface to be configured.

MAC address

This field displays the MAC address of the selected interface (read only).

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 Dynamic Host Configuration Protocol (DHCP).

IPv4 Address

If DHCP is disabled, specify a static Subnet Mask to be configured for the selected interface.

- IP Address consists of four sets of numbers separated by dots as in 'xxx.xxx.xxx.xxx'.
- Each set ranges from 0 to 255.
- First Number must not be 0.

IPv4 Subnet

If DHCP is disabled, specify a static Default Gateway to be configured for the selected interface.

- IP Address consists of four sets of numbers separated by dots as in 'xxx.xxx.xxx.xxx'.
- Each set ranges from 0 to 255.
- First Number must not be 0.

IPv4 Gateway

If DHCP is disabled, specify a static Default Gateway to be configured for the selected interface.

- IP Address consists of four sets of numbers separated by dots as in 'xxx.xxx.xxx.xxx'.
- Each set ranges from 0 to 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 Dynamic HostConfiguration v6 Protocol (DHCPv6).

IPv6 Index

Choose the IPv6 Index.

IPv6 Address

Specify a static IPv6 address to be configured for the selected interface.

Subnet Prefix Length

Specify a static IPv6 address to be configured for the selected interface.

- Value ranges from 0 to 128.

Enable VLAN

Check this option to enable VLAN support for the selected interface.

VLAN ID

Specify the Identification for VLAN configuration.

- Value ranges from 1 to 4094.

ⓘ NOTE: VLAN ID cannot be changed without resetting the VLAN configuration. VLAN ID 0, 4095 are reserved VLAN ID's.

VLAN Priority

Specify the priority for VLAN configuration.

- Value ranges from 0 to 7.

ⓘ NOTE: 7 is the highest priority for VLAN.

Network IP settings screen

Network IP settings screen

PAM order settings

- PAM authentication 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 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

💾 Save

PAM authentication order screen

Platform event filters

- Event filters
- Alert policies
- LAN destinations
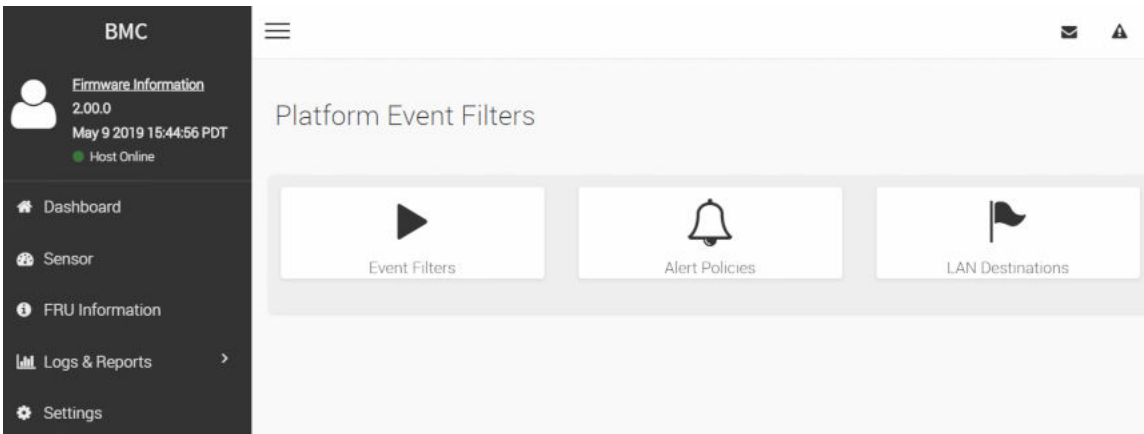
Setup each Platform event filters section using the options supplied.

Platform event filters screen

Event filters

Event filters options:

- All
- Configured
- Unconfigured

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

1. Choose `All` option to view available configured and unconfigured slots.
2. Choose `Configured` option to view available Configured slots which are in Enabled/Disabled.
3. Choose `Unconfigured` option to view available `Unconfigured` or free slots which are denoted by the tilde symbol '~'.
4. Choose `X` icon to delete an event filter from the list.
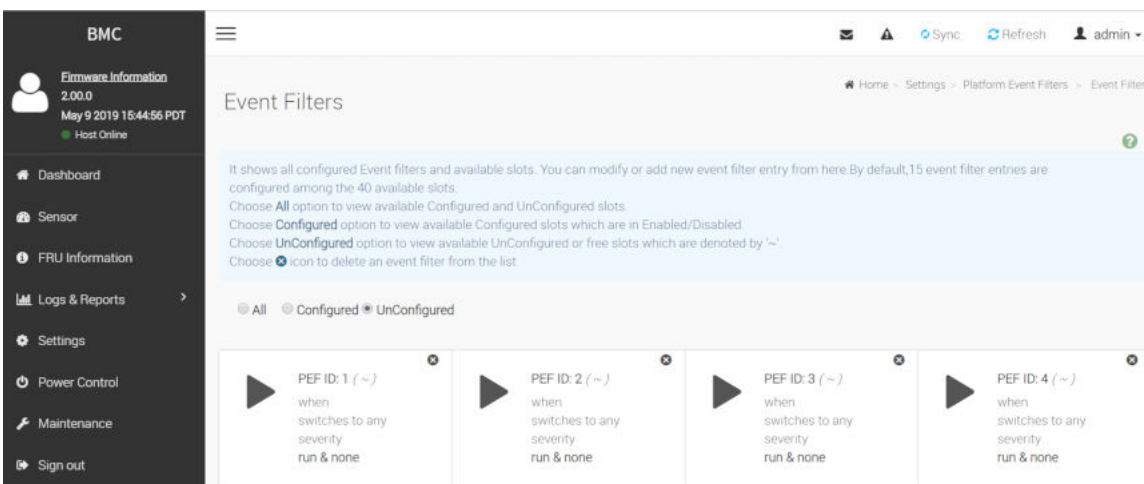
Event filters screen

Event filters

- All
- Configured
- Unconfigured

Displays all configured Event filters and available slots. You can modify or add new event filter entry. By default, fifteen Event filter entries are configured among the 40 available slots.

1 Choose `All` option to view available configured and unconfigured slots.
2 Choose `Configured` option to view available Configured slots which are in Enabled/Disabled.
3 Choose `Unconfigured` option to view available `Unconfigured` or free slots which are denoted by the tilde symbol '~'.
4 Choose `X` icon to delete an event filter from the list.
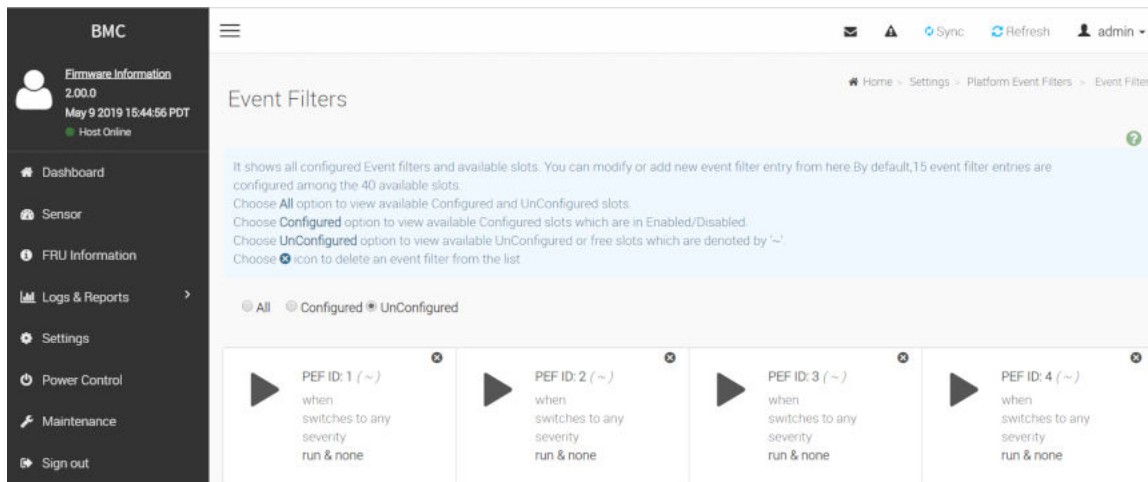
Event filters screen

Alert policies settings

Alert policies settings options:

Policy Group Number

select from the drop-down menu a policy number that was configured in Event filter table.

Enable this alert

Check the option `Enable` to enable the policy settings.

Policy action

Choose from the drop-down menu a Policy set value.

