



Gigabyte Server Management Console

(for S260-NF Series System)

Copyright

© 2019 GIGA-BYTE TECHNOLOGY CO., LTD. All rights reserved.

The trademarks mentioned in this manual are legally registered to their respective owners.

Disclaimer

Information in this manual is protected by copyright laws and is the property of GIGABYTE. Changes to the specifications and features in this manual may be made by GIGABYTE without prior notice. No part of this manual may be reproduced, copied, translated, transmitted, or published in any form or by any means without GIGABYTE's prior written permission.

Documentation Classifications

In order to assist in the use of this product, GIGABYTE provides the following types of documentation:

- User Manual: detailed information & steps about the installation, configuration and use of this product (e.g. motherboard, server barebones), covering hardware and BIOS.
- User Guide: detailed information about the installation & use of an add-on hardware or software component (e.g. BMC firmware, rail-kit) compatible with this product.
- Quick Installation Guide: a short guide with visual diagrams that you can reference easily for installation purposes of this product (e.g. motherboard, server barebones).

Please see the support section of the online product page to check the current availability of these documents.

For More Information

For related product specifications, the latest firmware and software, and other information please visit our website at <http://www.gigabyte.com>

For GIGABYTE distributors and resellers, additional sales & marketing materials are available from our reseller portal: <http://reseller.b2b.gigabyte.com>

For further technical assistance, please contact your GIGABYTE representative or visit <https://esupport.gigabyte.com/> to create a new support ticket

For any general sales or marketing enquiries, you may also message GIGABYTE server directly by email: server.grp@gigabyte.com

Table of Contents

Chapter 2 Getting Started	5
1-1 Software Requirement	5
1-2 Log In Gigabyte Management Console	6
1-2-1 Required Browser Settings:	6
1-3 Quick Button and Logged-in User	8
1-4 Help	9
1-5 Menu Bar	9
Chapter 2 Enter Gigabyte Management Console	11
2-1 Dashboard	11
2-2 Sensor	12
2-2-1 Sensor Detail	13
2-2-2 Sensor Events	14
2-3 Sensor History	15
2-4 FRU Information	17
2-5 Logs & Reports	19
2-5-1 IPMI Event Log	19
2-5-2 System Log	21
2-5-3 Audit Log	22
2-6 Settings	23
2-6-1 Date & Time	23
2-6-2 External User Services	24
2-6-3 Log Settings	36
2-6-4 Network Settings	39
2-6-5 PAM Order Settings	45
2-6-6 Platform Event Filter	46
2-6-7 Services	55
2-6-8 SMTP Settings	58
2-6-9 SSL Settings	61
2-6-10 System Firewall	66
2-6-11 User Management	76
2-6-12 Fan Policy	81
2-6-13 Power Consumption	82
2-6-14 NVMeOF Device Management	83
2-6-15 Network Port IP	85
2-6-16 Network Port Auto-Negotiation	86
2-6-17 Target NQN Table	88
2-6-18 Drive Status	89

2-7	Power Control	93
2-8	Maintenance Group.....	94
2-8-1	Backup Configuration	95
2-8-2	Firmware Image Location	97
2-8-3	Firmware Information.....	98
2-8-4	Firmware Update.....	99
2-8-5	Preserve Configuration.....	102
2-8-6	Restore Configuration.....	107
2-8-7	Restore Factory Defaults.....	108
2-8-8	System Administrator.....	109
2-8-9	Switchtec Information	110
2-8-10	Sign Out.....	112

Chapter 2 Getting Started

1-1 Software Requirement

- Client machine with 8GB RAM.
- If the client machine has 4GB RAM, there will be lag in Video/keyboard/mouse functionality.
-

Supported Browsers

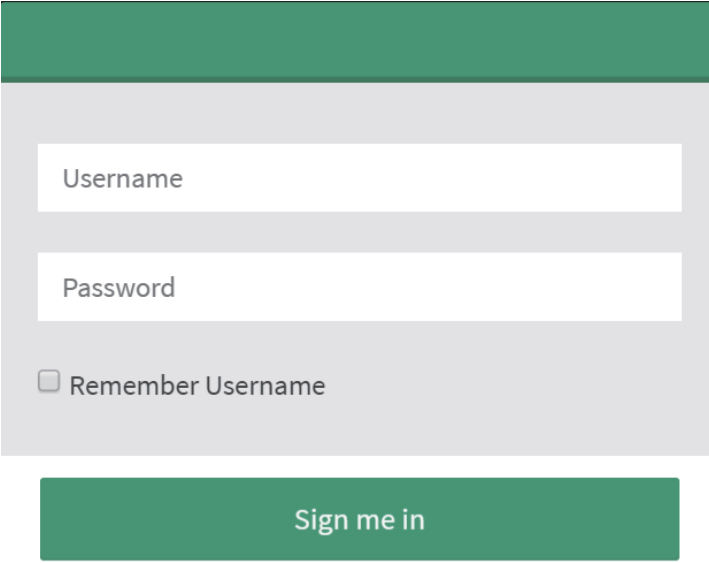
- Chrome latest version.
- IE 11 and above.
- Firefox (with limited support).



Note: It is advisable to use Chrome or IE for H5Viewer, since Firefox has its own memory limitations

1-2 Log In Gigabyte Management Console

To access the Gigabyte Management Console, the BMC Web utility will prompt you to enter the User Name and Password.



The login form consists of a light gray rectangular area. At the top is a dark green header bar. Below the header are two white input fields: the first is labeled 'Username' and the second is labeled 'Password'. Below the password field is a checkbox labeled 'Remember Username'. At the bottom of the gray area is a dark green button labeled 'Sign me in'. Below the button is a blue text link that says 'I forgot my password'.

The fields are explained as follows:

For basic login to the BMC Web UI, use the following login:

- **Username:** admin
- **Password:** password

Remember Username: Check this option to remember your login credentials.

Sign me in: After entering the required credentials, click the **Sign me in** to login to GUI.

I forgot my password: If you forget your password, you can generate a new one using this link.

Enter the username, click on **Forgot Password** link. This will send the newly generated password to the configured Email-ID for the user.

1-2-1 Required Browser Settings:

Allow file download from this site: For Internet Explorer, Choose **Tools ->Internet Options**

->**Security Tab**, based on device setup, select among Internet, Local intranet, trusted sites and restricted sites. Click **Custom level....** In the Security Settings - Zone dialog opened, under settings, find Downloads option, Enable File download option. Click **OK** to the entire dialog boxes.

For all Other Browsers, accept file download when prompted.

Enable javascript for this site: The icon indicates whether the javascript setting is enabled in browser.

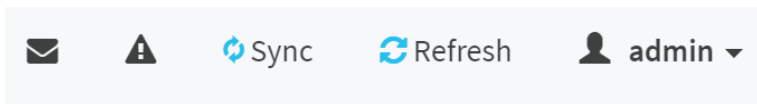
Enable cookies for this site: The icon indicates whether the cookies setting are enabled in browser.



Cookies must be enabled in order to access the website.

1-3 Quick Button and Logged-in User

The user information and quick buttons are located at the top right of the Web GUI. A screenshot of the logged-in user information is shown below.



User Information

The logged-in user information shows the logged-in user, his/her privilege and the four quick buttons allowing you to perform the following functions:

Logged-in user and its privilege level

This option shows the logged-in user name and privilege. There are five kinds of privileges.

User: Only valid commands are allowed.

Operator: All BMC commands are allowed except for the configuration commands that can change the behavior of the out-of-hand interfaces.

Administrator: All BMC commands are allowed.

No Access: Login access denied.

OEM: All OEM commands are allowed.

Notification: Click the icon to view the notification messages.

Refresh: Click the icon to reload the current page.

Sync: Click the icon to synchronize with Latest Sensor and Event Log updates.

Sign-out: Click the icon to log out of the Web GUI.

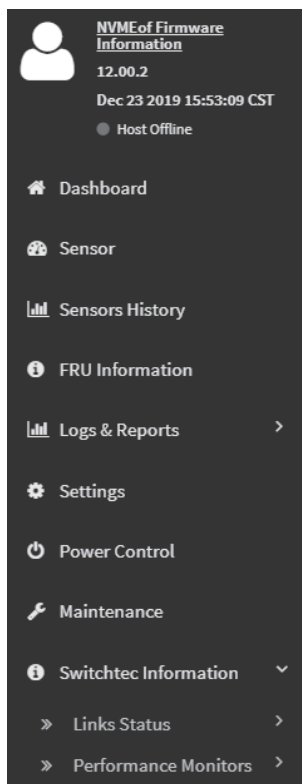
Warning: Click to view the warning messages.

1-4 Help

Help - The Help icon (?) is Located at the top right of the each page in Web GUI. Click this help icon to view more detailed field descriptions.

1-5 Menu Bar

The menu bar displays the following:



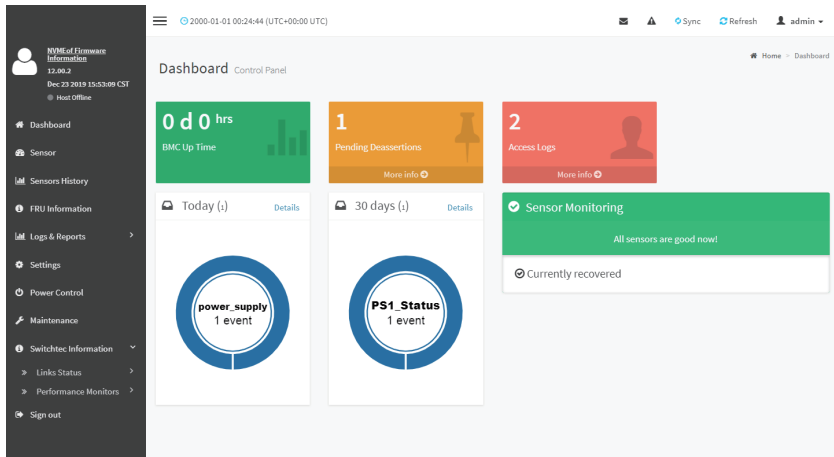
This page intentionally left blank

Chapter 2 Enter Gigabyte Management Console

2-1 Dashboard

The Dashboard page gives the overall information about the status of a device.

To open the Dashboard page, click **Dashboard** from the menu bar. It displays the following:



Dashboard

A brief description of the Dashboard page is given below.

BMC Up Time

It indicates the Power On time.

Pending Deassertions

It lists the all pending events incurred by various sensors and occupied/available space in logs can be viewed. To know about the pending events details, click the More info link. This navigates to the Event Log page.

Access Logs

A graphical representation of all events incurred by various sensors and occupied/available space in logs can be viewed, if you click on the More info link, you can view the Audit Log page.

Today & 30 Days (Event Logs)

This page displays the list of event logs occurred by the different sensors on this device. Click Details link on Today and 30 days to view the event logs for Today and 30 days respectively.

Sensor Monitoring

It lists all the critical sensors on the device. If you click on any list sensor, you can view the Sensor detail page with the Sensor information and Sensor Events details.

2-2 Sensor

The Sensor Readings page displays all the sensor related information.

To open the Sensor Readings page, click Sensor from the menu. Click on any sensor to show more information about that particular sensor, including thresholds and a graphical representation of all associated events.

A sample screenshot of Sensor Readings page is shown below.

Sensor Reading Live reading of all sensors

Critical Sensors (0)

All threshold sensors are normal

Discrete Sensor States (4)

Sensor Name	State
PS1_Status	Presence Detected
PS2_Status	No state defined
SEL	No state defined
Watchdog	No state defined

Normal Sensors (6)

Sensor Name	Reading	Behavior
NCT771BW_0x40	28.00 °C	
NVMe0_TEMP	24.00 °C	
NVMeG1_TEMP	23.00 °C	
PSU1_HOTSPOT	45.00 °C	
SYS_POWER	0.00 Watts	
TMPT5_0x90_left	24.00 °C	

Disabled Sensors (30)

PM8536_Di4Temp_m

PM8536_Di4Temp_s

TMPT5_0x92_midl

TMPT5_0x94_right

TMPT5_0x90_OB

NCT771BW_0x46

NVMeG2_TEMP

NVMeG3_TEMP

PCIEslot1_TEMP_m

PCIEslot2_TEMP_m

PCIEslot3_TEMP_m

PCIEslot1_TEMP_s

PCIEslot2_TEMP_s

PCIEslot3_TEMP_s

P_12V

P_3V3

P_0V9_SW_E

P_0V9_SW

P_1V8_SW

P_12V_N1

P_12V_N2

P_12V_FAN

PSU2_HOTSPOT

12V_N1

12V_N2

12V_FAN

FAN1

FAN2

FAN3

FAN4

The Sensor Readings page contains the following information:

In this Sensor Reading page, Live readings for all the available sensors with details like Sensor Name, Status, Current Reading and Behavior will be appeared, else you can choose the sensor

type that you want to display from the list. Some examples for sensors are Temperature Sensors, Fan Sensors, Watchdog Sensors and Voltage Sensors etc.

Note: Four DIMM Temp sensors are deployed for monitoring the DIMM temperature on the system. Users must take notice that the live reading of each DIMM Temp sensor indicates the temperature of a DIMM group, not the temperature of a specific DIMM.



Note: Four DIMM Temp sensors are deployed for monitoring the DIMM temperature on the system. Users must take notice that the live reading of each DIMM Temp sensor indicates the temperature of a DIMM group, not the temperature of a specific DIMM.

2-2-1 Sensor Detail

Select a particular Sensor from the Critical Sensor or Normal Sensor lists. The Sensor Information as Live Widget and Thresholds for the selected sensor will be displayed as shown below.



Note:For Illustrative Purpose, a sample screenshot of Sensor detail page with Change Thresholds option is shown and explained below.

Sensor detail All information about this sensor

PS1_Status Sensor Information

0x8001

Upper Non-Recoverable	NA
Upper Critical	NA
Upper Non-Critical	NA
Lower Non-Critical	NA
Lower Critical	NA
Lower Non-Recoverable	NA

Change Thresholds



Note: Widgets are little gadgets, which provide real time information about a particular sensor. User can track a sensor's behavior over a specific amount of time at specific intervals. The result will be displayed as a line graph in the widget. The session will not expire, until the widgets gets a live data of the last widget that is kept opened.

For the selected sensor, this widget gives a dynamic representation of the readings for the sensor.

There are six types of thresholds:

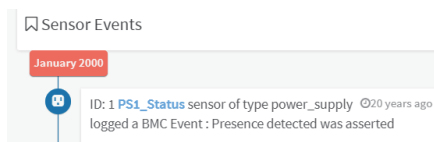
- Lower Non-Recoverable (LNR)
- Lower Critical (LC)
- Lower Non-Critical (LNC)
- Upper Non-Recoverable (UNR)
- Upper Critical (UC)
- Upper Non-Critical (UNC)

The threshold states could be Lower Non-critical - going low, Lower Non-critical - going high, Lower Critical - going low, Lower Critical - going high, Lower Non-recoverable - going low, Lower Non-recoverable - going high, Upper Non-critical - going low, Upper Non-critical - going high, Upper Critical - going low, Upper Critical - going high, Upper Non-recoverable - going low, Upper Non-recoverable - going high.

A graphical view of these events (Number of Entries vs. Thresholds) can be viewed as shown in the Sensor Readings page screenshot.

2-2-2 Sensor Events

The Sensor Events page displays information about events that have triggered the system's sensor. A sample screenshot of Sensor Events page is shown below.



2-3 Sensor History

The Sensor History page displays all the sensor history information.

To open the Sensor Readings page, click Sensor from the menu. Click on any sensor to show more information about that particular sensor, including thresholds and a graphical representation of all associated events.

A sample screenshot of Sensor History page is shown below.

The screenshot displays the 'Sensors History' page in the Gigabyte Server Management Console. The left sidebar contains navigation links: Dashboard, Sensor, Sensors History, FRU Information, Logs & Reports, Settings, Power Control, Maintenance, Switchtec Information, Links Status, Performance Monitors, and Sign out. The top header shows the date and time: 2000-01-01 00:27:17 (UTC+08:00 UTC). The page title is 'Sensors History' with the subtitle 'Reading history of all sensors'. The main content area shows a list of 41 sensors, with the first few being 12V_FAN, 12V_N1, 12V_N2, FAN1, FAN2, FAN3, FAN4, and NCT7718W_0xE2. The support status for each sensor is listed as 'Disabled' or 'Enabled'. The page also includes a 'Save' button and a 'Total numbers: (41)' indicator.

Sensor name	Support status: (8)
12V_FAN	Disabled
12V_N1	Disabled
12V_N2	Disabled
FAN1	Enabled
FAN2	Enabled
FAN3	Enabled
FAN4	Enabled
NCT7718W_0xE2	Disabled
NCT7718W_0xE4	Disabled
NCT7718W_BP	Disabled
NVMeG0_TEMP	Enabled
NVMeG1_TEMP	Enabled
NVMeG2_TEMP	Enabled
NVMeG3_TEMP	Enabled
PCIeSlot1_TEMP_m	Disabled
PCIeSlot1_TEMP_s	Disabled
PCIeSlot2_TEMP_m	Disabled
PCIeSlot2_TEMP_s	Disabled
PCIeSlot3_TEMP_m	Disabled
PCIeSlot3_TEMP_s	Disabled
PM8536_DieTemp_m	Disabled
PM8536_DieTemp_s	Disabled
PSU1_HOTSPOT	Disabled
PSU2_HOTSPOT	Disabled
P_0V9_SW	Disabled
P_0V9_SW_E	Disabled
P_12V	Disabled
P_12V_FAN	Disabled
P_12V_N1	Disabled
P_12V_N2	Disabled
P_1V8_SW	Disabled
P_3V3	Disabled
SYS_POWER	Disabled
TMPT5_0x0_0B	Disabled
TMPT5_0x0_left	Disabled
TMPT5_0x02_middel	Disabled
TMPT5_0x04_right	Disabled

It allows you to clear all entries sensor history in detail by clicking on **Clear Sensor History**. Click **Download Sensor History** to download all the sensor history logs.

2-4 FRU Information

FRU Information page displays the BMC's FRU device information. FRU page shows information like Basic Information, Chassis Information, Board Information and Product Information of the FRU device.

To open the FRU Information page, click **FRU Information** from the menu bar. Select a FRU Device ID from the FRU Information section to view the details of the selected device. A screenshot of FRU Information page is shown below.

The screenshot displays the FRU Information page in the Gigabyte Server Management Console. The page is titled "FRU Field Replaceable Units" and shows a list of available FRU devices. The selected device is "BMC_FRU". The page is divided into three main sections: Chassis Information, Board Information, and Product Information.

Available FRU Devices

FRU Device ID	FRU Device Name
0	BMC_FRU

Chassis Information

Chassis Information	Area Format Version
Chassis Type	Rack Mount Chassis
Chassis Part Number	01234567
Chassis Serial Number	01234567890123456789AB
Chassis Extra	

Board Information

Board Information	Area Format Version
Language	0
Manufacture Date Time	Fri Jan 7 00:00:00 2000
Board Manufacturer	GIGABYTE
Board Product Name	CPBD530-00
Board Serial Number	01234567890123456789AB
Board Part Number	123456789AB
FRU File ID	
Board Extra	NULL

Product Information

Product Information	Area Format Version
Language	0
Product Manufacturer	GIGABYTE
Product Name	S260-NF1-00
Product Part Number	0000000000001
Product Version	0100
Product Serial Number	01234567890123456789AB
Asset Tag	01234567890123456789AB
FRU File ID	

The following fields are displayed here for the selected device:

Available FRU Devices

- FRU device ID - Select the device ID from the drop down list
- FRU Device Name - The device name of the selected FRU device.

Chassis Information

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

Board Information

- Board Information Area Format Version
- Language
- Manufacture Date Time
- Board Manufacturer
- Board Product Name
- Board Serial Number
- Board Part Number
- FRU File ID
- Board Extra

Product Information

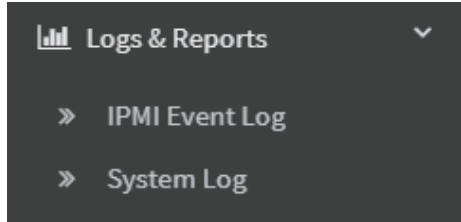
- Board Information Area Format Version
- Language
- Manufacture Date Time
- Board Manufacturer
- Board Product Name
- Board Serial Number
- Board Part Number
- FRU File ID
- Board Extra

2-5 Logs & Reports

The Logs & Reports page displays the following information:

- IPMI Event Log
- Video Log

A screenshot displaying the menu items under Logs & Reports is shown below.



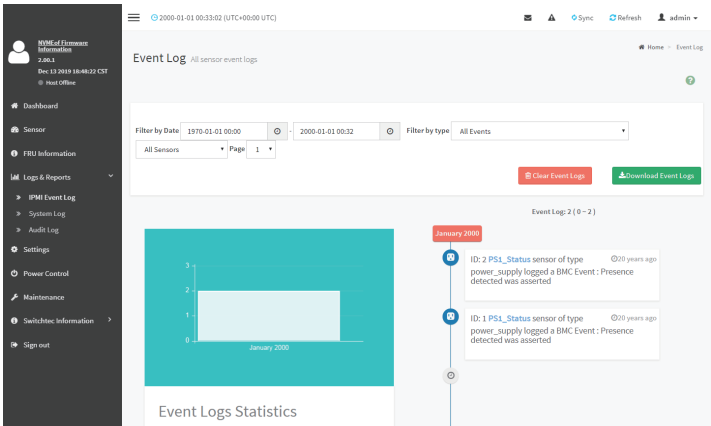
A detailed description of Logs & Reports is given below.

2-5-1 IPMI Event Log

This page displays the list of event logs occurred by the different sensors on this device. Double 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 or you can also sort the list of entries by clicking on any of the column headers.

To open the Event Log page, click **Logs & Reports > IPMI Event Log** from the menu bar.

