BMC Configuration Manual

Document Version: V2.7

Release Date: October 28, 2022

Disclaimer

The purchased products, services and features shall be bound by the contract made between the customer and us. All or part of the products, services and features described herein may not be within your purchase or usage scope. Unless otherwise agreed in the contract, we make no express or implied statement or warranty on the contents herein. Images provided herein are for reference only and may contain information or features that do not apply to your purchased model. This manual is only used as a guide. We shall not be liable for any damage, including but not limited to loss of profits, loss of information, interruption of business, personal injury, or any consequential damage incurred before, during, or after the use of our products. We assume you have sufficient knowledge of servers and are well trained in protecting yourself from personal injury or preventing product damages during operation and maintenance. The information in this manual is subject to change without notice. We shall not be liable for technical or editorial errors or omissions contained in this manual.

Trademarks

All the trademarks or registered trademarks mentioned herein may be the property of their respective holders.

Support

Email	Technical Support	serversupport@aivres.com
	RMA/ARMA Support	serversupportusa@aivres.com
Web	Official Website	www.aivres.com
	Service Portal	service.aivres.com

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	**Description**
⚠ DANGER	A potential for serious injury, or even death if not properly handled.

Symbol	Description
⚠ WARNING	A potential for minor or moderate injury if not properly handled.
⚠ CAUTION	A potential loss of data or damage to equipment if not properly handled.
ⓘ IMPORTANT	Operations or information that requires special attention to ensure successful installation or configuration.
🗒 NOTE	Supplementary description of document information.

Revision History

Version	Date	Description of Changes
V1.0	2021/02/07	Initial release.
V2.0	2021/06/30	Overall optimization of format and content.
V2.1	2021/09/04	Added the description that the BMC Web GUI and some of the features may vary with different models.
V2.2	2021/09/20	Added 4 server models in Table 1-1 Product Model.
V2.3	2021/11/15	Added 2 server models in Table 1-1 Product Model.
V2.4	2022/01/18	Optimized some descriptions.
V2.5	2022/03/04	Unified the width of all tables.
V2.6	2022/06/06	Added 2 server models in Table 1-1 Product Model.
V2.7	2022/10/28	Optimized formats of some tables

Table of Contents

1 Overview

1.1 Purpose

This manual introduces the configuration process and methods of BMC-related functions in detail so that the technicians can have a better understanding on the specific operations.

1.2 Intended Audience

This manual is intended for:

- Technical support engineers
- Product maintenance engineers
- Server administrators

It is recommended that server installation, configuration, or maintenance is performed by only experienced technicians with knowledge in servers.

⚠ CAUTION

Some interfaces and commands for production, assembly and return-to-depot, and advanced commands for locating faults, if used improperly, may cause equipment abnormality or business interruption. This is not described herein. Please contact us for such information.

1.3 Scope

This manual applies to the following products:

Table 1-1 Product Model

Product model	**Two-socket Server**	**Four-socket Server**	**AI Server**	**Multi-node Server**
NF8260M6		●		
NF8480M6		●		
NF5280M6	●			
NF5180M6	●			
NF5270M6	●			

Product model	Two-socket Server	Four-socket Server	AI Server	Multi-node Server
NF5260M6	●			
NF5466M6	●			
NF5266M6	●			
NF5468M6	●		●	
NF5488M6	●		●	
NF5688M6	●		●	
i24M6	●			●
i48M6	●			●
SA5280M6	●			
SA5112M6	●			
SA5270M6	●			
SA5212M6	●			
SN5160FM6	●			
SN5264FM6	●			
i24LM6	●			●
NF5260FM6	●			

NOTE

The BMC Web GUI and some of the features may vary with different models.

2 Querying the IP Address of the Management Network Port

2.1 Function

You can access BMC via the dedicated/shared management network port. First you need to obtain the IP address of the BMC management network port by checking it on the BIOS Setup screen or via IPMItool in the Linux OS.

2.2 Obtaining the IP Address of the Management Network Port in BIOS

Scenario

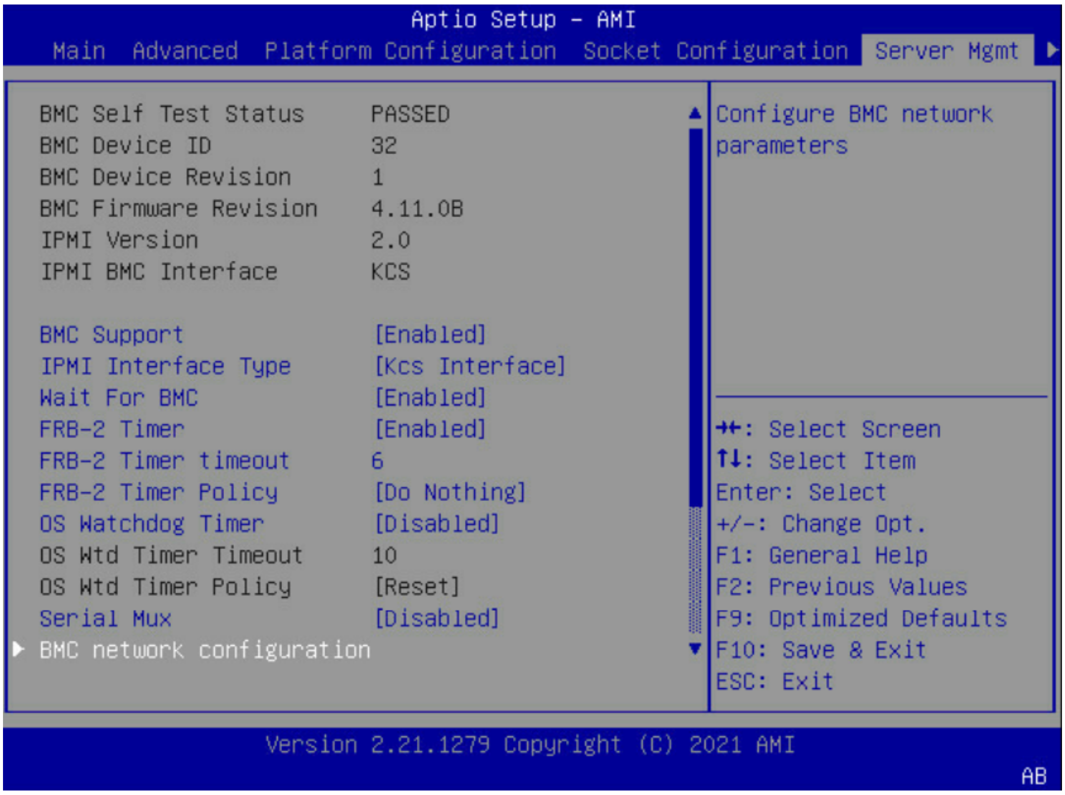
Obtain the IP address of the BMC management network port via BIOS.

Procedure

1. Enter the BIOS Setup screen. For details, see Section 16.2 Entering the BIOS Setup Screen.

2. Select the **Server Mgmt** tab, as shown below.

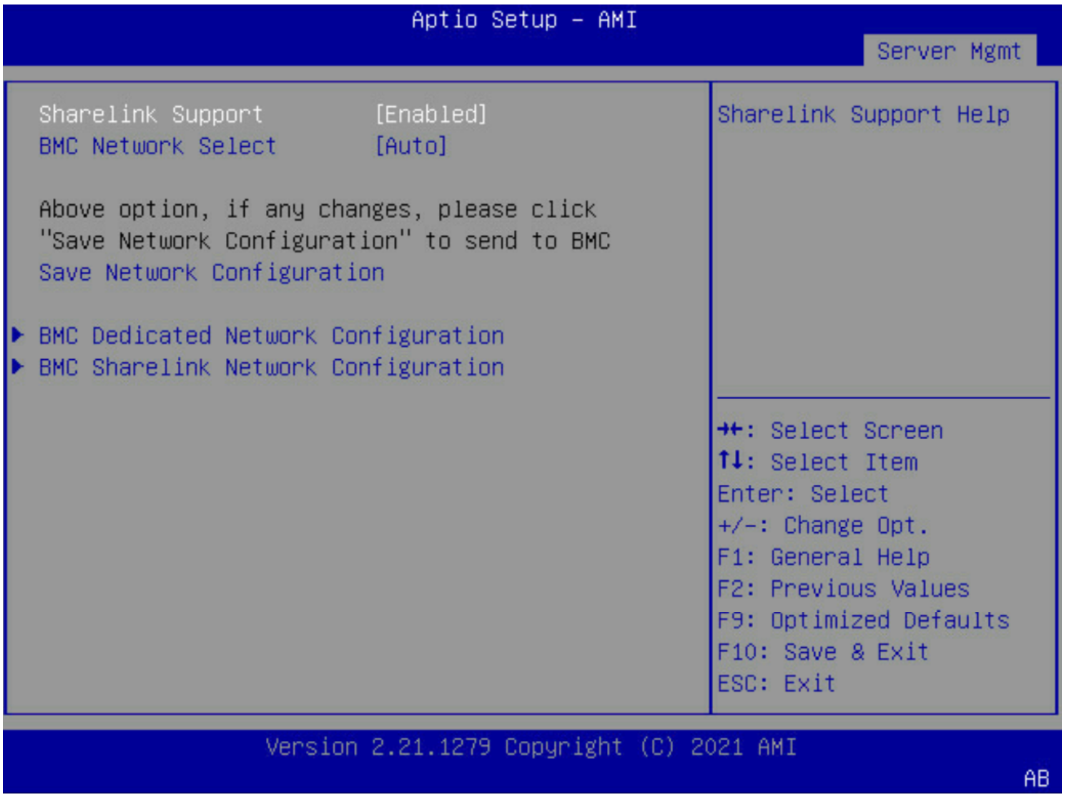
Figure 2-1 Server Mgmt Screen



```
                         Aptio Setup - AMI
   Main  Advanced  Platform Configuration  Socket Configuration  Server Mgmt  ▶

  BMC Self Test Status        PASSED                 ▲ Configure BMC network
  BMC Device ID               32                       parameters
  BMC Device Revision         1
  BMC Firmware Revision       4.11.0B
  IPMI Version                2.0
  IPMI BMC Interface          KCS

  BMC Support                 [Enabled]
  IPMI Interface Type         [Kcs Interface]
  Wait For BMC                [Enabled]
  FRB-2 Timer                 [Enabled]                →←: Select Screen
  FRB-2 Timer timeout         6                        ↑↓: Select Item
  FRB-2 Timer Policy          [Do Nothing]             Enter: Select
  OS Watchdog Timer           [Disabled]               +/-: Change Opt.
  OS Wtd Timer Timeout        10                       F1: General Help
  OS Wtd Timer Policy         [Reset]                  F2: Previous Values
  Serial Mux                  [Disabled]               F9: Optimized Defaults
▶ BMC network configuration                          ▼ F10: Save & Exit
                                                       ESC: Exit

              Version 2.21.1279 Copyright (C) 2021 AMI
                                                                           AB
```

3. Select **BMC network configuration** and press <Enter> to proceed, as shown below.

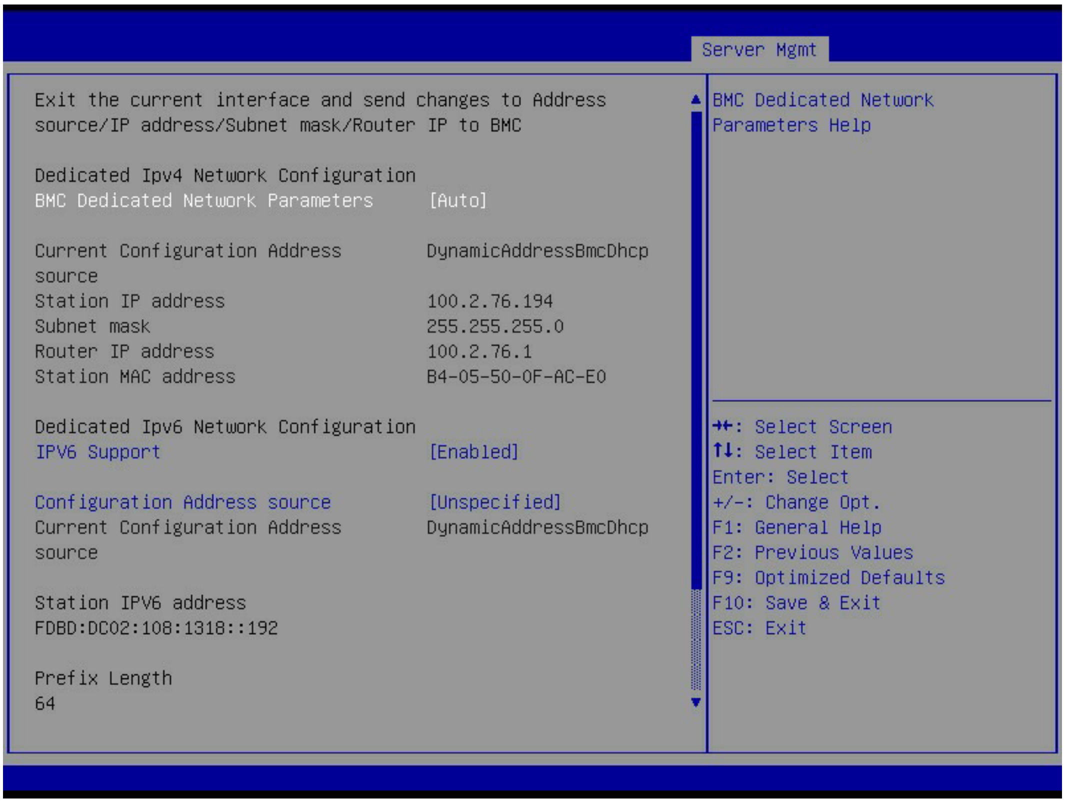
Figure 2-2 BMC Network Configuration Screen



```
                         Aptio Setup - AMI
                                                    Server Mgmt

 Sharelink Support          [Enabled]         Sharelink Support Help
 BMC Network Select         [Auto]

 Above option, if any changes, please click
 "Save Network Configuration" to send to BMC
 Save Network Configuration

▶ BMC Dedicated Network Configuration
▶ BMC Sharelink Network Configuration
                                              →←: Select Screen
                                              ↑↓: Select Item
                                              Enter: Select
                                              +/-: Change Opt.
                                              F1: General Help
                                              F2: Previous Values
                                              F9: Optimized Defaults
                                              F10: Save & Exit
                                              ESC: Exit

              Version 2.21.1279 Copyright (C) 2021 AMI
                                                               AB
```

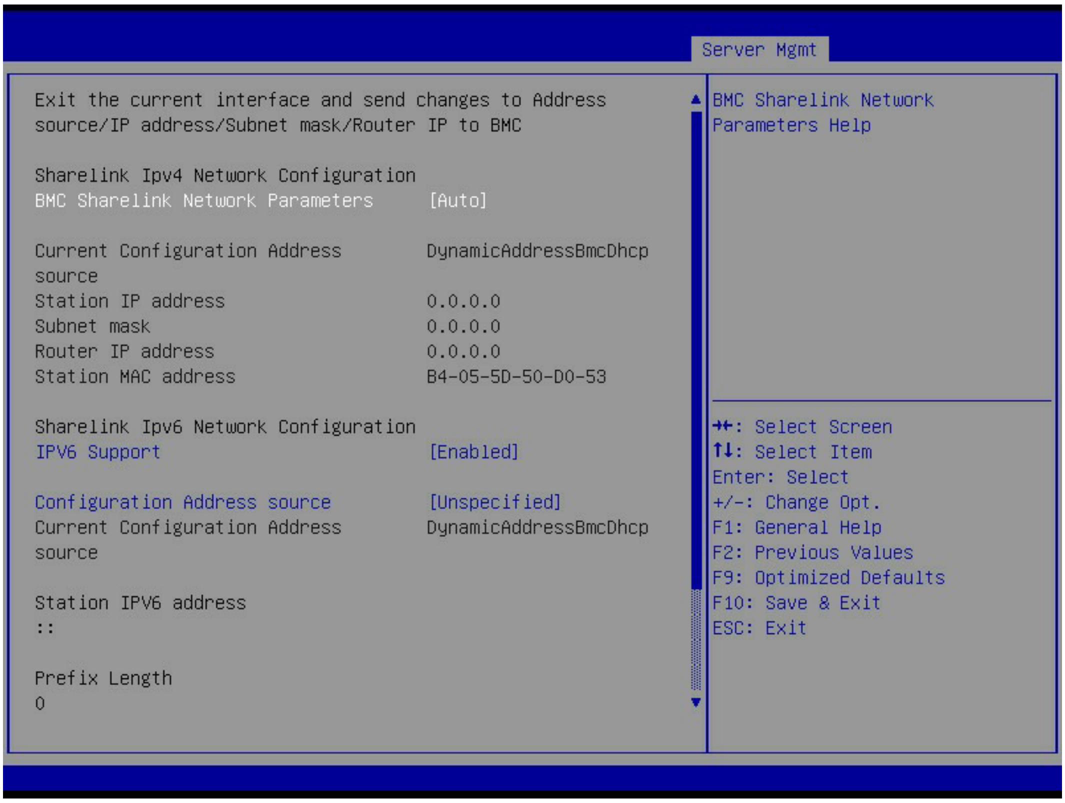
4. Select **BMC Dedicated Network Configuration** or **BMC Sharelink Network Configuration**, press <Enter> to view the current BMC Dedicated Network Parameters or BMC Sharelink Network Parameters, as shown below. You can find the IP address of the management network port from the following screens.