- Always send alert to this destination.
- If alert to previous destination was successful, do not send alert to this destination. Proceed to 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. Proceed to 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. Proceed to 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: LAN Destination have to be configured - under `Configuration->PEF->LAN` Destination.

Event Specific Alert String

Check the box to specify an event-specific Alert String.

Alert String Key

Select from the drop-down menu a set of values, all linked to strings kept in the PEF configuration parameters, to specify which string is to be sent for this Alert Policy entry.

Alert policies settings screen

LAN destinations

LAN destinations sections:

Displays configured LAN destinations and available slots. You can modify or add new LAN destination entry from here.

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

A maximum of 15 slots are available.

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

> (i) **NOTE: Test alert can be sent only when SMTP configuration is enabled. SMTP support can be enabled under `Settings->SMTP`. Also make sure that SMTP server address and port numbers are configured properly.**
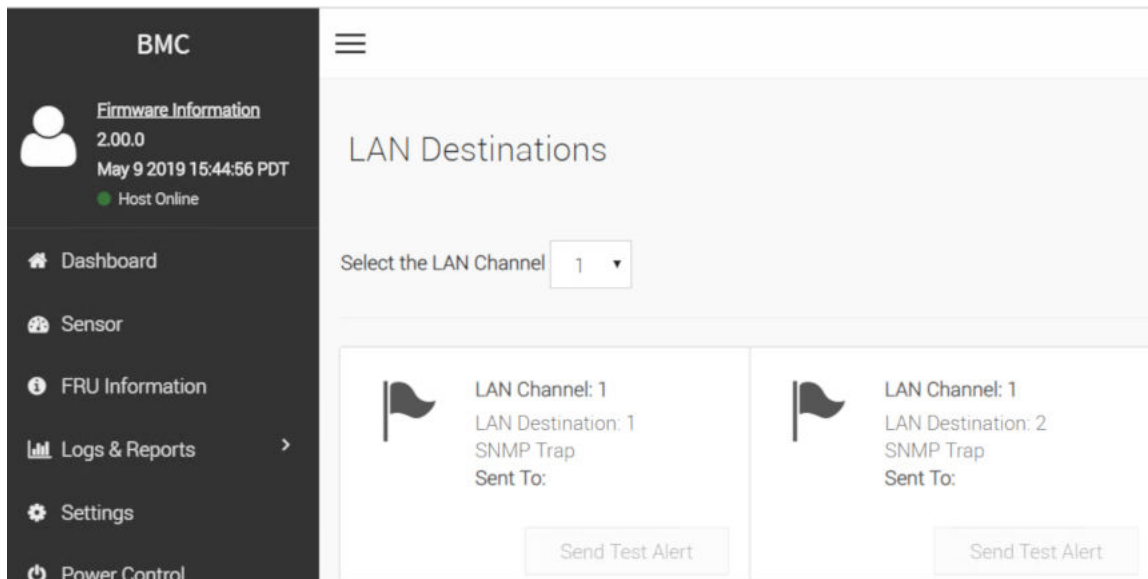
LAN destinations screen

LAN destinations configuration

LAN Channel
Displays LAN Channel Number of the selected slot (read-only).

Destination Type
- SNMP Trap
- E-Mail

SNMP Destination Address
If Destination type is SNMP Trap, then give the IP address of the system that will receive the alert. Destination address will support the following:

- IPv4 address format.
- IPv6 address format.

BMC Username

If Destination type is Email Alert, then choose the user to whom the email alert has to be sent.NOTE: Email address for the user has to be configured under `Settings->Users Management.`

Email Subject

These fields must be configured if email alert is chosen as destination type. An email will be sent to the configured email address of the user in case of any severity events with a subject specified in subject field and will contain the message field's content as the email body.

Email Message

These fields must be configured if email alert is chosen as destination type. An email will be sent to the configured email address of the user in case of any severity events with a subject specified in subject field and will contain the message field's content as the email body.

ⓘ | **NOTE: These fields are not applicable for `AMI-Format` email 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

[   ]

💾 Save

LAN destinations configuration screen

SMTP settings

LAN Interface

Select the LAN interface to be configured.

Sender Email ID

Enter the valid `Sender Email ID` on the SMTP Server. Maximum allowed size for Email ID is 64 bytes which includes 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.

- Machine Name is a string of maximum 25 alpha-numeric characters.
- Space, special characters are not allowed.

Primary Server IP

Enter the Server Address for the SMTP Server. It is a mandatory field.

- IP Address made of 4 numbers separated by dots as in `xxx.xxx. xxx.xxx`.
- Each Number ranges from 0 to 255.
- First Number must not be 0.

Server address will support the following:

- IPv4/IPV6 Address format.
- ost name format.

Primary SMTP port

Specify the SMTP Port. It is a mandatory field.

- Default port is 25.
- Port value ranges from 1 to 65535.

Primary Secure SMTP port

Specify the SMTP Secure port.

- Default Port is 465.
- Port value ranges from 1 to 65535.

Primary SMTP Authentication

Check the option `Enable` to enable SMTP Authentication.

> ⓘ | **NOTE: SMTP Server Authentication types supported are:**

- CRAM-MD5
- LOGIN
- PLAIN

Primary Username

Enter the username to access SMTP Accounts.

- User Name can be of length 4 to 64 alpha-numeric characters, dot(.), hyphen(-), and underscore(_).
- It must start with an alphabet.
- Other special characters are not allowed.

Primary password

Enter the password for the SMTP User Account.

- Password must be at least 4 characters long.
- White space is not allowed.

ⓘ | **NOTE: This field will not allow more than 64 characters.**

Primary SMTP SSLTLS Enable

Check the option `Enable` to enable SMTP SSLTLS protocol.

Primary SMTP STARTTLS Enable

Check the option `Enable` to enable SMTP STARTTLS protocol.

Secondary SMTP Support

Check this option to enable Secondary SMTP support for the BMC.

SMTP settings screen

SSL settings

SSL sections:

- View SSL certificate
- Generate SSL certificate
- Upload SSL certificate

Setup each SSL settings section using the options supplied.
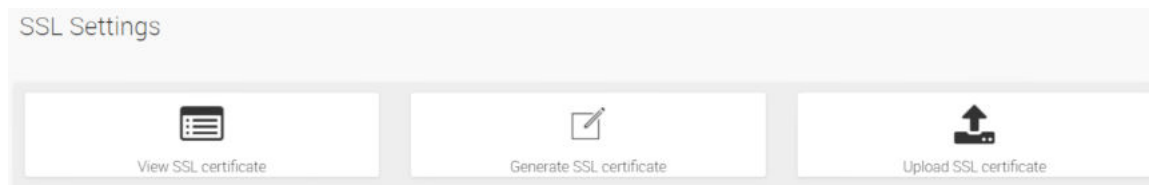
SSL settings screen

View SSL Certificate

Current Certificate Information

Displays basic information about the uploaded SSL certificate with the following fields:

- Version- Serial Number
- Signature Algorithm
- Public Key

It displays the basic information about the uploaded SSL certificate.It displays the following fields.

Issued from

Contains the following information about the Certificate Issuer:

- 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

It displays about 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

View SSL Certificate

Current Certificate Information

Certificate Version

3

Serial Number

92046422C980E206

Signature Algorithm

sha256WithRSAEncryption

Public Key

(2048 bit)

Issuer Common Name (CN)

AMI

Issuer Organization (O)

American Megatrends Inc

Issuer Organization Unit (OU)

Service Processors

Issuer City or Locality (L)

Atlanta

Issuer State or Province (ST)

Georgia

Issuer Country (C)

US

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

SSL Certificate screen

Generate SSL certificate

Common Name (CN)

Common name for which the generated certificate:

- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

It displays the basic information about the uploaded SSL certificate.It displays the following fields.

Organization (O)

Organization name for which certificate to be generated:

- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

Organization Unit (OU)

Over all organization section unit name for which certificate to be generated.

- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

City or Locality (L)

City or Locality (L):

- Maximum length of 128 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

State or Province (ST)

Over all organization section unit name for which certificate to be generated.

- Maximum length of 128 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

Country (C)

Country code has to be given:

- Only two characters are allowed.
- Special characters are not allowed.

Email Address

Email Address of the organization has to be given.

Valid for

Number of days the certificate to be validated.

- Value ranges from 1 to 3650 days.

Key Length

Choose the key length bit value of the certificate.

Generate SSL certificate screen

Upload SSL certificate

Current certificate

The information as Current certificate and uploaded date/time will be displayed (read-only).