A sample screenshot of Event Log page is shown below.



The Event Log page consists of the following fields:

Filter By Date: Filtering can be done by selecting **Start Date** and **End Date**.

Filter By Type: The category could be either All Events, System Event Records, OEM Event Records, BIOS Generated Events, SMI Handler Events, System Management Software Events, System Software - OEM Events, Remote Console software Events, Terminal Mode Remote Console software Events.



Note: Once the Filter By Date and Filter type are selected, the list of events will be displayed with the Event ID, Time Stamp, Sensor Type, Sensor Name and Description.

Event Log Statistics: Displays the statistical graph for the selected date.

Clear Event Logs: To delete all the event logs.

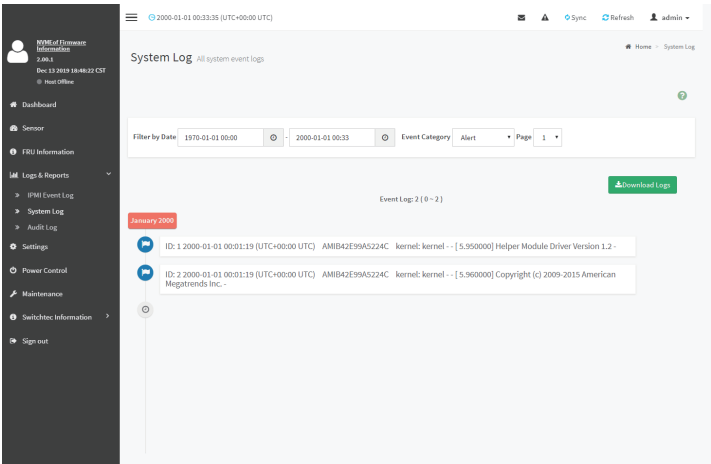
Download Event Logs: To download the event logs.

Procedure

1. From the Filter By Date field, select the time period by **Start Date** and **End Date** using Calendar for the event categories.
2. From the **Filter By Type** field, select the **Type** of the event and **Sensor** name to view the events for the date. The events will be displayed based on the selected time period.
3. To clear all events from the list, click **Clear All Event Logs**.
4. To download the event logs, click **Download Event Logs**.

2-5-2 System Log

To open the System Log page, click **Logs & Reports > System Log** from the menu bar. A sample screenshot of System Log page is shown below.

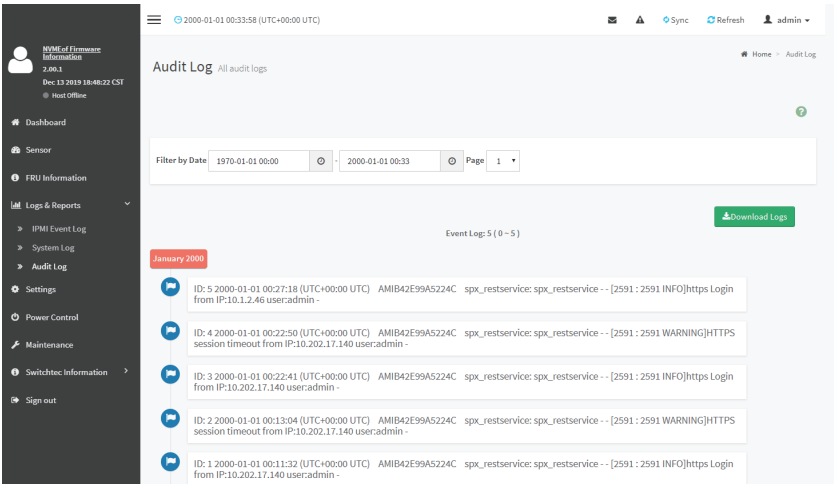


Procedure

1. From the Filter By Date field, select the time period by **Start Date** and **End Date** using Calendar for the event categories.
2. From the **Event Category** field, select the **Category** of the event.
3. To download the system logs, click **Download Logs**.

2-5-3 Audit Log

To open the Audit Log page, click **Logs & Reports > Audit Log** from the menu bar. A sample screenshot of Audit Log page is shown below.

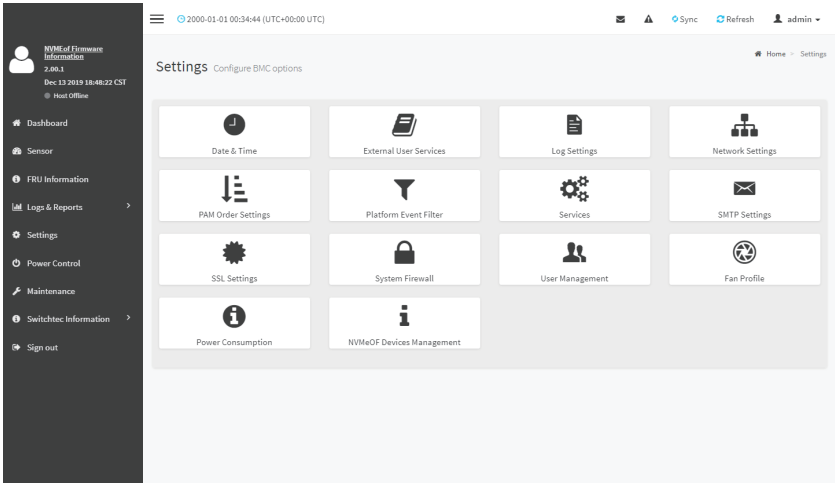


Procedure

1. From the Filter By Date field, select the time period by **Start Date** and **End Date** using Calendar for the event categories.
2. To download the audio logs, click **Download Logs**.

2-6 Settings

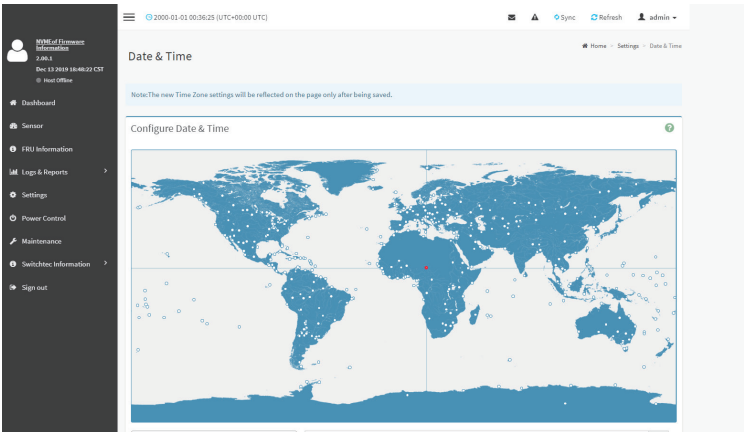
This group of pages allows you to access various configuration settings. A screenshot of Configuration Group menu is shown below.



A detailed description of the Settings menu is given below.

2-6-1 Date & Time

This field is used to set the date and time on the BMC. A Sample screenshot of Date & Time is shown below.



The Date & Time section consists of the following fields:

Configure Date & Time: Displays Time zone list containing the UTC offset along with the locations and Navigational line to select the location which can be used to display the exact local time.

Automatic Date & Time: To automatically synchronize Date and Time with the NTP Server.

Save: To save the configured settings.

Procedure

1. Select the Time zone location from the map.
2. Enable Automatic Date & Time option.
3. Click Save button to save the settings.

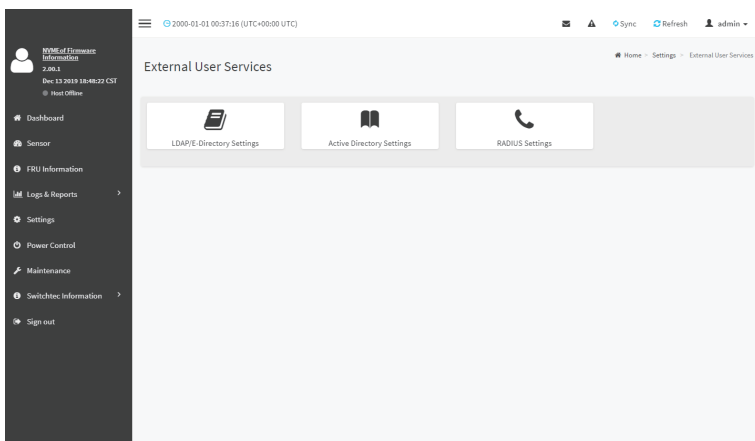
2-6-2 External User Services

LDAP/E-Directory Settings

The **Lightweight Directory Access Protocol (LDAP)/E-Directory Settings** is an application protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.

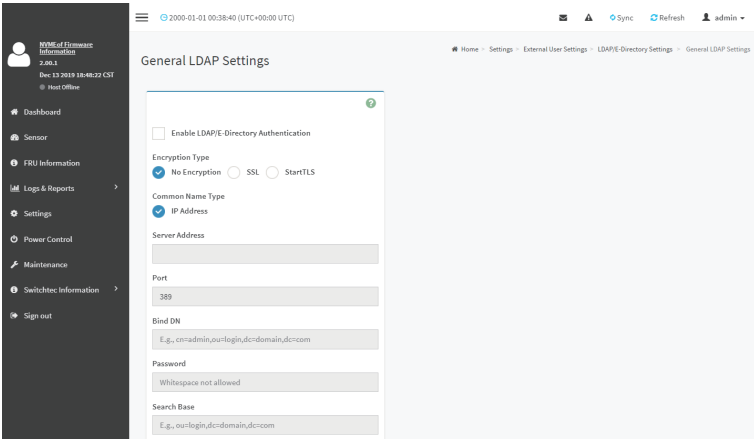
In Web GUI, LDAP is an Internet protocol that BMC can use to authenticate users. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate BMC users. This is done by passing login requests to your LDAP Server. This means that there is no need to define an additional authentication mechanism, when using the BMC. Since your existing LDAP Server keeps an authentication centralized, you will always know who is accessing the network resources and can easily define the user or group- based policies to control access.

To open External User Services page, click **Settings > External User Services** from the menu bar. A sample screenshot of External User Services page is shown below.



To open LDAP/E-DIRECTORY **Settings** page, click **Settings > External User Services > LDAP/E-Directory Settings** from the menu bar.

A sample screenshot of External User Services page is shown below.



The fields of LDAP/E-Directory Settings page are explained below.

General Settings: To configure LDAP/E-Directory Settings. Options are Enable LDAP/E-Directory Authentication, IP Address, Port and Search base.

Role Groups: To add a new role group to the device. Alternatively, double click on a free slot to add a role group.

Procedure

1. In the LDAP/E-Directory Settings page, click General Settings. A sample screenshot of General LDAP Settings page is given below.

2. Click **Enable LDAP/E-Directory Authentication**, to enable LDAP/E-Directory Settings.



Note: Configure proper port number, when SSL is enabled.

3. Select the Common Name Type as IP Address.
4. Enter the IP address of LDAP server in the Server Address field.



Note: 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.

Supports IPv4 Address format and IPv6 Address format.

Configure FQDN address, when using StartTLS with FQDN.

5. Specify the LDAP Port in the **Port** field.



Note: Default Port is 389. For SSL connections, default port is 636. The Port value ranges from 1 to 65535.

6. Specify the Bind DN that is used during bind operation, which authenticates the client to the server.



Note: Bind DN is a string of 4 to 64 alpha-numeric characters.

It must start with an alphabetical character.

Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.

Example: cn=manager, ou=login, dc=domain, dc=com

7. Enter the password in the **Password** field.



Note: Password must be at least 1 character long.

Blank space is not allowed

This field will not allow more than 48 characters.

8. Enter the **Search Base**. The Search base allows the LDAP server to find which part of the external directory tree to be searched. The search base may be something equivalent to the organization, group of external directory.



Note: Search base is a string of 4 to 63 alpha-numeric characters.

It must start with an alphabetical character.

Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.

Example: ou-login, dc-domain, dc-com

9. Select Attribute of User Login to find the LDAP/E-Directory server which attribute should be used to identify the user.



Note: It only supports cn or uid.

10. Select **CA Certificate File** from the Browse field to identify the certificate of the trusted CA certs.
11. Select the **CA Certificate File** to find the client certificate filename.
12. Select **Private Key** to find the client private key filename.



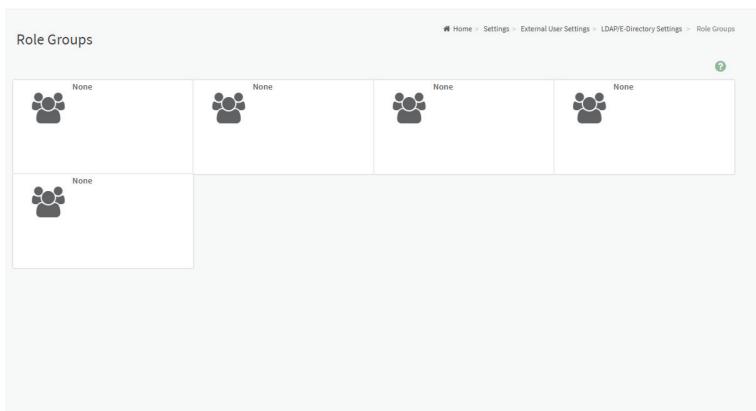
Note: All the 3 files are required, when StartTLS is enabled.

13. Click Save to **save** the settings.

To add a new Role Group

1. In the LDAP/E-Directory Settings page, click Role Groups and select a blank row.
2. Click **Add Role Group** or alternatively double click on the blank row to open the Add

Role group page as shown in the screenshot below.



3. In the Group Name field, enter the name that identifies the role group.



Note: Role Group Name is a string of 255 alpha-numeric characters. Special symbols hyphen and underscore are allowed.

4. In the Group Domain field. Enter the Role Group Domain where the role group is located.



Note: Domain Name is a string of 4 to 64 alpha-numeric characters. It must start with an alphabetical character.

Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed. Example: cn=manager, ou=login, dc=domain, dc=com

5. In the Group Privilege field, enter the level of privilege (User, Administrator, Operator, None) to assign to this role group.
6. Select one or both of the required options
 - KVM Access
 - VMedia Access
7. Click **Save** to save the new role group and return to the Role Group List.

Active Directory Settings

An active directory is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains. An active directory (sometimes referred to as AD) does a variety of functions including the ability to provide information on

objects. It also helps to organize these objects for easy retrieval and access, allows access by end users and administrators and allows the administrator to set security up for the directory. Active Directory allows you to configure the Active Directory Server Settings. The displayed table shows any configured Role Groups and the available slots. You can modify, add or delete role groups from here. Group domain can be the AD domain or a trusted domain. Group Name should correspond to the name of an actual AD group.

Note: To view the page, you must be at least a User and to modify or add a group, you must be an Administrator.

To open Active Directory Settings page, click **Settings > External User Settings > Active Directory** from the menu bar. A sample screenshot of Active Directory Settings page is shown below.

The fields of Active Directory page are explained below.

General Settings: This option is used to configure Active Directory General Settings. Options are Enable Active Directory Authentication, Secret User Name, Secret Password, User Domain name, and up to three Domain Controller Server Addresses.

Role Groups: To add a new role group to the device. Alternatively, double click on a free slot to add a role group.

Procedure

Entering the details in General Active Directory Settings page:

1. Click on **General Settings** to open the General Active Directory Settings page.

2. In the Active Directory Settings page, check or uncheck the **Enable Active directory Authentication** check box to enable or disable **Active Directory Authentication** respectively.



Note: If you have enabled Active Directory Authentication, enter the required information to access the Active Directory server.

3. Specify the Secret user name and password in the Secret User Name and Secret Password fields respectively.



Note: Secret username/password for AD is not mandatory. When secret username & password is empty, Authentication fails will be always treated as Invalid Password error. For Invalid Password error PAM will not try other Authentication Methods. So it is recommended to keep AD in the last location in PAM order.

User Name is a string of 1 to 64 alpha-numeric characters.

It must start with an alphabetical character.

It is case-sensitive.

Special characters like comma, period, colon, semicolon, slash, backslash, square brackets,

Blank space is not allowed, angle brackets, pipe, equal, plus, asterisk, question mark, ampersand, double quotes, space are not allowed.

Password must be at least 6 character long and will not allow more than 127 characters.

4. Specify the Domain Name for the user in the User Domain Name field. E.g. MyDomain.com
5. Configure IP addresses in Domain **Controller Server Address1**, **Domain Controller Server Address2** and **Domain Controller Server Address3**



Note: IP address of Active Directory server: At least one Domain Controller Server Address must be configured. IP Address made of 4 numbers separated by dots as in

"XXX.XXX.XXX.XXX".

Each number ranges from 0 to 255.

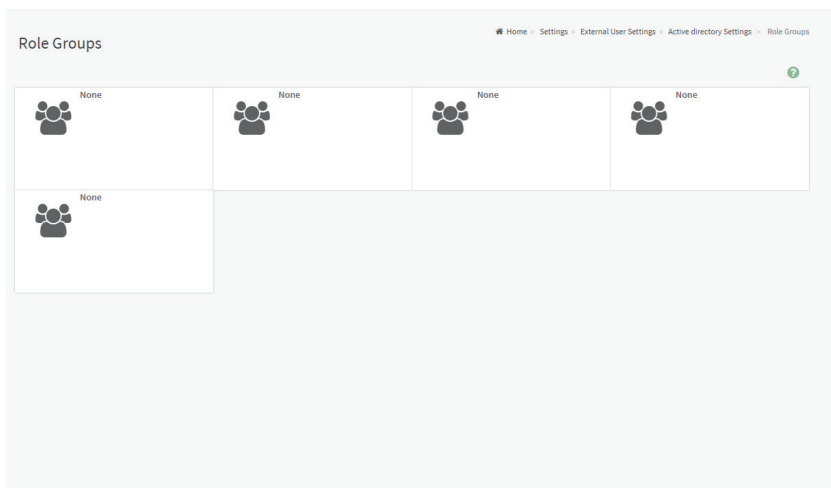
First number must not be 0.

Domain Controller Server Addresses will supports IPv4 Address format and IPv6 Address format.

6. Click Save to **save** the entered settings and return to Active Directory Settings page.

Role Groups

To open Role Group page, click **Settings > External User Settings > Active Directory > Role Groups** from the menu bar. A sample screenshot of Role Groups page is shown below.



The fields of Role Group page are explained below.

Role Group Name: The name that identifies the role group in the Active Directory.



Note: Role Group Name is a string of 64 alpha-numeric characters. Special symbols hyphen and underscore are allowed.

Group Name: This name identifies the role group in Active Directory.



Note: Role Group Name is a string of 64 alpha-numeric characters. Special symbols hyphen and underscore are allowed.

Group Domain: The domain where the role group is located.



Note: Domain Name is a string of 255 alpha-numeric characters.
Special symbols hyphen, underscore and dot are allowed.

Group Privilege: The level of privilege to assign to this role group.

KVM Access: To provide access to KVM for AD authenticated role group user.

VMedia Access: To provide access to VMedia for AD authenticated role group user.

To add a new Role Group

1. In the Active Directory Settings page, select a Role Group and click Add Role Group or alternatively double click on the blank row to open the Add Role group page as shown in the screenshot below.

2. In the **Group Name** field, enter the name that identifies the role group in the Active Directory.



Note: Role Group Name is a string of 64 alpha-numeric characters.
Special symbols hyphen and underscore are allowed.

3. In the Group Domain field, enter the domain where the role group is located.



Note: Domain Name is a string of 255 alpha-numeric characters. - Special symbols hyphen, underscore and dot are allowed.

4. In the **Group Privilege** field, enter the level of privilege to assign to this role group.
5. Select the required options

6. Click **Save** to add the new role group and return to the Role Group List.

To Delete a Role Group

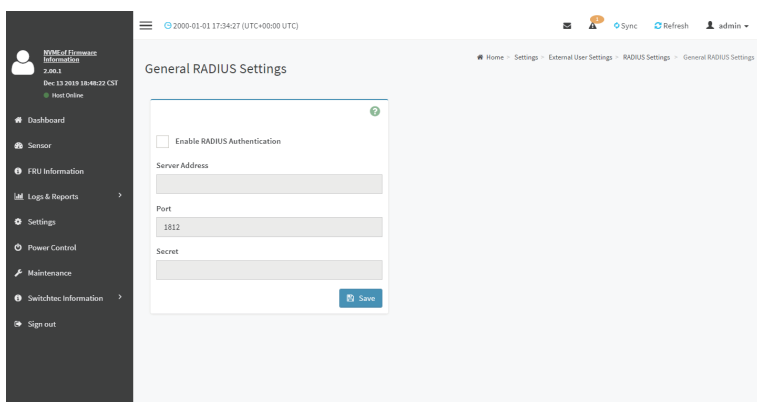
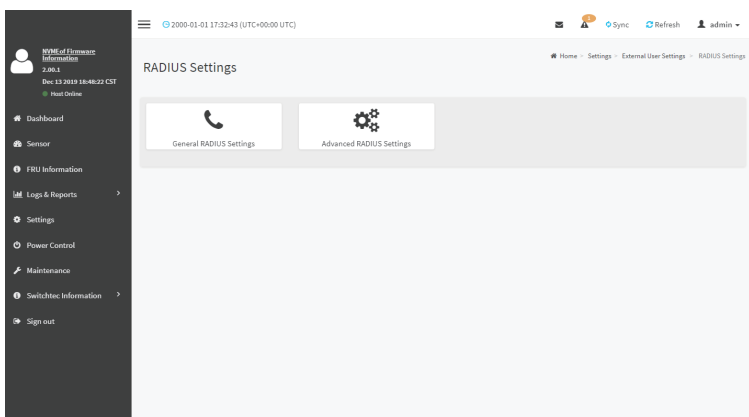
1. In the **Role Groups** Page, select the row that you wish to delete
2. Click Delete Role Group.

RADIUS Settings

RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities.

In Web GUI, this page is used to set the RADIUS Authentication.