Figure 2-3 BMC Dedicated Network Configuration Screen



```
                                                                Server Mgmt

Exit the current interface and send changes to Address      BMC Dedicated Network
source/IP address/Subnet mask/Router IP to BMC              Parameters Help

Dedicated Ipv4 Network Configuration
BMC Dedicated Network Parameters     [Auto]

Current Configuration Address        DynamicAddressBmcDhcp
source
Station IP address                   100.2.76.194
Subnet mask                          255.255.255.0
Router IP address                    100.2.76.1
Station MAC address                  B4-05-50-0F-AC-E0

Dedicated Ipv6 Network Configuration                        →←: Select Screen
IPV6 Support                         [Enabled]              ↑↓: Select Item
                                                            Enter: Select
Configuration Address source         [Unspecified]          +/-: Change Opt.
Current Configuration Address        DynamicAddressBmcDhcp  F1: General Help
source                                                      F2: Previous Values
                                                            F9: Optimized Defaults
Station IPV6 address                                        F10: Save & Exit
FDBD:DC02:108:1318::192                                     ESC: Exit

Prefix Length
64
```

Figure 2-4 BMC Sharelink Network Configuration Screen



```
                                                                Server Mgmt

Exit the current interface and send changes to Address      BMC Sharelink Network
source/IP address/Subnet mask/Router IP to BMC              Parameters Help

Sharelink Ipv4 Network Configuration
BMC Sharelink Network Parameters     [Auto]

Current Configuration Address        DynamicAddressBmcDhcp
source
Station IP address                   0.0.0.0
Subnet mask                          0.0.0.0
Router IP address                    0.0.0.0
Station MAC address                  B4-05-5D-50-D0-53

Sharelink Ipv6 Network Configuration                        →←: Select Screen
IPV6 Support                         [Enabled]              ↑↓: Select Item
                                                            Enter: Select
Configuration Address source         [Unspecified]          +/-: Change Opt.
Current Configuration Address        DynamicAddressBmcDhcp  F1: General Help
source                                                      F2: Previous Values
                                                            F9: Optimized Defaults
Station IPV6 address                                        F10: Save & Exit
::                                                          ESC: Exit

Prefix Length
0
```

2.3 Obtaining the IP Address of the Management Network Port in Linux

Scenario

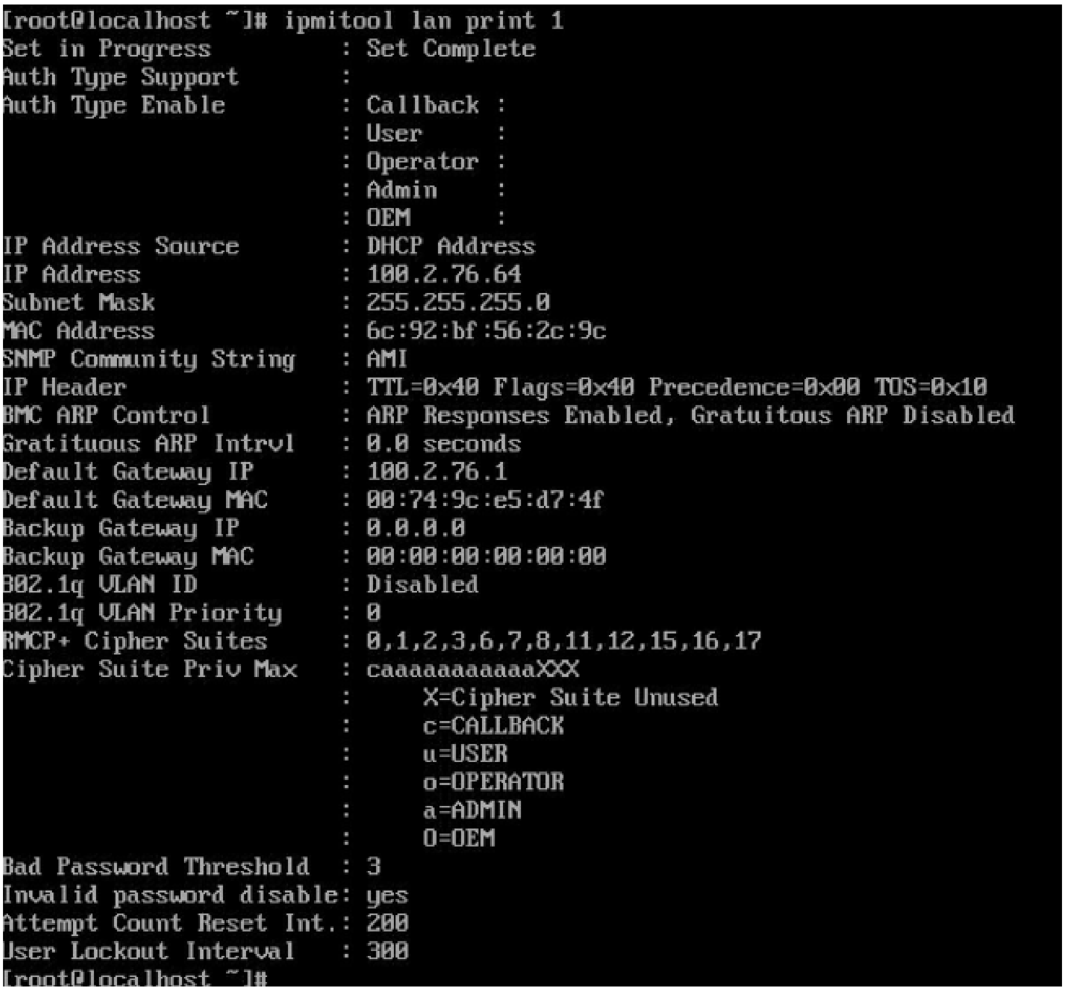
Obtain the IP address of the BMC management network port in Linux OS.

Procedure

1. Install the IPMItool. For details, see Section 18.1 Introduction to IPMItool.

2. Run the command **ipmitool lan print 1** to obtain the IP address of the dedicated management network port. Run the command **ipmitool lan print 8** to obtain the IP address of the shared management network port. The following figure shows a screenshot of the command to obtain the IP address of the dedicated management network port.

Figure 2-5 Obtaining the IP Address of BMC Dedicated Management Network Port



```
[root@localhost ~]# ipmitool lan print 1
Set in Progress         : Set Complete
Auth Type Support       :
Auth Type Enable        : Callback :
                        : User     :
                        : Operator :
                        : Admin    :
                        : OEM      :
IP Address Source       : DHCP Address
IP Address              : 100.2.76.64
Subnet Mask             : 255.255.255.0
MAC Address             : 6c:92:bf:56:2c:9c
SNMP Community String   : AMI
IP Header               : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10
BMC ARP Control         : ARP Responses Enabled, Gratuitous ARP Disabled
Gratituous ARP Intrvl   : 0.0 seconds
Default Gateway IP      : 100.2.76.1
Default Gateway MAC     : 00:74:9c:e5:d7:4f
Backup Gateway IP       : 0.0.0.0
Backup Gateway MAC      : 00:00:00:00:00:00
802.1q VLAN ID          : Disabled
802.1q VLAN Priority    : 0
RMCP+ Cipher Suites     : 0,1,2,3,6,7,8,11,12,15,16,17
Cipher Suite Priv Max   : caaaaaaaaaaaXXX
                        :     X=Cipher Suite Unused
                        :     c=CALLBACK
                        :     u=USER
                        :     o=OPERATOR
                        :     a=ADMIN
                        :     O=OEM
Bad Password Threshold  : 3
Invalid password disable: yes
Attempt Count Reset Int.: 200
User Lockout Interval   : 300
[root@localhost ~]#
```

3 User Management

3.1 Function

The user management function mainly displays the BMC user information, including user names, user groups, and user privileges, and allows you to perform operations such as adding/deleting users, and modifying information.

3.2 User Detail Management

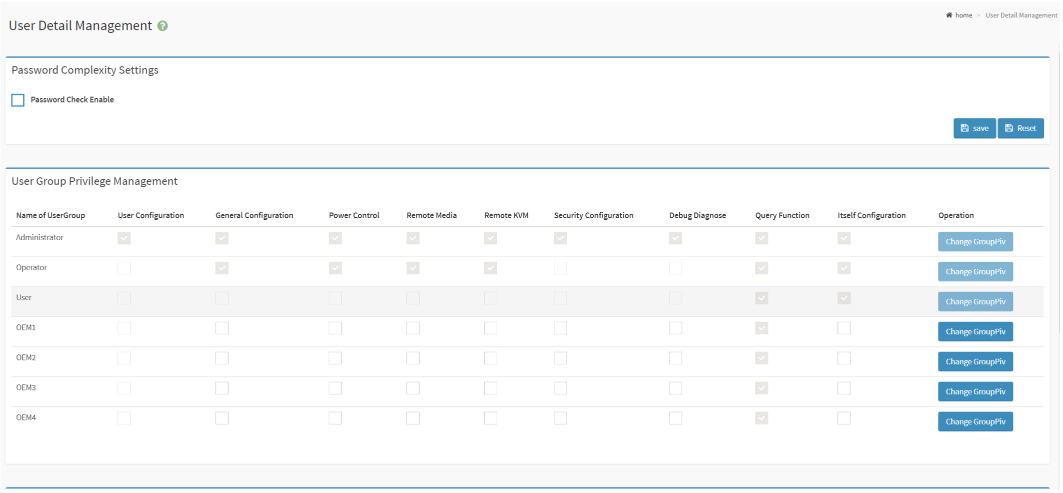
Scenario

Configure the settings related to user detail management through Web GUI.

Procedure

1. Log in to the Web GUI, and enter the **BMC Settings** > **User Detail Management** page, as shown below. The system supports detailed user management, allowing you to set privileges for different user groups.

Figure 3-1 User Detail Management



User Detail Management

Password Complexity Settings

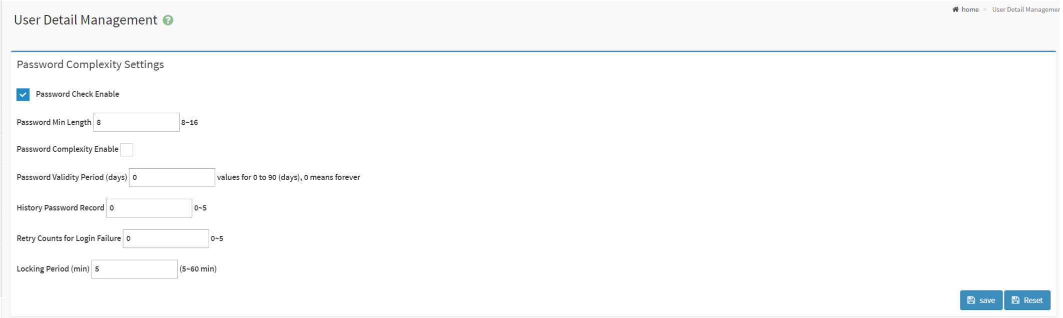
□ Password Check Enable

User Group Privilege Management

Name of UserGroup	User Configuration	General Configuration	Power Control	Remote Media	Remote KVM	Security Configuration	Debug Diagnose	Query Function	Itself Configuration	Operation
Administrator	☑	☑	☑	☑	☑	☑	☑	☑	☑	Change GroupPiv
Operator	□	☑	☑	☑	☑	□	□	☑	☑	Change GroupPiv
User	□	□	□	□	□	□	□	☑	☑	Change GroupPiv
OEM1	□	□	□	□	□	□	□	☑	□	Change GroupPiv
OEM2	□	□	□	□	□	□	□	☑	□	Change GroupPiv
OEM3	□	□	□	□	□	□	□	☑	□	Change GroupPiv
OEM4	□	□	□	□	□	□	□	☑	□	Change GroupPiv

2. To use a complex password, select the **Password Check Enable** check box, and then click the **Save** button. See Table 3-1 for the field description. After this check box is selected, the following page will be displayed.

Figure 3-2 Password Complexity Settings



User Detail Management

Password Complexity Settings

☑ Password Check Enable

Password Min Length 8 8~16

Password Complexity Enable □

Password Validity Period (days) 0 values for 0 to 90 (days), 0 means forever

History Password Record 0 0~5

Retry Counts for Login Failure 0 0~5

Locking Period (min) 5 (5~60 min)

3. User privileges for system default user groups **Administrator**, **Operator**, and **User** cannot be modified. While user privileges for other 4 customized user groups **OEM1**, **OEM2**, **OEM3**, and **OEM4** can be modified. Select required privileges, and click the **Change GroupPiv** button to allow the change to take effect. See Table 3-2 and Table 3-3 for user group privileges and their descriptions.

The following table shows the privilege configuration parameters on the **User Detail Management** page.

Table 3-1 Password Complexity Settings

Parameter	Description
Password Check Enable	• Checked: Password check enabled. • Unchecked: Password check disabled.
Password Min Length	It defaults to 8. An integer between 8 and 16 can be selected.
Password Complexity Enable	• Checked: To select the following components for a password: uppercase letters, lowercase letters, numbers, and special characters. For example, select **Uppercase Letters** if uppercase letters are required in a password. • Unchecked: The password complexity limit is disabled.
Password Validity Period (days)	You can set the validity period (days) of the password. After the validity period expires, users can no longer log in.
History Password Record	You can set to store a maximum of 5 most recently used passwords, which are prohibited from reuse. Value range: 0 - 5.

Parameter	Description
Retry Controls for Login Failure	You can set the maximum number of retries that a user is allowed to retry their password after login failure. The user will be locked out after a specified number of failed login attempts. Value range: 0 – 5.
Locking Period (min)	It defaults to 5. Value range: 5 – 60. You can only log in again after the locking period ends.

Table 3-2 User Group Privilege Management

User Group	Privilege
Administrator	User Configuration, General Configuration, Power Control, Remote Media, Remote KVM, Security Configuration, Debug Diagnose, Query Function, and Itself Configuration.
Operator	General Configuration, Power Control, Remote Media, Remote KVM, Query Function, and Itself Configuration.
User	Query Function and Itself Configuration.
OEM*	OEM1, OEM2, OEM3, and OEM4 are reserved user groups that have the Query Function and Itself Configuration privileges by default. You can also select other privileges to configure.

Table 3-3 User Group Privileges Description

Privilege	Description
User Configuration	User Group Management, User Management, Service Session, General LDAP Settings, and Role Groups.
General Configuration	DNS Configuration, Password Complexity Settings, IDL Clearing, System Event Log Clearing, Services Configuration, General Firewall Settings, IP Address Firewall Rules, Port Firewall Rules, Date & Time, PAM Sequence, Save Configuration, SEL Setting Policy, Syslog Settings, SNMP Trap Settings, SNMP Set/Get Settings, Mailbox Alarm, Sensor Threshold, HPM Firmware Update, Firmware Image Location, Restore Factory Defaults, Restore Configuration, Power Key Settings of Front Control Panel, Fan Management, Network Adaptive Configuration, Shared NIC Switch,

Privilege	Description
	Network Bond Configuration, Network IP Settings, and BIOS Boot Options.
Power Control	Controls the power supply.
Remote Media	KVM Mouse Settings, Local Image, Remote Image, General Settings, VMedia Instance Device Settings, Remote Session, VNC, and Active Redirections.
Remote KVM	H5Viewer and JViewer.
Security Configuration	Generate SSL Certificate, Upload SSL Certificate, System Administrator, and Audit Log.
Debug Diagnose	Downtime Screenshot, Manual Screenshot, Video Trigger Settings, Video Remote Storage, Pre-Event Video Recording, Module Restart, and One-Key Collection Log.
Query Function	You can log in and view information other than the security configuration.
Itself Configuration	You can configure your own password and email address, and manage the SSH public key.

3.3 Obtaining the User List

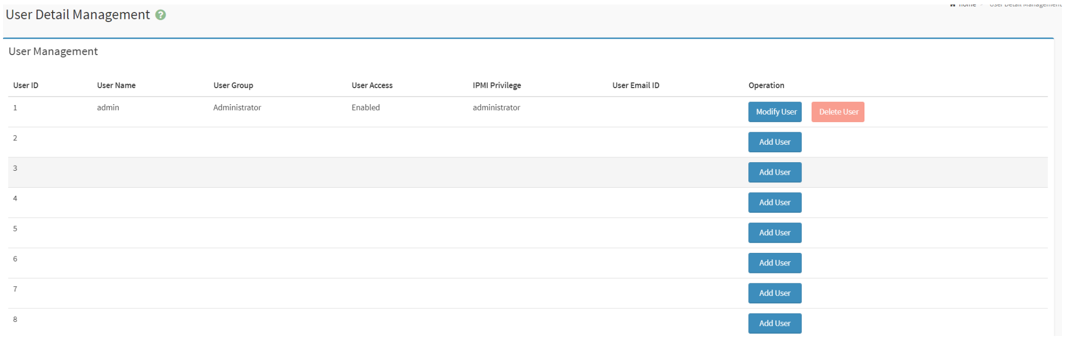
Scenario

Obtain the user list through Web GUI.

Procedure

1. Log in to the Web GUI, and enter the **BMC Settings** > **User Detail Management** page. Existing users will be displayed on the **User Detail Management** page, as shown below. For these users, you can click **Modify User** or **Delete User** in the **Operation** column. Click **Add User** in the **Operation** column on the right side of a blank line to add a user.

Figure 3-3 User List



Home > User Detail Management

User Detail Management

User Management

User ID	User Name	User Group	User Access	IPMI Privilege	User Email ID	Operation
1	admin	Administrator	Enabled	administrator		Modify User Delete User
2						Add User
3						Add User
4						Add User
5						Add User
6						Add User
7						Add User
8						Add User

3.4 Adding a User

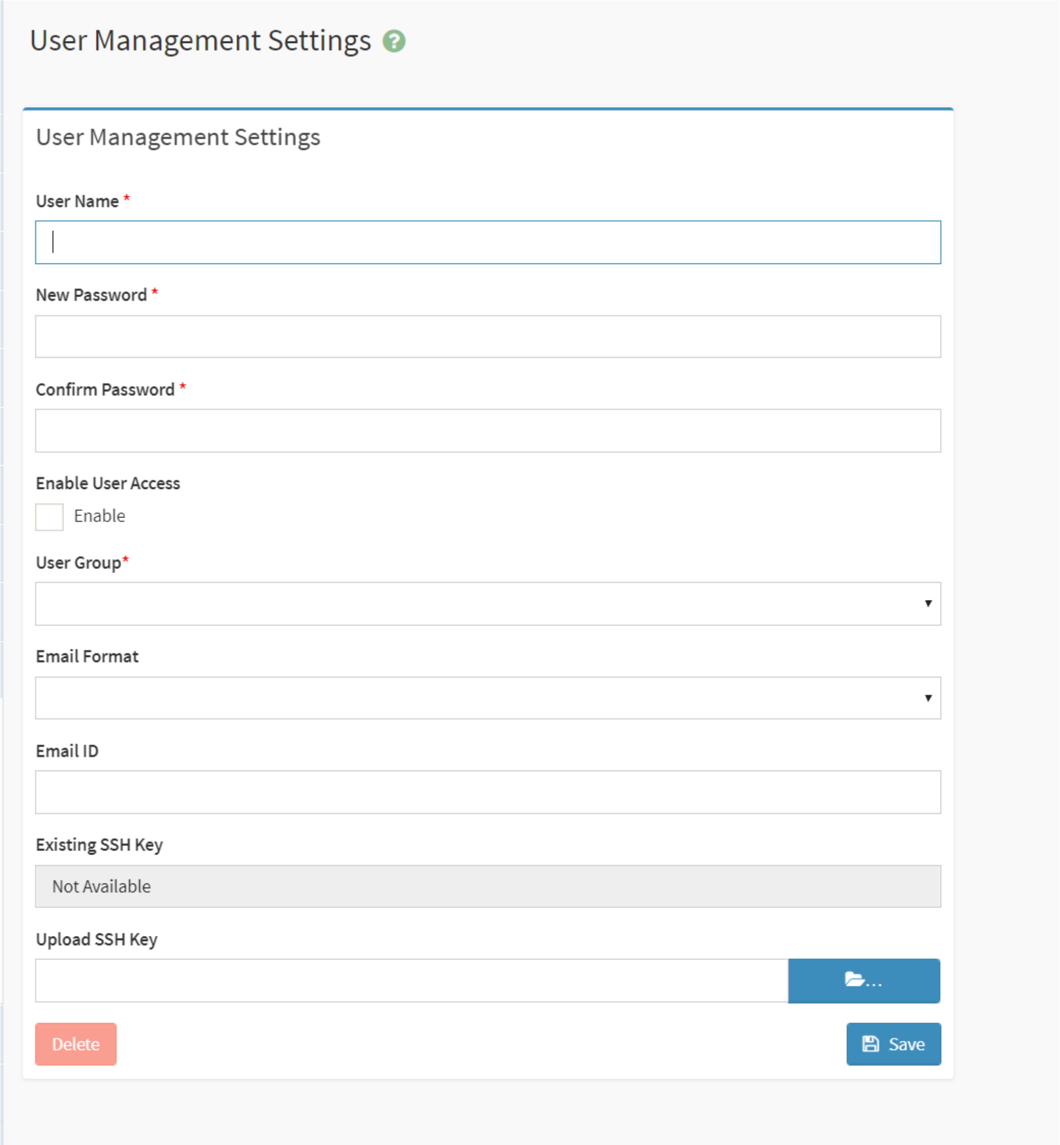
Scenario

Add a user through Web GUI.

Procedure

1. Click the **Add User** button on the right side of a blank line in the **User Detail Management** page to open the **User Management Settings** page, as shown below.

Figure 3-4 Add User Settings



User Management Settings

User Management Settings

User Name *

New Password *

Confirm Password *

Enable User Access

□ Enable

User Group*

Email Format

Email ID

Existing SSH Key

Not Available

Upload SSH Key

The following table shows the user configuration parameters.

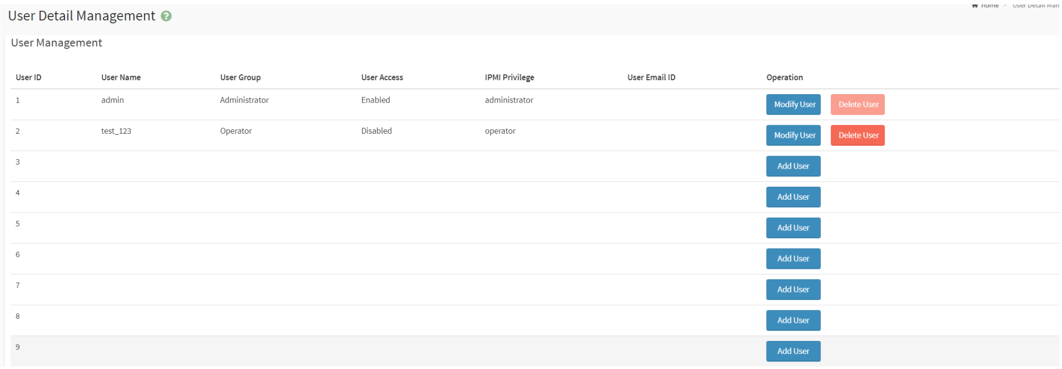
Table 3-4 User Configuration Parameters

Parameter	Description
User Name	Enter the name of the new user. - A user name is a string of 1 to 16 characters comprised of letters (case-sensitive), numbers, en dash (-), underline (_) and at (@). It must start with a letter. - The following special characters, such as comma (,), period (.), colon (:), semicolon (;), space, slash (/), backslash (\), left bracket ((), and right bracket ()), are not allowed.