New certificate

Browse and navigate to the certificate file:

- Certificate file should be of pem type.

Current private key

The information as current private key and uploaded date/time will be displayed (read-only).

New private key

Browse and navigate 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

[📂 ...]

[💾 Save]

Upload SSL certificate screen

System firewall

- System firewall order

This page is used to configure the System firewall order for user authentication into the BMC. It shows the list of available System firewall modules supported in the BMC.

System Firewall

| General Firewall Settings | IP Address Firewall Rules | Port Firewall Rules |

System firewall screen

General firewall settings

General firewall settings screen

The Settings screen include the following sections:

- Existing firewall settings
- Add firewall settings

General Firewall Settings
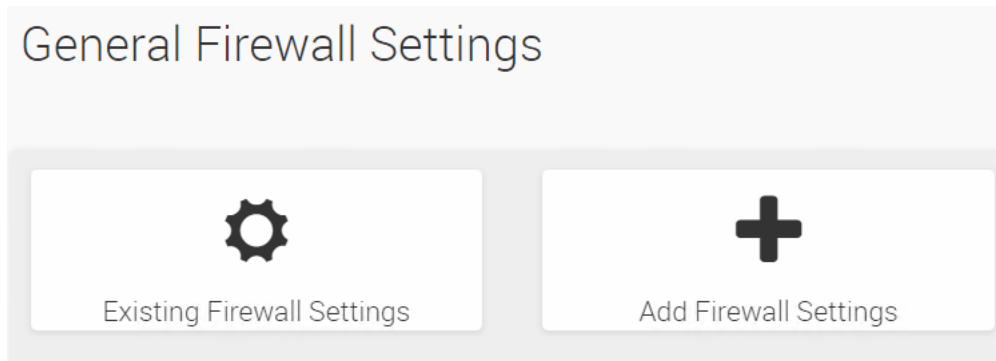
General firewall settings screen

Existing firewall settings

This page displays list of general firewall configurations.

Click X icon to delete an item from the list.

To view the page, user must at least be an Operator. To add or delete a firewall, user must be an Administrator.

Add firewall settings

Block all

This option will block all incoming IPs and Ports.

Flush all

This is used to flush all the system firewall rules.

Timeout

This option is used to enable or disable firewall rules with timeout.

Start Date

The respective firewall rule effect will start from this date.

Start Time

The respective firewall rule effect will start from this time.

End Date

The respective firewall rule effect will end from this date.

End Time

The respective firewall rule effect will end from 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

💾 Save

Add firewall settings screen

IP address firewall rules

IP address firewall rules screen

The IP address firewall rules screen include the following sections:

- Existing IP rules
- Add new IP rule

IP Firewall Rules
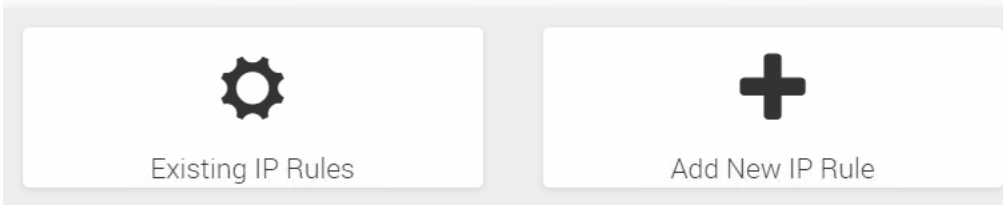
IP address firewall rules screen

Existing IP Rules

This page displays list of Existing IP firewall rules.

Click X icon to delete an item from the list.

To view the page, user must at least be an Operator. To add or delete a firewall, user must be an Administrator.

Add IP Rule

IP Single (or) Range Start

This field is used to configured the IP address or Range of IP addresses. An IP address will support IPv4 address format only:

- IPv4 Address made of 4 numbers separated bydots as in xxx.xxx.xxx.xxx.
- Each number ranges from 0 to 255.
- First number must not be 0.

IP Range End

This field is used to configured the IP address or Range of IP addresses. An IP address will support IPv4 address format only:

- IPv4 Address made of 4 numbers separated bydots as in xxx.xxx.xxx.xxx.
- Each number ranges from 0 to 255.
- First number must not be 0.

Enable Timeout

This option used to enable or disable firewall rules with timeout.

Start Date

The respective firewall rule effect will start from this date.

Start Time

The respective firewall rule effect will start from this time.

End Date

The respective firewall rule effect will end from this date.

End Time

The respective firewall rule effect will end from 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 ▼

🖫 Save

Add IP rule screen

Port firewall rules

Port firewall rules screen

The port firewall rules screen include the following sections:

· Existing port rules
· Add new port rule

Port Firewall Rules

⚙	➕
Existing Port Rules	Add New Port Rule
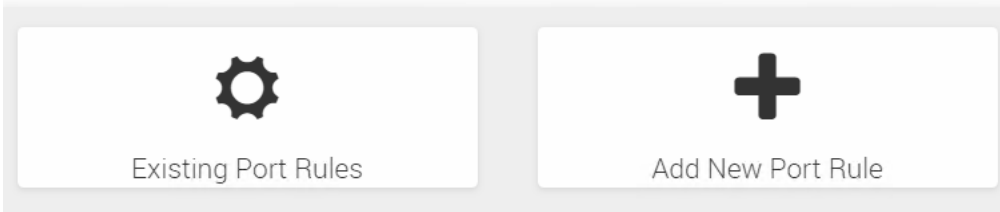
Port firewall rules screen

Existing port Rules

This page displays list of Existing port firewall rules.

Click X icon to delete an item from the list.

To view the page, user must at least be an Operator. To add or delete a firewall, user must be an Administrator.

Add port rule

Port Single (or) Range Start

This field is used to configure the port address or range of port addresses. A port address will support portv4 address format only:

- Port value ranges from 1 to 65535.

    ⓘ | **NOTE: Port 80 is blocked for TCP/UDP protocols.**

Port Range End

This field is used to configure the port address or range of port addresses. A port address will support portv4 address format only:

- Port value ranges from 1 to 65535.

    ⓘ | **NOTE: Port 80 is blocked for TCP/UDP protocols.**

Enable Timeout

This option used to enable or disable firewall rules with timeout.

Start Date

The respective firewall rule effect will start from this date.

Start Time

The respective firewall rule effect will start from this time.

End Date

The respective firewall rule effect will end from this date.

End Time

The respective firewall rule effect will end from this time.

Add port rule screen

User management

* User management order

This page is used to configure the User management order for user authentication into the BMC. It shows the list of available User management modules supported in the BMC.

The list below shows the current list of available users by channel. To Add or Edit a user, click on icon.

To Delete a particular user from the list, click icon.

A maximum of 10 slots are available and include the default of admin and anonymous.

It is advised that the anonymous user's privilege and password should be modified as a security measure. To view the page, you must have Operator privileges. To modify or add a user, You must have Administrator privileges.

User management screen

User management configuration

Username

Enter the name of the new user:

- IP Address consists of four sets of numbers separated by dots as in 'xxx.xxx.xxx.xxx'.
- Each set ranges from 0 to 255.
- 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 which consist of atleast one upper case letter, alphanumeric and special characters.

ⓘ **NOTE: Password is mandatory to be entered while enabling SNMP Access and should have minimum 8 characters when SNMP status is enabled.**

Enable User Access

Check the box to enable user access for the user. Upon enabling the user Access, the IPMI messaging privilege will be assigned to user.

ⓘ **NOTE: It is recommended that the IPMI messaging option should be enabled for the user to choose the User Access option, while creating User through IPMI.**

Privilege

Select the privilege level assigned to this user when the user accesses BMC through network interface.

There are four levels of Network Privileges:

- User

- Administrator
- Operator
- None

SNMP Access

Check the box to enable SNMP access for the user.

SNMP Authentication Protocol

Choose an Authentication Protocol for SNMP settings. NOTE: Password field is mandatory, if Authentication protocol is changed.

SNMP Privacy Protocol

Choose the Encryption algorithm to use for SNMP settings.

Email Format

Check this option to enable IPv6 DHCP to dynamically configure IPv6 address using Dynamic HostConfiguration v6 Protocol (DHCPv6).

- 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`.
- FixedSubject-Format: This format displays the message according to user's setting. You must set the subject and message for email alert.

Email ID

Enter the email ID for the user. If user forgets the password, new password will be mailed to the configured email ID.