To open RADIUS Settings page, click **Settings > External User Settings > RADIUS Settings** from the menu bar. A sample screenshot of RADIUS Settings page is shown below.



The fields of General RADIUS Settings page are explained below.

Enable RADIUS Authentication: Option to enable/disable RADIUS authentication.

Server Address: The IP address of RADIUS server.



Note: IP Address (Both IPv4 and IPv6 format).
FQDN (Fully Qualified Domain Name) format.

Port: The RADIUS Port number.



Note: Default Port is 1812.
Port value ranges from 1 to 65535.

Secret: The Authentication Secret for RADIUS server.



Note: This field will not allow more than 31 characters.
Secret must be at least 4 characters long.
Blank space is not allowed.

Procedure

1. Enable the **RADIUS Authentication** check box to authenticate the RADIUS.
2. Click **Advanced RADIUS Settings**. This opens the Radius Authorization window as shown below.



Note: For Authorization Purpose, configure the Radius user with Vendor Specific Attribute in Server side.

Example: 1

testadmin Auth-Type: =PAP, Cleartext-Password:="admin"

Auth-Type: =PAP, Vendor-Specific= "H=4 "

Example: 2

test operator Auth-Type: = PAP, Cleartext-Password:="operator"

Auth-Type: =PAP, Vendor-Specific= "H=3 "

If you change the Vendor-Specific value in server then you should change the same

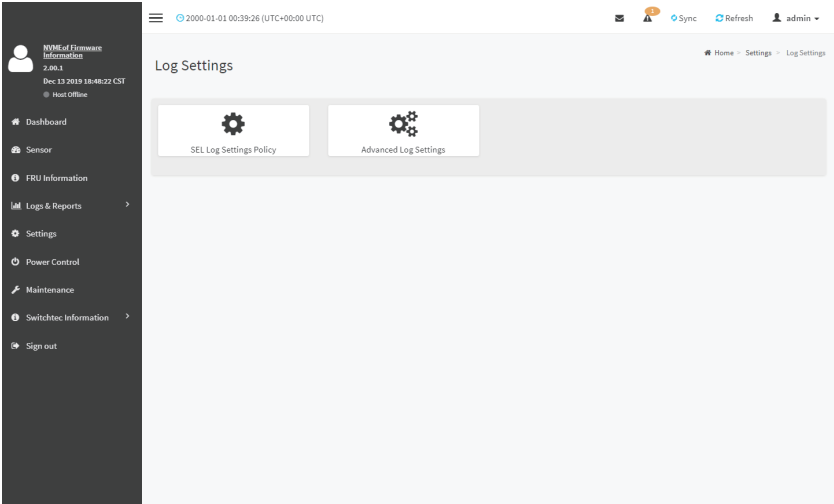
values in this page.

3. Click **Save** to save the changes made.

2-6-3 Log Settings

In BMC Web GUI, System and Audit log page displays a list of system logs and audit logs occurred in this device.

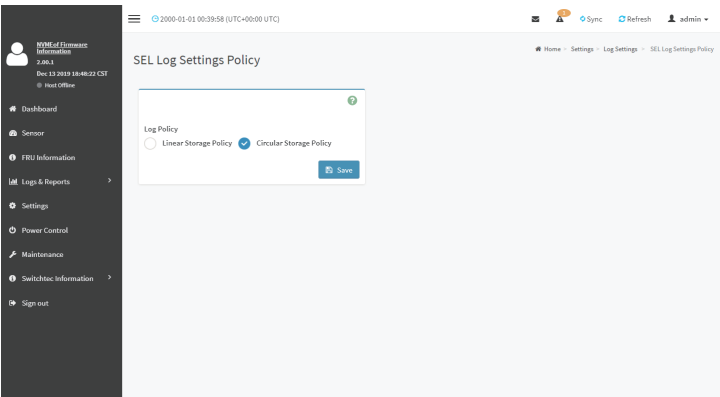
To open Log Settings page, click **Settings > Log Settings** from the menu bar. A sample screenshot of Log Settings page is shown below.



The fields of Log Settings page are explained below.

SEL Settings Policy

To open SEL Settings Policy page, click **Settings > Log Settings > SEL Settings Policy** from the menu bar. A sample screenshot of SEL Settings Policy page is shown below.



Advanced Log Settings

To open Advanced Log Settings page, click **Settings > Log Settings > Advanced Log Settings** from the menu bar. A sample screenshot of Advanced Log Settings Policy page is shown below.

The screenshot shows the 'Advanced Log Settings' page. On the left is a dark sidebar with a user profile 'HVM of Firmware Information 2.06.1 Dec 13 2019 18:46:23 CST @ Host Office' and a menu with items like Dashboard, Sensor, FRU Information, Logs & Reports, Settings, Power Control, Maintenance, Switchtec Information, and Sign out. The main area has a top bar with a clock '2009-01-01 00:40:23 (UTC+00:00 UTC)' and user controls 'Sync', 'Refresh', and 'admin'. Below the title 'Advanced Log Settings' is a form with the following fields: 'System Log' (checked), 'Local Log' (checked), 'Remote Log' (unchecked), 'Port Type' (radio buttons for UDP and TCP, with UDP selected), 'File Size' (text input with '50000'), 'Rotate Count' (text input with '0'), 'Remote Log Server' (text input with 'Server IP or Hostname'), 'Remote Server Port' (text input with '0'), and 'Enable Audit Log' (checked). A 'Save' button is at the bottom right.

This page is used to configure the log policy for the event log. The fields are as follows.

Enable System Log: This field is to enable or disable the System Logs.

Location: Specifies the Location for system logs, whether it should be preserved in a **Local Log** or on a **Remote Log**.



Note: Local file resides at `/var/log/`

File Size: This field is to specify the size of the file in bytes if the selected log type is local.



Note: Size ranges from 3 to 65535. Log files are rotated when they grow bigger than size bytes mentioned, with regards for the last rotation time interval (1 minute).

Rotate Count: To back up the log information in back up files.



Note: Values supported are 0 and 1.

When log information exceeds the file size, the old log information is automatically moved to back up files based on the rotate count value. If rotate count is zero, then old log information gets cleared permanently.

File Size and Rotate Count options will be available only when Local Log is enabled.

Remote Log Server: This field is to specify the Remote server address to log the system events.



Note: Server address will support the following:

IPv4 address format.

FQDN (Fully qualified domain name) format.

Remote Server Port: This field is to specify the Remote Server port address to log the system

events.



Note: Remote Log Server and Remote Server Port options will be available only when Remote Log is enabled.

Enable Audit Log: To enable or disable the audit log.

Save: To save the current changes.

Procedure

1. In the **System Log** field, enable or disable the option.
2. Select the Log type: Local Log or Remote Log.
3. If Local log is selected, enter the file size in the **File Size** field and rotate count in the **Rotate Count** field.



Note: If Remote log is selected, the fields file size and rotate count need not be mentioned.

4. If remote log is selected specify the **Server Address** of the remote server, where the system events are logged.
5. In the **Audit Log** field, check or uncheck the **Enable** option as desired.
6. Click **Save** to save the changes.

Steps to configure the remote server to enable syslogging



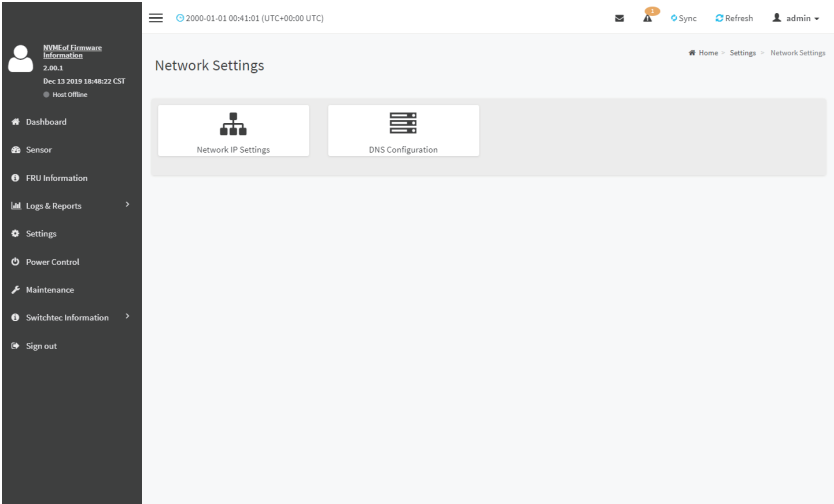
Note: This example uses FC13 as the remote machine to log syslog.

On FC machine, disable the following lines for UDP in /etc/rsyslog.conf:

1. MODLOAD imudp
2. UDPSERVER 514

2-6-4 Network Settings

The Network Settings page is used to configure the network settings for the available LAN channels. It also allows users to manage the DNS settings or configure Network Controller Sideband Interface of a device. To open the Network Settings page, click **Settings > Network Settings** from the menu bar.



Network IP Settings

To open Network IP Settings page, click **Settings > Network Settings > Network IP Settings** from the menu bar. A sample screenshot of Network IP Settings page is shown below.

The screenshot shows the 'Network IP Settings' page. On the left is a dark sidebar with a user profile 'jane.a' and a menu with options: Dashboard, Sensor, FRI Information, Logs & Reports, Settings (selected), Power Control, Maintenance, Switches Information, and Sign out. The main content area has a top bar with a clock '2020-01-01 09:41:45 (UTC+08:00 UTC)' and buttons for Sync, Refresh, and Admin. Below the title 'Network IP Settings' is a form with sections: 'Enable LAN' (checked), 'LAN Interface' (bond0), 'MAC Address' (84:2E:59:AB:22:4C), 'Enable IPv4' (checked), 'Enable IPv4 DHCP' (checked), 'IPv4 Address' (10.1.27.147), 'IPv4 Subnet' (255.255.255.0), 'IPv4 Gateway' (10.1.27.251), 'Enable IPv6' (checked), 'Enable IPv6 DHCP' (checked), 'IPv6 Index' (0), 'IPv6 Address' (empty), 'Subnet Prefix Length' (0), 'Enable VLAN' (unchecked), 'VLAN ID' (0), and 'VLAN Priority' (0). A 'Save' button is at the bottom right.

The fields of Network IP Settings page are explained below.

Enable LAN: To enable or disable the LAN Settings.

LAN Interface: Lists the LAN interfaces.

MAC Address: This field displays the MAC Address of the device. This is a read only field.

Enable IPv4: This option is to enable/disable the IPv4 settings in the device.

Enable IPv4 DHCP: This option is to enable IPv4 DHCP support for the selected interface.

IPv4 Address, IPv4 Subnet Mask, and IPv4 Default Gateway: These fields are for specifying the static IPv4 address, Subnet Mask and Default Gateway to be configured to the device.



Note: 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.

Enable IPv6: To Enable/Disable the IPv6 configuration settings.

Enable IPv6 DHCP: To Enable/Disable the IPv6 settings in the device. It dynamically configures IPv6 address using DHCP (Dynamic Host Configuration Protocol).

IPv6 Index: To specify a static IPv6 Index to be configured to the device. E.g.: 0

IPv6 Address: To specify a static IPv6 address to be configured to the device. E.g.: 2004::2010

Subnet Prefix length: To specify the subnet prefix length for the IPv6 settings.



Note: Value ranges from 0 to 128.

Default Gateway: Specify v6 default gateway for the IPv6 settings.



Note: If core feature IPV6_COMPLIANCE is enabled, the IPV6 default Gateway field will not be displayed.

Enable VLAN: To enable/disable the VLAN support for selected interface.

VLAN ID: The Identification for VLAN configuration.



Note: Value ranges from 2 to 4094.

VLAN Priority: The priority for VLAN configuration.



Note: Note: Value ranges from 0 to 7.
7 is the highest priority for VLAN.

Save: To save the entries.

Procedure

1. Check **Enable LAN** to enable LAN support for the selected interface.
2. Select the **LAN Interface** to be configured.
3. Check **Enable IPv4** to enable IPv4 support for the selected interface.
4. Check **Enable IPv4 DHCP** to dynamically configure IPv4 address using DHCP.
5. If the field is disabled, enter the **IPv4 Address, IPv4 Subnet Mask and IPv4 Default Gateway** in the respective fields.
6. In IPv6 Configuration, if you wish to enable the IPv6 settings, check **Enable IPv6**.
7. If the IPv6 setting is enabled, enable or disable the option **Enable IPv6 DHCP**.
8. If the field is disabled, enter the **IPv6 Address, Subnet Prefix length and IPv6 Index** in the given field.
9. In VLAN Configuration, if you wish to enable the VLAN settings, check **Enable LAN**.
10. Enter the **VLAN ID** in the specified field.
11. Enter the **VLAN Priority** in the specified field.
12. Click **Save** to save the entries.

DNS Configuration

The **Domain Name System (DNS)** is a distributed hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates the information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

The DNS Server settings page is used to manage the DNS settings of a device.

To open DNS Server Settings page, click **Settings > Network Settings > DNS Configuration** from the menu bar. A sample screenshot of DNS Configuration page is shown below.

NYM of Firmware Information
2.80.1
Dec 13 2019 18:48:22 CST
Host Offline

Dashboard
Sensor
FRU Information
Logs & Reports
Settings
Power Control
Maintenance
Switchtec Information
Sign out

2000-01-01 00:42:17 (UTC+00:00)

Sync
Refresh
admin

Home - Settings - Network Settings - DNS Configuration

DNS Configuration

☒ DNS Enabled
☐ mDNS Enabled

Host Name Setting
☒ Automatic ☐ Manual

Host Name
AMI842E99A5224C

BMC Registration Settings
BMC Interface:
bond0
☒ Register BMC
Registration method:
☒ Nsupdate ☐ DHCP Client FQDN ☐ Hostname

TSIG Configuration
☐ TSIG Authentication Enabled
Current TSIG Private File Info
Not Available
New TSIG Private File

Domain Setting
☒ Automatic ☐ Manual
Domain Interface
bond0_v4

Domain Name Server Setting
☒ Automatic ☐ Manual
DNS Interface
bond0

IP Priority
☒ IPv4 ☐ IPv6

Domain Name Service Configuration

DNS Enabled: To enable/disable all the DNS Service Configurations.

mDNS Enable: To enable/disable the mDNS Support Configurations.

Host Name Settings: Choose either Automatic or Manual settings.

Host Name: It displays host name of the device. If the Host setting is chosen as Manual, then specify the host name of the device.



Note: Value ranges from 1 to 64 alpha-numeric characters.

Special characters '-'(hyphen) and '_'(underscore) are allowed.

It must not start or end with a '-'(hyphen). IE browsers won't work correctly if any part of the host name contain underscore (_)character.

BMC Registration Settings

BMC Interface: Options to register the BMC through the Interfaces (eth0ð1).

Register BMC: To register BMC through registration method.

Registration Method

Options to register the BMC are through **NS Update** or **DHCP Client FQDN** or **Hostname**.

TSIG Configuration

Both: Check this option to modify TSIG authentication for both interfaces.

Eth 0&1:

- **TSIG Authentication Enabled:** Check this box to enable TSIG authentication while registering DNS via nsupdate. Separate TSIG files can be uploaded for each LAN interface.
- **Current TSIG Private File:** The information of Current TSIG private file along with its uploaded date/time will be displayed (readonly).
- **New TSIG Private File:** Browse and navigate to the TSIG private file.



Note: TSIG file should be of private type.

Domain Setting: Select whether the domain interface will be configured manually or automatically.

- **Automatic** - If you Select Automatic, the Domain Name cannot be configured as it will be done automatically. The field will be disabled.
- **Manual** - If the Domain setting is chosen as Manual, then specify the domain name of the device.



Note: If you select "Automatic" it displays the Domain Interface option. If you select "Manual" it displays "Domain name".

- **Domain Name:** It displays the domain name of the device.

Domain Name Server Setting

Automatic - If you select Automatic "DNS Interface" option should be explained.

Manual - Specify the DNS (Domain Name System) server address to be configured for the BMC.

IP Priority:

- If IP Priority is IPv4, it will have 2 IPv4 DNS servers and 1 IPv6 DNS server.
- If IP Priority is IPv6, it will have 2 IPv6 DNS servers and 1 IPv4 DNS server.



Note: This is not applicable for Manual configuration.

DNS Server 1, 2 & 3

To specify the DNS (Domain Name System) server address to be configured for the BMC.



Note: IPv4 Addresses should be given in dotted decimal representation.

IPv6 Addresses are supported and must be global unicast addresses.

DNS Server Address will support the following:

- IPv4 Address format.
- IPv6 Address format.

Save: To save the current changes.

Procedure

1. In Domain Name Service Configuration, Enable DNS Service.
 - Check the option **DNS Enabled** to enable all the DNS Service Configurations.
2. Choose the Host Name Setting either Automatic or Manual.



Note: If you choose Automatic, you need not enter the Host Name and if you choose Manual, you need to enter the Host Name.

3. Enter the **Host Name** in the given field if you have chosen Manual Configuration.
4. Under Register BMC, choose the BMC's network port to register with DNS settings.
5. Check **Register BMC** option to register with DNS settings.
 - **Nsupdate** - Choose Nsupdate option to register with DNS server using nsupdate application.
 - **DHCP Client FQDN** - Choose DHCP Client FQDN option to register with DNS Server using DHCP option 81.
 - **Hostname** - Choose Hostname option to register with DNS server using DHCP option 12.

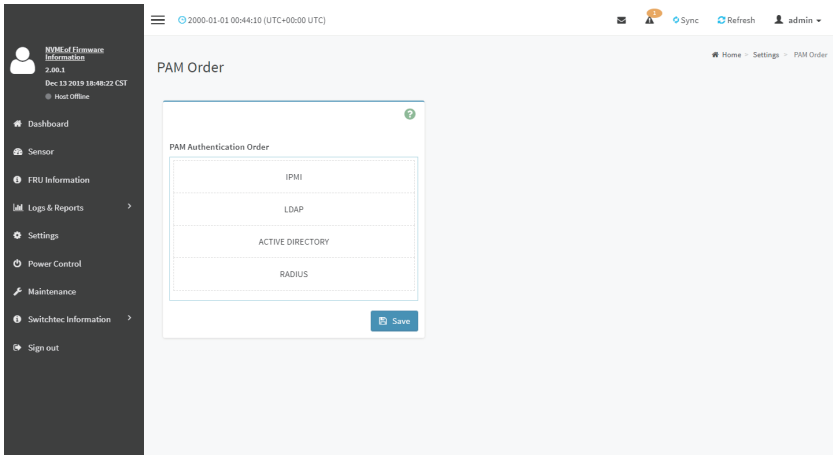


Note: Hostname option should be selected, if the DHCP client FQDN option is not supported by DHCP server.

6. Check **Both** option to modify TSIG authentication for both interfaces (eth0&1).
7. In **Eth 0&1 TSIG Configuration**, Check TSIG Authentication Enabled option to enable/disable TSIG authentication while registering DNS via nsupdate.
 - The current file name will be displayed in Current TSIG Private file info field.
 - To view a new one, click New TSIG private file to browse and navigate to the TSIG private file.
8. In the Domain Settings,
 - Select the domain settings (Automatic or Manual).
 - Enter the Domain Name in the given field if the option "Manual" is being selected in domain settings field.
9. In Domain Name Server Setting,
 - Select the DNS Name Server Setting.
 - Choose the IP Priority, either IPv4 or IPv6.
 - Enter the DNS Server address.
10. In DNS Server1, DNS Server2 and DNS Server3, enter the server addresses to be configured for the BMC.
11. Click **Save** to save the entries.

2-6-5 PAM Order Settings

This page is used to configure the PAM ordering for user authentication in to the BMC.
To open PAM Ordering page, click **Settings > PAM Order Settings** from the menu bar. A sample screenshot of PAM Order page is shown below:



The fields of **Settings > PAM Ordering** page are explained below.

PAM Module: It shows the list of available PAM modules supported in BMC.



Note: It is recommended to not to keep same username for different PAM modules.

If Authentication fails, the reason of fail could be invalid User or Invalid Password.

If Radius Authentication fails, we can't differentiate whether it is invalid user or invalid password. So it is always treated as Invalid username error and PAM will try other Authentication Methods.

If AD contains secret username & password as empty, Authentication fails will be always treated as Invalid Password error. For Invalid Password error PAM will not try other Authentication Methods. So it is recommended to keep AD in the last location in PAM order.

Procedure

1. Select the required PAM module and click and drag the required PAM module. It can be moved UP or DOWN to change its arrangement order.
2. Click **Save** to save any changes made.



Note: Whenever the configuration is modified, the web server will be restarted automatically. Logged-in session will be logged out.

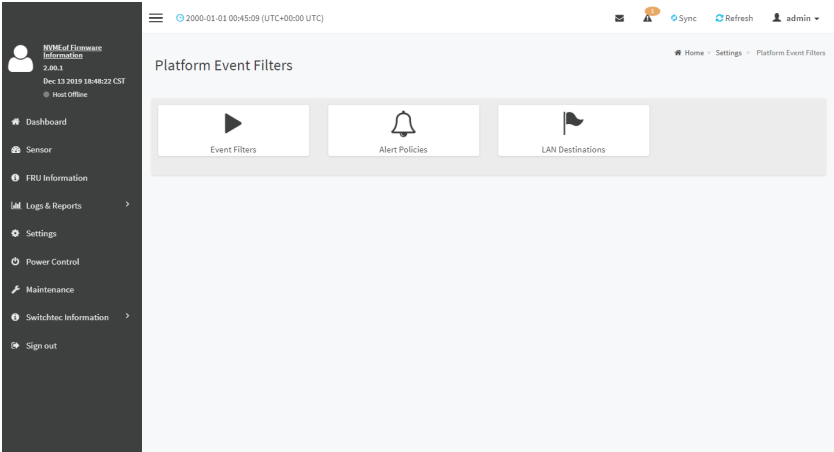
2-6-6 Platform Event Filter

Platform Event Filter (PEF) provides a mechanism for configuring the BMC to take selected actions on event messages that it receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert.