Parameter	Description
	- **sshd**, **ntp**, **stunnel4**, **sysadmin**, and **daemon** are reserved user names and cannot be used.
New Password	Enter and confirm the new password. - When **Password Check Enable** is not selected, the password must contain at least 1 character and spaces are not allowed. - When **Password Check Enable** is selected, the password must be a string of at least 8 characters comprised of special characters, uppercase letters, lowercase letters, and numbers, and spaces are not allowed. Note: The password cannot exceed 16 characters.
Confirm Password	Enter the new password again.
Enable User Access	Select this option to enable user access.
User Group	Select a user group to assign privileges to users.
Email Format	Specify the format for the email. This format will be used, when sending emails. Two type of formats are available: • AMI-Format: The subject of this mail format is 'Alert from (your Hostname)'. The mail content includes sensor information, ex: Sensor type and description. • FixedSubject-Format: This format displays the specific subject and message configured for email alerts for the specified user.
Email ID	Enter the user's email ID. If the user forgets the password, the new password will be sent to this email ID. Note: You should configure an SMTP server to send emails.
Existing SSH Key	The uploaded SSH key information (read-only) is displayed.
Upload SSH Key	Use the Browse button to navigate to the SSH public key file. - The SSH key file should be a .pub file.

2. After filling in the information, click the **Save** button to return to the **User Management** page, where you can view the information of the added user, as shown below.

Figure 3-5 New User Information



User Detail Management

User Management

User ID	User Name	User Group	User Access	IPMI Privilege	User Email ID	Operation
1	admin	Administrator	Enabled	administrator		Modify User Delete User
2	test_123	Operator	Disabled	operator		Modify User Delete User
3						Add User
4						Add User
5						Add User
6						Add User
7						Add User
8						Add User
9						Add User

3.5 Modifying a User

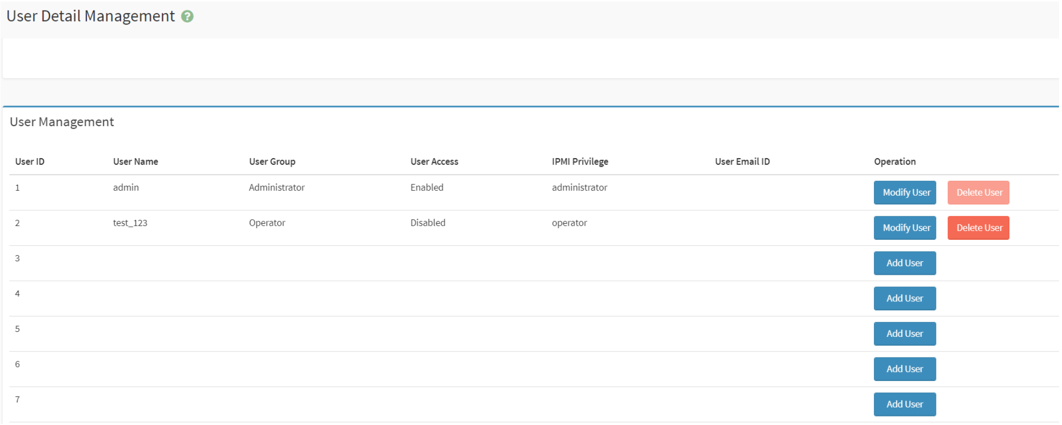
Scenario

Modify a user through Web GUI.

Procedure

1. On the **User Management** page, click the **Modify User** button on the right side of a user information line, as shown below.

Figure 3-6 Selecting the User Information to Be Modified



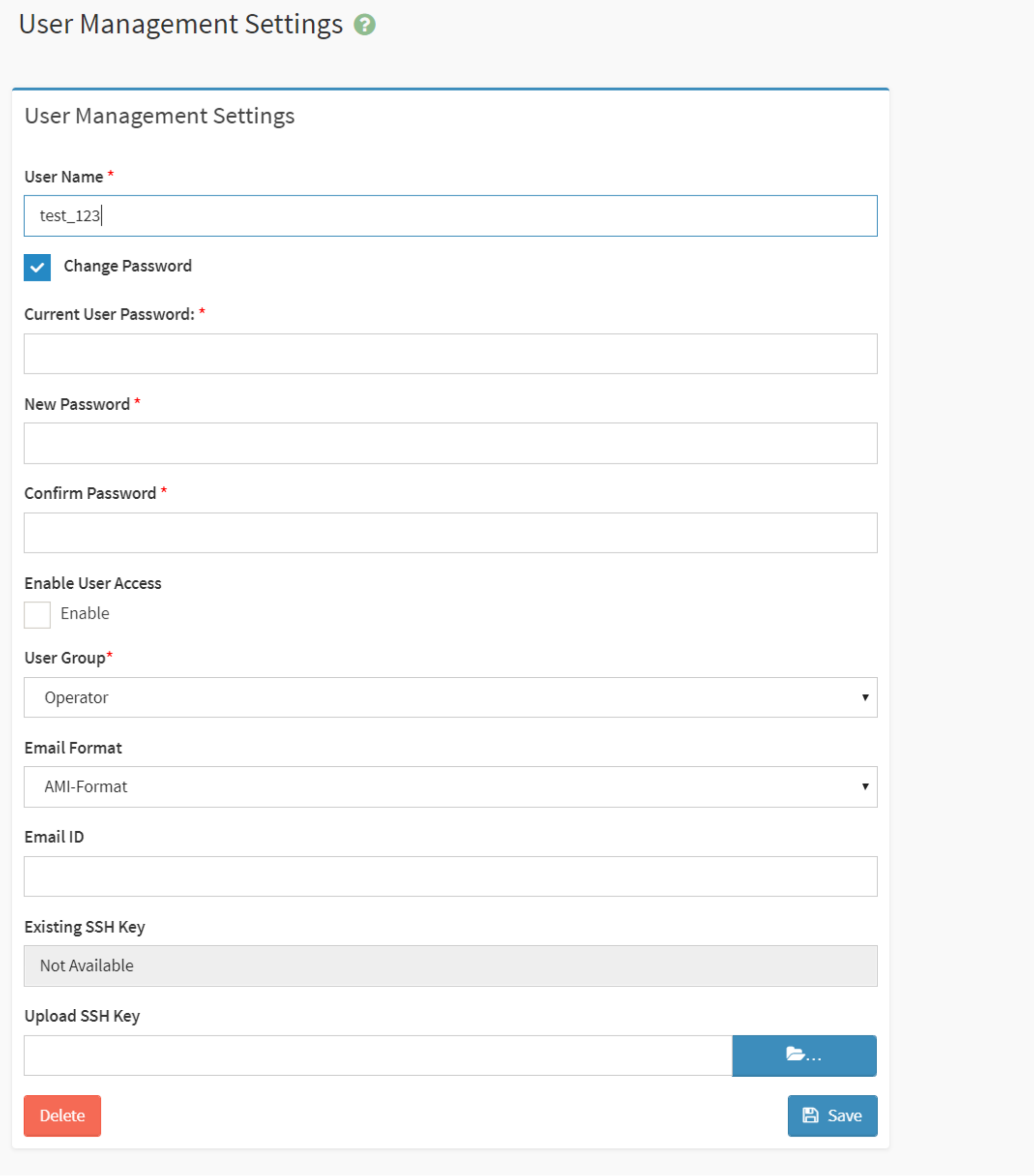
User Detail Management

User Management

User ID	User Name	User Group	User Access	IPMI Privilege	User Email ID	Operation
1	admin	Administrator	Enabled	administrator		Modify User Delete User
2	test_123	Operator	Disabled	operator		Modify User Delete User
3						Add User
4						Add User
5						Add User
6						Add User
7						Add User

2. On the **User Management Settings** page, you can modify the configuration information of the current user, and save the change by clicking the **Save** button, as shown below. Return to the **User Management** page to check whether the change takes effect.

Figure 3-7 Modifying User Information



User Management Settings

User Management Settings

User Name *

test_123

☑ Change Password

Current User Password: *

New Password *

Confirm Password *

Enable User Access

□ Enable

User Group*

Operator

Email Format

AMI-Format

Email ID

Existing SSH Key

Not Available

Upload SSH Key

3.6 Deleting a User

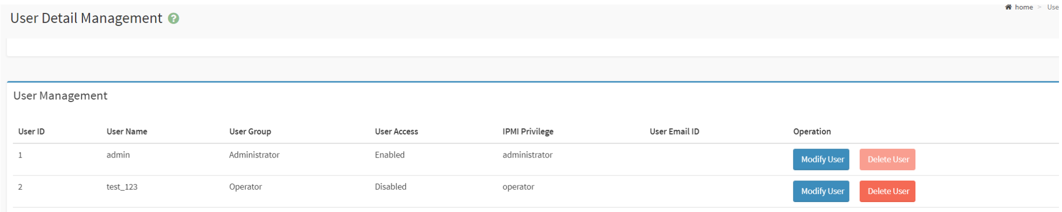
Scenario

Delete a user through Web GUI.

Procedure

1. On the **User Management** page, click the **Delete User** button on the right side of a user information line, as shown below.

Figure 3-8 Deleting a Specified User



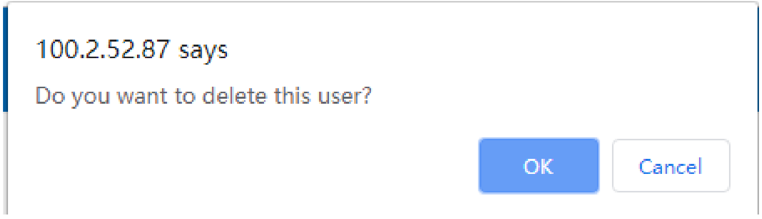
User Detail Management

User Management

User ID	User Name	User Group	User Access	IPMI Privilege	User Email ID	Operation
1	admin	Administrator	Enabled	administrator		Modify User Delete User
2	test_123	Operator	Disabled	operator		Modify User Delete User

2. After clicking the button, you will be prompted to confirm whether you want to delete this user. You can select **Cancel** to cancel the deletion, or select **OK** to confirm the deletion, as shown below.

Figure 3-9 Confirming User Deletion

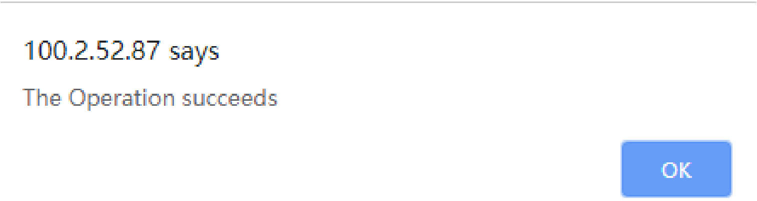


100.2.52.87 says

Do you want to delete this user?

3. After you click **OK**, a prompt that says **The Operation succeeds** pops up, as shown below. You can see that the user has been deleted from the user list.

Figure 3-10 Deletion Completed



100.2.52.87 says

The Operation succeeds

4 Network Settings

4.1 Function

The network settings module allows you to obtain the BMC network configuration, configure the BMC LAN interface and dynamic or static IPv4/IPv6 address, and set the VLAN.

4.2 Obtaining the Network Configuration

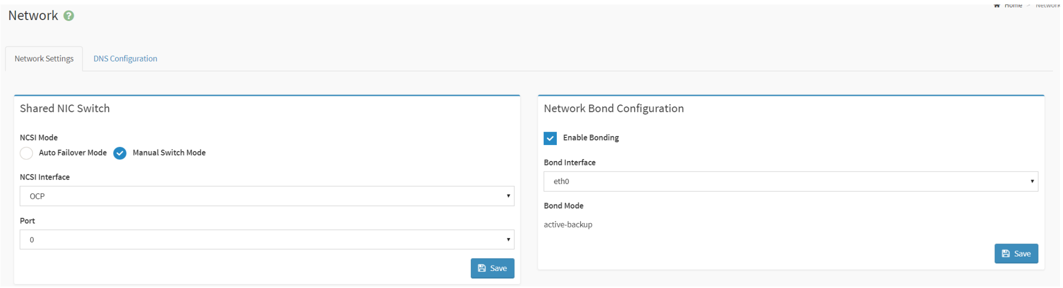
Scenario

Obtain the network configuration through Web GUI.

Procedure

1. Log in to the Web GUI, and enter the **BMC Setting**s > **Network** page. Click the **Network Settings** tab, on which you can configure the shared NIC, bind a network interface, and set the network IP address, as shown below.

Figure 4-1 Shared NIC Switch and Network Bond Configuration



Shared NIC Switch

NCSI Mode

○ Auto Failover Mode ● Manual Switch Mode

NCSI Interface: OCP

Port: 0

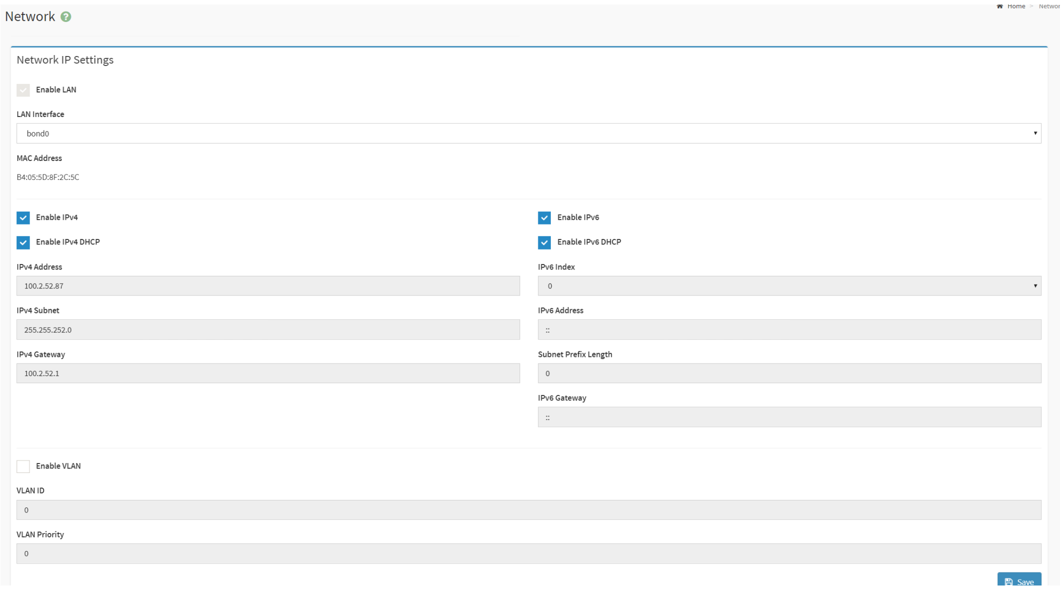
Network Bond Configuration

☑ Enable Bonding

Bond Interface: eth0

Bond Mode: active-backup

Figure 4-2 Network IP Settings



Network

Network IP Settings

☑ Enable LAN

LAN Interface: bond0 ▾

MAC Address: B4:05:5D:8F:2C:5C

☑ Enable IPv4

☑ Enable IPv4 DHCP

IPv4 Address: 100.2.52.87

IPv4 Subnet: 255.255.252.0

IPv4 Gateway: 100.2.52.1

☑ Enable IPv6

☑ Enable IPv6 DHCP

IPv6 Index: 0 ▾

IPv6 Address: ::

Subnet Prefix Length: 0

IPv6 Gateway: ::

□ Enable VLAN

VLAN ID: 0

VLAN Priority: 0

The following table shows the configuration parameters of the BMC network.

Table 4-1 Parameters of Network IP Settings

Parameter	Description
Enable LAN	Select this option to enable LAN support for the selected interface.
LAN Interface	Select the dedicated NIC and shared NIC. Options: bond0 and bond1.
MAC Address	This field displays the MAC address (read-only) of the selected interface.
IPv4 Configuration	
Enable IPv4	Select this option to enable IPv4 support for the selected interface.
Enable IPv4 DHCP	Select this option to configure a dynamic IPv4 address via DHCP.
IPv4 Address	If DHCP is disabled, the user need to specify a static IPv4 address, subnet mask, and default gateway for the selected interface. - The IP address contains 4 sets of digits xxx.xxx.xxx.xxx separated by periods. - Each set ranges from 0 to 255. - The first set cannot be 0.
IPv4 Subnet	To specify the default IPv4 subnet mask.
IPv4 Gateway	To specify the default IPv4 gateway.
IPv6 Configuration	

Parameter	Description
Enable IPv6	Select this option to enable IPv6 support for the selected interface.
Enable IPv6 DHCP	Select this option to configure a dynamic IPv6 address via DHCP.
IPv6 Index	Select an IPv6 index.
IPv6 Address	To specify a static IPv6 address for the selected interface.
Subnet Prefix Length	To set the IPv6 subnet prefix length.
IPv6 Gateway	To set the default IPv6 gateway. - Value range: 0 - 128.
VLAN Configuration	
Enable VLAN	Select this option to enable VLAN support for the selected interface.
VLAN ID	To set the VLAN ID. - Value range: 1 - 4094. Note: In case of VLAN change, you must restart the system.
VLAN Priority	To set the VLAN priority. - Value range: 0 - 7. Note: 7 indicates the highest priority.

4.3 Shared NIC Configuration

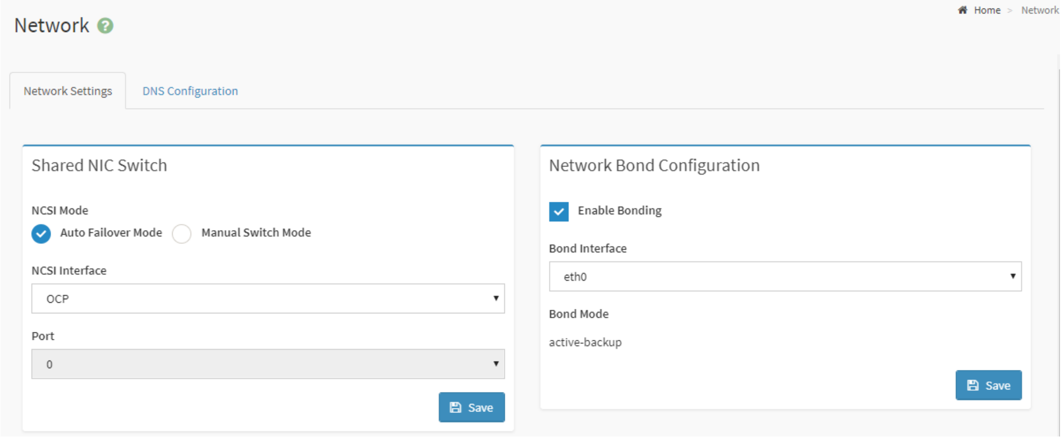
Scenario

Configure the shared NIC through Web GUI.

Procedure

1. Log in to the Web GUI, and enter the **BMC Settings** > **Network** page. Click the **Network Settings** tab, on which you can configure the shared NIC, as shown below.

Figure 4-3 Shared NIC Switch and Network Bond Configuration



Shared NIC Switch

NCSI Mode
● Auto Failover Mode ○ Manual Switch Mode

NCSI Interface
OCP

Port
0

Network Bond Configuration

☑ Enable Bonding

Bond Interface
eth0

Bond Mode
active-backup

2. Select the **NCSI Mode** and **NCSI Interface**. If **Manual Switch Mode** is selected, you need to select a port. Click the **Save** button.

The following table shows the configuration parameters of the BMC shared NIC.