ⓘ **NOTE: SMTP Server must be configured to send the email. Maximum allowed size for Email ID is 64 bytes which includes username and domain name.**

Existing SSH Key

The uploaded SSH key information will be displayed (read-only).

Upload SSH Key

Use Browse button to navigate to the public SSH key file.

- SSH key file should be of pub type.

User management configuration screen

Power control

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 (cold boot).

Hard reset

Select this option to reboot the system without powering off (warm boot).

Select this option to initiate operating system shutdown prior to the shutdown..
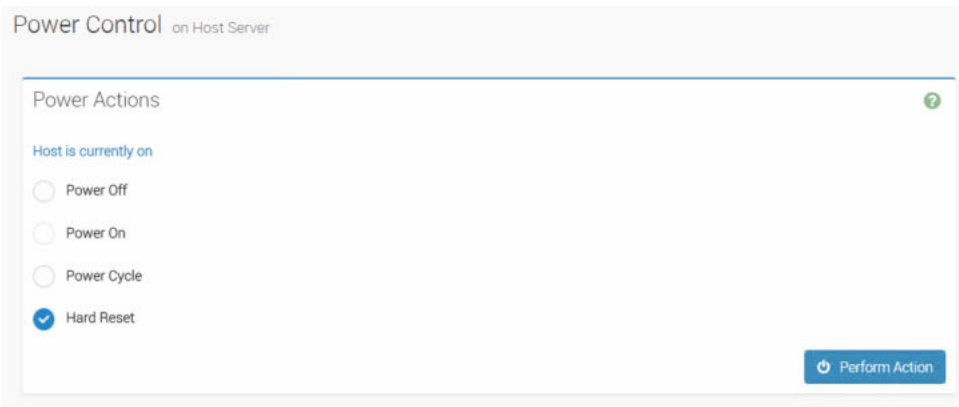
Power control screen

Maintenance

The Maintenance screen include the following sections:

- Backup configuration
- Dual image configuration
- Firmware image location
- Firmware information
- Preserve configuration
- Restore configuration
- Restore factory defaults
- System administrator

Maintenance screen

Backup configuration

Check the configuration that needs to be backed up. Use the downloaded to restore the configuration.

> ⓘ **NOTE: Network configurations are inter-related to IPMI, and hence by default IPMI configurations will be selected automatically when you select `Network and Services` to be backed up.**

Backup configuration screen

Firmware image location

Image location type

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

Firmware image location screen

Firmware information

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
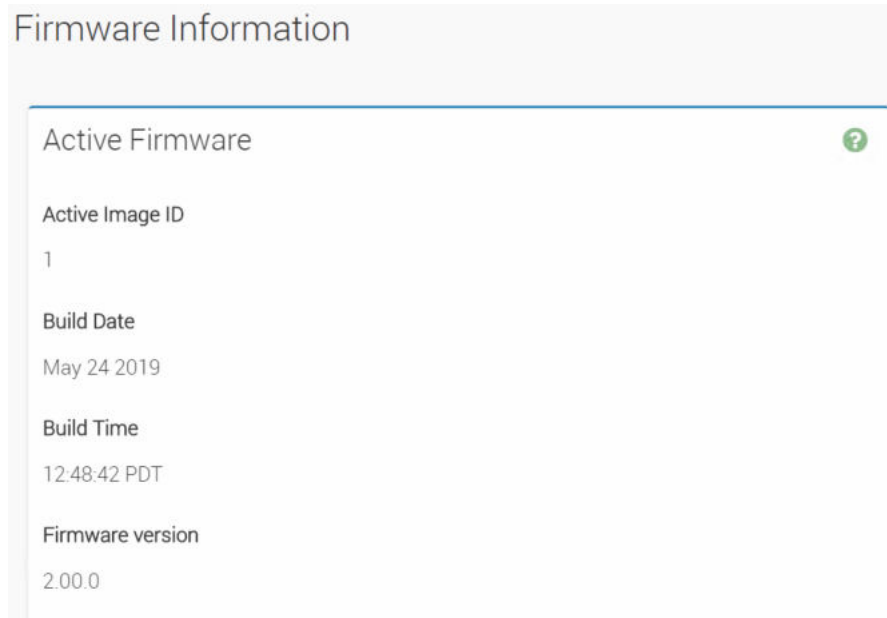
Firmware information screen

Preserve configuration

Restore Configuration

Check the configuration that needs to be preserved, while the Restore Configuration is done.

Check All

Select this option to check all the configuration list.

You can either check/uncheck a check box to preserve/overwrite the configuration for your system.

Preserve configuration screen

Restore configuration

Config file

Use Browse button to navigate to the Configuration file.

Restore configuration screen

Restore factory defaults

Preserve configuration page

Use Browse button to navigate to the Configuration file.

To preserve any existing configuration data, goto preserve configuration page and select them.

Restore factory defaults screen

System Administrator

Username

Username of System Administrator is displayed (read only).

Enable User Access

Check this option to enable user access for system administrator.

Change Password

Check this option to change the existing password. This will enable the password fields.

Password

Enter the new password here.

- Password must be at least 8 characters long.
- White space is not allowed.
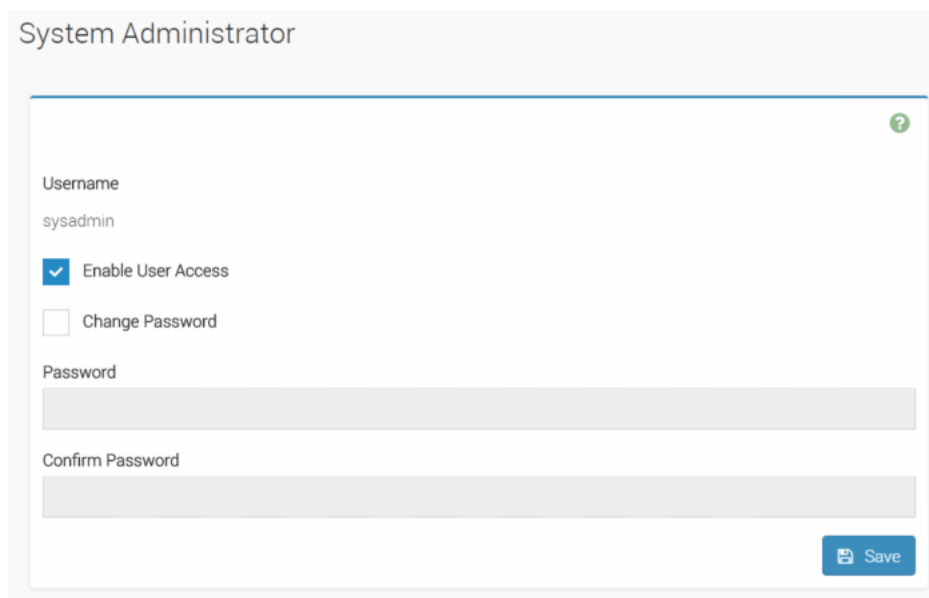
ⓘ | **NOTE: This field will not allow more than 64 characters.**

Confirm Password

Enter the same password which you have entered in the Password field to confirm the Password.

- Password must be at least 8 characters long.
- White space is not allowed.

ⓘ | **NOTE: This field will not allow more than 64 characters.**

System Administrators screen

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.

ⓘ **NOTE: The information in the following chapter is intended for developers and system administrators. Users are recommended to use the Web GUI as described BMC web GUI chapter.**