In BMC Web GUI, the PEF Management is used to configure the following:

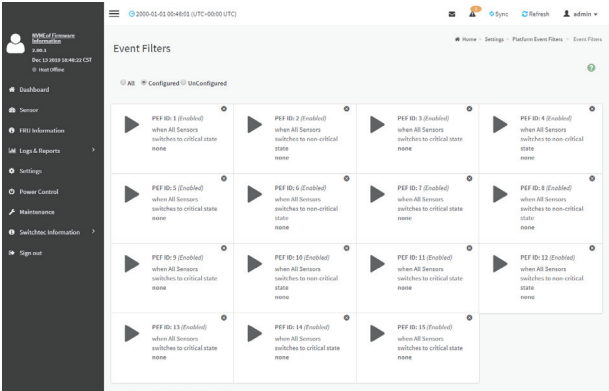
- Event Filters
- Alert Policies
- LAN Destinations

To open PEF Management Settings page, click Settings > Platform Event Filter from the menu bar. Each tab is explained below.



Event Filters

A PEF implementation is recommended to provide at least 40 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over-temperature, power system failure, fan failure events, etc. Remaining entries can be made available for 'OEM' or System Management Software configured events. Note that individual entries can be tagged as being reserved for system use - so this ratio of pre-configured entries to run-time configurable entries can be reallocated if necessary.



The fields of Platform Event Filters Tab are explained below.
This page contains Pre-configured 40 Events with PEF IDs.

Procedure

1. Click the Event Filters section to configure the event filters in the available slots.
2. To Add an Event Filter entry, select a free section to open the Event Filter entry page. A sample screenshot of Event Filter Configuration page is shown below.

The screenshot displays the 'Event Filter Configuration' interface. On the left is a dark sidebar with navigation options: Dashboard, Sensor, PEK Information, Logs & Reports, Settings, Power Control, Maintenance, Serial/Port Information, and Sign out. The main content area is titled 'Event Filter Configuration' and includes a status bar at the top showing '2020-05-05 17:49:02 (UTC+0800 UTC)'. The configuration form contains the following sections:

- Enable this filter:** A checkbox that is checked.
- Event severity to trigger:** A dropdown menu set to 'Critical state'.
- Event Filter Action Alert:** A checkbox that is unchecked.
- Power Action:** A dropdown menu set to 'None'.
- Alert Policy Group Number:** A dropdown menu set to '1'.
- Show Status:** A checkbox that is checked.
- Generator ID 1:** A text field with '0x01' entered.
- Generator ID 2:** A text field with '0x02' entered.
- Generator Type:** Radio buttons for 'BIOS' (selected) and 'Software'.
- BIOS Address/Software ID:** A text field.
- Channel Number:** A dropdown menu set to '0'.
- IPMI Device ID:** A dropdown menu set to '0'.
- Sensor type:** A dropdown menu set to 'Temperature'.
- Sensor name:** A dropdown menu set to 'All Sensors'.
- Event Options:** A dropdown menu set to 'All Events'.
- Sensor Events:** A section with multiple rows for configuring event triggers and data. Each row includes fields for 'Event trigger' (set to '255'), 'Event Data 1 AND Mask' (set to '0'), 'Event Data 1 Compare 1' (set to '255'), 'Event Data 1 Compare 2' (set to '0'), 'Event Data 2 AND Mask' (set to '0'), 'Event Data 2 Compare 1' (set to '255'), 'Event Data 2 Compare 2' (set to '0'), 'Event Data 3 AND Mask' (set to '0'), and 'Event Data 3 Compare 1' (set to '255').

At the bottom of the form are 'Apply' and 'Clear' buttons.

In the Event Filter Configuration section:

- In Enable this filter, check this option to enable the PEF settings.
- In Event Severity to trigger, select any one of the Event severity from the list.
- Check Event Filter Action Alert to enable alerts for event filter actions.
- Select any one of the Power Action either Power down, Power reset or Power cycle from the drop down list
- Choose any one of the configured Alert Policy Group Number from the drop down list.



Note: Alert Policy has to be configured - under **Settings->PEF->Alert Policy**.

- Check Raw Data option to fill the Generator ID with raw data.
- **Generator ID 1** field is used to give raw generator ID 1 data value.
- **Generator ID 2** field is used to give raw generator ID2 data value.



Note: In **RAW** data field, specify hexadecimal value prefix with '0x '.

- In the **Event Generator** section, choose the event generator as Slave Address - if event was generated from IPMB. Otherwise as System Software ID - if event was generated from system software.
- In the **Slave Address/Software ID** field, specify corresponding I2C Slave Address or System Software ID.
- Choose the particular **Channel Number** that event message was received over. Or choose '0' if the event message was received via the system interface, primary IPMB, or internally generated by the BMC.
- Choose the corresponding **IPMB Device LUN** if event generated by IPMB.
- Select the **Sensor Type** of sensor that will trigger the event filter action.
- In the **SensorName** field, choose the particular sensor from the sensor list.
- Choose **Event Option** to be either All Events or Sensor Specific Events.
- In the Sensor Events field, choose the type of event levels.
- **Event Trigger** field is used to give Event/Reading type value.



Note: Value ranges from 1 to 255.

- **Event Data 1 AND Mask** field is used to indicate wildcarded or compared bits.



Note: Value ranges from 1 to 255.

- **Event Data 1 Compare 1 & Event Data 1 Compare 2** fields are used to indicate whether each bit position's comparison is an exact comparison or not.



Note: Value ranges from 1 to 255.

- **Event Data 2 AND Mask** field is similar to Event Data 1 AND Mask.
- **Event Data 2 Compare 1 & Event Data 2 Compare 2** fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
- **Event Data 3 AND Mask** field is similar to Event Data 1 AND Mask.
- **Event Data 3 Compare 1 & Event Data 3 Compare 2** fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.

3. Click **Save** to save the changes and return to event filter list.

4. Click **Delete** to delete the existing filter.

Alert Policies

This page is used to configure the Alert Policy for the PEF configuration. You can add, delete or modify an entry in this page.

MEMU Cloud

MEMU Cloud

For 15 Days (show 20) CPU

Dashboard

Sensor

FRU Information

Logs & Reports

Settings

Power Control

Maintenance

Switchgear Information

Sign out

2000-01-01 10:46:58 (UTC+0800 UTC)

Home

Settings

Platform Event Filter

Alert Policies

Alert Policies

Group 1 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 2 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 3 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 4 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 5 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 6 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 7 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 8 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 9 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 10 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 11 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 12 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 13 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 14 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 15 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 1 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 2 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 3 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 4 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 5 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 6 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 7 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 8 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 9 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 10 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 11 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 12 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 13 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 14 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 15 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 1 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 2 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 3 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 4 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 5 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 6 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 7 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 8 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 9 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 10 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 11 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 12 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 13 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 14 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 15 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 1 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 2 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 3 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 4 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 5 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 6 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 7 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 8 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 9 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 10 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 11 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group 13 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 14 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 15 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group 1 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0

The fields of Platform Event Filter - Alert Policies section are explained below.

Policy Group Number: Displays the Policy number of the configuration.

Enable this alert: To enable or disable the policy settings.

Policy Action: To choose any one of the Policy set values (0-5) from the list.

0 - Always send alert to this destination.

1 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set.

2 - If alert to previous destination was successful, do not send alert to this destination. Do not process any more entries in this policy set.

3 - 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.

4 - 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: To choose a particular channel from the available channel list.

Destination Selector: To choose a particular destination from the configured destination list.



Note: LAN Destination has to be configured - under **Settings->Platform Event Filters >LAN Destinations**.

Event Specific Alert String: To specify an event-specific Alert String.

Alert String Key: To specify which string is to be sent for this Alert Policy entry.

Save: To save the Alert Policies entries.

Delete: To delete the selected configured Alert Policy.

Procedure

1. In the Alert Policies Section, select the slot for which you have to configure the Alert policy. That is, In the **Alert Policies page**, if you have chosen Alert Policy Group Number as 4, you have to configure the 4th slot (the slot with Policy Number 4) in the Alert Policy Tab.
2. Select the slot and click on the empty slot to open the **Alert Policies** page as shown in the screenshot below.

3. Select **Policy Group Number** from the drop-down list.
4. Check **Enable this alert** to enable the policy settings.
5. Choose any of the **Policy Action** from the list.

6. Choose particular **LAN Channel** from the available channel list.
7. In the **Destination Selector**, choose particular destination from the configured destination list.



Note: LAN Destination has to be configured under **Settings-> Platform Event Filters->LAN Destinations**.

That is if you select the number 4 for destination selector in Alert Policy Entry page, then you have to configure the 4th slot (LAN Destination Number 4) in the LAN Destinations tab.

8. Enable **Event Specific Alert String**, if the Alert policy entry is Event Specific.
9. In the **Alert String Key** field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.



Note: Using Web UI, Alert strings cannot be configured but option for Event Specific alert strings can be enabled/disabled. There is an option to select only the alert string keys, but alert strings has to be configured using IPMI Command (Set PEF Config Parameter 'Alert String').

10. Click **Save** to save the new alert policy and return to Alert Policy list.
11. Click **Delete** to delete a configuration.

LAN Destinations

This page is used to configure the LAN destination of PEF configuration. A sample screenshot of LAN Destination page is given below.

The screenshot displays the 'LAN Destinations' configuration page. It features a sidebar on the left with navigation links: Dashboard, Sensor, FRU Information, Logs & Reports, Settings, Power Control, Maintenance, Switchtec Information, and Sign out. The main content area is titled 'LAN Destinations' and includes a 'Select the LAN Channel' dropdown menu set to '1'. Below this is a 3x4 grid of configuration slots. Each slot contains a flag icon, a 'LAN Channel' field (all set to '1'), a 'LAN Destination' field (numbered 1 through 12), and a 'Sent To' field (all set to 'SNMP Trap'). Each slot also has a 'Save' button at the bottom. The top of the page shows the user 'admin' and system status indicators like 'Sync' and 'Refresh'.

The fields of Platform Event Filters - LAN Destinations are explained below.
Select any empty slot to configure LAN Destinations.

Select the LAN Channel: To select the LAN Channel number

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

LAN Destination: Displays ID for setting Destination Selector of Alert Policy (read-only).

Destination Type: Destination type can be either an SNMP Trap or an E-mail alert. For E-mail alerts, the four fields - SNMP Destination Address, BMC User Name, Email subject and Email message needs to be filled. The SMTP server information also has to be added - under **Settings ->SMTP Settings**. For SNMP Trap, only the SNMP Destination Address has to be filled.

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

- IPv4 address format.
- IPv6 address format.

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

Email Subject & 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. These fields are not applicable for 'AMI- Format' email users.



Note: User should be configured under Settings-->User Management

Save: To add a new entry to the device. Alternatively, double click on a free slot.

Delete: To delete the selected configured LAN Destination.

Procedure

1. In the **LAN Destinations** section, choose the number of slots to be configured. This should be the same number of slot that you have selected in the Alert Policies - Destination Selector field. That is if you have chosen the Destination Selector as 4 in the Alert Policies page of Alert Policies tab, then you have to configure the 4th slot of LAN Destination page.
2. Select the slot and click on the empty slot. This opens the **LAN Destination entry**.
3. In the **LAN Channel Number** field, the LAN Channel Number for the selected slot is displayed and this is a read only field.
4. In the **LAN Destination** field, the destination for the newly configured entry is displayed and this is a read only field.
5. In the **Destination Type** field, select the one of the types.
6. In the **SNMP Destination Address** field, enter the destination address.
7. If the destination type is Email alert, select the BMC User Name from the list of users.



Note: E-mail address should be configured under **Settings-->User Management**.

8. In the **Email Subject** field, enter the subject.
9. In the **Email Message** field, enter the message.
10. Click **Save** to save the new LAN destination and return to LAN destination list.
11. Click **Delete** to delete a configuration.
12. Click **Send Test Alert** to send sample alert to configured destination.



Note: Test alert can be sent only with enabled SMTP configuration. SMTP support can be enabled under **Settings->SMTP Settings**.

2-6-7 Services

This page displays the basic information about services running in the BMC. Only Administrator can modify the service.

To open Services page, click **Settings > Services** from the menu bar. A sample screenshot of Services page is shown below.

The screenshot shows the BMC Services page. The left sidebar contains the navigation menu with the following items: Dashboard, Sensor, FRU Information, Logs & Reports, Settings (selected), Power Control, Maintenance, Switchtec Information, and Sign out. The main content area displays a table of services. The table has columns: Service, Status, Interfaces, Secure Port, Timeout, and Maximum Sessions. Two services are listed: 'web' and 'ssh'. Both are 'Active'. The 'web' service has interface 'bond0', secure port '443', timeout '1800', and maximum sessions '20'. The 'ssh' service has interface 'NA', secure port '22', timeout '600', and maximum sessions 'N/A'. Each row has a 'Stop' button and a green checkmark icon.

Service	Status	Interfaces	Secure Port	Timeout	Maximum Sessions		
web	Active	bond0	443	1800	20	Stop	✓
ssh	Active	NA	22	600	N/A	Stop	✓

The fields of Services page are explained below.

Services: Displays service name of the selected slot (read-only).

Status: Displays the current status of the service, either active or inactive state.

Interfaces: It shows the interface in which service is running.

Nonsecure Port: This port is used to configure non secure port number for the service.

- Web default port is 80
- SSH default port is 52123



Note: SSH service will not support non secure port. If single port feature is enabled,

Secure Port: Used to configure secure port number for the service.

- Web default port is 443
- SSH default port is 22



Note: SSH will not support secure port.

Port listening status on various feature settings:

Timeout: Displays the session timeout value of the service. For web, SSH and telnet service, user can configure the session timeout value.



Note: Web timeout value ranges from 300 to 1800 seconds.

SSH timeout value ranges from 60 to 1800 seconds.

SSH timeout value ranges from 60 to 1800 seconds.

SSH will be using the same timeout value. If you configure SSH timeout value, it will be applied to telnet service also and vice versa.

Maximum Sessions: Displays the maximum number of allowed sessions for the service.

Active Sessions: To view the current active sessions for the service.

Procedure to view the Active Sessions:

1. Click **View** Icon () to view the details about the active sessions for the service.
2. This opens the Active Session screen (for example - Service Sessions) as shown in the screenshot below.

Service Sessions

Active Session - Web

Session ID	Session Type	User ID	User Name	Client IP	Privilege
4*	Web HTTPS	2	admin	10.1.2.38	Administrator

Session Type: Displays the type of the active sessions.

User ID: Displays the ID of the user.

User Name: Displays the name of the user.

Client IP: Displays the IP addresses that are already configured for the active sessions.

Privilege: Displays the access privilege of the user.

3. Select a slot and click **Terminate** icon () to terminate the particular session of the service.

Procedure to modify the existing services:

1. Select a slot and click Edit icon (✎) to modify the configuration of the service.



Note: Whenever the configuration is modified, the service will be restarted automatically. User has to close the existing opened session for the service if needed.

2. This opens the **Service Configuration** screen as shown in the screenshot below.

The screenshot displays the 'Service Configuration' interface. On the left is a dark sidebar with a user profile 'NONE of Ethernet Information' and a list of menu items. The main panel has a top bar with a timestamp '2000-01-01 18:06:36 (UTC+00:00 UTC)' and navigation links. The 'Service Configuration' form includes the following fields: 'Service Name' (web), 'Active' (checked checkbox), 'Interface Name' (bond0), 'Secure port' (443), 'Timeout' (1800), and 'Maximum Sessions' (20). A 'Save' button is located at the bottom right of the form.

3. **Service Name** is a read only field.

4. Activate the Current State by enabling the Active check box.



Note: Interfaces, Non-secure port, Secure port, Time out and Maximum Sessions will not be active unless the current state is active.

5. Enter the Secure Port Number in the **Secure Port** field.

6. Enter the timeout value in the **Timeout** field.



Note: The values in the **Maximum Sessions** field cannot be modified.

7. Click **Save** to save all changes you have made.

2-6-8 SMTP Settings

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

Using BMC Web GUI, you can configure the SMTP settings of the device.

To open SMTP Settings page, click **Settings > SMTP Settings** from the menu bar. A sample screenshot of SMTP Settings page is shown below.

The screenshot displays the BMC Web GUI interface for configuring SMTP settings. On the left is a dark sidebar with a user profile and navigation menu. The main area shows the 'SMTP Settings' form with various input fields and checkboxes. The 'Primary SMTP Support' checkbox is checked, and the 'Primary SMTP port' is set to 25. The 'Primary Secure SMTP port' is set to 465. There are sections for Primary and Secondary SMTP configurations, including fields for server name, IP, port, username, password, and authentication options like SSLTLS and STARTTLS.

The fields of SMTP Settings page are explained below.

LAN Interface: Displays the list of LAN channels available

Sender Email ID: A valid 'Sender Address' to indicate the BMC, whenever e-mail is sent.

Primary Server Name: The 'Machine Name' of the BMC, from where the e-mail is sent.



Note: Machine Name is a string of maximum 15 alpha-numeric characters. Space, special characters are not allowed.

Primary SMTP Support: To enable/disable SMTP support for the BMC.

Primary SMTP Port: To specify the SMTP Normal Port.

Primary Secure SMTP Port: To specify the SMTP Secure Port.



Note: For Primary SMTP Port - Default Port is 25, and the Port value ranges from 1 to 65535.

For Primary Secure SMTP Port - Default Port is 465, and the Port value ranges from 1 to 65535.

Primary Server IP: The **IP address** of the SMTP Server. It is a mandatory field.



Note: 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.
Supports IPv4 Address format and IPv6 Address format.

Primary SMTP Authentication: To enable/disable SMTP Authentication.



Note: SMTP Server Authentication Types supported are:

- CRAM-MD5
- LOGIN
- PLAIN

If the SMTP server does not support any one of the above authentication types, the user will get an error message stating "**Authentication type is not supported by SMTP Server.**"

Primary Username: Enter username to access SMTP Accounts.



Note: User Name can be of length 4 to 64 alpha-numeric characters, dot(.), dash(-), and underline(_).
It must start with an alphabet.
Other Special Characters are not allowed.

Primary Password: Enter password for the SMTP User Account.



Note: Password must be at least 4 characters long.
Blank space is not allowed.
This field will not allow more than 64 characters.

Primary SMTP STARTTLS Enable: To enable STARTTLS support for the SMTP Client.

- **Upload SMTP CA Certificate File:** File that contains the certificate of the trusted CA certs. CACERT key file should be of pem type, LOGIN
- **Upload SMTP Certificate File:** Client certificate filename. CERT key file should be of pem type.
- **Upload SMTP Private Key:** Client private key filename. SMTP key file should be of pem type.



Note: To enable STARTTLS support, the respective SMTP support option should be enabled.

Secondary SMTP Support: It lists the Secondary SMTP Server configuration. It is an optional field. If the Primary SMTP server is not working fine, then it uses Secondary SMTP Server configuration.



Note: Options of Secondary SMTP Support are same as Primary SMTP Support.

Save: To save the new SMTP server configuration.

Procedure

1. Select the **LAN Interface** from the drop-down list.
2. Enter the **Sender Email ID** in the specified field.
3. Check **Primary SMTP Support** option to enable SMTP support for the BMC.
4. Enter the Machine Name of the SMTP Server in the **Primary Server Name**.



Note: - Machine Name is a string of maximum 15 alpha-numeric characters. Space, special characters are not allowed.

5. Enter IP address of the SMTP Server in the **Primary Server IP** field. It is a mandatory field.
6. Enter the **Primary SMTP Port** in the specified field.
7. Enter the **Primary Secure SMTP Port** in the specified field.
8. Enable the check box **Primary SMTP Authentication** if you want to authenticate SMTP Server.
9. Enter your **Primary User name** and **Primary Password** in the respective fields.
10. Enable the check box **Primary SMTP SSLTLS Enable** to send data through secure Port.



Note: If this option is selected, STARTTLS option and Normal Port will be hidden.

11. Check the **Secondary SMTP Support** option to enable Secondary SMTP support for the BMC.
12. Enter the **Secondary Server Name**, **Secondary Server IP**, **Secondary SMTP Port** and **Secure**
13. Port values in the respective fields.
14. Enable the check box **SMTP Server Authentication** if you want to authenticate SMTP Server.
15. Enter your **Secondary User name** and **Password** in the respective fields.
16. Enable the check box **Secondary SMTP SSLTLS** to send data through secure Port.



Note: If this option is selected, STARTTLS option and Normal Port will be hidden.

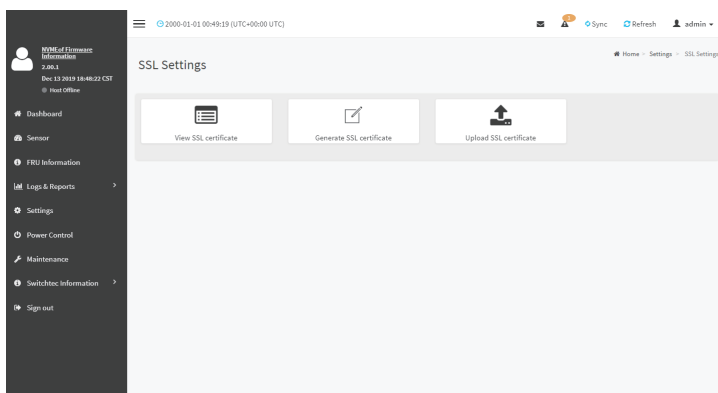
17. Click **Save** to save the entered details.

2-6-9 SSL Settings

The **Secure Socket Layer** protocol was created by Netscape to ensure secure transactions between web servers and browsers. The protocol uses a third party, a **Certificate Authority (CA)**, to identify one end or both end of the transactions.