Table 4-2 Shared NIC Switch

Parameter	Description
NCSI Mode	• Auto Failover Mode. • Manual Switch mode.
NCSI Interface	Choose the interface name for which to configure NCSI settings. Options: OCP and PCIE.
Port	Choose the port to be configured for the selected interface. Options: 0, 1, 2, and 3.

Table 4-3 Network Bond Configuration

Parameter	Description
Enable Bonding	Check this option to enable bonding for the network interfaces. Note: If VLAN is enabled for either slave interface, then bonding cannot be enabled (VLAN can be disabled, under this page).
Bond Interface	This option is used to configure bonding for the network interfaces. This is enabled by default. Note: A minimum of 2 network interfaces is required to enable network bonding for the device. **eth0** is the dedicated NIC and **eth1** is the shared NIC.

Parameter	Description
Bond Mode	This field displays the network bonding mode in effect. Note: This field is not configurable. The MAC address of **eth0** is used after network bonding.

4.4 Network IP Settings

Scenario

Configure an IP address through Web GUI.

Procedure

1. Log in to the Web GUI, enter the **BMC Settings** > **Network** page, and click the **Network Settings** tab.

2. Select **LAN Interface**, and select the network interface to be configured.

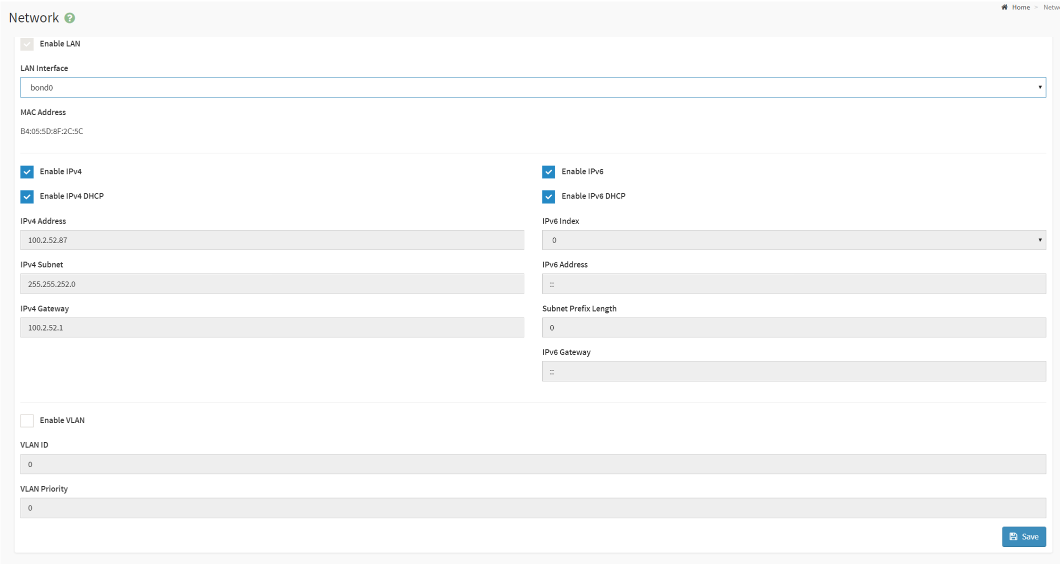
3. Check or uncheck **Enable LAN** to confirm whether to enable the interface.

4. Check or uncheck **Enable IPv4** and **Enable IPv6** to confirm whether to enable IPv4 and IPv6.

5. If **Enable IPv4** is selected, then check or uncheck **Enable IPv4 DHCP**. If **Enable IPv4 DHCP** is not selected, manually configure IPv4 related settings, including address, subnet mask, and default gateway.

6. If **Enable IPv6** is selected, then check or uncheck **Enable IPv6 DHCP**. If **Enable IPv6 DHCP** is not selected, manually configure IPv6 related settings, including index, address, subnet mask length, and default gateway.

Figure 4-4 IP Settings



Network

☑ Enable LAN

LAN Interface

bond0

MAC Address

B4:05:5D:8F:2C:5C

☑ Enable IPv4

☑ Enable IPv4 DHCP

IPv4 Address

100.2.52.87

IPv4 Subnet

255.255.252.0

IPv4 Gateway

100.2.52.1

☑ Enable IPv6

☑ Enable IPv6 DHCP

IPv6 Index

0

IPv6 Address

::

Subnet Prefix Length

0

IPv6 Gateway

::

□ Enable VLAN

VLAN ID

0

VLAN Priority

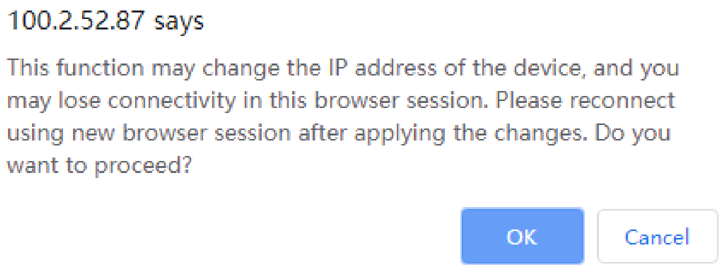
0

7. Click the **Save** button to save settings, and the following prompt box will pop up.

NOTE

After the IP address changes, you need to use the new IP address to access BMC.

Figure 4-5 IP Settings Prompt



100.2.52.87 says

This function may change the IP address of the device, and you may lose connectivity in this browser session. Please reconnect using new browser session after applying the changes. Do you want to proceed?

4.5 VLAN Settings

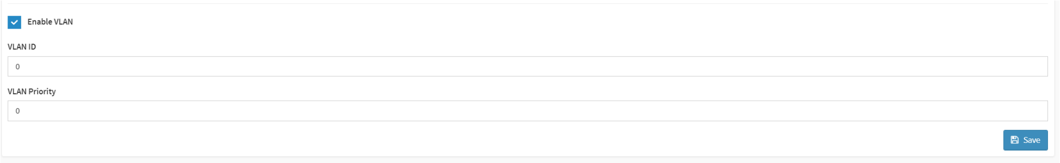
Scenario

Configure the VLAN through Web GUI.

Procedure

1. Log in to the Web GUI, enter the **BMC Settings** > **Network** page, and click the **Network Settings** tab. Select **Enable VLAN**, and enter **VLAN ID** and **VLAN Priority**, as shown below. Then click the **Save** button.

Figure 4-6 VLAN Settings



☑ Enable VLAN

VLAN ID

0

VLAN Priority

0

4.6 DNS Configuration

Scenario

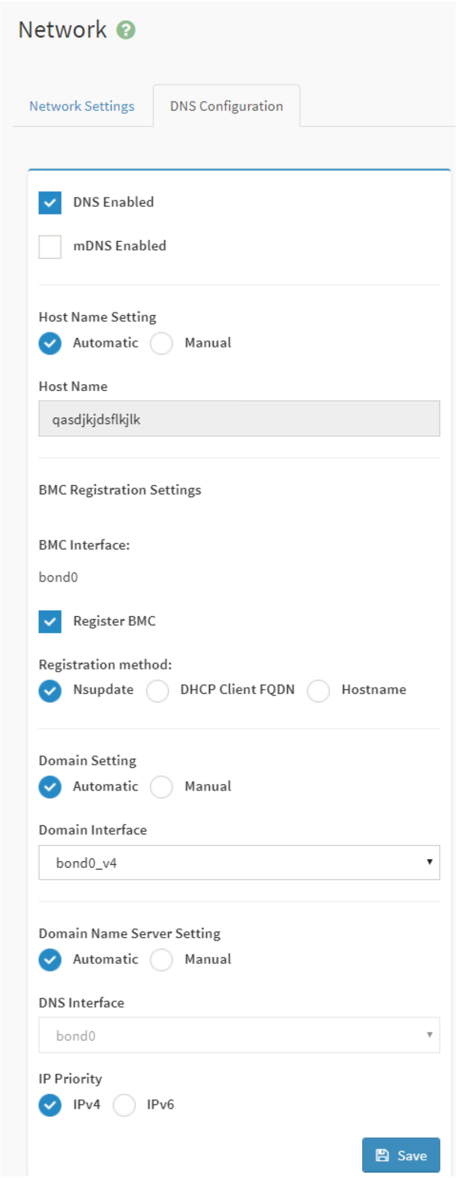
Configure the DNS through Web GUI.

Procedure

1. Log in to the Web GUI, and enter the **BMC Settings** > **Network** page. Click the **DNS Configuration** tab, on which you can configure the host, domain name, and domain name server.

2. You can enable or disable the DNS function by checking or unchecking the **DNS Enabled** option. The page also provides configuration options such as **Host Name Setting**, **BMC Registration Settings**, **Domain Setting**, **Domain Name Server Setting**, and **IP Priority**. Users can manually configure parameters or use automatic mode to allow BMC to automatically configure relevant parameters.

Figure 4-7 DNS Configuration



Network

Network Settings | DNS Configuration

☑ DNS Enabled

□ mDNS Enabled

Host Name Setting

● Automatic ○ Manual

Host Name

qasdjkjdsflkjlk

BMC Registration Settings

BMC Interface:

bond0

☑ Register BMC

Registration method:

● Nsupdate ○ DHCP Client FQDN ○ Hostname

Domain Setting

● Automatic ○ Manual

Domain Interface

bond0_v4

Domain Name Server Setting

● Automatic ○ Manual

DNS Interface

bond0

IP Priority

● IPv4 ○ IPv6

3. Then, click the **Save** button to save the settings.

The following table shows the DNS configuration parameters.

Table 4-4 DNS Configuration Parameters

Parameter	Description
DNS Settings	
DNS Enabled	• Checked: All DNS services enabled. • Unchecked: DNS services disabled.

Parameter	Description
mDNS Enabled	• Checked: All mDNS services enabled. • Unchecked: mDNS services disabled.
Host Settings	
Host Name Setting	Options: Automatic and Manual.
Host Name	Displays the host name. If **Manual** is selected for **Host Name Setting**, you need to specify the server name. For IPv6 servers, only names that start with a letter can be displayed.
BMC Registration Settings	
BMC Interface	bond0.
Register BMC	• Checked: To register BMC. • Unchecked: Not to register BMC.
Registration method	Options: **Nsupdate**, **DHCP Client FQDN**, and **Hostname** **Nsupdate**: Use the Nsupdate application to register BMC with the DNS server. **DHCP Client FQDN**: Use the DHCP option 81 to register BMC with the DNS server. **Hostname**: Use the DHCP option 12 to register BMC with the DNS server.
Domain Setting	Options: Automatic and Manual.
Domain Interface	Options: bond0_v4 and bond1_v4.
Domain Name Server Setting	Options: Automatic and Manual.
DNS Interface	Displays bond0 or bond1.
IP Priority	Options: IPv4 and IPv6.

5 Fan Management

5.1 Function

The fan control module is mainly used to control the fan speed manually or automatically. The setting takes effect immediately.

5.2 Auto Fan Configuration

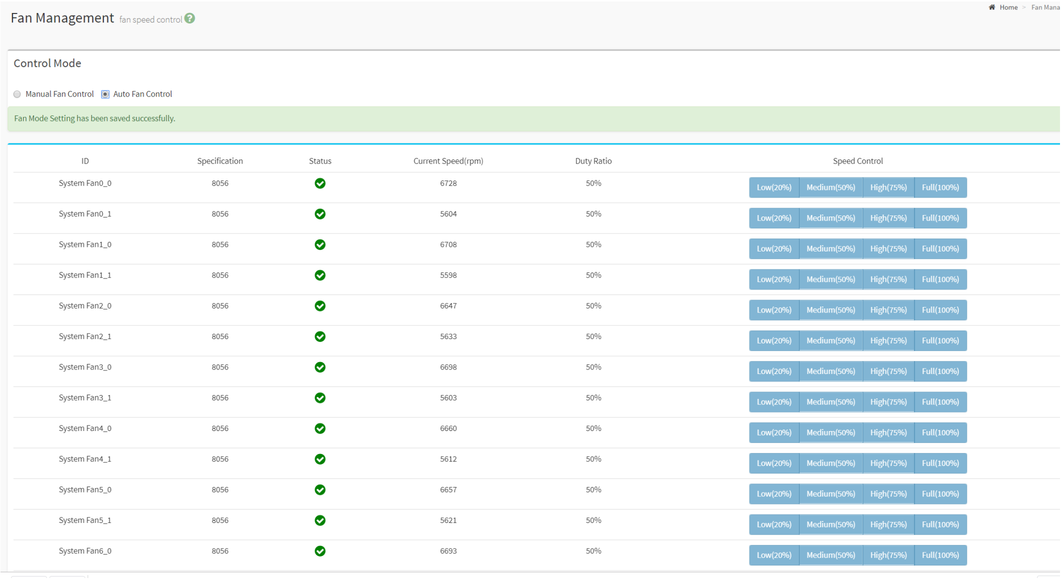
Scenario

Set the fan control mode to auto through Web GUI.

Procedure

1. Log in to the Web GUI, and enter the **Fan Management** page, on which you can set the fan control mode and control the fan speed. Click **Auto Fan Control** at the upper left of the page, as shown below.

Figure 5-1 Auto Fan Control



Fan Management fan speed control

Control Mode

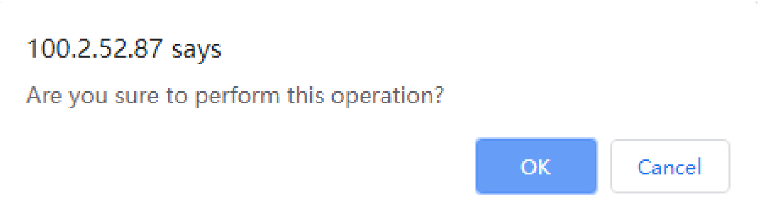
○ Manual Fan Control ● Auto Fan Control

Fan Mode Setting has been saved successfully.

ID	Specification	Status	Current Speed(rpm)	Duty Ratio	Speed Control
System Fan0_0	8056	✓	6728	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan0_1	8056	✓	5604	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan1_0	8056	✓	6708	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan1_1	8056	✓	5598	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan2_0	8056	✓	6647	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan2_1	8056	✓	5633	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan3_0	8056	✓	6698	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan3_1	8056	✓	5603	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan4_0	8056	✓	6660	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan4_1	8056	✓	5612	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan5_0	8056	✓	6657	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan5_1	8056	✓	5621	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan6_0	8056	✓	6693	50%	Low(20%) Medium(50%) High(75%) Full(100%)

2. After **Auto Fan Control** is selected, the following prompt box pops up, and click **OK** to complete the setting.

Figure 5-2 Auto Fan Control Confirmation



100.2.52.87 says

Are you sure to perform this operation?

5.3 Manual Fan Configuration

Scenario

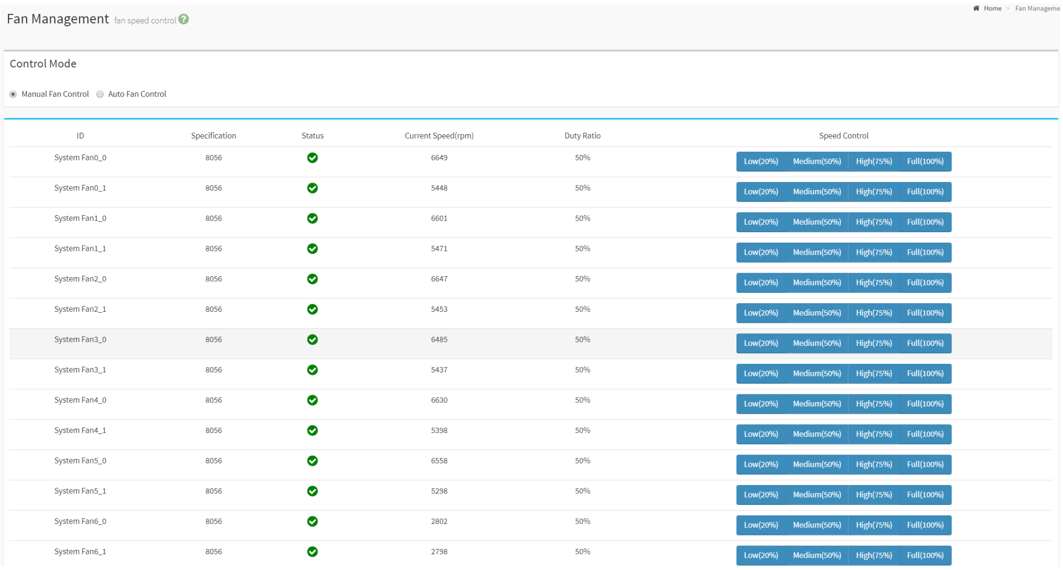
Set the fan control mode to manual through Web GUI.

Procedure

1. Log in to the Web GUI, and enter the **Fan Management** page, on which you can set the fan control mode and control the fan speed. Click **Manual Fan Control** at the upper left of the page to switch to manual fan control.

2. Locate the ID of the fan which requires manual configuration, and click the speed option (**Low**, **Medium**, **High**, and **Full**) to manually set the fan speed. For example, set the Fan0 speed to Medium (50%), as shown below.

Figure 5-3 Manual Fan Control



Fan Management fan speed control

Control Mode

● Manual Fan Control ○ Auto Fan Control

ID	Specification	Status	Current Speed(rpm)	Duty Ratio	Speed Control
System Fan0_0	8056	✓	6649	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan0_1	8056	✓	5448	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan1_0	8056	✓	6601	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan1_1	8056	✓	5471	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan2_0	8056	✓	6647	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan2_1	8056	✓	5453	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan3_0	8056	✓	6485	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan3_1	8056	✓	5437	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan4_0	8056	✓	6630	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan4_1	8056	✓	5398	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan5_0	8056	✓	6558	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan5_1	8056	✓	5298	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan6_0	8056	✓	2802	50%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan6_1	8056	✓	2798	50%	Low(20%) Medium(50%) High(75%) Full(100%)

6 Log Collection

6.1 Function

The log module mainly supports system event log, audit log, IDL log, and one-key log collection. Log information can be displayed on the page. Logs can be filtered by date and log level. You can also download and clear logs.

6.2 Operation Guide

Refer to the BMC log collection and analysis guide.

6.3 Syslog Settings

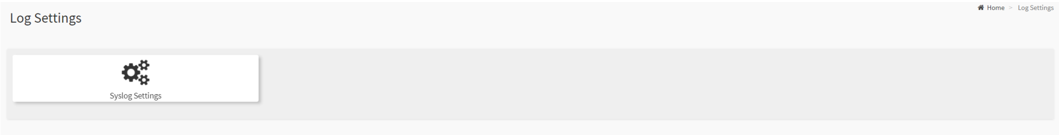
Scenario

Configure the syslog settings through Web GUI.

Procedure

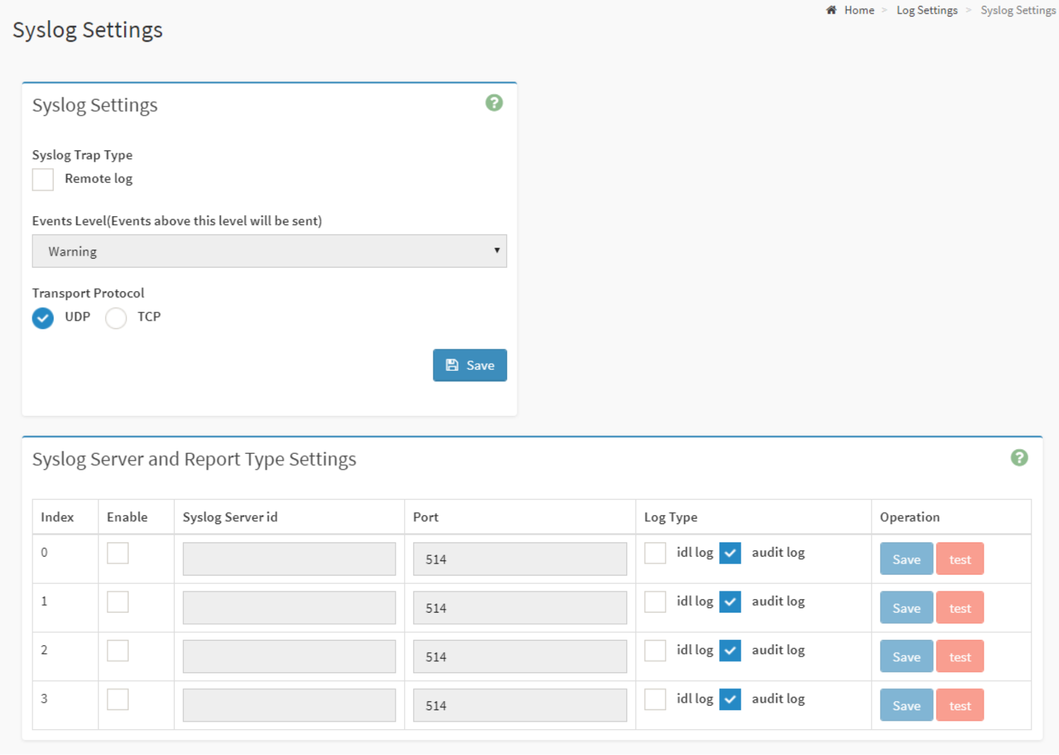
1. Log in to the Web GUI, and enter the **Logs & Alarms** > **Log Settings** page.