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

ⓘ **NOTE: -I `[-I <interface>]` and -H `[-H <address>]` 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:/opt/dellemc/diag/bin# ipmitool sensor
XP12R0V        | 12.160      | Volts      | ok    | 8.512  | 9.792   | 10.944 | 13.440 | 14.656
| 15.872
VNN_AUX_PCH    | 0.903       | Volts      | ok    | 0.539  | 0.630   | 0.721  | 1.197  | 1.169
| 1.260
XP2R5V_VPPB    | 2.548       | Volts      | ok    | 1.750  | 2.002   | 2.254  | 2.758  | 2.996
| 3.248
XP1R2V_VDDRB   | 1.190       | Volts      | ok    | 0.840  | 0.959   | 1.078  | 1.316  | 1.442
| 1.561
XP0R6V_VTTB    | 0.595       | Volts      | ok    | 0.420  | 0.476   | 0.539  | 0.658  | 0.721
| 0.784
XP5R0V         | 5.177       | Volts      | ok    | 3.627  | 4.123   | 4.650  | 5.673  | 6.200
| 6.727
XP3R3V_AUX_CP  | 3.325       | Volts      | ok    | 2.310  | 2.643   | 2.975  | 3.623  | 3.955
| 4.288
XP3R3V_AUX_PCH | 3.308       | Volts      | ok    | 2.310  | 2.643   | 2.975  | 3.623  | 3.955
| 4.288
XP1R8V_AUX_PCH | 1.785       | Volts      | ok    | 1.265  | 1.438   | 1.622  | 1.979  | 2.162
| 2.336
XP1R05V_PCH    | 1.050       | Volts      | ok    | 0.735  | 0.840   | 0.945  | 1.155  | 1.260
| 1.365
XP2R5V_VPPA    | 2.548       | Volts      | ok    | 1.750  | 2.002   | 2.254  | 2.758  | 2.996
| 3.248
XP1R2V_VDDRA   | 1.204       | Volts      | ok    | 0.840  | 0.959   | 1.078  | 1.316  | 1.442
| 1.561
XP0R6V_VTTA    | 0.602       | Volts      | ok    | 0.420  | 0.476   | 0.539  | 0.658  | 0.721
| 0.784
VCCIO_CP       | 1.001       | Volts      | ok    | 0.504  | 0.602   | 0.700  | 1.197  | 1.302
| 1.400
VCCIN_CP       | 1.775       | Volts      | ok    | 0.898  | 1.081   | 1.265  | 2.162  | 2.336
| 2.519
VCCSA_CP       | 0.854       | Volts      | ok    | 0.259  | 0.343   | 0.427  | 1.190  | 1.274
```

```
| 1.358
Power_Status   | 0x0       | discrete   | 0x0180| na       | na       | na      | na      | na
| na
Watchdog2      | 0x0       | discrete   | 0x0080| na       | na       | na      | na      | na
| na
SEL            | 0x0       | discrete   | 0x0080| na       | na       | na      | na      | na
| na
BMC boot       | 0x0       | discrete   | 0x0180| na       | na       | na      | na      | na
| na
Outlet_Temp    | 31.000    | degrees C  | ok    | na       | na       | na      | na      | na
| na
Inlet1_Temp    | 25.000    | degrees C  | ok    | na       | na       | na      | na      | na
| na
Inlet2_Temp    | 23.000    | degrees C  | ok    | na       | na       | na      | na      | na
| na
Inlet3_Temp    | 22.000    | degrees C  | ok    | na       | na       | na      | 59.000 | 62.000
| na
Inlet4_Temp    | 29.000    | degrees C  | ok    | na       | na       | na      | na      | na
| na
Fan1           | 11400.000 | RPM        | ok    | na       | 1080.000 | na      | na      | na
| na
Fan2           | 11400.000 | RPM        | ok    | na       | 1080.000 | na      | na      | na
| na
Fan3           | 11640.000 | RPM        | ok    | na       | 1080.000 | na      | na      | na
| na
```

The command parameters change slightly when using `ipmitool` over LAN:

```
$ ./ipmitool -U admin -P admin -I lanplus -H 10.11.227.53 sensor
XP12R0V        | 12.160    | Volts      | ok    | 8.512  | 9.792  | 10.944 | 13.440 | 14.656
| 15.872
VNN_AUX_PCH    | 0.910     | Volts      | ok    | 0.539  | 0.630  | 0.721  | 1.197  | 1.169
| 1.260
XP2R5V_VPPB    | 2.548     | Volts      | ok    | 1.750  | 2.002  | 2.254  | 2.758  | 2.996
| 3.248
XP1R2V_VDDRB   | 1.190     | Volts      | ok    | 0.840  | 0.959  | 1.078  | 1.316  | 1.442
| 1.561
XP0R6V_VTTB    | 0.595     | Volts      | ok    | 0.420  | 0.476  | 0.539  | 0.658  | 0.721
| 0.784
XP5R0V         | 5.177     | Volts      | ok    | 3.627  | 4.123  | 4.650  | 5.673  | 6.200
| 6.727
XP3R3V_AUX_CP  | 3.325     | Volts      | ok    | 2.310  | 2.643  | 2.975  | 3.623  | 3.955
| 4.288
XP3R3V_AUX_PCH | 3.308     | Volts      | ok    | 2.310  | 2.643  | 2.975  | 3.623  | 3.955
| 4.288
XP1R8V_AUX_PCH | 1.775     | Volts      | ok    | 1.265  | 1.438  | 1.622  | 1.979  | 2.162
| 2.336
XP1R05V_PCH    | 1.050     | Volts      | ok    | 0.735  | 0.840  | 0.945  | 1.155  | 1.260
| 1.365
XP2R5V_VPPA    | 2.548     | Volts      | ok    | 1.750  | 2.002  | 2.254  | 2.758  | 2.996
| 3.248
XP1R2V_VDDRA   | 1.204     | Volts      | ok    | 0.840  | 0.959  | 1.078  | 1.316  | 1.442
| 1.561
XP0R6V_VTTA    | 0.602     | Volts      | ok    | 0.420  | 0.476  | 0.539  | 0.658  | 0.721
| 0.784
VCCIO_CP       | 1.001     | Volts      | ok    | 0.504  | 0.602  | 0.700  | 1.197  | 1.302
| 1.400
VCCIN_CP       | 1.775     | Volts      | ok    | 0.898  | 1.081  | 1.265  | 2.162  | 2.336
| 2.519
VCCSA_CP       | 0.847     | Volts      | ok    | 0.259  | 0.343  | 0.427  | 1.190  | 1.274
| 1.358
Power_Status   | 0x0       | discrete   | 0x0180| na     | na     | na     | na     | na
| na
Watchdog2      | 0x0       | discrete   | 0x0080| na     | na     | na     | na     | na
| na
SEL            | 0x0       | discrete   | 0x0080| na     | na     | na     | na     | na
| na
BMC boot       | 0x0       | discrete   | 0x0180| na     | na     | na     | na     | na
| na
```

```
Outlet_Temp     | 30.000    | degrees C | ok     | na      | na       | na      | na      | na
| na
Inlet1_Temp     | 26.000    | degrees C | ok     | na      | na       | na      | na      | na
| na
Inlet2_Temp     | 22.000    | degrees C | ok     | na      | na       | na      | na      | na
| na
Inlet3_Temp     | 22.000    | degrees C | ok     | na      | na       | na      | 59.000  | 62.000
| na
Inlet4_Temp     | 29.000    | degrees C | ok     | na      | na       | na      | na      | na
| na
Fan1            | 11280.000 | RPM       | ok     | na      | 1080.000 | na      | na      | na
| na
Fan2            | 11160.000 | RPM       | ok     | na      | 1080.000 | na      | na      | na
| na
Fan3            | 11040.000 | RPM       | ok     | na      | 1080.000 | na      | na      | na
| na
Fan4            | 11280.000 | RPM       | ok     | na      | 1080.000 | na      | na      | na
| na
Fan5            | 11040.000 | RPM       | ok     | na      | 1080.000 | na      | na      | na
| na
Fan1_Status     | 0x0       | discrete  | 0x0280| na      | na       | na      | na      | na
| na
Fan2_Status     | 0x0       | discrete  | 0x0280| na      | na       | na      | na      | na
| na
Fan3_Status     | 0x0       | discrete  | 0x0280| na      | na       | na      | na      | na
| na
Fan4_Status     | 0x0       | discrete  | 0x0280| na      | na       | na      | na      | na
| na
Fan5_Status     | 0x0       | discrete  | 0x0280| 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 IPMI resources that is hosted by Intel 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*.

In addition to 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 XXXXXXXXXXXXXXX   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 EMC 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 refers to the LAN channel, which is `1` in this BMC implementation.

Dell EMC recommends executing 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 https://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. For more information about the `ipmiutil` command, see ipmiutil package.

Install the `ipmiutil` package and use the `iseltime` command.

To override the date and time 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://sourceforge.net/. Also, various Linux distributions have binary packages prebuilt and available for download.