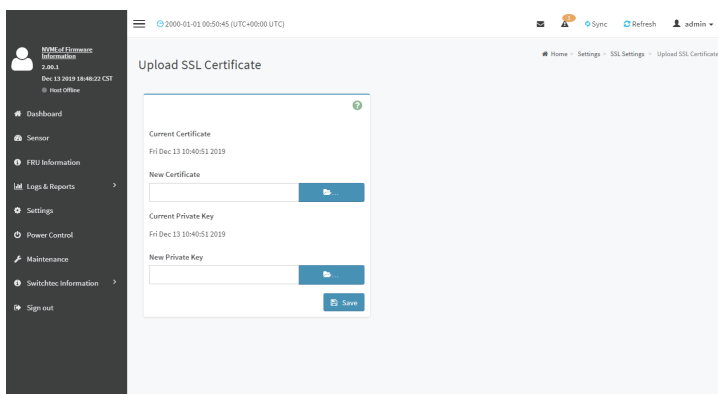
Using BMC Web GUI, configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode.

To open the SSL Certificate Configuration page, click Settings > SSL Settings from the menu bar. There are three tabs in this page.



- **Upload SSL Certificate** option is used to upload the certificate and private key file into the BMC.
- **Generate SSL Certificate** option is used to generate the SSL certificate based on configuration details.
- **View SSL Certificate** option is used to view the uploaded SSL certificate in readable format.

A sample screenshot of Upload SSL Certificate page is shown below.



The fields of SSL Settings - Upload SSL Settings tab are explained below.

Current Certificate: Current certificate and uploaded date/time will be displayed (read-only).

New Certificate: Certificate file should be of pem type

Current Private Key: Current Private key information will be displayed (read-only).

New Private Key: Private key file should be of pem type

Upload: To upload the SSL certificate and privacy key into the BMC.



Note: After successful upload, HTTPs service will restart to use the newly uploaded SSL certificate.

The screenshot shows the 'Generate SSL Certificate' page in the BMC. On the left is a dark sidebar with navigation links: Dashboard, Sensor, FRU Information, Logs & Reports, Settings (selected), Power Control, Maintenance, Switchtec Information, and Sign out. The main content area has a header with a menu icon, a timestamp '2000-01-01 00:00:00 (UTC+00:00 UTC)', and user controls (Sync, Refresh, admin). Below the header is a breadcrumb trail: Home > Settings > SSL Settings > Generate SSL Certificate. The form itself contains the following fields: Common Name (CN), Organization (O), Organization Unit (OU), City or Locality (L), State or Province (ST), Country (C), Email Address, Valid for (in days), and Key Length (set to 2048 bits). A blue 'Save' button is located at the bottom right of the form.

The fields of SSL Settings - Generate SSL Certificate are explained below.

Common Name(CN): Common name for which certificate is to be generated.

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

Organization(O): Organization name for which the certificate is 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 is 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 of the organization (mandatory).

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

State or Province(ST): State or Province of the organization (mandatory).

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

Country(C): Country code of the organization (mandatory).

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

Email Address: E-mail Address of the organization (mandatory).

Valid for: Validity of the certificate.

- Value ranges from 1 to 3650 days.

Key Length: The key length bit value of the certificate.

Save: To generate the new SSL certificate.



Note: HTTPs service will get restarted, to use the newly generated SSL certificate.

The fields of SSL Settings - View SSL Certificate are explained below.

Basic Information: This section displays the basic information about the uploaded SSL certificate. It displays the following fields:

- Version Serial Number
- Signature Algorithm
- Public Key
- Issuer Common Name(CN)
- Issuer Organization(O)
- Issuer Organization Unit(OU)
- Issuer City or Locality(L)
- Issuer State or Province(ST)
- Issuer Country(C)
- Issuer E-mail Address
- Valid From
- Valid Till

NAME of Firmware

Information

2.00.1

Dec 13 2019 16:46:22 CST

© Your Office

Dashboard

Sensor

FRU Information

Logs & Reports

Settings

Power Control

Maintenance

Switchtec Information

Sign out

2000-01-01 00:49:41 (UTC+00:00 UTC)

Sync

Refresh

admin

Home

Settings

SSL Settings

View SSL Certificate

View SSL Certificate

Current Certificate Information

Certificate Version

3

Serial Number

SADE171D

Signature Algorithm

sha256WithRSAEncryption

Public Key

[2048 bit]

Issuer Common Name (CN)

www.aml.com

Issuer Organization (O)

American Magatrends Incorporated

Issuer Organization Unit (OU)

Service Processors

Issuer City or Locality (L)

Noncross

Issuer State or Province (ST)

Georgia

Issuer Country (C)

US

Issuer Email Address

support@aml.com

Valid From

Apr 23 17:25:49 2018 GMT

Valid Till

Jun 22 17:25:49 2037 GMT

Issued to Common Name (CN)

www.aml.com

Issued to Organization (O)

American Magatrends Incorporated

Issued to Organization Unit (OU)

Service Processors

Issued to City or Locality (L)

Noncross

Issued to State or Province (ST)

Georgia

Issued to Country (C)

US

Issued to Email Address

support@aml.com

Gigabyte Server Management Console

- 64 -

Procedure

1. Click the Upload SSL Certificate tab, Browse the New Certificate and New Private key.
2. Click Upload to upload the new certificate and private key.
3. In Generate SSL Certificate, enter the following details in the respective fields:
 - The **Common Name** for which the certificate is to be generated.
 - The **Organization** for which the certificate is to be generated.
 - The **Organization Unit** name for which certificate to be generated.
 - The **City or Locality** of the organization
 - The **State or Province** of the organization
 - The **Country** of the organization
 - The **Email address** of the organization.
 - The number of days the certificate will be valid in the **Valid For** field.
4. Choose the **Key Length** bit value of the certificate
5. Click **Save** to generate the certificate.
6. Click **View SSL** Certificate tab to view the uploaded SSL certificate in user readable format.



Note: Once you Upload/Generate the certificates, only HTTPs service will get restarted.

You can now access your Web securely using the following format in your IP Address field from your Internet browser: `https://<your BMC's IP address here>`

For example, if your BMC's IP address is 192.168.0.30, enter the following:

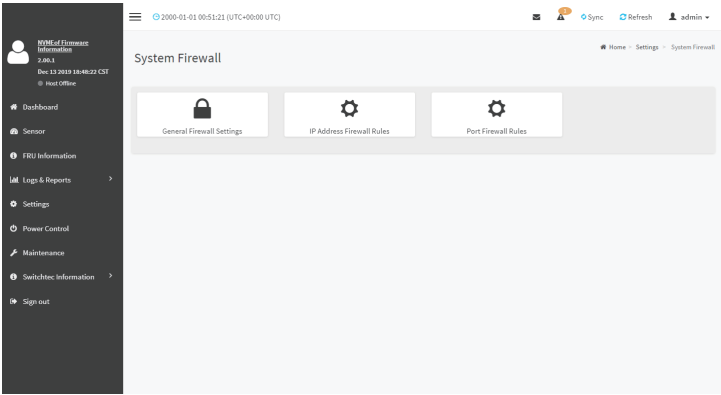
`https://192.168.030`

Please note the `<s>` after `<http>`. You must accept the certificate before you are able to access your Web.

2-6-10 System Firewall

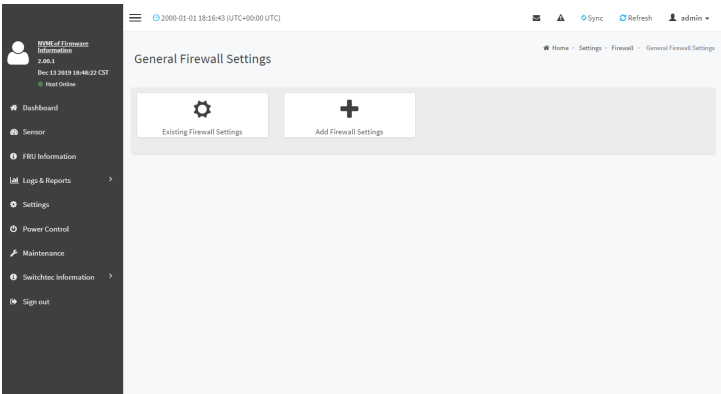
In BMC Web GUI, the System Firewall page allows you to configure the firewall settings. The firewall rule can be set for an IP or range of IP Addresses or Port numbers. To view this page, you must at least be an operator. Only administrators can add or delete a firewall.

To open System Firewall page, click **Settings > System Firewall** from the menu bar.



General Firewall Settings

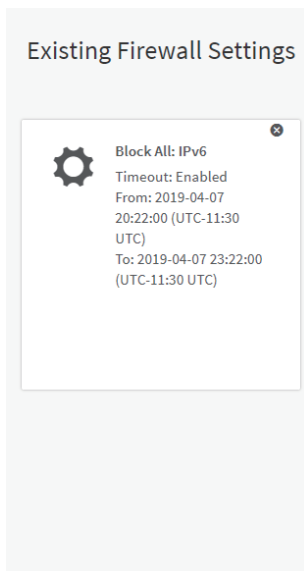
Click **General Firewall Settings** page. A sample screenshot of General Firewall Settings page is shown below.



The fields of Firewall Settings tab are explained below.

To View Existing Firewall Settings

Click **General Firewall Settings > Existing Firewall Settings** icon. A blank page will be opened if you did not add anything in “Add Firewall Settings”. If any settings are added, then the added rule will be listed in “Existing Firewall Settings” page. A sample screenshot of Existing Firewall Settings page is shown below.



The Existing Firewall Settings page allows you to remove any particular Existing Firewall Settings.

Procedures

1. Select the Existing Firewall Settings you want to remove.
2. Click on Delete to remove the selected Existing Firewall Settings.

Existing Firewall Settings

Block All

IPv6

☐ Flush All

☒ Timeout

Start Date&Time

1970-01-18 12:21:49 (UTC-11:30 UTC)

End Date&Time

1970-01-18 12:22:00 (UTC-11:30 UTC)

Delete

Add Firewall Settings

Click **General Firewall Settings > Add Firewall Settings**. This opens the Add Firewall Settings page as shown below.

The screenshot shows the 'Add Firewall Settings' page. On the left is a sidebar with a user profile (FMC Firmware Information, 2 PL 189217, Jan 28 2019 10:44:04 CST, Host Order) and a 'Quick Links...' section with icons for Dashboard, Sensor, System Inventory, FRU Information, Logs & Reports, Settings, Remote Control, Image Redirection, Power Control, Maintenance, and Sign out. The main content area has a top bar with a clock (2019-04-07 20:25:42 UTC-11:30 UTC), icons for Sync, Refresh, and a user menu (admin). Below the top bar is a breadcrumb trail: Home > Settings > Firewall > General Firewall Settings > Add Firewall Settings. The main form is titled 'Add Firewall Settings' and contains a 'Block All' dropdown menu, checkboxes for 'Flush All' and 'Timeout', and input fields for 'Start Date' (2019-04-07), 'Start Time' (20:25), 'End Date' (2019-04-07), and 'End Time' (20:25). A 'Save' button is at the bottom right of the form.

1. Select **Block All** to block all the incoming IP's and Port's.
2. Select **Flush All** to flush all the system firewall rules.
3. Select **Timeout** to enable or disable firewall rules with timeout.
4. Enter **Start Time** to start the respective firewall rule effect from this time.
5. Enter **End Time** to end the respective firewall rule effect from this time.

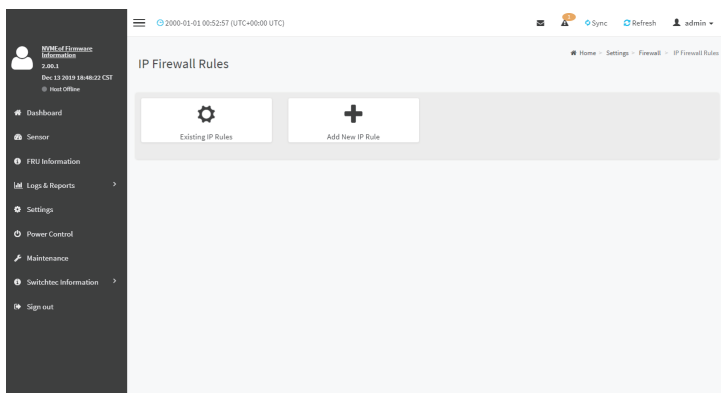


Note: The time should be in the dd-mm-yy:hh-mm format.

6. Click **Save** to save the changes made else click **Cancel** to go back to the previous screen.

IP Address Firewall Rules

Click **IP Firewall Rules** page. A sample screenshot of IP Firewall Rules page is shown below.

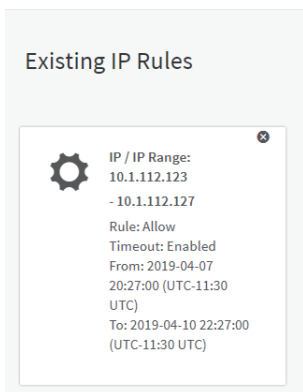


The fields of **IP Address Firewall** tab are explained below.

To View Existing IP Rules or a range of IP Addresses

Click **Settings > System Firewall > IP Address Firewall Rules > Existing IP Rules**. A blank page will be opened if you did not add anything in "Add IP Rule". If any rule is added, then the added rule will be listed in "Existing IP Rules" page.

A sample screenshot of Existing IP Rules page is shown below.



The Existing IP Rules page allows you to remove any particular Existing IP Rules.

Procedures

1. Select the Existing IP Rules you want to remove.
2. Click on Delete to remove the selected Existing IP Rules.

Existing IP Rules

Home > Settings > Firewall > IP Oriented Firewall Rules > Existing IP Rules > Existing IP Rules

IP Single (or) Range Start

10.1.112.123

IP Range End

10.1.112.127

☒ Enable Timeout

Start Date&Time

2019-04-07 20:27:00 (UTC-11:30 UTC)

End Date&Time

2019-04-10 22:27:00 (UTC-11:30 UTC)

Rule

Allow

Delete

IP Single (or) Range Start - To show the configured Port Address or Range of Ports.

IP Range End - To show the configured Port Address or Range of Ports.

Enable Timeout - To enable/disable 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.

Rule - To indicate the current setting of the listed Port or Range of Port rules (Allow or Block) status.

Delete - To delete the selected slot.

Procedures

1. Click **Settings > System Firewall > IP Address Firewall Rules > Add New IP Rule** to add a new IP or range of IP address.

2. In the **Add new rule for IP** page, Enter the IP address and a range of IP addresses in the **IP Single or IP Range Start** field.



Note: IP Address will support IPv4 Address format only:

IPv4 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.

IPv6 Address made of 8 groups of 4 Hexadecimal digits separated by colon as in

xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.

3. Enter IP range end value in the **IP Range End** field.
4. Enable **Timeout** to enable firewall rules with timeout.
5. Enter **Start Date** to start the respective firewall rule effect from this date.
6. Enter **End Date** to end the respective firewall rule effect from this date.
7. Enter **Start Time** to start the respective firewall rule effect from this time.
8. Enter **End Time** to end the respective firewall rule effect from this time.

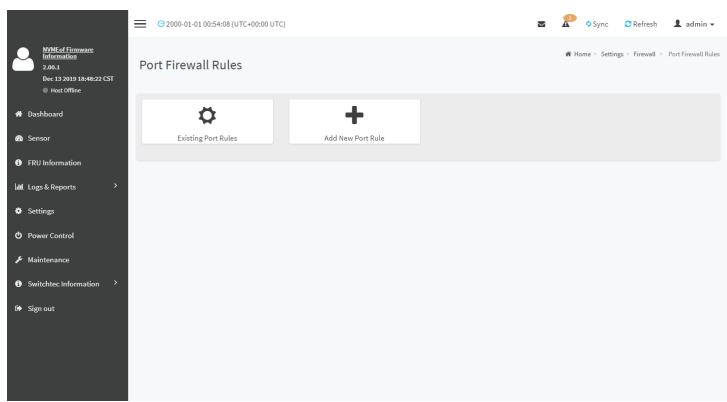


Note: The date and time should be in the YYYY/MM/DD and hh-mm format respectively.

9. Determine the rule to block or accept.
10. Click **Save** to save the changes made.

Port Firewall Rules

Click **Port Firewall Rules** page. A sample screenshot of Port Firewall Rules page is shown below.

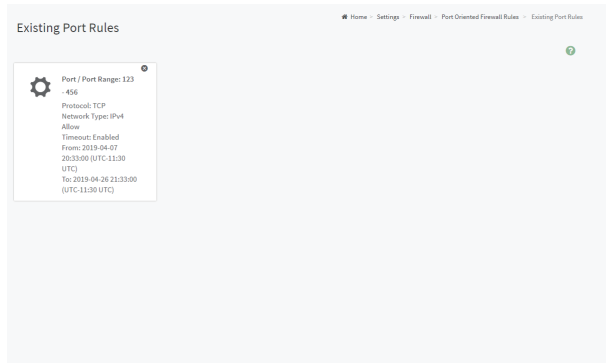


The fields of Port Firewall Rules tab are explained below.

To view Existing Port Rules

Click **Settings > System Firewall > Port Firewall Rules > Existing Port Rules**. A blank page will be opened if you did not add anything in “Add New port Rule”. If any rule is added, then the added rule will be listed in “Existing Port Rules” page. A sample screenshot of Existing Port Rules is shown below.

The Existing Port Rules page allows you to remove any particular Existing Port Rules.



Procedures

1. Select the Existing Port Rules you want to remove.
2. Click on Delete to remove the selected Existing Port Rules.

Existing Port Rules

Home - Settings - Firewall - Port Oriented Firewall Rules - Existing Port Rules - Existing Port Rules

Port Single (or) Range Start
123

Port Range End
456

Protocol
TCP

Network Type
IPv4

☒ Enable Timeout

Start Date&Time
2019-04-07 20:33:00 (UTC+11:30 UTC)

End Date&Time
2019-04-26 21:33:00 (UTC+11:30 UTC)

Rule
Allow

Delete

The fields of System Firewall - Existing Port Rules page are explained below.

Port Single (or) Range Start - To configure the Port or Range of Port Addresses.

Port Range End - To configure the Port or Range of Port Addresses.

Protocol - This field specifies the protocols for the configured Port or Port Ranges.

Network Type - This field specifies the affected network type for the particular Port or Port Ranges.

Enable Timeout - To enable or disable firewall rules with timeout.

Start Date - The respective firewall rule effect will start from this time.

Start Time - The respective firewall rule will start from this time.

End Date - The respective firewall rule effect will end on this date.

End Time - The respective firewall rule will end at this time.

Rule - To indicate Allow or Block status.

Delete - To delete the entry to the firewall rules list.

Procedure to add Port/Range of ports

1. To add a new range of Port address, click the Add button

The screenshot shows the 'Add Port Rule' window in the Gigabyte Server Management Console. The window is titled 'Add Port Rule' and has a 'Save' button at the bottom right. The form contains the following fields:

- Port Single (or) Range Start:** A text input field.
- Port Range End:** A text input field with a placeholder 'optional'.
- Protocol:** A dropdown menu with 'TCP' selected.
- Network Type:** A dropdown menu with 'IPv4' selected.
- Enable Timeout:** A checkbox that is currently unchecked.
- Start Date:** A date picker showing '2000-01-01'.
- Start Time:** A time picker showing '00:04'.
- End Date:** A date picker showing 'YYYY/MM/DD'.
- End Time:** A time picker.
- Rule:** A dropdown menu with 'Allow' selected.

The left sidebar shows the user 'NOME of Username' with a 'Host Office' role. The top navigation bar includes 'Home', 'Settings', 'Firewall', 'Port Oriented Firewall Rules', and 'Add Port Rule'.

2. In the **Add new rule** for Port window, enter the port number or a range of port numbers in the **Port Single (or) Range Start** field.
3. Enter the end value in the **Port Range End** field.
4. Select the **Protocol** to be either TCP or UDP or Bot.
5. Select the **Network Type**. It may be IPv4 or IPv6 or Both.
6. Select **Timeout** to enable or disable firewall rules with timeout.
7. Enter **Start Time** to start the respective firewall rule effect from this time.
8. Enter **Start Date** to start the respective firewall rule effect from this date.
9. Enter **End Date** to end the respective firewall rule effect on this date.
10. Enter **End Time** to end the respective firewall rule effect at this time.



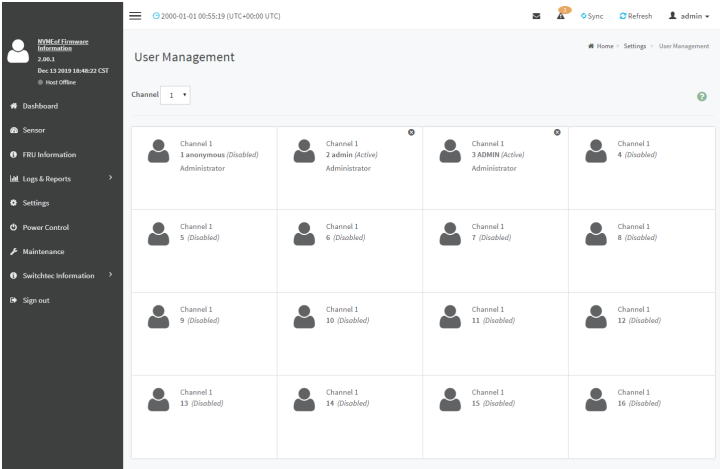
Note: The time should be in the YYYY/MM/DD:hh-mm format.

11. Select the **Rule** to determine the rule to Block or Allow.
12. Click **Save** to save the changes made.

2-6-11 User Management

In BMC Web GUI, the User Management page allows you to view the current list of user slots for the server. You can add a new user and modify or delete the existing users.

To open User Management page, click **Settings > User Management** from the menu bar. A sample screenshot of User Management page is shown below.



Click user icon () and select any free slot to add a new user from the User Management main page.