Figure 6-1 Log Settings



2. Click **Syslog Settings** to set syslog trap type, events level, transport protocol, syslog server and report type, as shown below. You can enable either **idl log** or **audit log**, and then select the record type as **Local log** or **Remote log**. When **Remote log** is selected, you need to enter the server id, port, and protocol type.

Figure 6-2 Syslog Settings



Home > Log Settings > Syslog Settings

Syslog Settings

Syslog Settings

Syslog Trap Type

□ Remote log

Events Level(Events above this level will be sent)

Warning ▾

Transport Protocol

● UDP ○ TCP

Save

Syslog Server and Report Type Settings

Index	Enable	Syslog Server id	Port	Log Type	Operation
0	□		514	□ idl log ☑ audit log	Save test
1	□		514	□ idl log ☑ audit log	Save test
2	□		514	□ idl log ☑ audit log	Save test
3	□		514	□ idl log ☑ audit log	Save test

Table 6-1 Syslog Settings

Parameter	Description
Syslog Trap Type	The location to store syslog alarm logs. Option: Remote log
Events Level	Events above this level will be sent. Options: • Warning • Info • Critical
Transport Protocol	Options: • UDP • TCP

Table 6-2 Syslog Server and Report Type Settings

Parameter	Description
Index	Index.
Enable	To enable or disable.
Syslog Server id	The address of the syslog server.
Port	The port number of the syslog server.
Log Type	Options: **idl log** and **audit log.** Select either or both.
Operation	**Save**: To save the syslog server information. **Test**: To test whether the syslog messages can be sent successfully.

7 BMC Time Settings

7.1 Function

The BMC time setting module is used to configure the BMC time. You can configure the NTP server, synchronization cycle, and other parameters to enable BMC to automatically synchronize the time of the NTP server.

7.2 Auto Sync with NTP

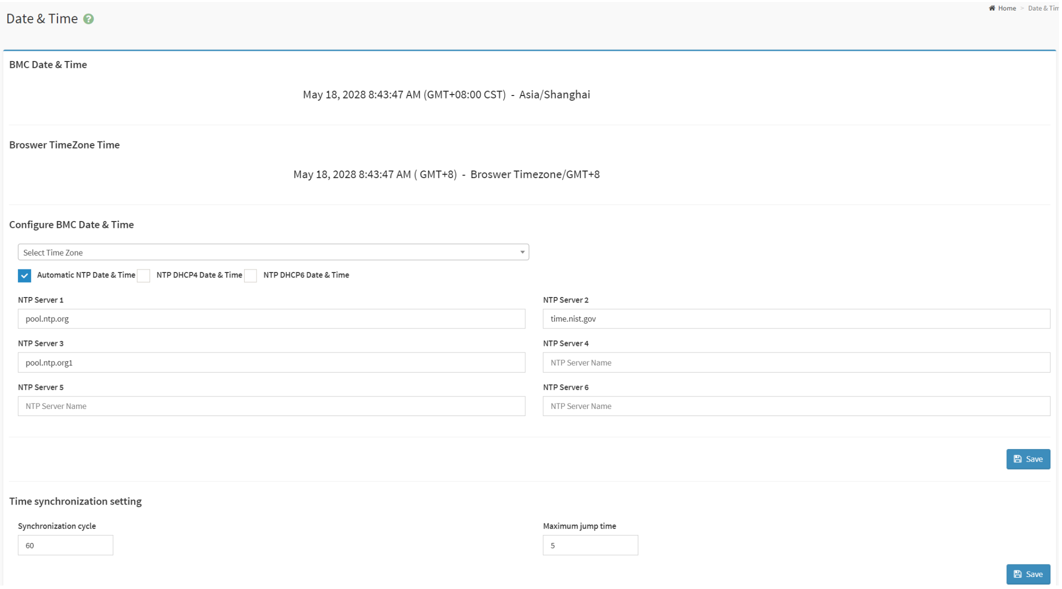
Scenario

Automatically synchronize time with the NTP server through Web GUI.

Procedure

1. Log in to the Web GUI, and enter the **BMC Settings** > **Date & Time** page, which displays the current BMC time and NTP settings, as shown below.

Figure 7-1 NTP Auto Sync Settings Page



Date & Time

BMC Date & Time

May 18, 2028 8:43:47 AM (GMT+08:00 CST) - Asia/Shanghai

Broswer TimeZone Time

May 18, 2028 8:43:47 AM (GMT+8) - Broswer Timezone/GMT+8

Configure BMC Date & Time

Select Time Zone

☑ Automatic NTP Date & Time □ NTP DHCP4 Date & Time □ NTP DHCP6 Date & Time

NTP Server 1: pool.ntp.org

NTP Server 2: time.nist.gov

NTP Server 3: pool.ntp.org1

NTP Server 4: NTP Server Name

NTP Server 5: NTP Server Name

NTP Server 6: NTP Server Name

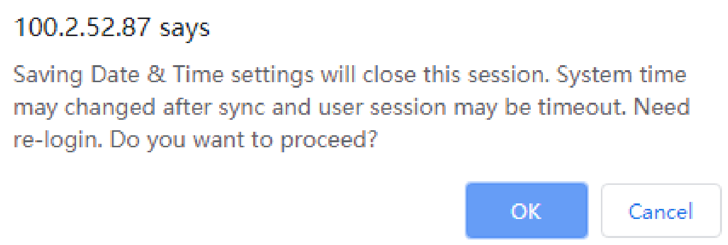
Time synchronization setting

Synchronization cycle: 60

Maximum jump time: 5

2. On the page, select **Auto NTP Date & Time**, **NTP DHCP 4 Date & Time**, or **NTP DHCP 6 Date & Time**, and set the **NTP Server** as well as the **Synchronization cycle** and **Maximum jump time** to enable auto sync with NTP. Then click the **Save** button to save the settings.

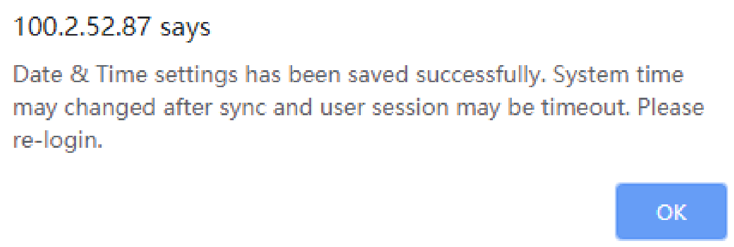
Figure 7-2 NTP Configuration Confirmation



100.2.52.87 says

Saving Date & Time settings will close this session. System time may changed after sync and user session may be timeout. Need re-login. Do you want to proceed?

Figure 7-3 NTP Configuration Success



100.2.52.87 says

Date & Time settings has been saved successfully. System time may changed after sync and user session may be timeout. Please re-login.

8 SNMP Trap Settings

8.1 Function

The SNMP trap settings module is used to configure the SNMP Trap parameters for sending event logs, and allows you to filter event logs to be sent by event severity and device type. You can specify the destination IP and port to receive the event logs on the **Alert Policies Settings** page.

8.2 SNMP Trap Settings

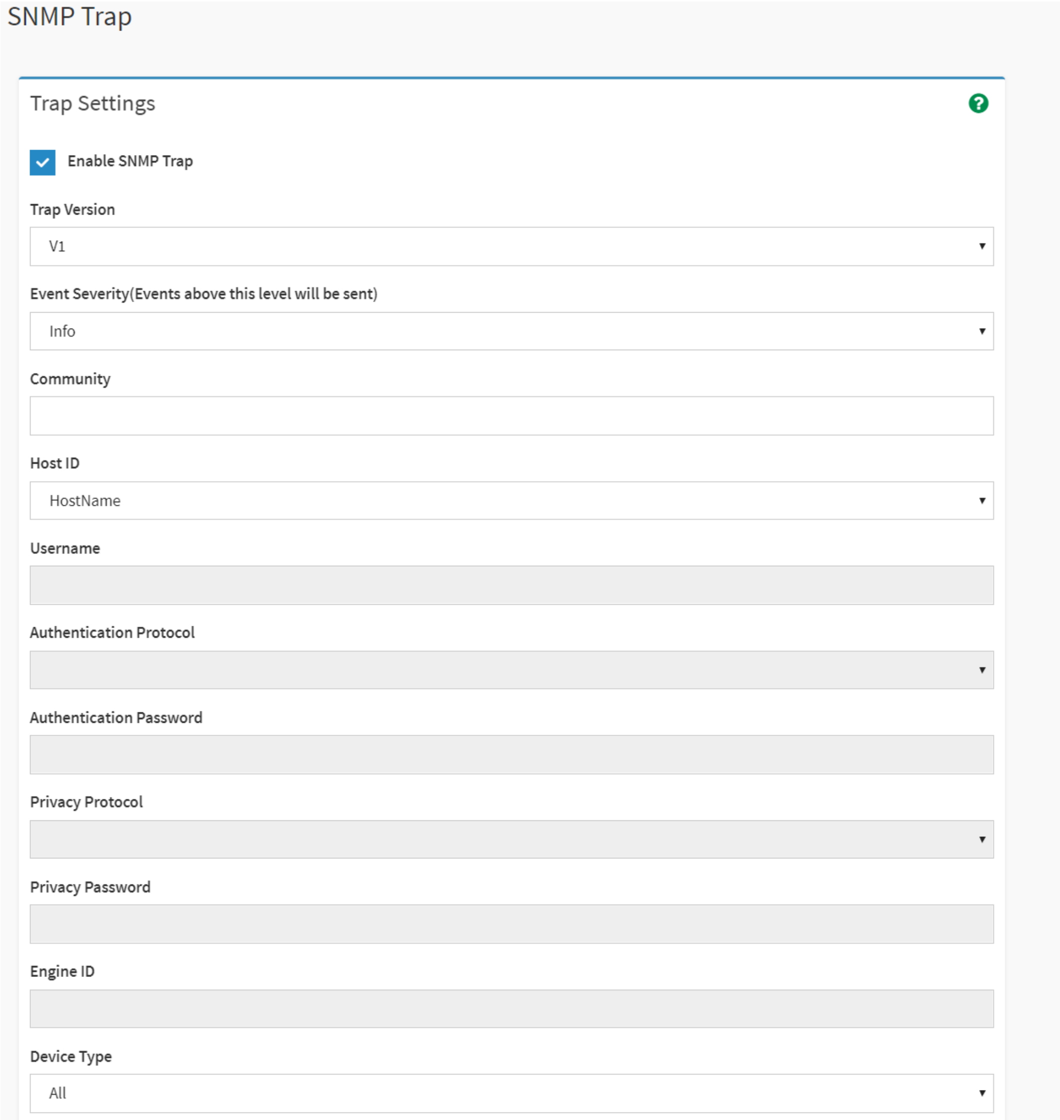
Scenario

Configure the SNMP Trap settings through Web GUI.

Procedure

1. Log in to the Web GUI, and enter the **Logs & Alarms** > **SNMP Trap** page to configure SNMP Trap parameters, including **Trap Version**, **Event Severity**, and **Community**, as shown below.

Figure 8-1 SNMP Trap Settings



SNMP Trap

Trap Settings

☑ Enable SNMP Trap

Trap Version

V1 ▾

Event Severity(Events above this level will be sent)

Info ▾

Community

Host ID

HostName ▾

Username

Authentication Protocol

Authentication Password

Privacy Protocol

Privacy Password

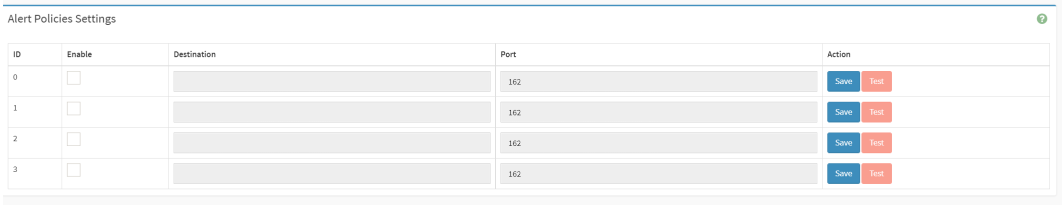
Engine ID

Device Type

All ▾

2. On the **Alert Policies Settings** page, set the IP of the client with the Trap receiver installed as **Destination**, and the port of the Trap receiver as **Port**, and click the **Save** button. Then click the **Test** button, and you can receive a test message at the Trap receiver.

Figure 8-2 Alert Policies Settings



Alert Policies Settings

ID	Enable	Destination	Port	Action
0	□		162	Save Test
1	□		162	Save Test
2	□		162	Save Test
3	□		162	Save Test

9 Mail Alarm

9.1 Function

The mail alarm module is used to enable the SMTP Trap and configure related information.

9.2 Mail Alarm Settings

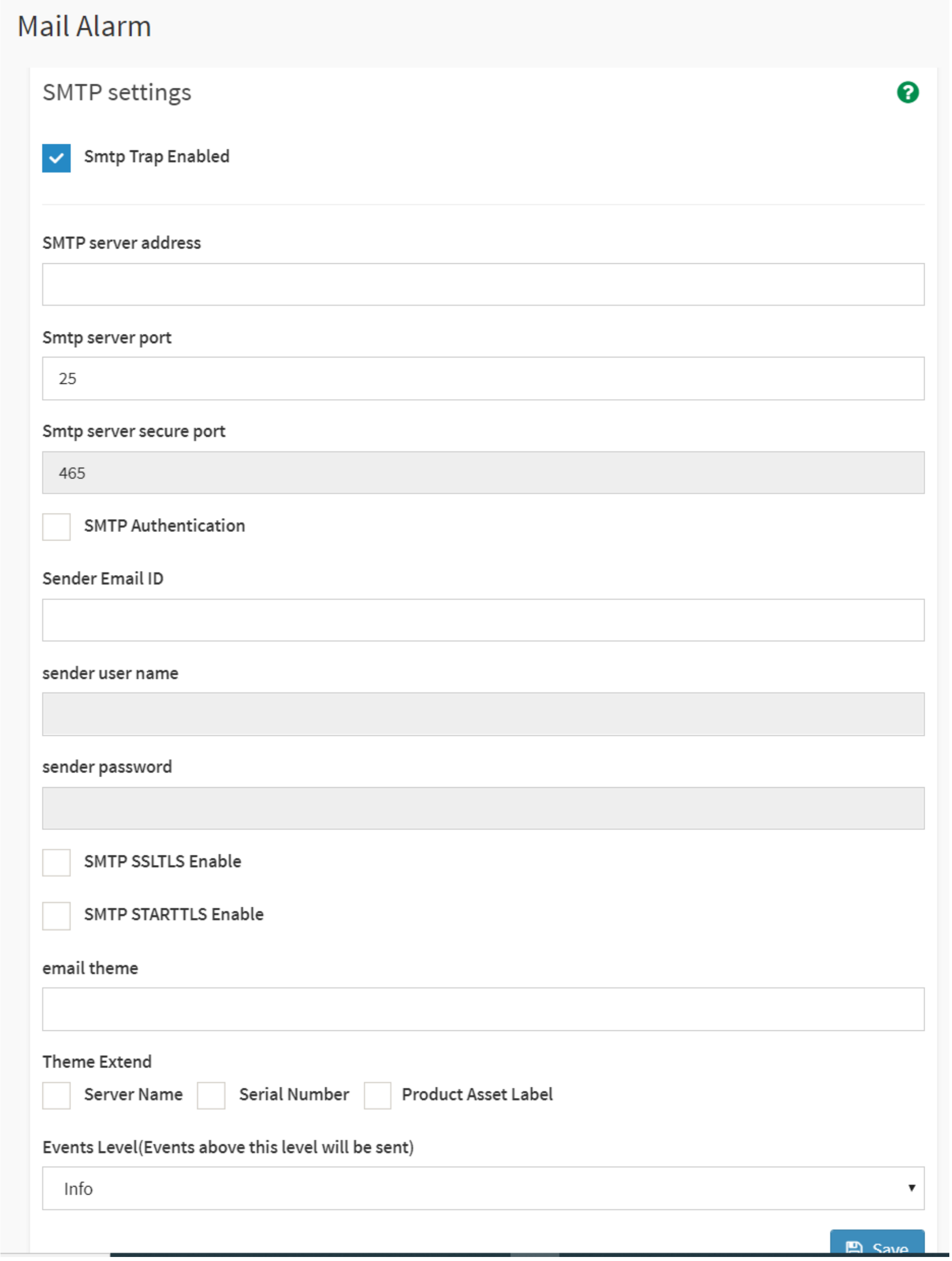
Scenario

Configure the mail alarm settings through Web GUI.

Procedure

1. Select **Logs & Alarms** > **Mail Alarm** in the navigation pane to enter the **SMTP settings** page.

Figure 9-1 SMTP Settings



Mail Alarm

SMTP settings

☑ Smtp Trap Enabled

SMTP server address

Smtp server port: 25

Smtp server secure port: 465

□ SMTP Authentication

Sender Email ID

sender user name

sender password

□ SMTP SSLTLS Enable

□ SMTP STARTTLS Enable

email theme

Theme Extend

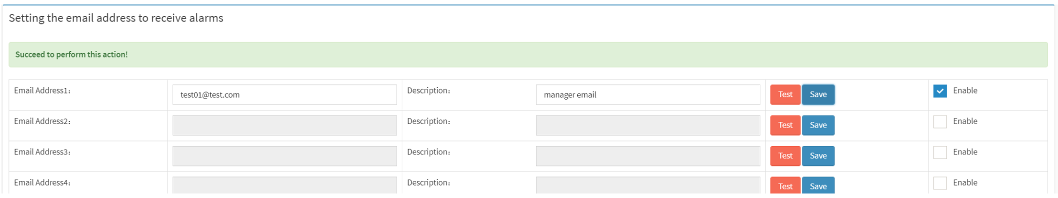
□ Server Name □ Serial Number □ Product Asset Label

Events Level(Events above this level will be sent): Info

2. Fill in required information such as **SMTP server address**, **Sender Email ID**, and **email theme**, and other information as needed, and then click the **Save** button.

3. Enter the email address for receiving the alarm, and click the **Save** button. Then click the **Test** button to test whether you can receive the test email. Once you receive the test email, the configuration is completed.

Figure 9-2 Setting the Email Address to Receive Alarms



Setting the email address to receive alarms

Succeed to perform this action!

Email Address1：	test01@test.com	Description：	manager email	Test Save	☑ Enable
Email Address2：		Description：		Test Save	□ Enable
Email Address3：		Description：		Test Save	□ Enable
Email Address4：		Description：		Test Save	□ Enable

10 BMC Service Settings

10.1 Function

The BMC service settings module lists the BMC related services, and allows you to view and modify the service configuration information.