For Fedora, to download the utilities, use https://pkgs.org/download/ipmiutil

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:

```
# 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:

 # ipmitool pef filter list
```
 1 | enabled, configurable | Any | Any | None | OEM | Any | Alert,OEM-defined | 1
 2 | enabled, pre-configured | Any | Any | Information | OEM | Any | Alert | 2
```

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 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 setup 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.

 # 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       : 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:

```
# ipmitool lan alert set 1 1 ipaddr 10.11.227.180
Setting LAN Alert 1 IP Address to 10.11.227.180
```

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

root@dellemc-diag-os:/opt/dellemc/diag/bin# ipmitool lan alert print 1 1
```
Alert Destination       : 1
Alert Acknowledge       : Unacknowledged
Destination Type        : OEM 1
```

```
Retry Interval         : 3
Number of Retries      : 3
Alert Gateway          : Default
Alert IP Address       : 10.11.227.180
Alert MAC Address      : 00:00:00:00:00:00
```

Alert policy setup

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

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

 # ipmitool pef policy list
```
 1 | 1 | disabled | Match-always | 1 | 802.3 LAN | PET | AMI | 0 | 0 | 0.0.0.0 |
00:00:00:00:00:00
 2 | 2 | disabled | Match-always | 1 | 802.3 LAN | PET | AMI | 0 | 0 | 0.0.0.0 |
00:00:00:00:00:00
 3 | 3 | disabled | Match-always | 1 | 802.3 LAN | PET | AMI | 0 | 0 | 0.0.0.0 |
00:00:00:00:00:00
 4 | 4 | disabled | Match-always | 1 | 802.3 LAN | PET | AMI | 0 | 0 | 0.0.0.0 |
00:00:00:00:00:00
 5 | 5 | disabled | Match-always | 1 | 802.3 LAN | PET | AMI | 0 | 0 | 0.0.0.0 |
00:00:00:00:00:00
 6 | 6 | disabled | Match-always | 1 | 802.3 LAN | PET | AMI | 0 | 0 | 0.0.0.0 |
00:00:00:00:00:00
..
60 | 15 | disabled | Match-always | 1 | 802.3 LAN | PET | AMI | 0 | 0 | 0.0.0.0 |
00:00:00:00:00:00
```

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*.

 # ipmitool raw 0x4 0x12 0x9 0x2 0x28 0x11 0x00
```
Byte 3 (0x9) – Alert policy table entry command
Byte 4 (02) – table entry number
Byte 5 (0x28) – policy number and enable bit
Byte 6 (0x11) – channel and destination
Byte 7 (0x00) – String
The 2nd entry after the command execution is show below
```

 # ipmitool pef policy list
```
 1 | 1 | enabled | Match-always | true | 1 | 802.3 LAN | PET | AMI | 3 | 3 | 10.11.227.180 |
00:00:00:00:00:00
```
 2 | 2 | enabled | Match-always | 1 | 802.3 LAN | PET | AMI | 3 | 3 | 10.11.227.180 | 00:00:00:00:00:00

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

Step 1 creates a user with no access.

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

```
$ ./ipmitool -H xx.xx.xxx.xx -I lanplus -U admin -P admin 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 admin user priv 3 2
Set Privilege Level command successful (user 3)
$ ./ipmitool -H xx.xx.xxx.xx -I lanplus -U admin -P admin user list
ID  Name     Callin  Link Auth  IPMI Msg   Channel Priv Limit
1            false   false      true       ADMINISTRATOR
2   admin    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
```

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:

```
$ ./ipmitool -H xx.xx.xxx.xxx -I lanplus -U admin -P admin 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 <name> 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 admin 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 <name> 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 2. 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 3. 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.

Parameter	#	Parameter data
		[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 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

Parameter	#	Parameter data
		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 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.

Parameter	#	Parameter data
		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

Parameter	#	Parameter data
		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 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

1 = UDP

Parameter	#	Parameter data
		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.
		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.

Parameter	#	Parameter data
		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

Parameter	#	Parameter data
		LS-byte first if little endian system. Two-byte data required to form year.
		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

12—month

Parameter	#	Parameter data
		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
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

Parameter	#	Parameter data
		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

Parameter	#	Parameter data
		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
		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

35—month

Parameter	#	Parameter data
		[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
		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

Parameter	#	Parameter data
		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

Parameter	#	Parameter data
		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.
		[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.

Parameter	#	Parameter data
		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 [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

Parameter	#	Parameter data
		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.
		[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 SEL command

Use reserve system event log (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

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

Firmware upgrades

Manual or automatic BMC, BIOS, and CPLD firmware upgrades is **required before** VEP4600 Expansion Card installation.

ⓘ | **NOTE: Minimum firmware requirements**

Table 4. Required firmware minimum release requirements.

Device	Firmware	Minimum firmware release required when installing an rNDC Card	Minimum firmware release required when installing the WIFI or LTE Card
VEP4600	BMC	v1.22	v1.23
	BIOS	v3.41.0.9-10	3.41.0.9-13
	CPLD	V0C	V0C
	DIAGS OS	3.41.3.81-4	3.41.3.81-5 (rNDC, WIFI/LTE)
	DIAGS Tools	3.41.4.81-15	3.41.4.81-16 (rNDC (WIFI/LTE)
Expansion Card - rNDC Carrier	CPLD	v02	n/a
Expansion Card - Wifi or LTE Card	CPLD	n/a	R01

Topics:

-
-

USB based firmware update

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

ⓘ | **NOTE: DIAG OS version 6 is the minimum configuration to install VEP4600 Expansion Cards.**

Power on VEP4600

Plug in a power cord to the back of VEP4600 platform. The platform starts to power 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 a VEP4600 console port.

ⓘ | **NOTE: Use a 115200 baud rate.**
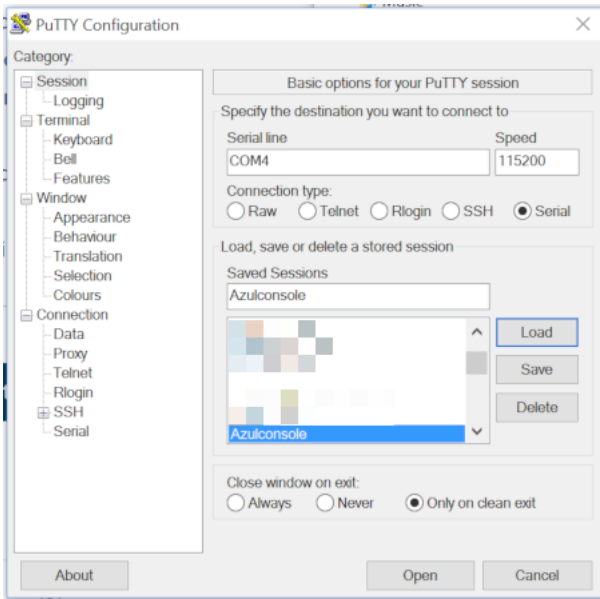
puTTY 115200 baud rate setup

BIOS access process

1   Press the **delete** button after the `POST Lower DRAM Memory test` appears on the screen.

Continue pressing the **delete** button 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.**

Figure 2. Initial boot up screen

Figure 3. Boot up screen

Figure 4. BIOS setup and configuration screen

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

Figure 5. Display BIOS and CPLD versions

Configure BIOS and boot into DIAG OS

Boot into BIOS setting and select **Boot Option #1** to boot from the hard disk.
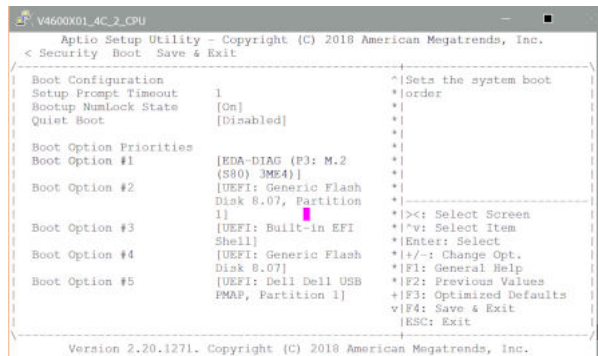
Figure 6. Select boot from hard disk

Select **Save & Exit setup** and select **Yes**.
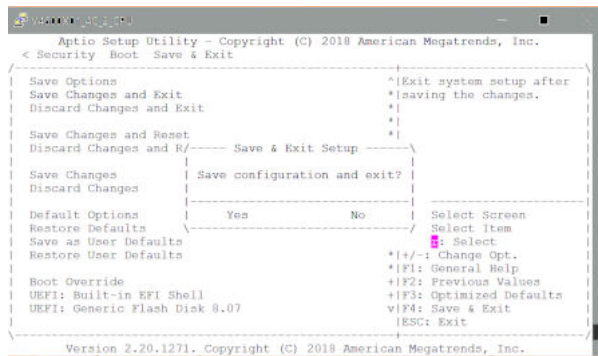

Figure 7. Save and exit

Type **root/calvin** to login.