Note: The Free slots are shown as “Disabled” in all columns for the slot. The fields of User Management page are explained below.

User ID: Displays the ID number of the user.



Note: The list contains a maximum of ten users only.

User Name: Displays the name of the user.

User Access: To enable or disable the access privilege of the user.

Network Privilege: Displays the network access privilege of the user.

SNMP Status: Displays if the SNMP status for the user is enabled or Disabled.

E-mail ID: Displays e-mail address of the user.

Add User: To add a new user.

Delete User: To delete an existing user.

Procedure to add a new User

1. To add a new user, select a free section and click on the empty section. This opens the Add User screen as shown in the screenshot below.

User Management Configuration

Username
anonymous

☐ Change Password

Password Size
16 bytes

Password

Confirm Password

☐ Enable User Access

Privilege
Administrator

☒ KVM Access

☒ VMedia Access

☐ SNMP Access

SNMP Access level

SNMP Authentication Protocol

SNMP Privacy Protocol

Email Format
AMI-Format

Email ID

Existing SSH Key
Not Available

Upload SSH Key

Deleting Save

2. Enter the name of the user in the User Name field.



Note: User Name is a string of 1 to 16 alpha-numeric characters. It must start with an alphabetical character. It is case-sensitive.

Special characters '-' (hyphen), '_' (underscore), '@' (at sign) are allowed. For 20 Bytes password, LAN session will not be established.

3. Set **Password Size** for the new password.
4. In the **Password** and **Confirm Password** fields, enter and confirm your new password.



Note: Password should be the combination of alphabets, numbers, symbol and upper case characters.

Blank space is not allowed.

This field will not allow more than 16/20 characters based on Password size field value.

This field will not allow the below mentioned characters.

The password should be a string, if you try to set password using "ipmitool user set password".

Hex	Char
00	NUL '\0'
01	SOH (start of heading)
02	STX (start of text)
03	ETX (end of text)
04	EOT (end of transmission.)
05	ENQ (enquiry)
06	ACK (acknowledge)
07	BEL '\a' (bell)
08	BS '\b' (backspace)
09	HT '\t' (horizontal tab)
0A	LF '\n' (new Line)
0B	VT '\v' (vertical tab)
0C	FF '\f' (form feed)
0D	CR '\r' (carriage ret)
0E	SO (shift out)
0F	SI (shift in)
10	DLE (data link escape)
11	DC1 (device control 1)
12	IDC2 (device control 2)
13	DG3 (device control 3)
14	DC4 (device control 4)
15	NAK (negative ack.)
16	SYN (synchronous idle)
17	ETB (end of trans. blk)
18	CAN (cancel)
19	EM (end of medium)
19	EM (end of medium)
1A	SUB (substitute)
1B	ESC (escape)
1C	FS (file separator)
1D	GS (group separator)
1E	RS (record separator)
1F	US (unit separator)
20	SPACE
7F	DEL

5. Enable or Disable the **Enable User Access** Privilege.



Note: Enabling User Access will intern assign the IPMI messaging privilege to user. It is recommended that the IPMI messaging option should be enabled for the user to enable the User Access option, while creating User through IPMI.

6. In the Network Privilege and Serial Privilege fields, select the privileges assigned to the user which could be Administrator, Operator, User, OEM or None.



Note: It is recommended that the privileges support to KVM and VMedia should be provided only to the ADMIN user and shouldn't be provided to USER and OPERATOR privilege level users. The Admin user can provide the privilege support to USER and OPERATOR privilege level users at their own risk.

VMedia Privilege only restricts initiating / starting media redirection. If a device is already being redirected and attached to the host, then in host it will be visible as normal device. Hence, it will be accessible to all the KVM sessions, which includes 'KVM Privilege only' sessions as well.

7. Check the **SNMP Access** check box to enable SNMP access for the user.



Note: Password field is mandatory, if SNMP Status is enabled.

8. Choose the SNMP Access level option for user from the **SNMP Access level** (SHA or MD5) drop-down list. Either it can be Read Only or Read Write.

9. Choose the **SNMP Authentication Protocol** (SHA or MD5) to use for SNMP settings from the drop down list.



Note: Password field is mandatory, if Authentication protocol is changed.

10. Choose the Encryption algorithm to use for SNMP settings from the SNMP Privacy protocol (AES or DES) drop-down list.

11. In the **Email ID** field, enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.



Note: SMTP Server must be configured to send emails.

Email Format: Two types of formats are available:

- **AMI-Format:** The subject of this mail format is 'Alert from (your Host name)'. The mail content shows sensor information, ex: Sensor type and Description.
- **Fixed-Subject Format:** This format displays the message according to user's setting. You must set the subject and message for email alert.

12. In the **Upload SSH Key** field, click Browse and select the SSH key file.

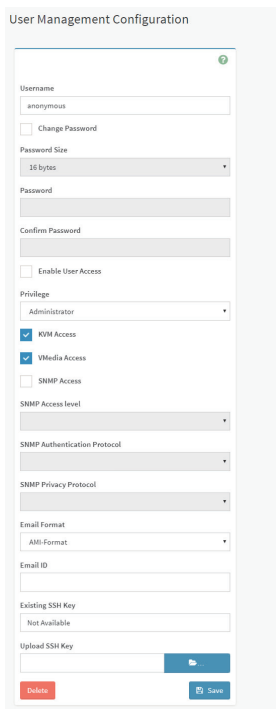


Note: SSH key file should be of pub type.

13. Click **Save** to save the new user and return to the users list.

To Modify User

1. To modify the existing user, click on the active user tab. This opens a User screen as shown in the screenshot below.



The screenshot shows the 'User Management Configuration' form for modifying a user. The form is titled 'User Management Configuration' and contains the following fields and options:

- Username:** A text field with the value 'anonymous'.
- Change Password:** A checkbox that is currently unchecked.
- Password Size:** A dropdown menu with the value '16 bytes'.
- Password:** A text field.
- Confirm Password:** A text field.
- Enable User Access:** A checkbox that is currently unchecked.
- Privilege:** A dropdown menu with the value 'Administrator'.
- KVM Access:** A checkbox that is checked.
- VMedia Access:** A checkbox that is checked.
- SNMP Access:** A checkbox that is unchecked.
- SNMP Access level:** A dropdown menu.
- SNMP Authentication Protocol:** A dropdown menu.
- SNMP Privacy Protocol:** A dropdown menu.
- Email Format:** A dropdown menu with the value 'AMI-Format'.
- Email ID:** A text field.
- Existing SSH Key:** A text field with the value 'Not Available'.
- Upload SSH Key:** A text field with a blue button to its right.
- Buttons:** At the bottom, there are two buttons: a red 'Delete' button and a blue 'Save' button.

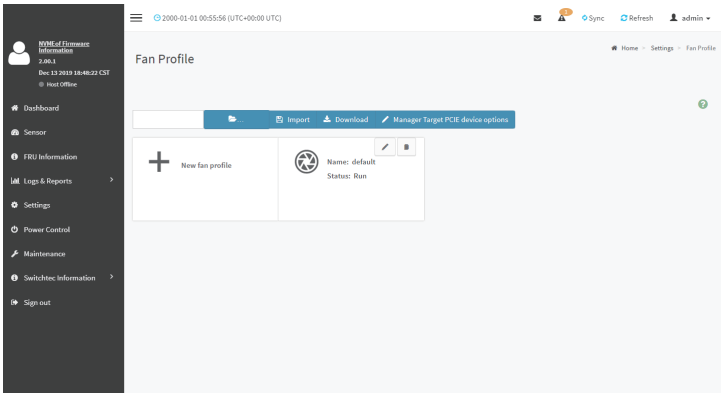
2. Check **Change Password**, if you wish to change the existing Password.
3. Follow the steps (3 to 15) of Procedure to add a new User.
4. Click **Save** to save the changes and return to the users list.
5. Click **Delete** to delete the user.

2-6-12 Fan Policy

The Fan Policy consists of the following:

1. Add New Fan Profile

A sample screenshot of the Fan Profile is given below.



Procedure to add Fan Profile

1. To add fan profile:

Edit New Fan Profile

9. Click Save to save the configuration

2. Select the Algorithm
3. Select Sensor Type, current or temperature
4. Set the Initialize Duty

1. Name the profile

5. Select the reference device sensor

6. Select the controlled fan

7. Click New to a new policy reference table

Policy Reference Table

Reference	Duty (%)
0	30

2. Click the + to add fan policy.
3. Enter the value in the respective field.
4. Click **Save** to save the configuration.

2-6-13 Power Consumption

The Power Consumption allows you to configure the power consumption of your server.
Enter the values in the respective column and click **Save** to save the power consumption values.

None of Firmware Information

2018

Dec 13 2019 18:48:29 CST

Host Office

Dashboard

Sensor

FBI Information

Logs & Reports

Settings

Power Control

Maintenance

Switchtec Information

Sign out

2000-01-01 00:56:29 (UTC+00:00 UTC)

Sync

Refresh

admin

Power Consumption

Save

Power Consumption Reading

Current Power Consumption (W)

Minimal Power Consumption (W)

Maximal Power Consumption (W)

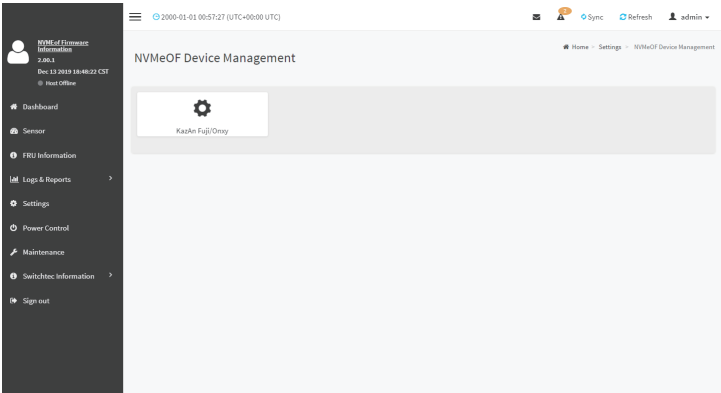
Average Power Consumption (W)

Power Consumption Limit

2-6-14 NVMeOF Device Management

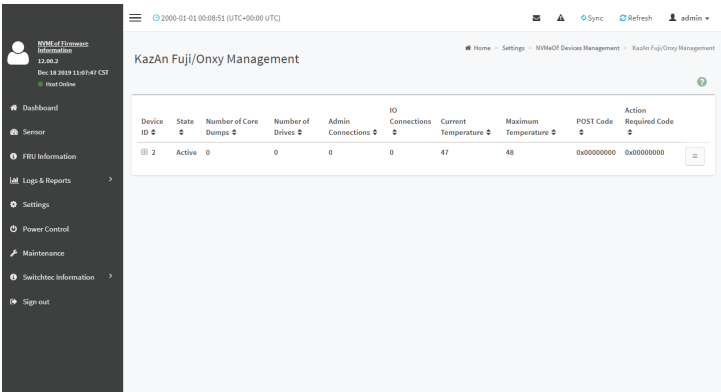
The NVMeOF Device Management page allows you to view the current list of NVMeOF devices for the server. You can configure the existing NVMeOF devices .

To open NVMeOF Device Management page, click **Settings > NVMeOF Device Management** from the menu bar. A sample screenshot of NVMeOF Device Management page is shown below.



KazAn Fuji/Onxy

To open KazAn Fuji/Onxy page, click **Settings > NVMeOF Device Management > KazAn Fuji/Onxy** from the menu bar. A sample screenshot of KazAn Fuji/Onxy page is shown below.



The fields of KazAn Fuji/Onxy page are explained below.

Device ID: Device ID: Displays the number of RDMA card's in system.

State: Displays the current state of bridge, either active or inactive state.

Number of Core Dumps: Displays the number of core dumps resident in flash.

Number of Drives: Displays the number of drives attached to bridge.

Admin Connections: Displays the number of established administration connections.

IO Connection: Displays the number of established I/O connections.

Current Temperature: Displays the internal temperature information.

Maximum Tempture: Displays the maximum temperature since last boot operation.

POST Code: Displays POST code information.

Action Required Code: Displays action required code.

Click Icon  to enter advanced meun.

2-6-15 Network Port IP


Click **Network Port IP**, a sample screenshot of network port IP page is shown below.

2000-01-01 00:56:28 (UTC+00:00 UTC)

KazAn Fuji/Onxy Net IP Config

Port ID	DHCP Used	IPv4 Address	IPv4 Mask	IPv4 Gateway	IPv4 Hostname
1	0	3.3.3.1	255.255.255.0	3.3.3.4	port1
2	1	0.0.0.0	255.255.255.255	255.255.255.255	

Procedures

1. Click **Settings > NVMeOF Device Management > KazAn Fuji/Onxy Information> Network Port IP** to enter Network Port IP page.
2. Click  to configure network IP.

DHCP Used: To enable or disable DHCP.

IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway, and IPv4 Hostname: These fields are for specifying the static IPv4 address, Subnet Mask and Default Gateway to be configured to the device.



Note: IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx". Each Number ranges from 0 to 255.

2000-01-01 00:57:29 (UTC+00:00 UTC)

Network IP Configuration

☐ DHCP Used


IPv4 Address
3.3.3.1

IPv4 Mask
255.255.255.0

IPv4 Gateway
3.3.3.4

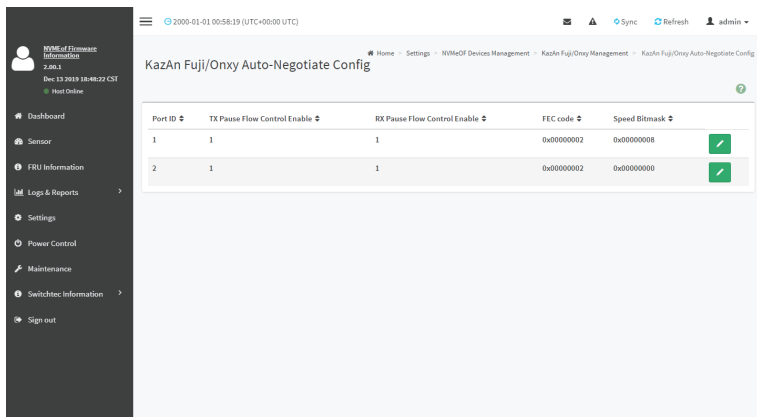
IPv4 Hostname
port1

Save

- Click  to configure network IP.

2-6-16 Network Port Auto-Negotiation



Click **Network Port Auto-Negotiation**, a sample screenshot of Network Port Auto-Negotiation page is shown below.



2000-01-01 00:58:19 (UTC+08:00 UTC)

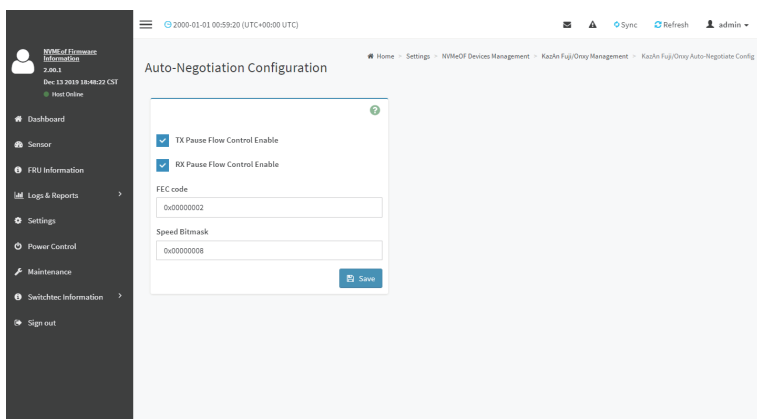
Home Settings NVMeOF Devices Management KazAn Fuji/Onxy Management KazAn Fuji/Onxy Auto-Negotiate Config

KazAn Fuji/Onxy Auto-Negotiate Config

Port ID	TX Pause Flow Control Enable	RX Pause Flow Control Enable	FEC code	Speed Bitmask	
1	1	1	0x00000002	0x00000008	
2	1	1	0x00000002	0x00000008	

Procedures

- Click **Settings > NVMeOF Device Management > KazAn Fuji/Onxy Information > Network Port Auto-Negotiation** to enter Network Port Auto-Negotiation.
- Click  to configure Auto Negotiation.



2000-01-01 00:59:20 (UTC+08:00 UTC)


Home Settings NVMeOF Devices Management KazAn Fuji/Onxy Management KazAn Fuji/Onxy Auto-Negotiate Config

Auto-Negotiation Configuration

☒ TX Pause Flow Control Enable
☒ RX Pause Flow Control Enable

FEC code

Speed Bitmask



3. Check both **TX Pause Flow Control Enable** and **RX Pause Flow Control Enable** boxes.
4. Enter **FEC code** and **Speed Bitmask**.
5. Click **Save** to finish configuration.

Parameter	Description																		
Port ID	Network port for which this status is given 1 for the 1 st port 2 for the 2 nd port (not used in 100Gb mode)																		
TX Pause Flow Control Enable	TX: If set, enable TX Pause Flow Control. Default: 1																		
RX Pause Flow Control Enable	TX: If set, enable RX Pause Flow Control. Default: 1																		
FEC code	<table><tr><th>Bit</th><th>CLI</th><th>FEC</th></tr><tr><td>0</td><td>1</td><td>FC-FEC (default)</td></tr><tr><td>1</td><td>2</td><td>RS-FEC</td></tr><tr><td>2</td><td>4</td><td>10Gb/s per lane FEC</td></tr></table> <p>*Reserved: Not Supported</p>	Bit	CLI	FEC	0	1	FC-FEC (default)	1	2	RS-FEC	2	4	10Gb/s per lane FEC						
Bit	CLI	FEC																	
0	1	FC-FEC (default)																	
1	2	RS-FEC																	
2	4	10Gb/s per lane FEC																	
Speed Bitmask	<p>Bitmask of technologies to advertise. Bit settings are as follow</p> <table><tr><th>Bit</th><th>CLI Value</th><th>Speed</th></tr><tr><td>-</td><td>0</td><td>Port Disabled</td></tr><tr><td>0</td><td>1</td><td>*10Gb</td></tr><tr><td>1</td><td>2</td><td>25Gb</td></tr><tr><td>2</td><td>4</td><td>50Gb</td></tr><tr><td>3</td><td>8</td><td>100Gb</td></tr></table> <p>*Reserved: Not Supported</p> <p>Note: If multiple bits are set, only highest speed will be used for configuration.</p>	Bit	CLI Value	Speed	-	0	Port Disabled	0	1	*10Gb	1	2	25Gb	2	4	50Gb	3	8	100Gb
Bit	CLI Value	Speed																	
-	0	Port Disabled																	
0	1	*10Gb																	
1	2	25Gb																	
2	4	50Gb																	
3	8	100Gb																	

2-6-17 Target NQN Table

Click **Target NQN Table**, a sample screenshot of Target NQN Table page is shown below.

The screenshot shows the 'KazAn Fuji/Onxy Target NQN Config' page. On the left is a dark sidebar with a user profile (NOME of Firmware Information, 2.00.4, Dec 13 2019 18:46:22 CST, Host Online) and a menu including Dashboard, Sensor, FRU Information, Logs & Reports, Settings, Power Control, Maintenance, Switchtec Information, and Sign out. The main content area has a top bar with a clock (2000-01-01 01:00:25 UTC+00:00 UTC), navigation icons (Sync, Refresh), and a user dropdown (admin). Below the top bar is a breadcrumb trail: Home > Settings > NVMeOF Devices Management > KazAn Fuji/Onxy Management > KazAn Fuji/Onxy Target NQN Config. The main table is titled 'KazAn Fuji/Onxy Target NQN Config' and contains 10 rows. Each row has a 'Slot ID' and a 'Target NQN' value, with a green pencil icon in the rightmost column for editing.

Slot ID	Target NQN	
1	nqn.2015-09.com.kazan-networks:nvme.1	
2	nqn.2015-09.com.kazan-networks:nvme.2	
3	nqn.2015-09.com.kazan-networks:nvme.3	
4	nqn.2015-09.com.kazan-networks:nvme.4	
5	nqn.2015-09.com.kazan-networks:nvme.5	
6	nqn.2015-09.com.kazan-networks:nvme.6	
7	nqn.2015-09.com.kazan-networks:nvme.7	
8	nqn.2015-09.com.kazan-networks:nvme.8	
9	nqn.2015-09.com.kazan-networks:nvme.9	
10	nqn.2015-09.com.kazan-networks:nvme.10	

Procedures

1. Click **Settings > NVMeOF Device Management > KazAn Fuji/Onxy Information> Target NQN Table** to enter Target NQN Table page.
2. Click to configure Target NQN Table.

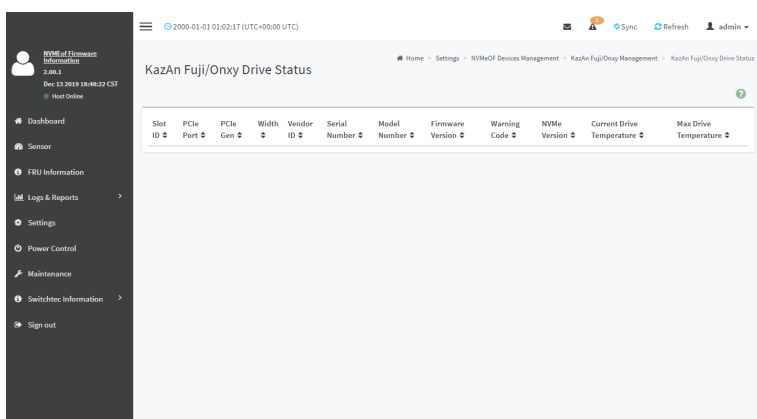
The screenshot shows the 'Target NQN Configuration' page. The sidebar and top navigation are identical to the previous screenshot. The main content area has a title 'Target NQN Configuration' and a breadcrumb trail: Home > Settings > NVMeOF Devices Management > KazAn Fuji/Onxy Management > KazAn Fuji/Onxy Target NQN Config. Below the title is a form with a text input field labeled 'Target NQN' containing the value 'nqn.2015-09.com.kazan-networks:nvme.1'. To the right of the input field is a blue 'Save' button.