10.2 Service Settings

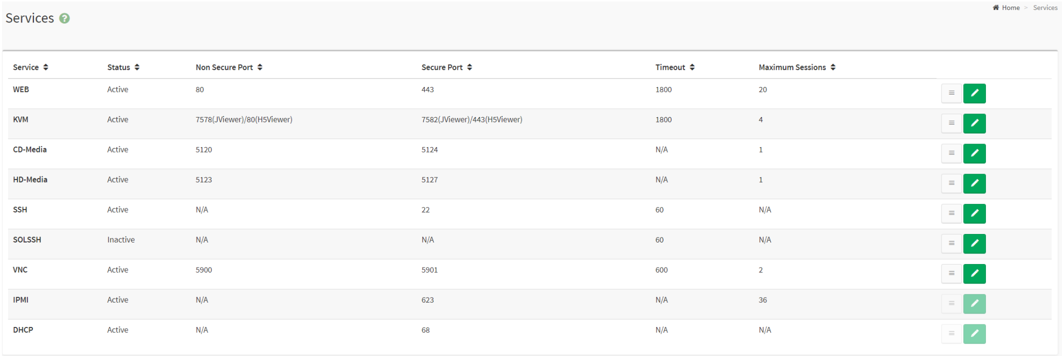
Scenario

Configure the port, timeout, and other properties of the service through Web GUI.

Procedure

1. Log in to the Web GUI, and enter the **BMC Settings** > **Services** page, which displays the basic information about BMC services in operation. Only the administrator has the privilege to modify the service information.

Figure 10-1 Services Page

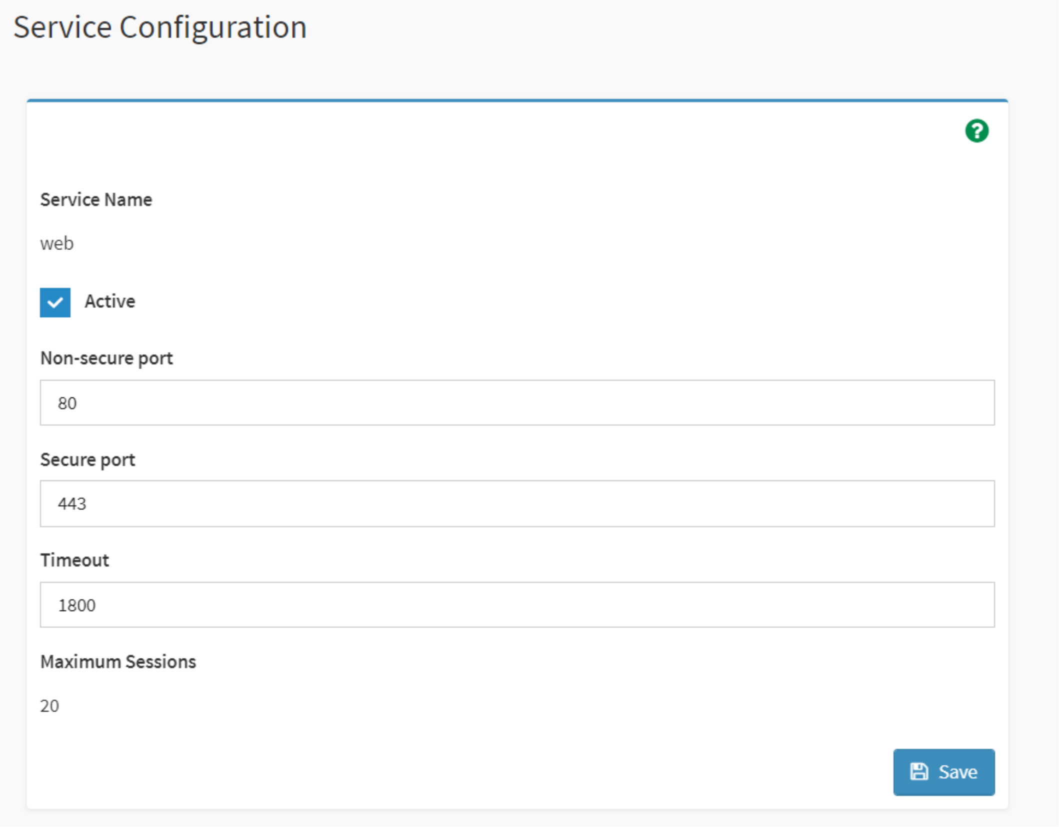


Services

Service	Status	Non Secure Port	Secure Port	Timeout	Maximum Sessions	
WEB	Active	80	443	1800	20	≡ ✎
KVM	Active	7578(JViewer)/80(H5Viewer)	7582(JViewer)/443(H5Viewer)	1800	4	≡ ✎
CD-Media	Active	5120	5124	N/A	1	≡ ✎
HD-Media	Active	5123	5127	N/A	1	≡ ✎
SSH	Active	N/A	22	60	N/A	≡ ✎
SOLSSH	Inactive	N/A	N/A	60	N/A	≡ ✎
VNC	Active	5900	5901	600	2	≡ ✎
IPMI	Active	N/A	623	N/A	36	≡ ✎
DHCP	Active	N/A	68	N/A	N/A	≡ ✎

2. Click the ✎ button on the right side of a service line to enter the **Service Configuration** page. You can modify the specific configuration options and click the **Save** button to complete the modification. The following figure shows an example of web service modification.

Figure 10-2 Service Configuration Modification


Service Configuration

Service Name

web

☑ Active

Non-secure port

80

Secure port

443

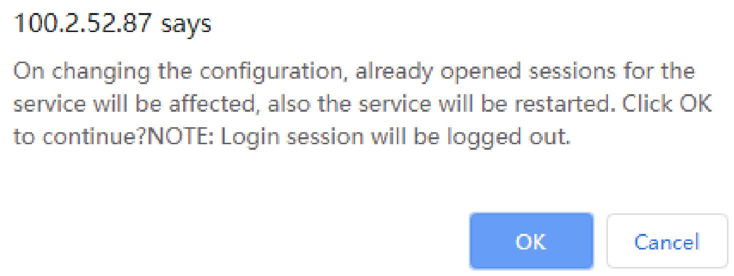
Timeout

1800

Maximum Sessions

20

Figure 10-3 Service Restart Confirmation


100.2.52.87 says

On changing the configuration, already opened sessions for the service will be affected, also the service will be restarted. Click OK to continue?NOTE: Login session will be logged out.

The following table shows the related parameters of BMC service settings.

Table 10-1 Service Settings

Parameter	Description
Service Name	Displays the service name (read-only) of the selected line.
Status	Displays the current service status. Options: Active and Inactive.
Non-secure Port	The non-secure port used to configure the service.

Parameter	Description
	- Default port of Web is 80. - Default port of KVM is 7578. - Default port of CD-Media is 5120. - Default port of HD-Media is 5123. - Default port of SOLSSH is N/A. - Default port of VNC is 5900. - Port number ranges from 1 to 65535. Note: SSH service does not support a non-secure port.
Secure Port	The secure port used to configure the service. - Default port of Web is 443. - Default port of KVM is 7582. - Default port of CD-Media is 5124. - Default port of HD-Media is 5127. - Default port of SSH is 22. - Default port of VNC is 5901. - Port number ranges from 1 to 65535. Note: SOLSSH service does not support a secure port.
Timeout	You can set the timeout value of a service session. - Timeout values of Web, KVM and VNC range from 300 to 1800 s. - Timeout values of SSH and SOLSSH range from 60 to 1800 s. - The timeout value should be a multiple of 60 s.
Maximum Sessions	The maximum sessions of the current service.

11 Storage Management

11.1 Function

This module is used to view the information of storage-related controllers, logical disks, and physical disks, and to create and delete logical disks.

11.2 Creating a Logical Disk

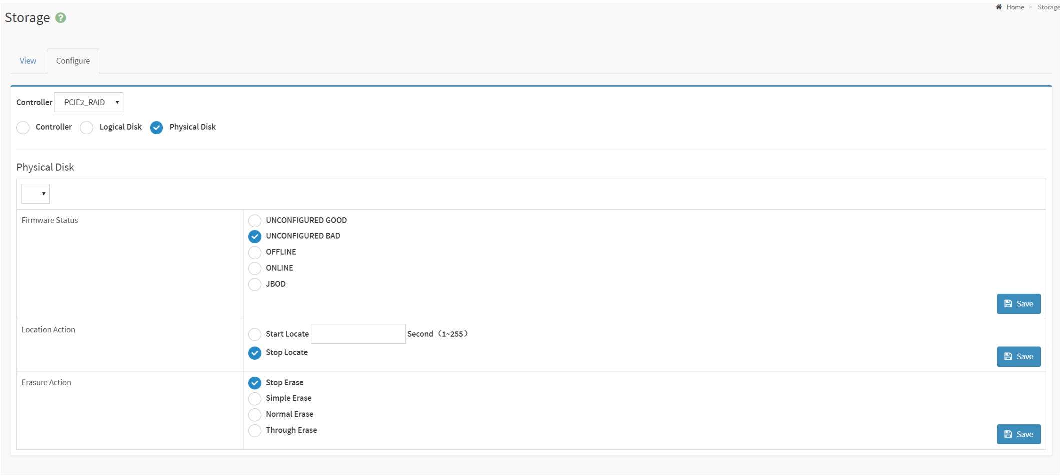
Scenario

Create a logical disk through Web GUI.

Procedure

1. Log in to the Web GUI, enter the **BMC Settings** > **Storage** page, and click the **Configure** tab. Only a physical disk in the **UNCONFIGURED GOOD** status can be used to create a logical disk. If the creation fails, first check the status of the physical disk. Select **Controller** > **Physical Disk** to view the status of the physical disk. As shown in the figure below, the physical disk is in the **UNCONFIGURED BAD** status, and cannot be used to create a logical disk.

Figure 11-1 Physical Disk Page



Storage

Home > Storage

View | Configure

Controller PCIE2_RAID ▾

○ Controller ○ Logical Disk ● Physical Disk

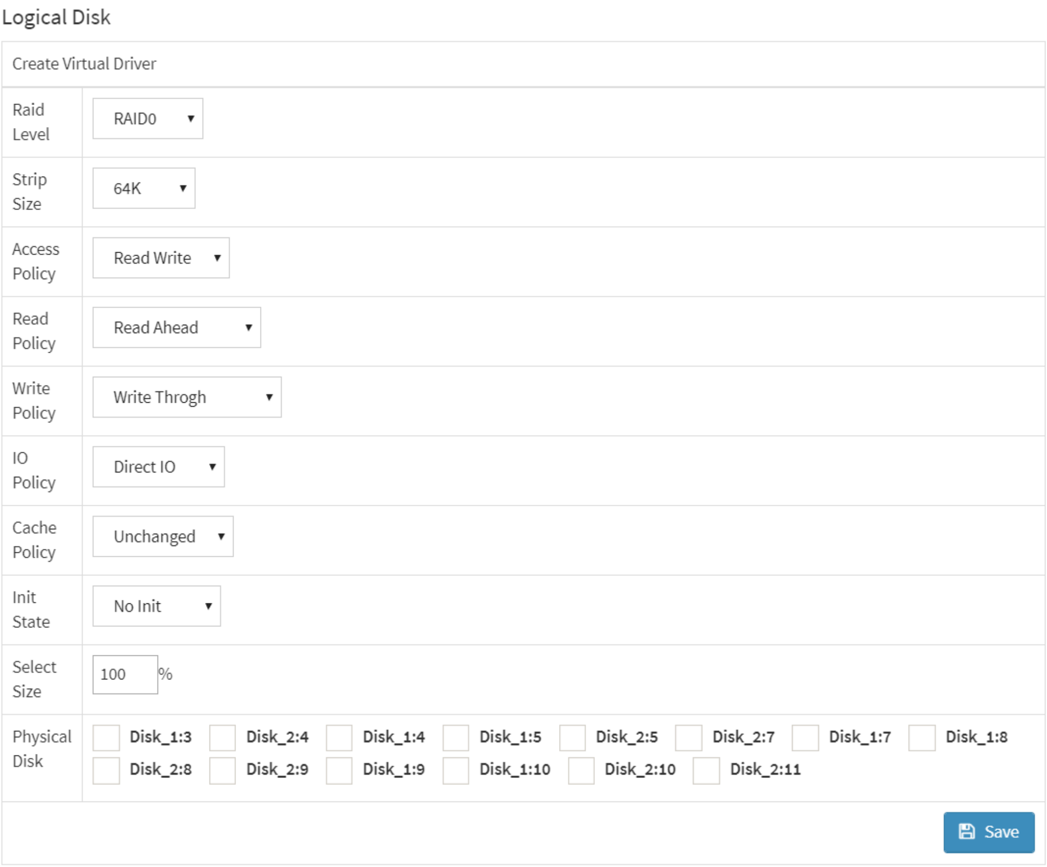
Physical Disk

▾

Firmware Status	○ UNCONFIGURED GOOD ● UNCONFIGURED BAD ○ OFFLINE ○ ONLINE ○ JBOD Save
Location Action	○ Start Locate □ Second（1~255） ● Stop Locate Save
Erasure Action	● Stop Erase ○ Simple Erase ○ Normal Erase ○ Through Erase Save

2. On the **Logical Disk** creation page, **Physical Disk** and **Raid Level** are required fields, and other fields can be specified as needed. Then click the **Save** button.

Figure 11-2 Logical Disk Creation Page



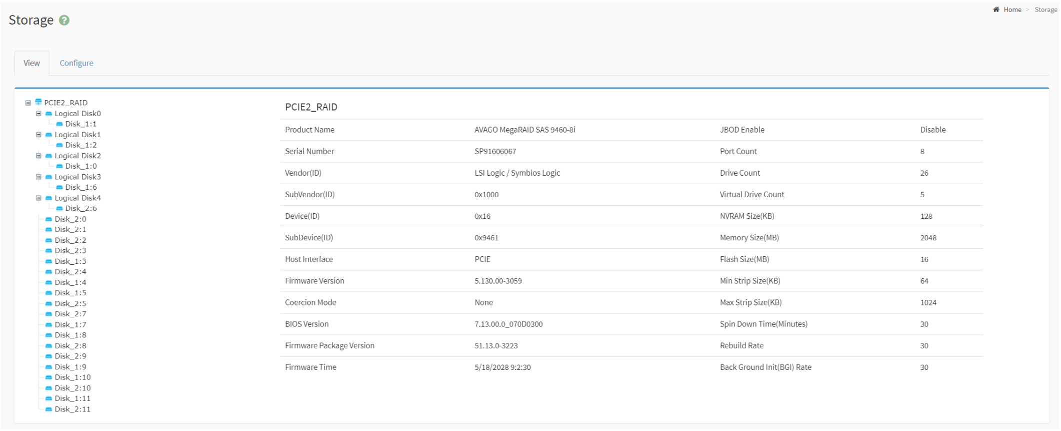
Logical Disk

Create Virtual Driver

Raid Level	RAID0 ▾
Strip Size	64K ▾
Access Policy	Read Write ▾
Read Policy	Read Ahead ▾
Write Policy	Write Throgh ▾
IO Policy	Direct IO ▾
Cache Policy	Unchanged ▾
Init State	No Init ▾
Select Size	100 %
Physical Disk	□ Disk_1:3 □ Disk_2:4 □ Disk_1:4 □ Disk_1:5 □ Disk_2:5 □ Disk_2:7 □ Disk_1:7 □ Disk_1:8 □ Disk_2:8 □ Disk_2:9 □ Disk_1:9 □ Disk_1:10 □ Disk_2:10 □ Disk_2:11

3. Click the **View** tab to see whether the changes have been displayed. It takes time to create a RAID array. If the creation fails, use the BIOS Setup screen of the RAID card or other tools to create a RAID array.

Figure 11-3 Storage View



- PCIE2_RAID
  - Logical Disk0
    - Disk_1:1
  - Logical Disk1
    - Disk_1:2
  - Logical Disk2
    - Disk_1:0
  - Logical Disk3
    - Disk_1:6
  - Logical Disk4
    - Disk_2:6
  - Disk_2:0
  - Disk_2:1
  - Disk_2:2
  - Disk_2:3
  - Disk_1:3
  - Disk_2:4
  - Disk_1:4
  - Disk_1:5
  - Disk_2:5
  - Disk_2:7
  - Disk_1:7
  - Disk_1:8
  - Disk_2:8
  - Disk_2:9
  - Disk_1:9
  - Disk_1:10
  - Disk_2:10
  - Disk_1:11
  - Disk_2:11

PCIE2_RAID

Product Name	AVAGO MegaRAID SAS 9460-8i	JBOD Enable	Disable
Serial Number	SP91606067	Port Count	8
Vendor(ID)	LSI Logic / Symbios Logic	Drive Count	26
SubVendor(ID)	0x1000	Virtual Drive Count	5
Device(ID)	0x16	NVRAM Size(KB)	128
SubDevice(ID)	0x9461	Memory Size(MB)	2048
Host Interface	PCIE	Flash Size(MB)	16
Firmware Version	5.130.00-3059	Min Strip Size(KB)	64
Coercion Mode	None	Max Strip Size(KB)	1024
BIOS Version	7.13.00.0_070D0300	Spin Down Time(Minutes)	30
Firmware Package Version	51.13.0-3223	Rebuild Rate	30
Firmware Time	5/18/2028 9:2:30	Back Ground Init(BGI) Rate	30

11.3 Other Operations on Logical Disk

Scenario

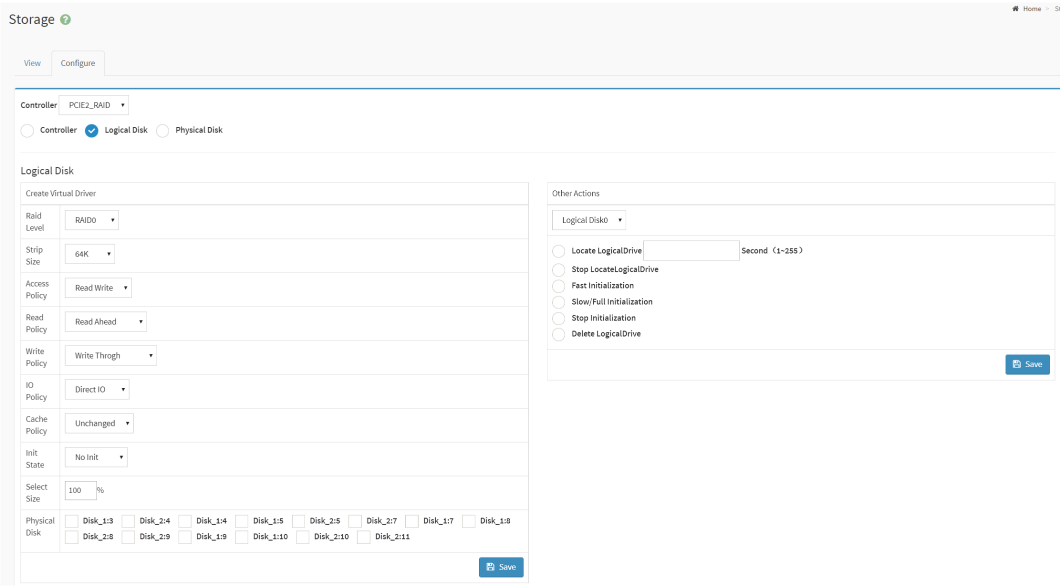
Perform operations such as locating, stop locating, initializing, and deleting a logical disk through Web GUI.

Procedure

1. Log in to the Web GUI, enter the **BMC Settings** > **Storage** page, click the **Configure** tab, and select **Logical Disk**.

2. Click the **Other Actions** button on the right to perform appropriate operations.

Figure 11-4 Logical Disk Page



Controller: PCIE2_RAID

○ Controller ● Logical Disk ○ Physical Disk

Logical Disk

Create Virtual Driver

Raid Level	RAID0
Strip Size	64K
Access Policy	Read Write
Read Policy	Read Ahead
Write Policy	Write Throgh
IO Policy	Direct IO
Cache Policy	Unchanged
Init State	No Init
Select Size	100 %
Physical Disk	□ Disk_1:3 □ Disk_2:4 □ Disk_1:4 □ Disk_1:5 □ Disk_2:5 □ Disk_2:7 □ Disk_1:7 □ Disk_1:8 □ Disk_2:8 □ Disk_2:9 □ Disk_1:9 □ Disk_1:10 □ Disk_2:10 □ Disk_2:11

Other Actions

Logical Disk0

○ Locate LogicalDrive [ ] Second（1~255）
○ Stop LocateLogicalDrive
○ Fast Initialization
○ Slow/Full Initialization
○ Stop Initialization
○ Delete LogicalDrive

12 Firmware Update

12.1 Function

This module is used to update firmware including BIOS, BMC, CPLD, PSU, and FPGA with the HPM firmware update function.