Figure 8. Type root/calvin to login

Update BMC in DIAG OS

Use the following DIAG OS command to update BMC:

```
updatetool -D MAIN-BMC -U -e ./VEP4600-BMC-vx.xx.ima
```

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

Use this command to update BMC:

> ⓘ **NOTE: This** *<BMC_update_filename>* **is the file from the USB drive that is mounted.**

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

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

root@dellemc-diag-os:~# updatetool -D MAIN-BMC -U -e *<BMC_update_filename>*
```
disable preserve BIOS configuration
 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:~#
```

Update BIOS in DIAG OS

Use the following DIAG OS command to update BIOS:

ⓘ **NOTE: For updating BIOS and preserving NVRAM(configuration information in BIOS) use the command: updatetool -D BIOS -N -U -e VEP4600-BIOS-x.xx.x.x-xx.BIN**

```
updatetool -D BIOS -N -U -e ./VEP4600-BIOS-x.xx.x.x-xx.BIN
```

Use this command to update BIOS:

ⓘ **NOTE: For updating BIOS and preserving NVRAM(configuration information in BIOS) use the command:**

```
updatetool -D BIOS -N -U -e <VEP4600-BIOS-x.xx.x.x-xx.BIN>
```

root@dellemc-diag-os:~# updatetool -D BIOS -N -U -e <VEP4600-BIOS-x.xx.x.x-xx.BIN> `disable preserve BIOS`
```
configuration
 00
Disable device protect

Disable BIOS protect operation success, wait HW reset
Write image to BIOS
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.
Beginning BIOS Update...
Uploading Image : 100%... done
Flashing  Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
write BIOS image success
Enable device protect

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

Update CPLD in DIAG OS

Use the following DIAG OS command to update CPLD:

```
updatetool -D CPLD --index=1 -U -e ./AZUL_CPLD_V0C.vme
```

Use this command to update CPLD

> ⓘ **NOTE: After successfully updating the firmware, power-off and power-on the unit. Make sure all the versions are current and correct.**

```
updatetool -D CPLD --index=1 -U -e <AZUL_CPLD_Vxx.vme>
```

root@dellemc-diag-os:~# updatetool -D CPLD --index=1 -U -e <AZUL_CPLD_Vxx.vme>
```
 00
Disable device protect

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

Creating IPMI session via USB...Done

--------------------------------------------------
YAFUFlash - Firmware Upgrade Utility (Version 5.0.0)
--------------------------------------------------
(C)Copyright 2016, American Megatrends Inc.
Beginning CPLD Update...
Uploading Image : 100%... done
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
write CPLD image success
Enable device protect

Update CPLD image success
root@dellemc-diag-os:~# shutdown -h now
[xxx.xxxxxx] reboot: Power down

BIOS Boot Selector for VEP4600
Primary BIOS Version x.xx.x.x-xx

CPLD Version:x.x
CPLD Reset Source=0x44

root@dellemc-diag-os:~# updatetool --dev=ALL --device_version
BIOS version:
x.xx.x.x-xx

CPLD version:
CPLD_VERSION : offset 0x600 = 0x9
7: 4 MAJOR_VER = x
3: 0 MINOR_VER = x

MAIN-BMC version:
x.xx

BACKUP-BMC version:
x.xx
```

When the update is complete, **you must either** unplug and replug power cables, or power down and back up using remote power cycle of system via IPMI, to update the version.

Remote firmware update

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

> ⓘ **NOTE: DIAG OS version 6 is the minimum configuration to install VEP4600 Expansion Cards.**

Boot into BIOS settings

1   Press the **delete** button after the `POST Lower DRAM Memory test` appears on the screen.

Continue pressing the **delete** button 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.**

2   Boot into BIOS settings.

Figure 9. Boot into BIOS settings

3   Go to **Server Mgmt->BMC network configuration**.

Figure 10. BMC network configuration

4   Select **Lan channel 1** and configure IP address.

> ⓘ **NOTE: Noticed when entering IP address in the text field, use ctrl-h to erase the characters entered by mistake.**

Figure 11. Lan channel 1 and configure IP address

5   Select **Save & Exit Setup** and choose **Yes**.
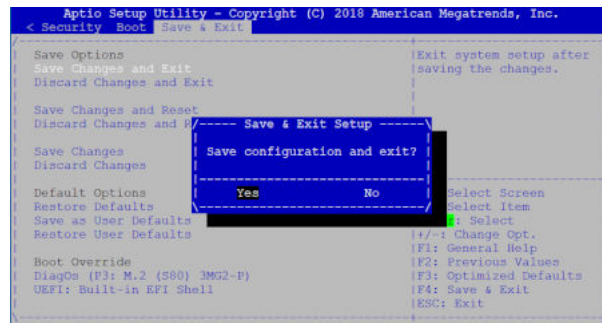
Figure 12. Save & Exit

Network interface settings

1   After booting up, go to BMC console to 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   Ping gateway to make sure the link is up and running:

```
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

1   To configure BMC network manually.

Log into BMC/IPMI console with sysadmin/superuser credential, and edit the /etc/network/interfaces file as the following:

```
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
```

2   Replace the IP network info with yours, then run the following command to restart network service:

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

If you reboot BMC, you may lose the network info and need to start all over again. That's because since you don't have BIOS configured and every time you reboot BMC, it fetches the information from BIOS configuration and refreshes the interfaces file.

Check BIOS, BMC, CPLD versions

1   After booting up the system, check BIOS and CPLD by scroll up the vertical scroll bar on the right in putty session:

```
BIOS Boot Selector for VEP-4600
Primary BIOS Version x.xx.x.x-xx

CPLD Version:x.x
CPLD Reset Source=0x44
```

2   Check the BMC version in BIOS settings:

Figure 13. BMC version in BIOS settings

Remote power cycle system

`ipmitool` remote BMC, DIAG OS power cycle shell commands.

Remote BMC, DIAG OS power cycle

Run **ipmitool** from the BMC serial console command prompt.

   a   Use this command to power cycle a remote system.
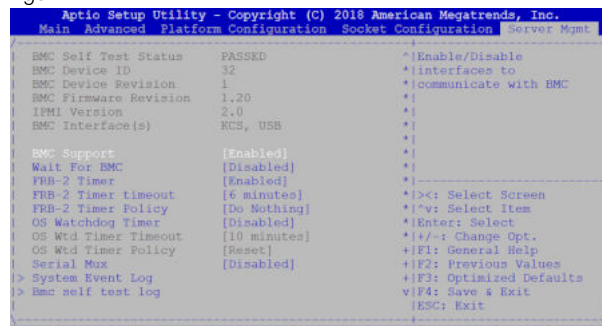
```
# ipmitool -H xxx.x.x.x -U admin -P admin power cycle
```

If BMC has a different administrator configured, replace the `-u` and `-p` parameters with **admin\admin**

> ⓘ | NOTE: **Username and password must be admin\admin**

- `-u`—admin
- `-p`—admin

```
~ # ipmitool -H xxx.x.x.x -U admin -P admin power status
Chassis Power is on
~ # ipmitool -H xxx.x.x.x -U admin -P admin 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 VEP4600, the kernel flag `CONFIG_IPMI_POWEROFF` should be set to n. Having this flag turned on will cause the kernel to send the ipmi command to power down the chassis when the CPU is powered-off. For example, pressing the push button for five seconds will power down the CPU.**

Pressing the push button for 5 secs with this flag set to n in the kernel will power down the chassis (standby mode). The only way to power-up the chassis will be to issue the ipmi command from remote station to the BMC to power-on the VEP4600.

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 admin power reset
```

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

```
ipmitool -I lanplus -H xxx.x.x.x -U admin -P admin power off
```

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

```
ipmitool -I lanplus -H xxx.x.x.x -U admin -P admin power on
```

    d   Use this command to cold reboot the remote system.

```
ipmitool -I lanplus -H xxx.x.x.x -U admin -P admin power cycle
```

2   Use this command to boot into BIOS settings.

```
ipmitool -I lanplus -H xxx.x.x.x -U admin -P admin chassis bootparam set bootflag force_bios

ipmitool -I lanplus -H xxx.x.x.x -U admin -P admin power reset
```