3. Enter Target NQN.
4. Click Save to finish configuration.

Parameter	Description
Slot ID	Slot number in the chassis/Shelf where this drive resides. Note: This field must be set for all CRUD operations.
Target NQN	When Create/Read/Update are used on this object, the length of this field can vary, but must be a multiple of 4-byte (i.e. the entire 4* 64 bytes are not required to be sent if the NQN is shorter than 256 bytes)

2-6-18 Drive Status

Click **Drive Status**, a sample screenshot of Drive Status page is shown below.



Procedures

1. Click **Settings > NVMeOF Device Management > KazAn Fuji/Onxy Information> Drive Status** to enter Drive Status page.

Parameter	Description												
Slot ID	Slot number in the chassis/Shelf where this drive resides. Note: This field must be set for all CRUD operations.												
PCIe Port	PCIe Port for which this status is given 0 for 1 st port 1 for the 2 nd port (not used in x16 mode)												
PCIe Gen	0=Link Down, 1=Gen1, 2=Gen2, 3=Gen3, All values reserved.												
Width	0=Link Down, 1=x1, 2=x2, 3=x4, 4=x8, 5=x16. All values reserved.												
Vendor ID	PCIe vendor ID												
Serial Number	32 character string for drive serial number.												
Model Number	32 character string for drive model number												
Firmware Version	16 character string for firmware version.												
Warning Code	<p>Returns the Critical Warning Field from the SMART/Health information</p> <table border="1"> <thead> <tr> <th>Bit</th><th>Definition</th></tr> </thead> <tbody> <tr> <td>0</td><td>Avail spare space below threshold</td></tr> <tr> <td>1</td><td>Over/Below temperature threshold</td></tr> <tr> <td>2</td><td>NVM Subsystem degrade due to media/internal errors</td></tr> <tr> <td>3</td><td>Media in read only mode</td></tr> <tr> <td>4</td><td>Volatile memory backup device failed</td></tr> </tbody> </table>	Bit	Definition	0	Avail spare space below threshold	1	Over/Below temperature threshold	2	NVM Subsystem degrade due to media/internal errors	3	Media in read only mode	4	Volatile memory backup device failed
Bit	Definition												
0	Avail spare space below threshold												
1	Over/Below temperature threshold												
2	NVM Subsystem degrade due to media/internal errors												
3	Media in read only mode												
4	Volatile memory backup device failed												
NVMe Version	<p>Indicates the major/minor version of the NVMe specification that the controller implementation supports. Valid versions of the specification are currently: 1.0, 1.1, and 1.2.</p> <p>31:16 0001h Major Version Number (MJR): Major Version is "1"</p> <p>15:08 00h Minor Version Number (MNR): can be 00, 01, 02</p> <p>00:00 00h Reserved</p> <p>07:00 00h Reserved</p>												
Current Drive Temperature	Displays current drive temperature information.												
Max Drive Temperature	Maximum drive temperature since boot.												
Namespace Available	Number of Namespace available on this drive												

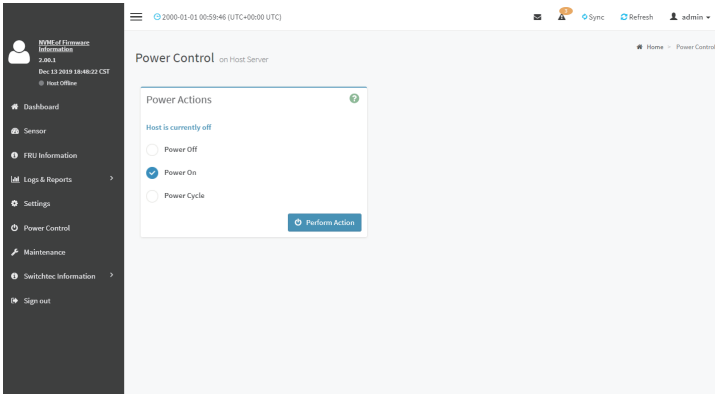
I/Q Queues allocation	Number of I/O queues allocated to drive						
PCIe BDF	Bus/Device/Function: PCIe bus ID Bus: (value>>8) & 0xFF Device: (value>>3) & 0x7 Function: (value & 0x7)						
Base Address Register	Assigned Base Address Register for drive						
MSI-Table Size	MSI-X Table size						
Doorbell Stride	This stride in bytes between submission/completion doorbell registers ($2^{(2 + \text{DSTRD})}$). A value of 0h indicates a stride of 4 bytes, where the doorbell registers are packed without reserved space between each register.						
NVM Subsystem Reset Supported	Set to '1' if the controller supports the NVM Subsystem Reset feature.						
Common Sets Supported	I/O Common Set(s) that the controller supports. <table border="1"> <thead> <tr> <th>Bit</th><th>Definition</th></tr> </thead> <tbody> <tr> <td>0</td><td>NVM common set</td></tr> <tr> <td>7:1</td><td>Reserved</td></tr> </tbody> </table>	Bit	Definition	0	NVM common set	7:1	Reserved
Bit	Definition						
0	NVM common set						
7:1	Reserved						
Memory Page Size Min	Memory Page Min						
Memory Page Size Max	Maximum host memory page size that the controller supports ($2^{(12 + \text{MPSMAX})}$)						
Maximum Queues Entries Supported	Maximum individual Submission queue size that the controller supports. This is a 0' based value. The minimum value is 1h, indicating two entries.						
Contiguous Queues Required	Set if the controller requires that I/O Submission/Completion Queues are required to be physically contiguous.						
Arbitration Mechanism Supported	Optional arbitration mechanisms supported by the controller. Bit 0: Weighted Round Robin with Urget Priority Case Bit 1: Vendor Specific.						

Timeout	<p>Worst case time that the host software shall wait for CSTS.RDY to transition from:</p> <ul style="list-style-type: none">a) '0' to '1' after CC.EN transition from '0' to '1'; orb) '1' to '0' after CC.EN transition from '1' to '0'. <p>This worst case time may be experienced after events such as an abrupt shutdown or activation of a new firmware image; typical time are expected to be much shorter. This field is in 500 millisecond units.</p>
---------	--

2-7 Power Control

This page allows you to view and control the power of your server.

To open Power Control, click **Power Control** from the menu bar. A sample screenshot of Power Control is shown below.



The various options of Power Control are given below.

Power Off: To immediately power off the server.

Power On: To power on the server.

Power Cycle: This option will first power off, and then reboot the system (cold boot).

Procedure

Select an action and click Perform Action to proceed with the selected action.



Note: During Execution you will be asked to confirm your choice. Upon confirmation, you will be informed about the status after few minutes.



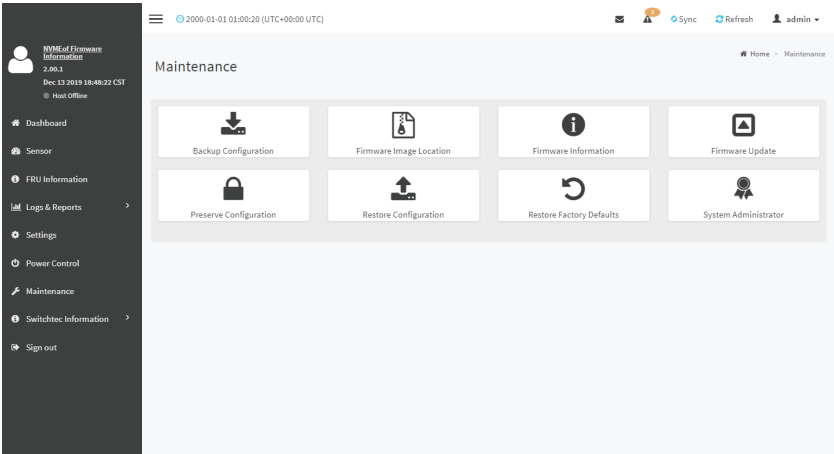
Note: It is advisable to use Chrome or IE for H5Viewer, since Firefox has its own memory limitations.

2-8 Maintenance Group

This group of pages allows you to do maintenance tasks on the device. The menu contains the following items:

- Backup Configuration
- Firmware Image Location
- Firmware Information
- Firmware Update
- Preserve Configuration
- Restore Configuration
- Restore Factory Defaults
- System Administrator

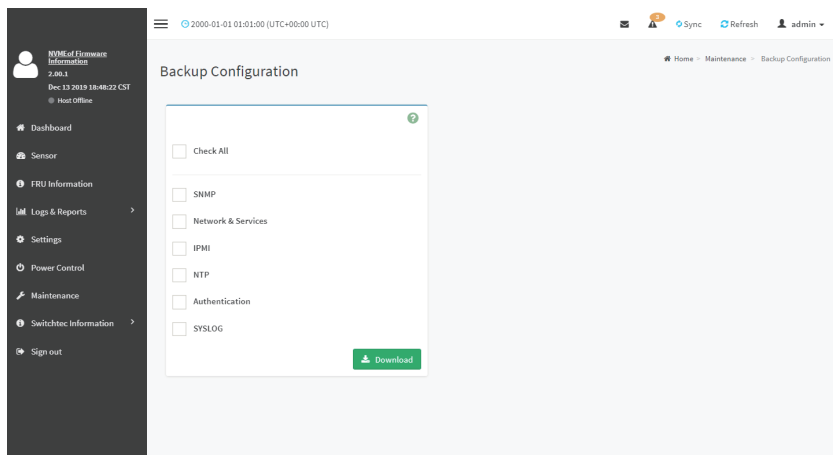
A sample screenshot of Maintenance is shown below.
A detailed description is given below.



2-8-1 Backup Configuration

This page allows you to select the specific configuration items to be backed up in case of “Backup Configuration”.

To open Backup Configuration page, click **Maintenance > Backup Configuration** from the menu bar. A sample screenshot of Backup Configuration page is shown below.



The various fields of Backup Configuration page are given below.

Check All - To select all the configuration list.

Download Config - To download and save the configuration files backup from BMC to client system.

Procedure

1. Click **Check All** to backup the selected configuration items. The Backup Configuration page will appear as shown above screenshot.
2. Click **Download Config** to save the backup file to the client system.
3. Click **OK** to perform the backup action. The Backup file will be saved in the client system.
4. Click **Cancel** to cancel the backup process.

TFTP server configuration

The TFTP server configuration is used for exporting the backup file.



Note: Ensure that no other TFTP servers are enabled, if so remove all other servers with all configuration files. Login as “super” user means “root” user.

Procedure to make the default tftp server

1. Install the application which is needed.

>apt-get install xinetd tftp tftpd

2. Edit the configuration file for TFTP.

```
>vi /etc/xinetd.d/tftp
```

Edit the file as below:

```
service tftp
{
  protocol = udp
  port = 69
  socket_type = dgram
  wait = yes
  user = nobody
  server = /usr/sbin/in.tftpd
  server_args = <DIR to which the file to be access>
  disable = no
}
#EOF
#example:server_args = /tftpboot
Note: No arguments to be passed to the server_args other than directory.
#####
>vi /etc/xinetd.conf
```

Add to the file:

```
defaults
{
  # Please note that you need a log_type line to use log_on_success and log_on_failure.
  The default is the following:
  # log_type = SYSLOG daemon info
}
includedir /etc/xinetd.d
>vi /etc/inetd.conf
```

```
ftp stream tcp nowait root /usr/sbin/tcpd /usr/sbin/ in.ftpd
tftp dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/ in.tftpd <DIR>
```

3. Restart the server.

```
>/etc/init.d/xinetd restart
```

4. Give permission to the file to access by all.

```
>mkdir <DIR>
```

```
>chmod -R 777 <DIR>
```

```
>chown -R nobody <DIR>
```

For Example:

```
mkdir /tftpboot
chmod -R 777 /tftpboot
chown -R nobody /tftpboot
```

5. To receive the file you have to touch the file and give permission to access by all users

```
>touch <DIR>/conf.bak
>chmod 777 <DIR>/conf.bak
```

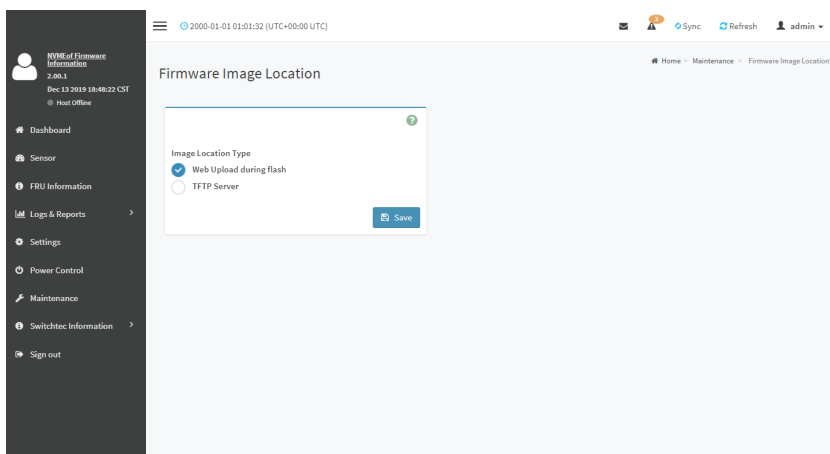
6. Even after all this step has been done and still facing error of timeout:
 - a) Check with /etc/xinetd.d/tftp file and uncomment the EOF (Remove the '#' before the EOF alone).
 - b) Restart the server.

2-8-2 Firmware Image Location

This page is used to configure firmware image into the BMC.

To open **Firmware Image Location**, click **Maintenance > Firmware Image Location** from the menu bar.

A sample screenshot of Firmware Image Location page is shown below.



The various options of Image Transfer Protocol are given below.

Image Location Type: Type of location to transfer the firmware image into the BMC either Web Upload during Flash or TFTP Server.

TFTP Server Address: Address of the server where the firmware image is stored.



Note: The Server supports both IPv4 and IPv6 addresses

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.

IPv6 Address made of 8 groups of 4 Hexadecimal digits separated by colon as in

"xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx."

Hexadecimal digits are expressed as lower-case letters.

TFTP Image Name: Full Source path with filename of the firmware image is stored on TFTP Server.

TFTP Retry Count: Number of times to be retried in case a transfer failure occurs. Retry count ranges from 0 to 255.

Save: To save the configured settings.

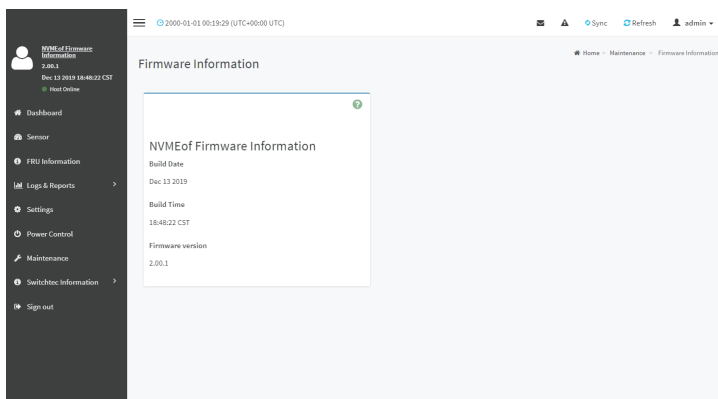
Procedure

1. Select the **Image Location Type (Web Upload during flash/ TFTP Server)**.
2. If the protocol selected is TFTP, enter the IP address of the server in the **TFTP Server Address** field.
3. Enter the **TFTP Image Name** in the given field
4. Enter the **TFTP Retry Count** value.
5. Click **Save** to save the changes.

2-8-3 Firmware Information

This wizard takes you through the process of firmware upgradation. A reset of the box will This page is used to configure the Firmware Information settings.

To open System Administrator page, click **Maintenance > Firmware Information** from the menu bar. A sample screenshot of Firmware Information page is shown below.



The various fields of Firmware Information page are given below.

BMC Firmware Information:

Build Date: 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.

BIOS Firmware Information:

Product Manufacturer: Describes the hardware manufacturer.

Product Name: Describes the model name of the device.

Build Date: Describes the Build Date of the device.

Firmware version: Describes the BIOS version of the device.

CPLD Firmware Information:

Firmware version: Describes the CPLD Firmware version.

2-8-4 Firmware Update

This wizard takes you through the process of firmware upgradation. A reset of the box will automatically follow if the upgrade is completed or cancelled. An option to Preserve All Configuration is available. Enable it, if you wish to preserve configured settings through the upgrade.



Warning: Please note that after entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically. If upgrade process is cancelled in the middle of the wizard, the device will be reset.



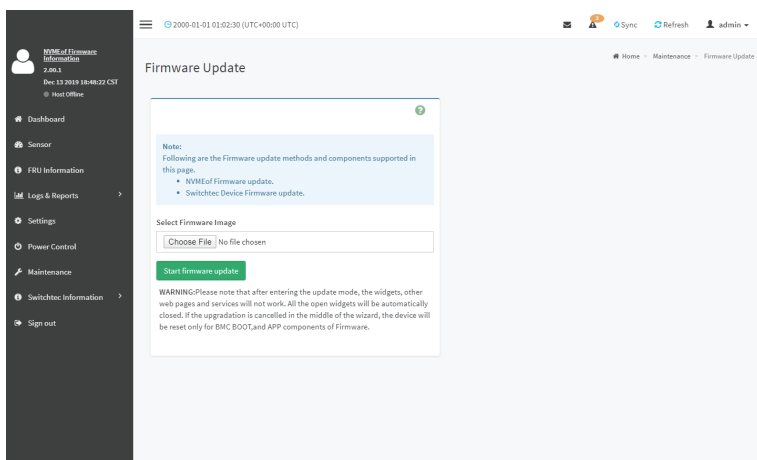
Note: The firmware upgrade process is a crucial operation. Make sure that the chances of a power or connectivity loss are minimal when performing this operation.

Once you enter into Update Mode and choose to cancel the firmware flash operation, the BMC must be reset. This means that you must close the Internet browser and log back onto the BMC before you can perform any other types of operations.

Once Firmware upgrade using web is started, the regular IPMI command will not be allowed for safety concern if Enable IPMI Command handling during flashing support is disabled in project configuration.

To configure, choose '**Firmware Image Location**' under Maintenance. To open Firmware Update page, click **Maintenance > Firmware Update** from the menu bar.

A sample screenshot of Firmware Update page is shown below.



The various fields of Firmware Update are as follows:

- **Select Firmware Image:** To select the Firmware image to be uploaded.
- **Start Firmware Update:** To start the Firmware Update.

This wizard takes you through the process of AMI based firmware upgradation. The protocol information to be used for firmware image transfer during this update is as follows:



Note: All configuration items will be preserved/overwrite as default during the restore configuration operation.

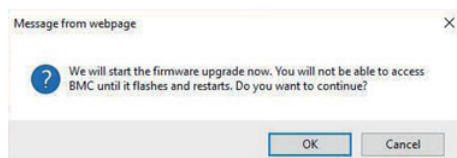
Procedure

6. Click Browse to select firmware image. The Firmware update undergoes the following steps:
 - a) Closing all active client requests
 - b) Preparing Device for Firmware Upgrade
 - c) Uploading Firmware Image



Note: A file upload pop-up will be displayed for http/https but in the case of tftp files, the file is automatically uploaded displaying the status of upload.

- d) Browse and select the Firmware image to flash and click **Upload**.
- e) Click **Start firmware update** start the Firmware Update. A warning message will be prompted you to proceed further.
- f) Click **OK** to start the Firmware Update. The sample screenshot is shown below
- g) Verifying Firmware Image



If flashing is required for all images, please select the following checkbox:

Only the selected sections will be updated:

Section Name	Existing version	Uploaded version	<input type="checkbox"/>
boot	2.4.000000	2.4.000000	<input checked="" type="checkbox"/>
conf	2.4.000000	2.4.000000	<input checked="" type="checkbox"/>
conf	2.4.000000	0.0.	<input checked="" type="checkbox"/>
root	2.4.000000	2.4.000000	<input checked="" type="checkbox"/>
osimage	2.4.000000	2.4.000000	<input checked="" type="checkbox"/>
www	2.4.000000	2.4.000000	<input checked="" type="checkbox"/>
testapps	2.4.000000	2.4.000000	<input checked="" type="checkbox"/>
ast2500e	0.1.000000	0.1.000000	<input checked="" type="checkbox"/>

Flash selected sections

If only few module versions are different, those modules will be flashed.



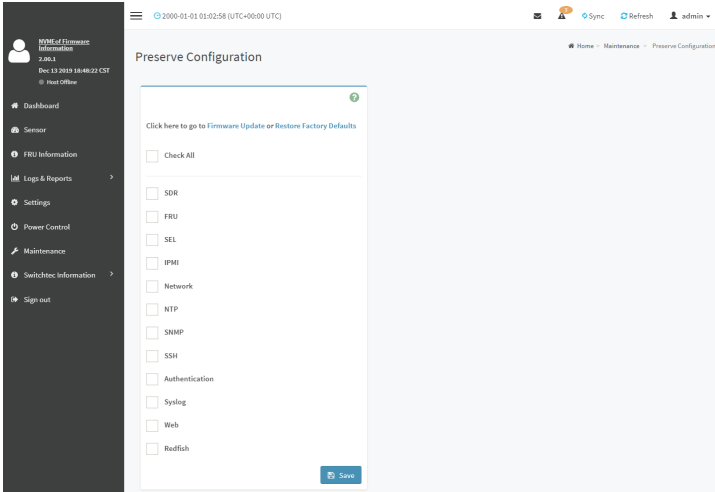
Note: Only selected sections of the firmware will be updated. Other sections are skipped. Before starting flash operation, you are advised to verify the compatibility between image sections.