12.2 Operation Guide

Refer to the BMC update manual.

13 Restoring Factory Defaults

13.1 Function

This function can restore the BMC configuration to factory default settings and any changes you have made on the BMC will be lost. Please perform this operation with caution when any changes made on the BMC cause functional abnormalities.

13.2 Restoring Factory Defaults

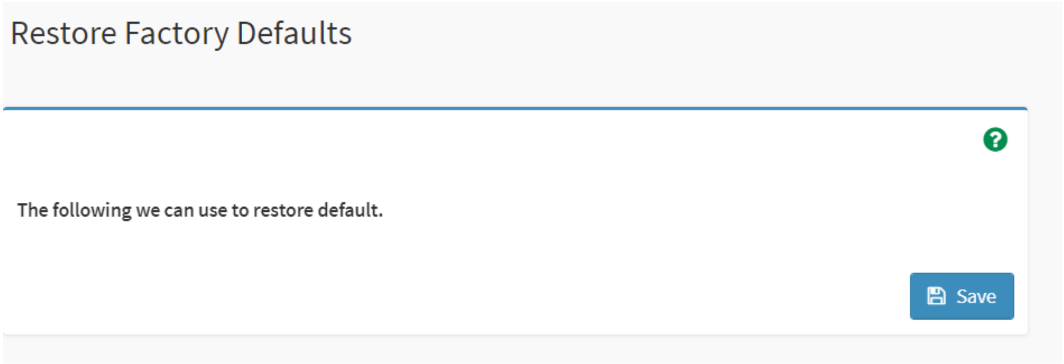
Scenario

Restore the BMC to factory defaults through Web GUI.

Procedure

1. Log in to the Web GUI, and enter the **System Maintenance** > **Restore Factory Defaults** page.

Figure 13-1 Restore Factory Defaults

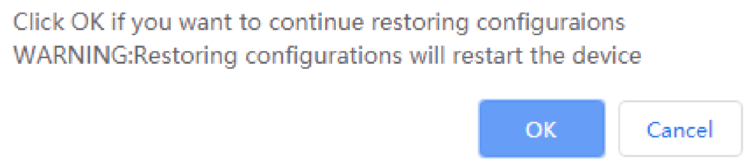


Restore Factory Defaults

The following we can use to restore default.

2. Click the **Save** button, and the following prompt box pops up, and then click **OK**.

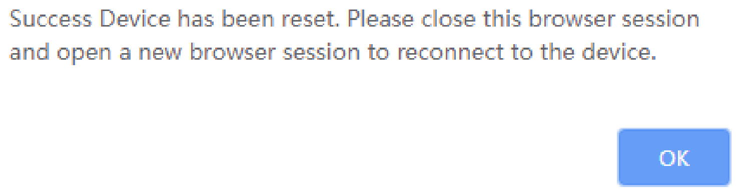
Figure 13-2 Prompt Box for Restoring Factory Defaults



Click OK if you want to continue restoring configuraions
WARNING:Restoring configurations will restart the device

3. If the operation is successful, the following prompt box pops up. Close the browser and open a new browser session to reconnect the device.

Figure 13-3 Operation Success


Success Device has been reset. Please close this browser session and open a new browser session to reconnect to the device.

14 SSL Settings

14.1 Function

This function is used to replace the SSL certificate. To improve security, it is suggested to replace the certificate and public-private key pair with your own, and update the certificate in a timely manner to ensure its validity.

14.2 Generating an SSL Certificate Online

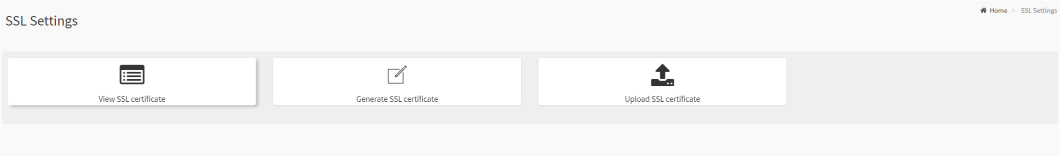
Scenario

Generate an SSL certificate online through Web GUI.

Procedure

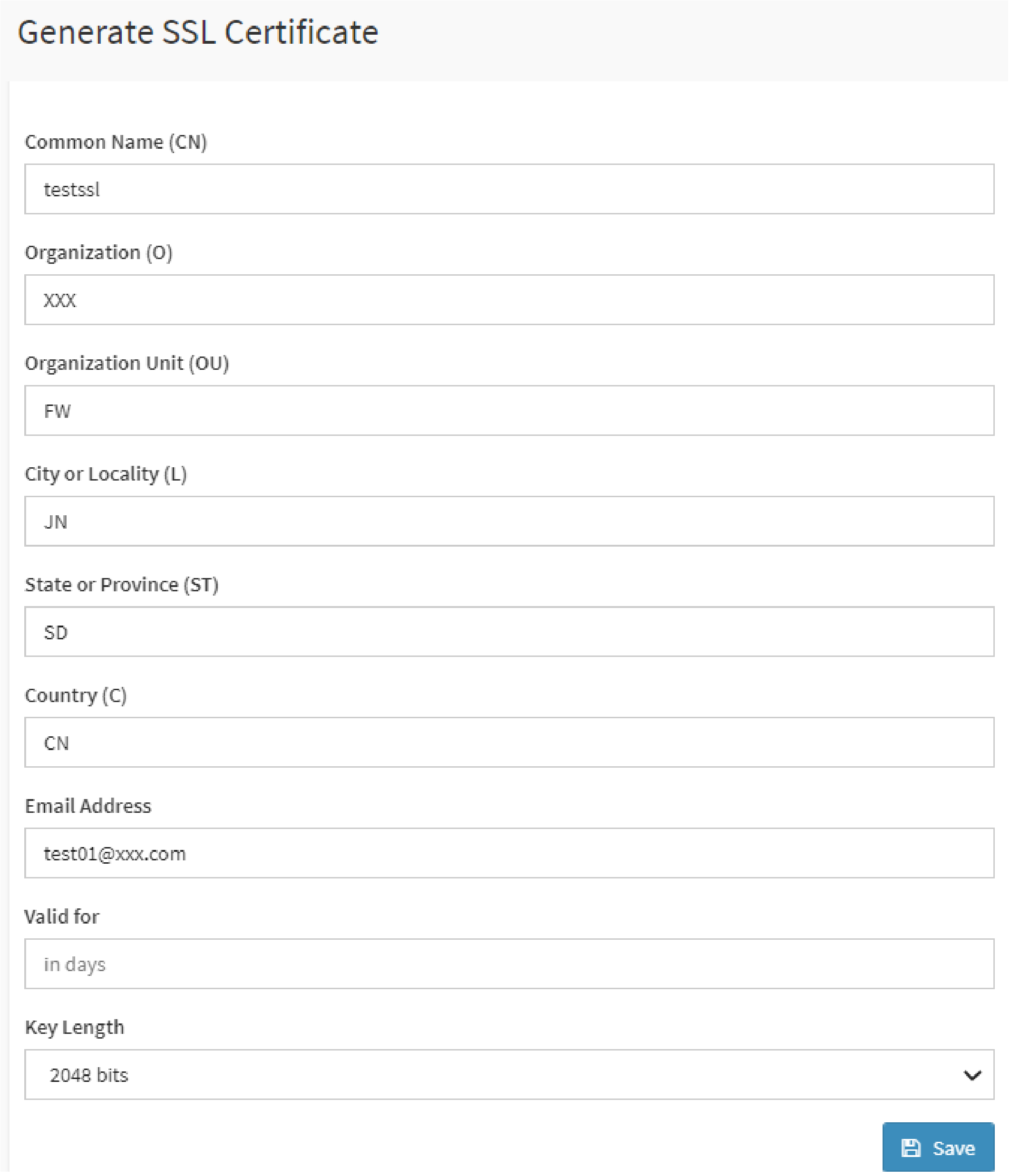
1. Log in to the Web GUI, enter the **BMC Settings** > **SSL Settings** page, and select **Generate SSL certificate**.

Figure 14-1 SSL Settings



2. Fill in the information on the following page. Refer to Table 14-1 for the field information.

Figure 14-2 Generate SSL Certificate



Generate SSL Certificate

Common Name (CN): testssl

Organization (O): XXX

Organization Unit (OU): FW

City or Locality (L): JN

State or Province (ST): SD

Country (C): CN

Email Address: test01@xxx.com

Valid for: in days

Key Length: 2048 bits

Table 14-1 SSL Settings

Parameter	Description
Common Name (CN)	A name or a purpose name, such as testssl.
Organization (O)	The name of an organization or a company.
Organizational Unit (OU)	The name of a subordinate unit under an organization or a company, such as FW, which refers to the Firmware Department.
City or Locality (L)	A city or place, such as JN, which refers to Jinan City.

Parameter	Description
State or Province (ST)	A state or province, such as SD, which refers to Shandong Province.
Country (C)	A country, such as CN, which refers to China.
Email Address	An email address.
Valid for	The validity period, which ranges from 365 to 3650 days.
Key Length	The key length, which defaults to 2048 bits.

14.3 Generating and Uploading an SSL Certificate

Scenario

Generate an SSL certificate with the OpenSSL tool, and upload the SSL certificate through Web GUI.

Procedure

1. Install the OpenSSL tool, and see Section 18.2 Introduction to OpenSSL for details. This step describes how to generate an SSL certificate with the OpenSSL tool. If there is an available certificate, you can directly proceed to step 6.

2. Generate a private key: **openssl genrsa -out privkey.pem 2048**.

3. Generate a certificate request (refer to Table 14-2): **openssl req -new -key privkey.pem -out cert_req.pem**.

Table 14-2 Inputing Parameters of the Certifate Request

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:SD
Locality Name (eg, city) []:JN
Organization Name (eg, company) [Internet Widgits Pty Ltd]:XXX
Organizational Unit Name (eg, section) []:FW
Common Name (e.g. server FQDN or YOUR name) []:webssl
Email Address []:test01@xxx.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

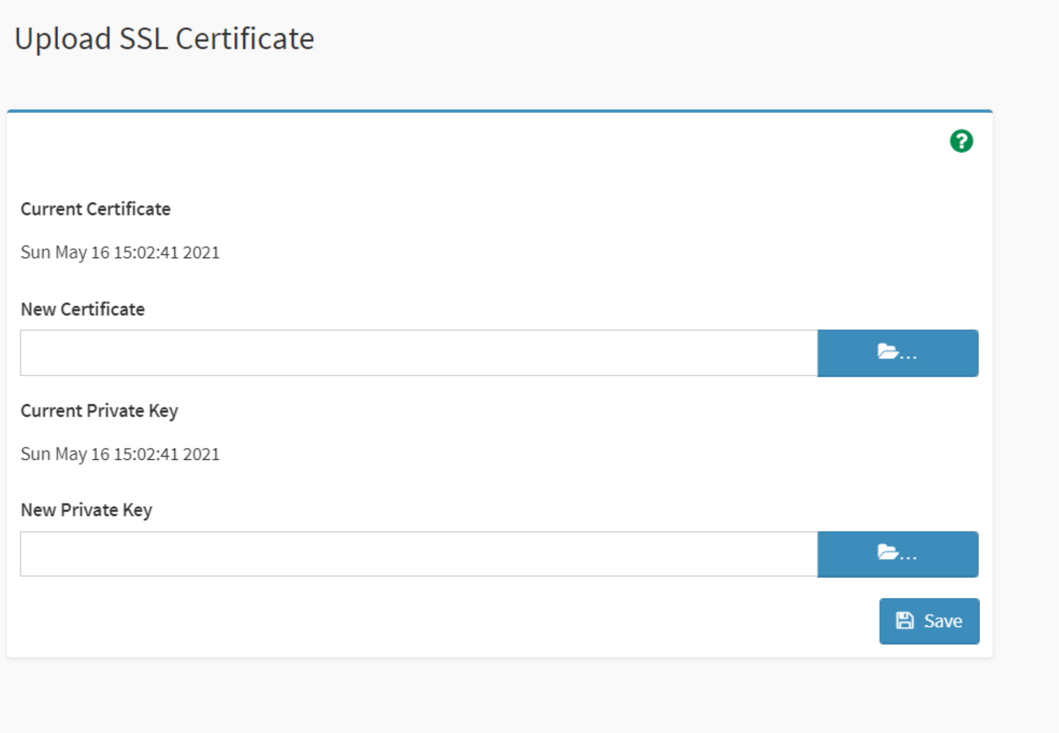
4. Generate the certificate: **openssl x509 -req -days 365 -in cert_req.pem -signkey privkey.pem -out sign_cert.pem**.

5. Merge the certificate into the private key file: **cat privkey.pem sign_cert.pem > server.pem**.

6. Log in to the Web GUI, enter the **BMC Settings** > **SSL Settings** page, and select **Upload SSL certificate**, as shown in the following figure.

7. In the dialog box that pops up, select the new certificate **sign_cert.pem**, and the new private key **server.pem**, and then click the **Save** button to complete the setting.

Figure 14-3 Upload SSL Certificate



Upload SSL Certificate

Current Certificate

Sun May 16 15:02:41 2021

New Certificate

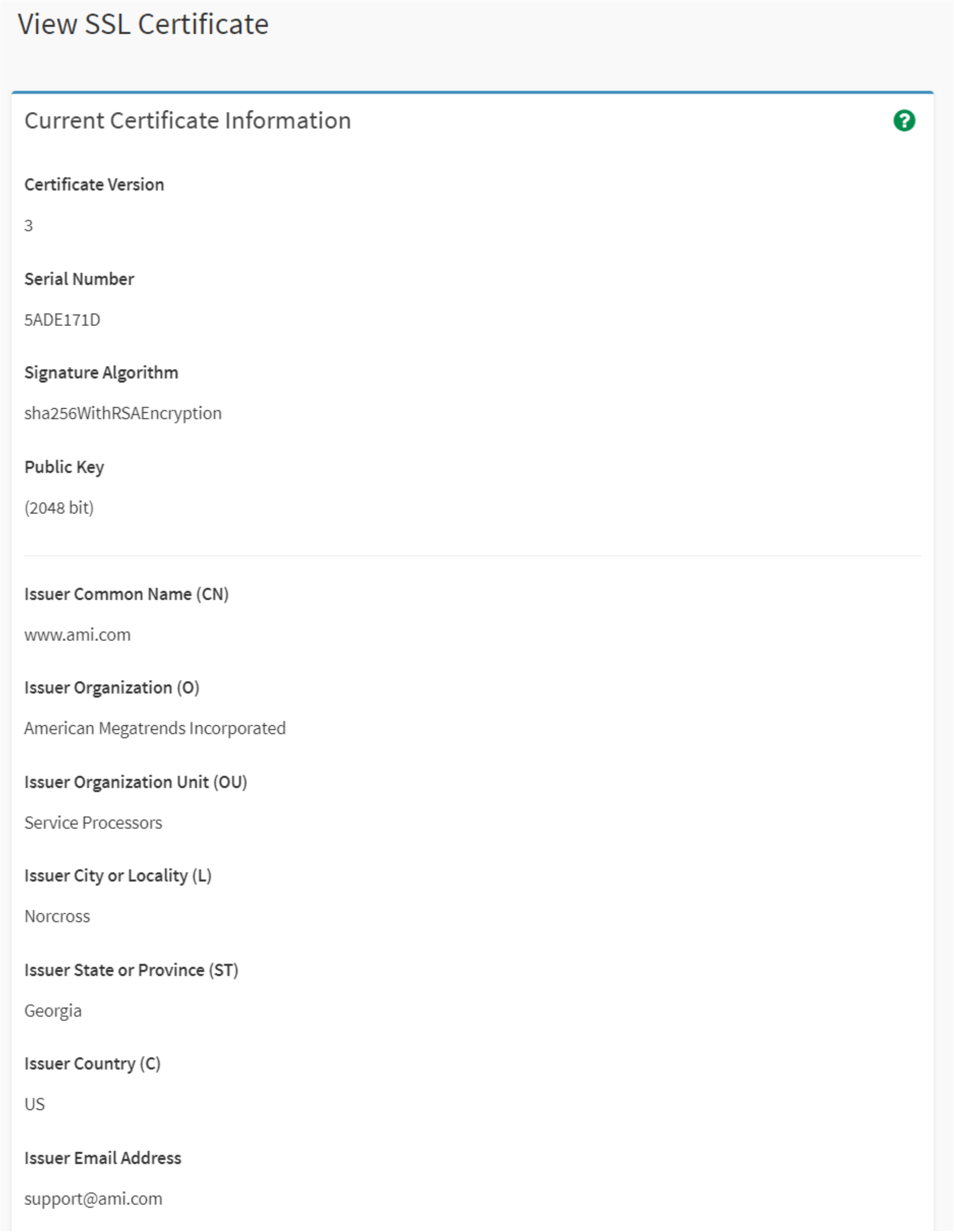
Current Private Key

Sun May 16 15:02:41 2021

New Private Key

8. Enter the **BMC Settings** > **SSL Settings** page again, and click **View SSL certificate** to confirm that the certificate information has been modified, as shown below.

Figure 14-4 View SSL Certificate



View SSL Certificate

Current Certificate Information

Certificate Version

3

Serial Number

5ADE171D

Signature Algorithm

sha256WithRSAEncryption

Public Key

(2048 bit)

Issuer Common Name (CN)

www.ami.com

Issuer Organization (O)

American Megatrends Incorporated

Issuer Organization Unit (OU)

Service Processors

Issuer City or Locality (L)

Norcross

Issuer State or Province (ST)

Georgia

Issuer Country (C)

US

Issuer Email Address

support@ami.com

15 Redfish

15.1 Overview

Redfish is an HTTPS-based management standard that uses RESTful interface to manage devices. Each HTTPS operation submits or returns a resource in JSON format encoded in UTF-8. Simliar to web applications that return HTML to the browser, RESTful APIs return data in JSON format to the client using the same transport mechanism (HTTPS).

Redfish fits into the development trend toward universal software interfaces in the Internet industry. Redfish is easy to implement, easy to use and easy to extend over previous technologies. The same Redfish data model can be used not only for traditional rack servers and blade servers, but also for new server systems. This is because the data model is designed to describe its service functions to clients and it has reserved enough room for flexible design from the beginning.

15.2 Operation Guide

Refer to the Redfish user manual.

16 Entering the BIOS System

16.1 Function

In the server system, BIOS and BMC communicate with each other for data exchange. You can view the BMC network configuration, user information, and other information via the BIOS screen.

16.2 Entering the BIOS System Locally

Scenario

Enter the BIOS system via the local keyboard and video monitor.