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
PSU2AF_temp      | 27.000      | degrees C | cr   | 24.000 | 29.000  | 34.000 | 41.000  |
60.000   | 68.000
PSU1AF_temp      | 28.000      | degrees C | cr   | 24.000 | 29.000  | 34.000 | 41.000  |
60.000   | 68.000
PT_Left_temp     | 26.000      | degrees C | cr   | 24.000 | 29.000  | 34.000 | 41.000  |
65.000   | 70.000
PT_Right_temp    | 26.000      | degrees C | cr   | 24.000 | 29.000  | 34.000 | 41.000  |
65.000   | 70.000
ILET_AF_temp     | 27.000      | degrees C | cr   | 24.000 | 29.000  | 34.000 | 41.000  |
60.000   | 68.000
CPU_Near_temp    | 30.000      | degrees C | nc   | 24.000 | 29.000  | 34.000 | 41.000  |
60.000   | 68.000
PT_Mid_temp      | 32.000      | degrees C | nc   | 24.000 | 29.000  | 34.000 | 41.000  |
80.000   | 85.000
NPU_Near_temp    | 35.000      | degrees C | ok   | 24.000 | 29.000  | 34.000 | 41.000  |
80.000   | 85.000
TC_Near_temp     | 32.000      | degrees C | nc   | 24.000 | 29.000  | 34.000 | 41.000  |
60.000   | 68.000
NPU_Mid_temp     | 0.000       | degrees C | nr   | 24.000 | 29.000  | 34.000 | 41.000  |
85.000   | 95.000
PSU1_Normal_temp | 39.000      | degrees C | ok   | 24.000 | 29.000  | 34.000 | 41.000  |
80.000   | 85.000
PSU1_Sys_temp    | 31.000      | degrees C | nc   | 24.000 | 29.000  | 34.000 | 41.000  |
80.000   | 85.000
```

Sensor	Reading	Unit	Status						
PSU1_Chass_temp	28.000	degrees C	cr	24.000	29.000	34.000	41.000	80.000	85.000
PSU2_Normal_temp	37.000	degrees C	ok	24.000	29.000	34.000	41.000	80.000	85.000
PSU2_Sys_temp	30.000	degrees C	nc	24.000	29.000	34.000	41.000	80.000	85.000
PSU2_Chass_temp	29.000	degrees C	cr	24.000	29.000	34.000	41.000	80.000	85.000
CPU_temp	35.000	degrees C	cr	0.000	36.000	40.000	52.000	60.000	68.000
DRAM1_temp	33.000	degrees C	cr	0.000	36.000	40.000	52.000	60.000	68.000
DRAM2_temp	0.000	degrees C	nr	0.000	36.000	40.000	52.000	60.000	68.000
FAN1_Rear_rpm	6570.000	RPM	ok	na	1350.000	na	na	15390.000	na
FAN2_Rear_rpm	6570.000	RPM	ok	na	1350.000	na	na	15390.000	na
FAN3_Rear_rpm	6570.000	RPM	ok	na	1350.000	na	na	15390.000	na
FAN4_Rear_rpm	6570.000	RPM	ok	na	1350.000	na	na	15390.000	na
FAN1_Front_rpm	6570.000	RPM	ok	na	1350.000	na	na	15390.000	na
FAN2_Front_rpm	6570.000	RPM	ok	na	1350.000	na	na	15390.000	na
FAN3_Front_rpm	6570.000	RPM	ok	na	1350.000	na	na	15390.000	na
FAN4_Front_rpm	6570.000	RPM	ok	na	1350.000	na	na	15390.000	na
PSU1_rpm	11220.000	RPM	ok	na	1275.000	na	na	15300.000	na
PSU2_rpm	11220.000	RPM	ok	na	1275.000	na	na	15300.000	na
PSU_Total_watt	280.000	Watts	ok	0.000	0.000	0.000	1000.000	1200.000	1600.000
PSU1_state	0x1	discrete	0x0180	na	na	na	na	na	na
PSU2_state	0x1	discrete	0x0180	na	na	na	na	na	na
PSU1_In_watt	136.000	Watts	ok	na	0.000	na	na	1016.000	na
PSU1_In_volt	206.000	Volts	ok	na	100.000	na	na	240.000	na
PSU1_In_amp	0.670	Amps	ok	na	0.000	na	na	2.540	na
PSU1_Out_watt	110.000	Watts	ok	na	0.000	na	na	254.000	na
PSU1_Out_volt	12.000	Volts	cr	na	100.000	na	na	240.000	na
PSU1_Out_amp	9.200	Amps	ok	na	0.000	na	na	25.400	na
PSU2_In_watt	148.000	Watts	ok	na	0.000	na	na	1016.000	na
PSU2_In_volt	204.000	Volts	ok	na	100.000	na	na	240.000	na
PSU2_In_amp	0.740	Amps	ok	na	0.000	na	na	2.540	na
PSU2_Out_watt	119.000	Watts	ok	na	0.000	na	na	254.000	na
PSU2_Out_volt	12.000	Volts	cr	na	100.000	na	na	240.000	na
PSU2_Out_amp	9.700	Amps	ok	na	0.000	na	na	25.400	na
ACPI_state	0x1	discrete	0x0180	na	na	na	na	na	na
FAN1_prsnt	0x1	discrete	0x0180	na	na	na	na	na	na
FAN2_prsnt	0x1	discrete	0x0180	na	na	na	na		

```
na           | na
FAN3_prsnt         | 0x1       | discrete  | 0x0180| na    | na       | na    | na        |
na           | na
FAN4_prsnt         | 0x1       | discrete  | 0x0180| na    | na       | na    | na        |
na           | na
Fan1_Rear_state    | 0x0       | discrete  | 0x0080| na    | na       | na    | na        |
na           | na
Fan2_Rear_state    | 0x0       | discrete  | 0x0080| na    | na       | na    | na        |
na           | na
Fan3_Rear_state    | 0x0       | discrete  | 0x0080| na    | na       | na    | na        |
na           | na
Fan4_Rear_state    | 0x0       | discrete  | 0x0080| na    | na       | na    | na        |
na           | na
Fan1_Front_state | 0x0       | discrete  | 0x0080| na    | na       | na    | na        |
na           | na
Fan2_Front_state | 0x0       | discrete  | 0x0080| na    | na       | na    | na        |
na           | na
Fan3_Front_state | 0x0       | discrete  | 0x0080| na    | na       | na    | na        |
na           | na
Fan4_Front_state | 0x0       | discrete  | 0x0080| na    | na       | na    | na        |
na           | na
root@dellemc-diag-os:~#
```

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 EMC 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        : Mon May 14 13:44:00 2018
Board Mfg             : DELL Board
Product               : Z9264F-ON
Board Serial          : TW0DYJR5DNT0085E0052
Board Part Number     : 0DYJR5
Product Manufacturer  : DELL Product
Name                  : Z9264F-ON
Product Version       : X1
Product Serial        : 9WJFXC2
Product Asset Tag     :
FRU Device Description : FRU_FAN1 (ID 1)
Board Mfg Date        : Mon May 14 13:44:00 2018
Board Mfg             : DELL
Board Product         :
Board Serial          : TW0M6X8JDNT008570205
Board Part Number     : 0M6X8JX01FRU Device
Description : FRU_FAN2 (ID 2)
Board Mfg Date        : Mon May 14 13:44:00 2018
Board Mfg             : DELL
Board Product         :
Board Serial          : TW0M6X8JDNT008570206
Board Part Number     : 0M6X8JX01FRU
Device Description : FRU_FAN3 (ID 3)
Board Mfg Date        : Mon May 14 13:44:00 2018
Board Mfg             : DELL
Board Product         :
Board Serial          : TW0M6X8JDNT008570207
Board Part Number     : 0M6X8JX01FRU
Device Description : FRU_FAN4 (ID 4)
```

```
Board Mfg Date        : Mon May 14 13:44:00 2018
Board Mfg             : DELL
Board Product         :
Board Serial          : TW0M6X8JDNT008570208
Board Part Number     : 0M6X8JX01FRU
Device Description : FRU_PSU1 (ID 6)
Board Mfg Date        : Fri Jan  5 20:43:00 2018
Board Mfg             : DELL
Board Product         : PWR SPLY,1600W,RDNT,DELTA
Board Serial          : CNDED0081500XQ
Board Part Number     : 095HR5A04FRU
Device Description : FRU_PSU2 (ID 7)
Board Mfg Date        : Fri Jan  5 20:51:00 2018
Board Mfg             : DELL
Board Product         : PWR SPLY,1600W,RDNT,DELTA
Board Serial          : CNDED0081506H8
Board Part Number     : 095HR5A04
root@dellemc-diag-os:~# root@dellemc-diag-os:/mnt/nfs/users/<name>/<program>#
```

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

Dell EMC support

The Dell EMC support site provides documents and tools to help you effectively 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, 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/manuals/.

To search for drivers and downloads, go to www.dell.com/drivers/.

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