2-8-5 Preserve Configuration

This page allows the user to configure the preserve configuration items, which will be used by the Restore factory defaults to preserve the existing configuration without overwriting with defaults/Firmware Upgrade configuration,

To open Preserve Configuration page, click **Maintenance > Preserve Configuration** from the menu bar.

A sample screenshot of Preserve Configuration page is shown below.



The various fields of Preserve Configuration are as follows:

Click here to go to Firmware Update or Restore Configuration: This link will redirect to the Firmware Update or Restore Configuration page which needs to be preserved.

Check All: To check the entire configuration list.

Save: To save the current changes.



Note: This configuration is used by Restore Factory Defaults process.

Files Preserved

SDR

Following files will be preserved:

SDR.dat: This file contains the sensor data record information that is used in IPMI.

Dependency Configurations - NIL

FRU

Following files will be preserved:

FRU.bin: This file contains the logical field replaceable unit data that are used by IPMI.

Dependency Configurations - SDR

FRU

Following files will be preserved:

FRU.bin: This file contains the logical field replaceable unit data that are used by IPMI.

Dependency Configurations - SDR

SEL

Following files will be preserved when Delete SEL reclaim space is disabled:

SEL.dat: This file contains the system event logs that are being logged by the IPMI.

Following files will be preserved when Delete SEL reclaim space is enabled:

Selreclaiminfo.ini - The file contains the SEL repository information.

SEL folder - This folder contains the multiple files of event logs.

Dependency Configurations - IPMI

IPMI

The following files are preserved in IPMI configuration:

IPMI.conf: This file contains the IPMI configurations such as SEL rep size, SDR rep size, interface specific, enable/disable, Primary/Secondary, IPMB Bus number etc.

Dependency Configurations - NIL

Network

To save network settings related with IPMI (LAN IP or DHCP configuration), select “IPMI” and “Network” options simultaneously. After restore configuration, the Network Configuration will be preserved successfully. Following files will also be preserved:

dhcp.conf: This file is to configure the host name in the FQDN format.

dns.conf: This file is used to configure the DNS registration method and DNS server for the particular interface, hostname: This file is used to store the Hostname of the BMC.

hostname.conf: This file is used to configure the host name creation method Manual/Automatic for the BMC.

Vlaninterfaces: This file helps to enable the vlan interface for the particular LAN interface

vlansetting.conf: This file is to store the vlan ID and Vlan priority for the particular VLAN interface entry.

bond.conf: This file is to enable the bond interface for the specified LAN interfaces.

Interfaces: This file is to configure the IP/IPv6 addresses for the LAN interface using static/DHCP method.

activeslave.conf: This file is to configure the active interface for the specified bond interface. This file depends on bond.conf.

hosts: This file is used to store the host name to map the IP address.

hosts.allow: This file contains the list of hosts that has permission to access the system

hosts.deny: This file contains the list of host that does not allow accessing the system

resolv.conf: This file is used to store the nameserver and domain name for hostname registration.

dhcp6c-script: This file is used to configure the domain name, DNS server IPv6 address and NTP address.

dhcp6c.conf: This file is to configure the IPv6 parameters for the DHCPv6 clients.

ncsicfg.conf: This file is to configure the NCSI related configurations.

nsupdate.conf: This file is to configure the channel ID, package ID for the NCSI interface.

phycfg.conf: This file is to configure the link speed, duplex and MTU value for the specified interface.

dhcp.preip_4: This file is to store the pre IPv4 address. This file will be created at runtime.

dns.conf: This file is used to configure the DNS registration method and DNS server for the particular interface.

hostname: This file is used to store the Hostname of the BMC.

hostname.conf: This file is used to configure the host name creation method Manual/Automatic for the BMC.

Vlaninterfaces: This file helps to enable the vlan interface for the particular LAN interface

vlansetting.conf: This file is to store the vlan ID and Vlan priority for the particular VLAN interface entry.

bond.conf: This file is to enable the bond interface for the specified LAN interfaces.

Interfaces: This file is to configure the IP/IPv6 addresses for the LAN interface using static/DHCP method.

activeslave.conf: This file is to configure the active interface for the specified bond interface. This file depends on bond.conf.

hosts: This file is used to store the host name to map the IP address.

hosts.allow: This file contains the list of hosts that has permission to access the system

hosts.deny: This file contains the list of host that does not allow accessing the system

resolv.conf: This file is used to store the nameserver and domain name for hostname registration.

dhcp6c-script: This file is used to configure the domain name, DNS server IPv6 address and NTP address.

dhcp6c.conf: This file is to configure the IPv6 parameters for the DHCPv6 clients.

ncsicfg.conf: This file is to configure the NCSI related configurations.

nsupdate.conf: This file is to configure the channel ID, package ID for the NCSI interface.

phycfg.conf: This file is to configure the link speed, duplex and MTU value for the specified interface.

dhcp.preip_4: This file is to store the pre IPv4 address. This file will be created at runtime.

NTP

Following files will be preserved:

ntp.conf: This file contains the NTP daemon protocol configuration parameters such as synchronization sources, nodes and other related information

ntp.stat: This file contains the auto or manual network type protocols

adjtime: This file contains the time to synchronize the system clock

Localtime: This file is the system link to the file local time or to the correct time zone in the system timezone directly.

Dependency Configurations - IPMI

SNMP

Following files will be preserved:

snmp_users.conf: This file contains the SNMP user configurations such as user name and password encryption mechanism for the specific users.

snmpcfg.conf: This file contains the SNMP users privilege levels such as ro user and rw user.

Dependency Configurations - NIL

SSH

Following files will be preserved:

sshd_config: This file contains the keyword argument pairs of configurations such as Address family, Accept Env, Allow, users, authorized key files etc.

ssh_host_dsa_key, ssh_host_rsa_key: These files contain the private parts of the host keys.

ssh_host_dsa_key.pub, ssh_host_rsa_key.pub: These files contain the public parts of the host keys.

Dependency Configurations - NIL

Authentication

Following files will be preserved:

activedir.conf: This file contains the configurations such as sslenable, timeout, racdomain, adtype, adfilterdc1, adfilterdc2, adfilterdc3, username, password, and rolegroup information such as name domain and privileges.

openldapGroup.conf: This file contains the oprnm ldap role group information such as name domain and privilege.

nsswitch.conf: This file contains the sources to obtain the name service information in the range of categories and in what order

pam_withunix: This file contains the PAM Order of modules such as IPMI,LDAP, RADIUS and UNIX.

pam_wounix: This contains the PAM Order of modules such as IPMI, LDAP and RADIUS.

group: This file contains the Linux group. It stores the group information or defines the user group information in Linux.

passwd: This file contains the user login information for the Linux system

shadow: This file contains the encrypted password information for the clients.

ldap.conf: This file contains the ldap server configuration details such as bindn, binpw, pam_password, nss_reconnect_tries, port, port secondary, host, host secondary.

radius.conf: This file contains the radius server IP address, port number, secret, timeout, privilege etc.

Dependency Configurations – NIL

Syslog

System Event Log

Web

Web Settings

Redfish

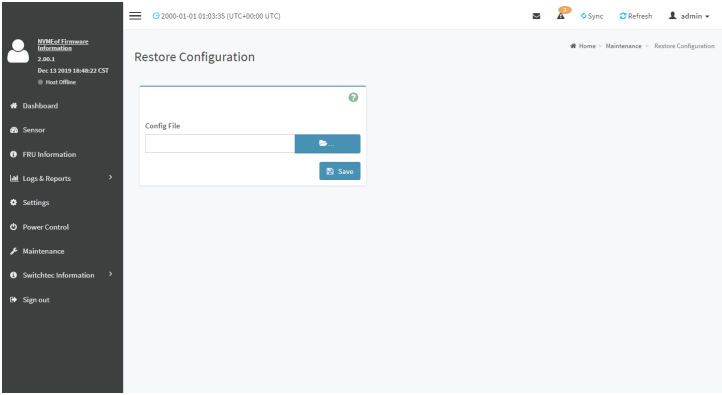
Redfish Audit Log

Procedure

1. Click **Firmware Update or Restore Configuration** link to view Firmware Update or Restore Configuration page accordingly.
2. Select the required Preserve Configuration items by either choosing the items individually by selecting the appropriate check boxes or by selecting all or none using **Check All**.
3. Click **Save** to save the changes.

2-8-6 Restore Configuration

This page allows you to restore the configuration files from the client system to the BMC. To open Restore Configuration page, click **Maintenance > Restore Configuration** from the menu bar. A sample screenshot of Restore Configuration page is shown below.



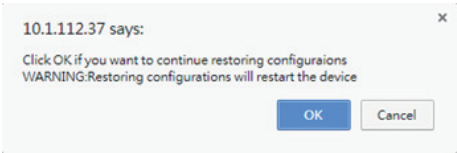
The various fields Restore Configuration page are given below.

Config File - This option is used to select the file which was backup earlier.

Upload - To upload the backup file to restore the backup files.

Procedure for Restore Configuration:

1. Click Browse to select the configuration file that needs to be backup and used to restore the configuration, when needed.
2. Click Upload to restore the backup files. The Restore Configuration page will appear as shown below.



3. Click OK to upload the new configuration file and restore.

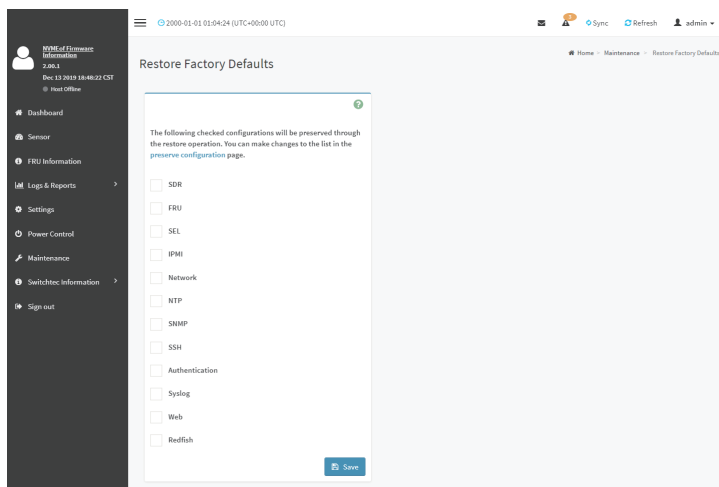
2-8-7 Restore Factory Defaults

In BMC Web GUI, this option is used to restore the factory defaults of the device firmware. This section lists the configuration items that will be preserved during restore factory default configuration.



Warning: Please note that after entering restore factory widgets, other web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within few minutes.

To open Restore Factory Defaults page, click **Maintenance > Restore Factory Defaults** from the menu bar. A sample screenshot of Restore Factory Defaults page is shown below.



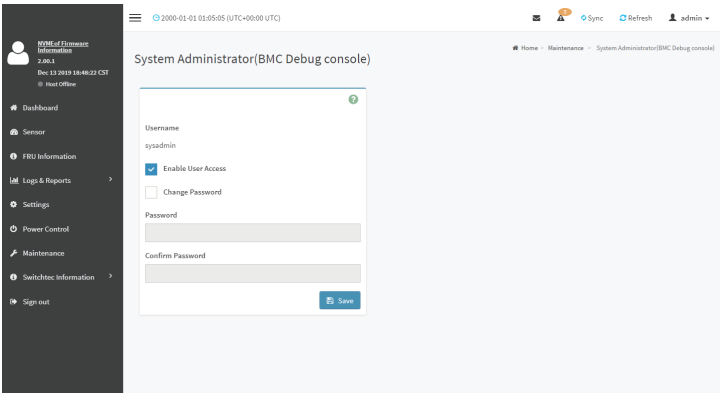
Procedure

1. Click Preserve Configuration to redirect to Preserve Configuration page, which is used to preserve the particular configuration not to be overwritten by the default configuration.
2. Click Restore Factory Defaults to restore the factory defaults of the device firmware

2-8-8 System Administrator

This page is used to configure the System Administrator settings.

To open System Administrator page, click **Maintenance > System Administrator** from the menu bar. A sample screenshot of System Administrator page is shown below.



The various fields of System Administrator page are given below.

Username: Username of System Administrator is a read only field.

Enable User Access: To enable user access for system administrator.

Change Password: To change the user's password.



Note: This field will not allow more than 64 characters.

Password must be at least 8 characters long and blank space is not allowed.

Save: To save the new configuration for system administrator.

Procedure

1. Check **Enable User Access** to enable user access for system administrator..
2. Enable **Change Password** option to change the user password. This action enables the password fields.
3. Enter the new password in the **Password** field.
4. Re-enter the password in the **Confirm Password** field.
5. Click **Save** to save the changes.

2-8-9 Switchtec Information

Switchtec Information page displays the Link Status and Processor Monitors of Node1 and Node 2. To open the Link Status Information page, click **Switchtec Information** from the menu bar. Select a N1 or N2 from the Switchtec Information section to view the details of the selected device. A screenshot of Link Status page is shown below.

Home

Link Status

Collector M1

Targeted M1

Switchtec Information

2000-02-01 00:00:00 (UTC+0800 UTC)

Sync

Refresh

Admin

Switchtec Information

Physical Port ID: 124 - (RD000)

Partition ID	Port Direction	Logical Port ID	Physical Port ID	Stack ID	Port ID in the Stack	Config Link Width	Negotiate Link Width	Link Rate	Link Status
0	DSP	1	24	3	0	4	0	Gen1	Down

Physical Port ID: 126 - (RD001)

Partition ID	Port Direction	Logical Port ID	Physical Port ID	Stack ID	Port ID in the Stack	Config Link Width	Negotiate Link Width	Link Rate	Link Status
0	DSP	2	26	3	2	4	0	Gen1	Down

Physical Port ID: 128 - (RD002)

Partition ID	Port Direction	Logical Port ID	Physical Port ID	Stack ID	Port ID in the Stack	Config Link Width	Negotiate Link Width	Link Rate	Link Status
0	DSP	3	28	3	4	4	0	Gen1	Down

Physical Port ID: 130 - (RD003)

Partition ID	Port Direction	Logical Port ID	Physical Port ID	Stack ID	Port ID in the Stack	Config Link Width	Negotiate Link Width	Link Rate	Link Status
1	DSP	1	30	3	6	4	0	Gen1	Down

Physical Port ID: 132 - (RD004)

Partition ID	Port Direction	Logical Port ID	Physical Port ID	Stack ID	Port ID in the Stack	Config Link Width	Negotiate Link Width	Link Rate	Link Status
1	DSP	2	32	4	0	4	0	Gen1	Down

Physical Port ID: 134 - (RD005)

Partition ID	Port Direction	Logical Port ID	Physical Port ID	Stack ID	Port ID in the Stack	Config Link Width	Negotiate Link Width	Link Rate	Link Status
1	DSP	3	34	4	2	4	2	Gen2	Up

Physical Port ID: 136 - (RD006)

Partition ID	Port Direction	Logical Port ID	Physical Port ID	Stack ID	Port ID in the Stack	Config Link Width	Negotiate Link Width	Link Rate	Link Status
2	DSP	1	36	4	4	4	0	Gen1	Down

Physical Port ID: 138 - (RD007)

Partition ID	Port Direction	Logical Port ID	Physical Port ID	Stack ID	Port ID in the Stack	Config Link Width	Negotiate Link Width	Link Rate	Link Status
2	DSP	2	38	4	6	4	0	Gen1	Down

Physical Port ID: 140 - (RD008)

Partition ID	Port Direction	Logical Port ID	Physical Port ID	Stack ID	Port ID in the Stack	Config Link Width	Negotiate Link Width	Link Rate	Link Status
2	DSP	3	40	5	0	4	0	Gen1	Down

Physical Port ID: 142 - (RD009)

Partition ID	Port Direction	Logical Port ID	Physical Port ID	Stack ID	Port ID in the Stack	Config Link Width	Negotiate Link Width	Link Rate	Link Status
3	DSP	1	42	5	2	4	0	Gen1	Down

Physical Port ID: 144 - (RD010)

Partition ID	Port Direction	Logical Port ID	Physical Port ID	Stack ID	Port ID in the Stack	Config Link Width	Negotiate Link Width	Link Rate	Link Status
3	DSP	2	44	5	4	4	0	Gen1	Down

Physical Port ID: 146 - (RD011)

Partition ID	Port Direction	Logical Port ID	Physical Port ID	Stack ID	Port ID in the Stack	Config Link Width	Negotiate Link Width	Link Rate	Link Status
3	DSP	3	46	5	6	4	0	Gen1	Down

Switchtec Information

2006-03-01 00:34:33 (UTC+08:00 UTC)

Sync

Refresh

Admin

Home

Processor Monitor

Switchtec Information

Link Status

NI (Main)

NI (Stand)

Processor Monitor

NI (Main)

NI (Stand)

Switchtec Information

Physical Port ID: 24 - (P020)

Physical Port ID	Port Direction	Internal mac	Egress Port BW Count	Egress Completion BW Count	Egress Non-paused BW Count	Ingress Port BW Count	Ingress Completion BW Count	Ingress Non-paused BW Count
24	DSP	250061	0	0	0	0	0	0

Physical Port ID: 24 - (P020)

Physical Port ID	Port Direction	Internal mac	Egress Port BW Count	Egress Completion BW Count	Egress Non-paused BW Count	Ingress Port BW Count	Ingress Completion BW Count	Ingress Non-paused BW Count
24	DSP	250061	0	0	0	0	0	0

Physical Port ID: 28 - (P020)

Physical Port ID	Port Direction	Internal mac	Egress Port BW Count	Egress Completion BW Count	Egress Non-paused BW Count	Ingress Port BW Count	Ingress Completion BW Count	Ingress Non-paused BW Count
28	DSP	250061	0	0	0	0	0	0

Physical Port ID: 30 - (P020)

Physical Port ID	Port Direction	Internal mac	Egress Port BW Count	Egress Completion BW Count	Egress Non-paused BW Count	Ingress Port BW Count	Ingress Completion BW Count	Ingress Non-paused BW Count
30	DSP	250061	0	0	0	0	0	0

Physical Port ID: 32 - (P020)

Physical Port ID	Port Direction	Internal mac	Egress Port BW Count	Egress Completion BW Count	Egress Non-paused BW Count	Ingress Port BW Count	Ingress Completion BW Count	Ingress Non-paused BW Count
32	DSP	250061	0	0	0	0	0	0

Physical Port ID: 34 - (P020)

Physical Port ID	Port Direction	Internal mac	Egress Port BW Count	Egress Completion BW Count	Egress Non-paused BW Count	Ingress Port BW Count	Ingress Completion BW Count	Ingress Non-paused BW Count
34	DSP	250061	0	0	0	0	0	0

Physical Port ID: 36 - (P020)

Physical Port ID	Port Direction	Internal mac	Egress Port BW Count	Egress Completion BW Count	Egress Non-paused BW Count	Ingress Port BW Count	Ingress Completion BW Count	Ingress Non-paused BW Count
36	DSP	250061	0	0	0	0	0	0

Physical Port ID: 38 - (P020)

Physical Port ID	Port Direction	Internal mac	Egress Port BW Count	Egress Completion BW Count	Egress Non-paused BW Count	Ingress Port BW Count	Ingress Completion BW Count	Ingress Non-paused BW Count
38	DSP	250061	0	0	0	0	0	0

Physical Port ID: 40 - (P020)

Physical Port ID	Port Direction	Internal mac	Egress Port BW Count	Egress Completion BW Count	Egress Non-paused BW Count	Ingress Port BW Count	Ingress Completion BW Count	Ingress Non-paused BW Count
40	DSP	250061	0	0	0	0	0	0

Physical Port ID: 42 - (P020)

Physical Port ID	Port Direction	Internal mac	Egress Port BW Count	Egress Completion BW Count	Egress Non-paused BW Count	Ingress Port BW Count	Ingress Completion BW Count	Ingress Non-paused BW Count
42	DSP	250061	0	0	0	0	0	0

Physical Port ID: 44 - (P020)

Physical Port ID	Port Direction	Internal mac	Egress Port BW Count	Egress Completion BW Count	Egress Non-paused BW Count	Ingress Port BW Count	Ingress Completion BW Count	Ingress Non-paused BW Count
44	DSP	250061	0	0	0	0	0	0

Physical Port ID: 46 - (P020)

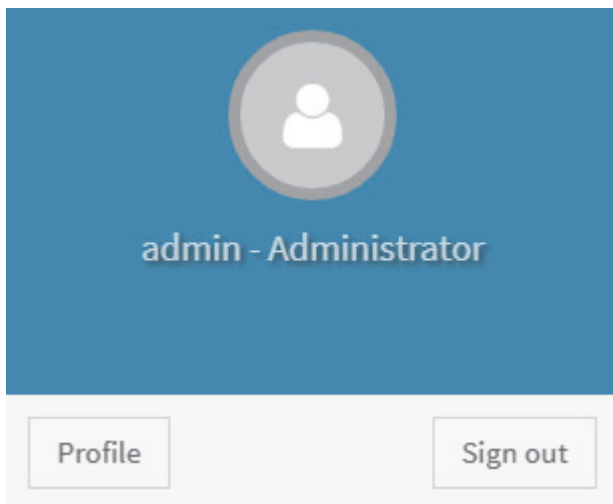
Physical Port ID	Port Direction	Internal mac	Egress Port BW Count	Egress Completion BW Count	Egress Non-paused BW Count	Ingress Port BW Count	Ingress Completion BW Count	Ingress Non-paused BW Count
46	DSP	250061	0	0	0	0	0	0

- 111 -

Gigabyte Server Management Console

2-8-10 Sign Out

To log out from the Web GUI, click the admin on the top right corner of the screen. A sample screenshot of admin option is shown below.



Click **Sign Out** to perform log out from the Web GUI. A Warning message will be prompted you to proceed further, click **OK** to log out else **Cancel** to retain the Web GUI.