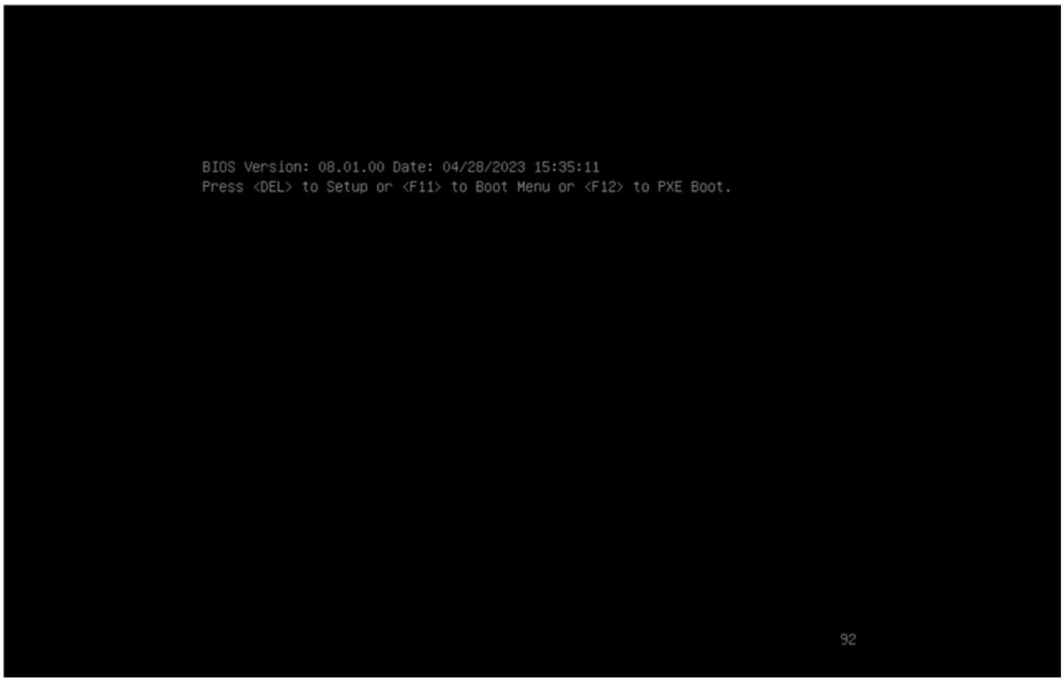
Procedure

1. Connect the power supply as well as the external keyboard, mouse, and video monitor.

2. Power on the server.

3. The system starts to boot. When the following prompt appears: **Press <DEL> to Setup or <F11> to Boot Menu or <F12> to PXE Boot**, as shown below, press <DEL> to enter the BIOS Setup screen.

Figure 16-1 BIOS Startup Screen 1

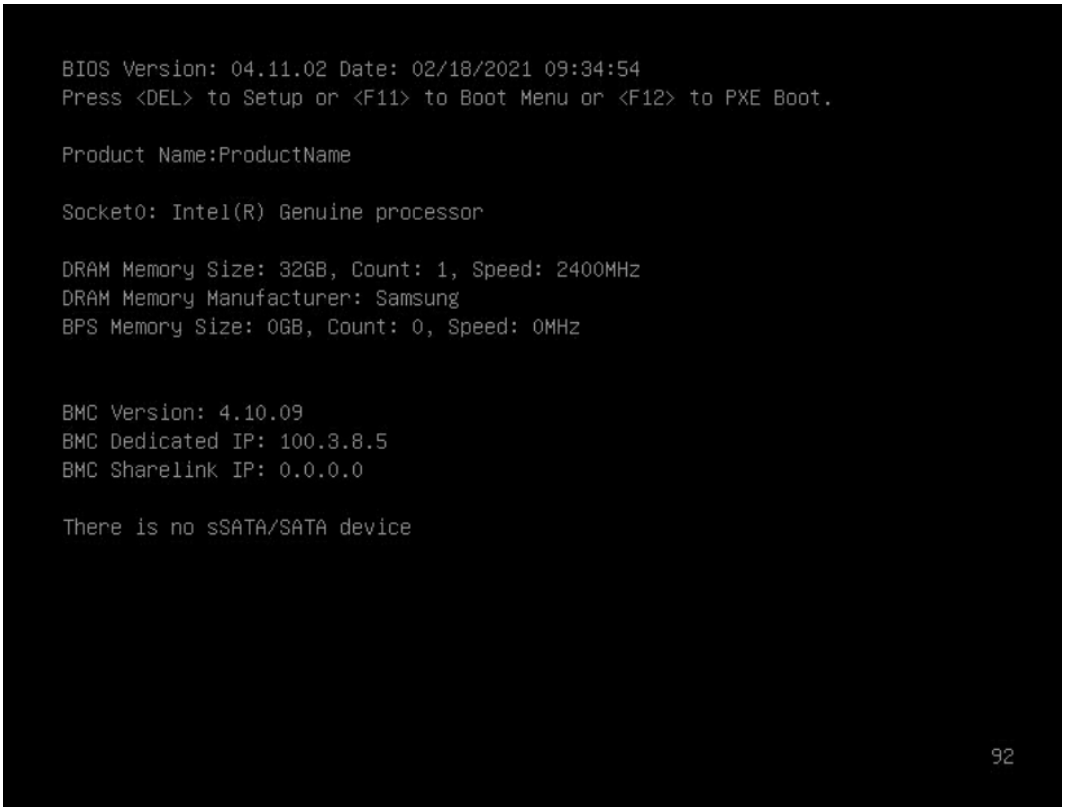


```
BIOS Version: 08.01.00 Date: 04/28/2023 15:35:11
Press <DEL> to Setup or <F11> to Boot Menu or <F12> to PXE Boot.

                                                               92
```

NOTE

You may see a different screen depending on when you press <DEL>.

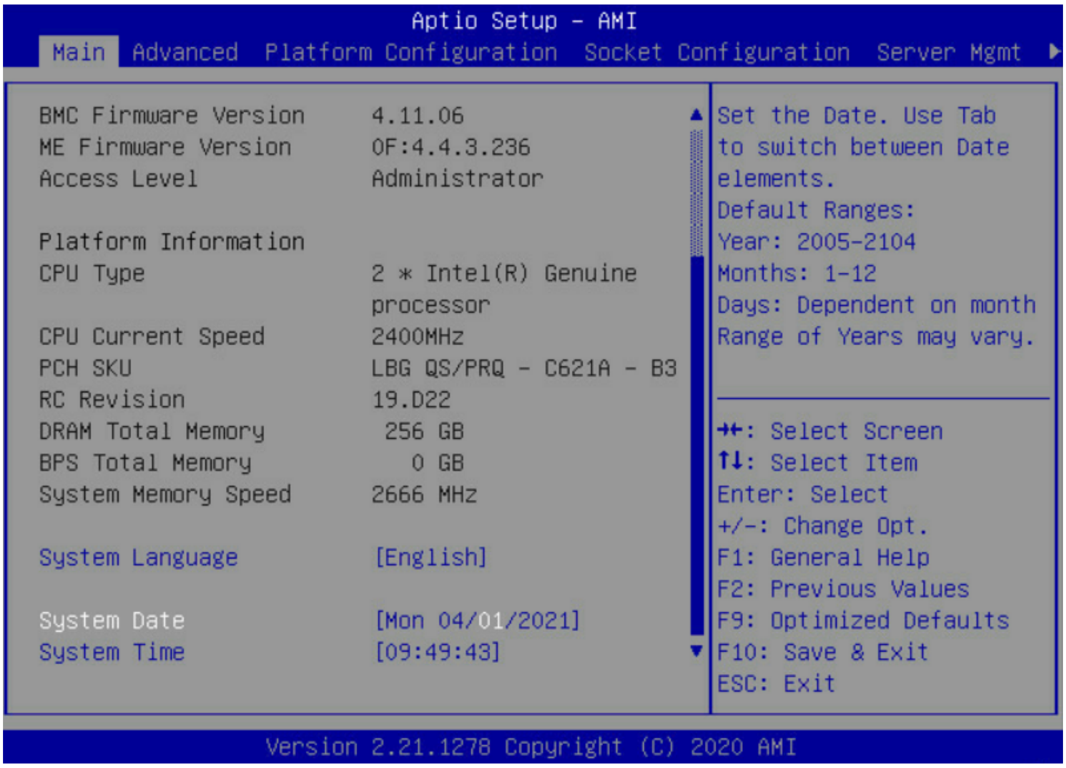
Figure 16-2 BIOS Startup Screen



```
BIOS Version: 04.11.02 Date: 02/18/2021 09:34:54
Press <DEL> to Setup or <F11> to Boot Menu or <F12> to PXE Boot.

Product Name:ProductName

Socket0: Intel(R) Genuine processor

DRAM Memory Size: 32GB, Count: 1, Speed: 2400MHz
DRAM Memory Manufacturer: Samsung
BPS Memory Size: 0GB, Count: 0, Speed: 0MHz


BMC Version: 4.10.09
BMC Dedicated IP: 100.3.8.5
BMC Sharelink IP: 0.0.0.0

There is no sSATA/SATA device







                                                                        92
```

4. The following figure shows the screen after you enter the BIOS.

Figure 16-3 BIOS Main Screen



```
BMC Firmware Version        4.11.06                    Set the Date. Use Tab
ME Firmware Version         0F:4.4.3.236               to switch between Date
Access Level                Administrator              elements.
                                                       Default Ranges:
Platform Information                                   Year: 2005-2104
CPU Type                    2 * Intel(R) Genuine       Months: 1-12
                            processor                  Days: Dependent on month
CPU Current Speed           2400MHz                    Range of Years may vary.
PCH SKU                     LBG QS/PRQ - C621A - B3
RC Revision                 19.D22
DRAM Total Memory            256 GB                    →←: Select Screen
BPS Total Memory               0 GB                    ↑↓: Select Item
System Memory Speed         2666 MHz                   Enter: Select
                                                       +/-: Change Opt.
System Language              [English]                 F1: General Help
                                                       F2: Previous Values
System Date                  [Mon 04/01/2021]          F9: Optimized Defaults
System Time                  [09:49:43]                F10: Save & Exit
                                                       ESC: Exit

              Version 2.21.1278 Copyright (C) 2020 AMI
```

17 Setting the U-Boot Password

17.1 Function

U-Boot commands are debugging commands used to load underlying software and debug underlying devices. Generally, you can log in to U-Boot over a serial port, which is physically secure. To log in to U-Boot, you need to enter a password, which is not part of the BMC user management. You can change the password with the IPMItool if needed.

17.2 Changing the U-Boot Password in Linux

Scenario

Change the U-Boot password in the Linux OS.

Procedure

1. Install the IPMItool. For details, see Section 18.1 Introduction to IPMItool.

2. Log in to the OS, and use the command **ipmitool raw 0x3c 0x18 <Length> <Password Data>** to change the password. Refer to the following table for specific parameters. Example: If you need to change the password to 123456, use the command **ipmitool raw 0x3c 0x18 0x06 0x31 0x32 0x33 0x34 0x35 0x36**.

Table 17-1 U-Boot Password Change Parameters

Request	NetFn	0x3c	
	Command	0x18	
	Byte[1]	Length	Password length. Maximum value: 31 (0x1FH).
	Byte[2-n]	Password Data	ASCII codes of the password characters. Only printable characters (0x20 - 0x80) are supported, and the password cannot be empty.
Response	Byte[0]	Complete Code	0: Successful. Others: Failed.

18 Common Tools

18.1 Introduction to IPMItool

18.1.1 Purpose and Scenario

IPMItool is used to send IPMI commands, including in-band commands over Open interface from the server OS, and out-of-band commands over LAN interface from a remote system. Ipmitool has a Windows version and a Linux version. Only the Linux version is supported under the Open interface.

Supported interfaces:

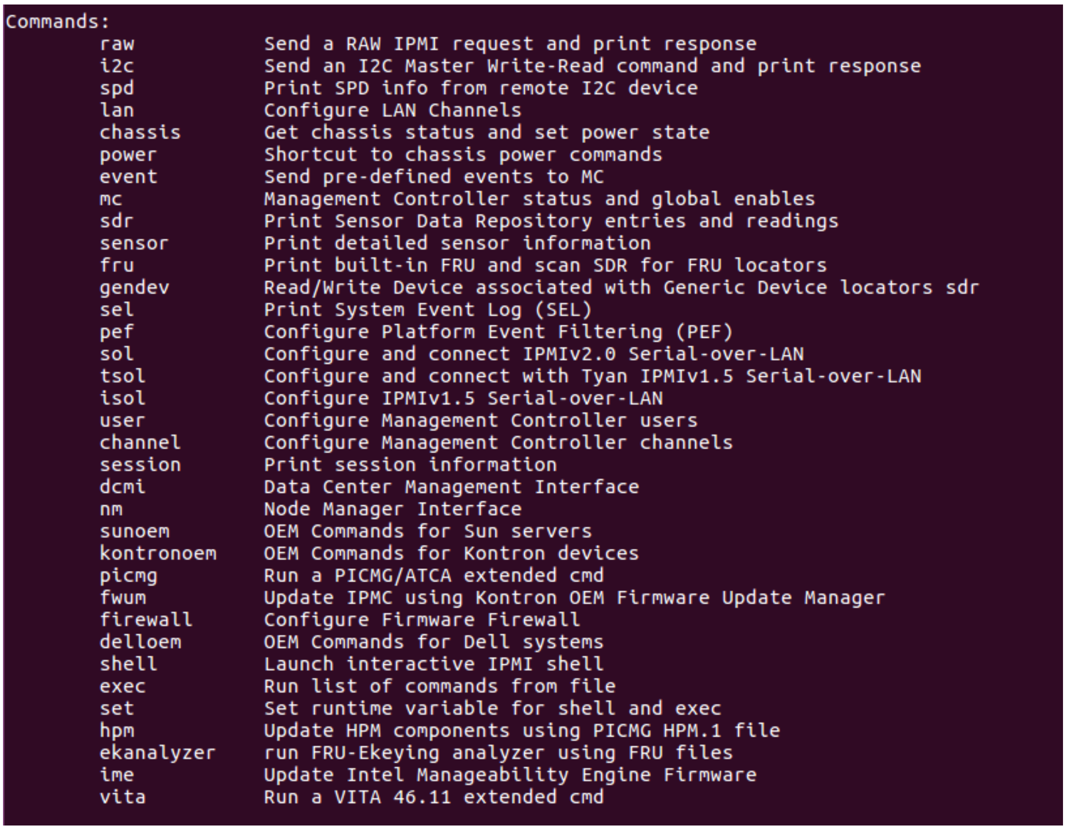
- Open: Linux OpenIPMI interface (default)
- LANPLUS: IPMI v2.0 RMCP+ LAN interface

18.1.2 Installing and Using IPMItool in Linux

To install IPMItool in Linux OS, you need to install 2 packages: OpenIPMI and IPMItool. OpenIPMI provides kernel drivers for IPMItool, enabling IPMItool to access the local server BMC via the Open interface.

For the supported ipmitool commands, refer to the following. For specific usage and parameter list, refer to the command line help. Use the command **ipmitool -h** to view the help information, as shown in the figure below, which is a partial screenshot of the supported commands returned by the IPMItool command.

Figure 18-1 IPMItool Commands



```
Commands:
        raw           Send a RAW IPMI request and print response
        i2c           Send an I2C Master Write-Read command and print response
        spd           Print SPD info from remote I2C device
        lan           Configure LAN Channels
        chassis       Get chassis status and set power state
        power         Shortcut to chassis power commands
        event         Send pre-defined events to MC
        mc            Management Controller status and global enables
        sdr           Print Sensor Data Repository entries and readings
        sensor        Print detailed sensor information
        fru           Print built-in FRU and scan SDR for FRU locators
        gendev        Read/Write Device associated with Generic Device locators sdr
        sel           Print System Event Log (SEL)
        pef           Configure Platform Event Filtering (PEF)
        sol           Configure and connect IPMIv2.0 Serial-over-LAN
        tsol          Configure and connect with Tyan IPMIv1.5 Serial-over-LAN
        isol          Configure IPMIv1.5 Serial-over-LAN
        user          Configure Management Controller users
        channel       Configure Management Controller channels
        session       Print session information
        dcmi          Data Center Management Interface
        nm            Node Manager Interface
        sunoem        OEM Commands for Sun servers
        kontronoem    OEM Commands for Kontron devices
        picmg         Run a PICMG/ATCA extended cmd
        fwum          Update IPMC using Kontron OEM Firmware Update Manager
        firewall      Configure Firmware Firewall
        delloem       OEM Commands for Dell systems
        shell         Launch interactive IPMI shell
        exec          Run list of commands from file
        set           Set runtime variable for shell and exec
        hpm           Update HPM components using PICMG HPM.1 file
        ekanalyzer    run FRU-Ekeying analyzer using FRU files
        ime           Update Intel Manageability Engine Firmware
        vita          Run a VITA 46.11 extended cmd
```

18.2 Introduction to OpenSSL

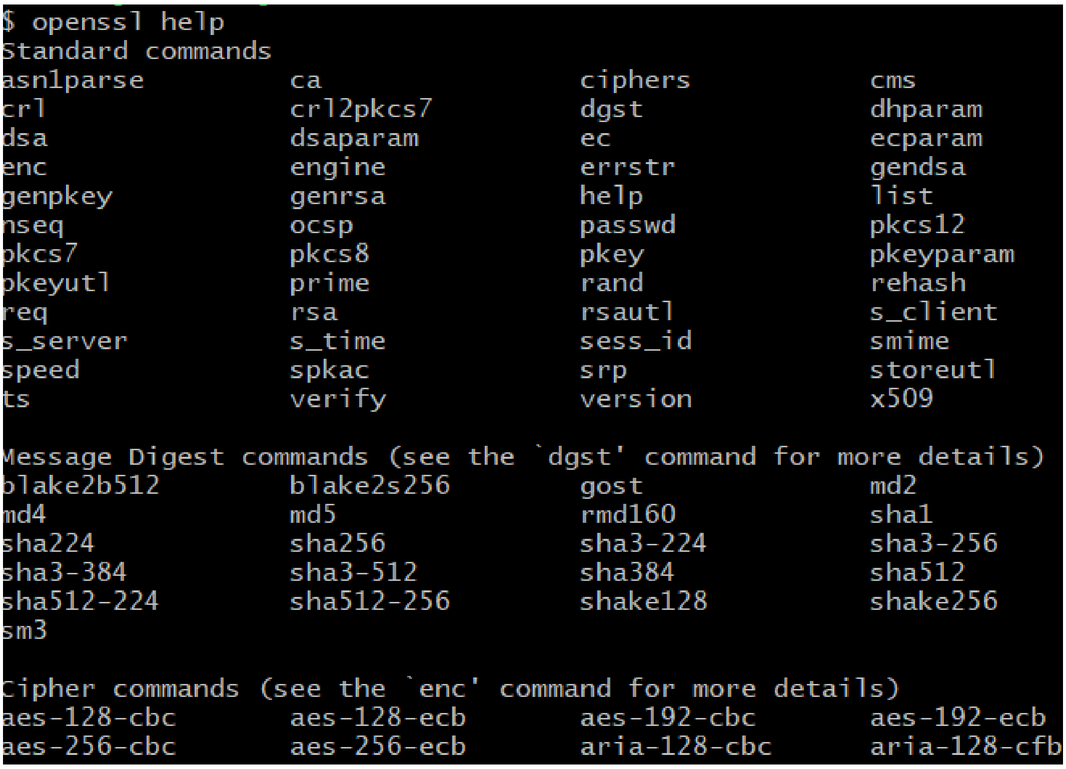
18.2.1 Purpose and Scenario

OpenSSL is an open source cryptography library for implementing the Secure Sockets Layer (SSL) protocol, covering the major cryptographic algorithms, common keys, and certificate management. The OpenSSL package has 3 main functional parts: SSL protocol library (libssl), application command tools, and cryptographic algorithm library (libcrypto).

18.2.2 Installing and Using OpenSSL in Linux

To install OpenSSL in Linux OS, you need to install 2 packages: OpenSSL and libssl-dev. For specific usage and parameter list, refer to the command line help. Use the command **openssl help** to view the help information, as shown in the figure below, which is a partial screenshot of the supported commands returned by the OpenSSL command.

Figure 18-2 OpenSSL Commands



```
$ openssl help
Standard commands
asn1parse         ca                ciphers           cms
crl               crl2pkcs7         dgst              dhparam
dsa               dsaparam          ec                ecparam
enc               engine            errstr            gendsa
genpkey           genrsa            help              list
nseq              ocsp              passwd            pkcs12
pkcs7             pkcs8             pkey              pkeyparam
pkeyutl           prime             rand              rehash
req               rsa               rsautl            s_client
s_server          s_time            sess_id           smime
speed             spkac             srp               storeutl
ts                verify            version           x509

Message Digest commands (see the `dgst' command for more details)
blake2b512        blake2s256        gost              md2
md4               md5               rmd160            sha1
sha224            sha256            sha3-224          sha3-256
sha3-384          sha3-512          sha384            sha512
sha512-224        sha512-256        shake128          shake256
sm3

Cipher commands (see the `enc' command for more details)
aes-128-cbc       aes-128-ecb       aes-192-cbc       aes-192-ecb
aes-256-cbc       aes-256-ecb       aria-128-cbc      aria-128-cfb
```