



# NETAŞ Server

## UniKits

### User Guide

---

Version: V01.24.03.01

NETAŞ TELEKOMÜNIKASYON A.Ş  
Yenişehir Mahallesi Osmanlı Bulvarı Aeropark Sitesi  
B Blok No:11B İç Kapı No:40  
Postcode: 34912  
Tel: +90 (216) 522 20 00  
URL: <https://destek.netas.com.tr>  
E-mail: [info@netas.com.tr](mailto:info@netas.com.tr)

## LEGAL INFORMATION

Copyright 2025 NETAŞ TELEKOMÜNİKASYON A.Ş..

The contents of this document are protected by copyright laws and international treaties. Any reproduction or distribution of this document or any portion of this document, in any form by any means, without the prior written consent of NETAŞ TELEKOMÜNİKASYON A.Ş is prohibited. Additionally, the contents of this document are protected by contractual confidentiality obligations.

All company, brand and product names are trade or service marks, or registered trade or service marks, of NETAŞ TELEKOMÜNİKASYON A.Ş or of their respective owners.

This document is provided as is, and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. NETAŞ TELEKOMÜNİKASYON A.Ş and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

NETAŞ TELEKOMÜNİKASYON A.Ş or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between NETAŞ TELEKOMÜNİKASYON A.Ş and its licensee, the user of this document shall not acquire any license to the subject matter herein.

NETAŞ TELEKOMÜNİKASYON A.Ş reserves the right to upgrade or make technical change to this product without further notice.

Users may visit the NETAŞ technical support website <https://support.netas.com.tr> to inquire for related information.

The ultimate right to interpret this product resides in NETAŞ TELEKOMÜNİKASYON A.Ş .

Statement on the Use of Third-Party Embedded Software:

If third-party embedded software such as Oracle, Sybase/SAP, Veritas, Microsoft, VMware, and Redhat is delivered together with this product of NETAŞ, the embedded software must be used as only a component of this product. If this product is discarded, the licenses for the embedded software must be void either and must not be transferred. NETAŞ will provide technical support for the embedded software of this product.

## Revision History

Revision No.	Revision Date	Revision Reason
R1.0	2024-12-05	First edition.

Serial Number: SJ-20241203105642-001

Publishing Date: 2024-12-05 (R1.0)

# Contents

---

<b>1 Overview.....</b>	<b>1</b>
1.1 Function.....	1
1.2 Compatibility.....	2
<b>Tool Installation.....</b>	<b>3</b>
2.1 Installation Preparations.....	3
2.2 Installing the UniKits.....	5
<b>Tool Usage.....</b>	<b>9</b>
3.1 Logging In to the UniKits.....	9
3.2 Adding a BMC.....	14
3.2.1 Manually Adding a BMC.....	15
3.2.2 Adding BMCs Through Auto Scan.....	24
3.2.3 Adding BMCs in Batches Through a Configuration File.....	26
3.3 Adding Hosts.....	30
3.3.1 Manually Adding a Host.....	31
3.3.2 Adding Hosts Through Auto Scan.....	33
3.3.3 Adding Hosts in Batches Through a Configuration File.....	35
3.4 Commissioning and Deployment.....	36
3.4.1 BMC Network Parameter Configuration.....	36
3.4.2 BMC (V3) Configuration.....	48
3.4.3 BMC (V4) Configuration.....	90
3.4.4 BIOS Configuration.....	116
3.4.5 RAID Configuration.....	124
3.4.6 Configuration Check.....	130
3.4.7 Configuring Commands.....	139
3.4.8 Controlling Power Supply.....	141
3.4.9 Perform PXE-Based Batch Configuration for a Server.....	143
3.4.10 OS Installation.....	145
3.5 Firmware Upgrade.....	152
3.5.1 Upgrading General Firmware.....	152
3.5.2 Upgrading Standard Cards and Hard Disk Firmware.....	157
3.6 Routine Inspection.....	159
3.6.1 Performing Out-of-Band Inspection.....	159

---

3.6.2 Performing In-Band Inspection.....	162
3.6.3 Collecting Asset Information.....	163
3.6.4 Asset Information Acceptance.....	164
<b>3.7 Troubleshooting.....</b>	<b>169</b>
3.7.1 Collecting and Analyzing BMC Logs Online.....	169
3.7.2 Analyzing BMC Logs Offline.....	171
3.7.3 Collecting Host Logs.....	173
3.7.4 Programming a UUID and Serial Number.....	174
3.7.5 Conducting a Stress Test.....	176
3.7.6 Setting a UID Indicator State.....	181
3.7.7 Clearing Historical BMC Alarms.....	182
<b>3.8 Fault Prediction.....</b>	<b>183</b>
3.8.1 Predicting a Hard Disk Fault.....	183
3.8.2 Predicting Memory Faults.....	184
3.8.3 Predicting Optical Module Faults.....	185
<b>3.9 System Management.....</b>	<b>186</b>
3.9.1 Adding a Local User.....	186
3.9.2 Adding a Domain User.....	188
3.9.3 Adding an LDAP Server.....	190
3.9.4 Importing a License.....	193
3.9.5 Querying Management Logs.....	194
3.9.6 Exporting Operational Logs.....	196
3.9.7 Viewing Version Information.....	196
<b>3.10 Task Center Management.....</b>	<b>197</b>
3.10.1 Creating a Task Schedule.....	197
Viewing Task Execution Records.....	199
<b>4</b>	<b>4</b>
<b>Troubleshooting.....</b>	<b>201</b>
4.1 Information Not Completely Displayed in the Installation Dialog Box.....	201
4.2 Front-End Page Improperly Displayed.....	202
4.3 IPMI Command Failure on a Server with an IPv6 Address.....	203
4.4 IPMI Link Error.....	204
4.5 ISO File Mounting Failure.....	206
4.6 Unable to Find Out the Administrator's DN and the LDAP Directory of the Logged-In User.....	207
4.7 Configuration Migration Failure.....	209
4.8 UniKits Operation Failure in the Windows Server 2012 R2 OS.....	209

4.9 UniKits Operation Failure in the 64-Bit Windows 7 OS.....	210
4.10 Common OS Installation Problems.....	211
4.11 SNMP Link Check.....	212
4.12 Failure in the Standard Card Firmware Upgrade, In-Band RAID Configuration, or Out-of-Band Stress Test.....	214
4.13 Operation Suggestions for Common Errors.....	215
<b>5 Reference: Enabling the SMB/CIFS File Sharing Function.....</b>	<b>217</b>
<b>Figures.....</b>	<b>219</b>
<b>Tables.....</b>	<b>225</b>
<b>Glossary.....</b>	<b>229</b>

# About This Manual

---

## Purpose

This manual describes how to install and use the UniKits tool.

## Intended Audience

This manual is intended for:

- Software commissioning engineers
- Maintenance engineers

## What Is in This Manual

This manual contains the following chapters.

Chapter 1, Overview	Describes the functions and compatibility of the UniKits tool.
Chapter 2, Tool Installation	Describes how to prepare the installation of the UniKits tool and install it.
Chapter 3, Tool Usage	Describes how to use the UniKits tool.
Chapter 4, Troubleshooting	Describes how to troubleshoot common problems related to the UniKits tool.
Chapter 5, Reference: Enabling the SMB/CIFS File Sharing Function	Describes how to enable the SMB/CIFS file sharing function.

## Conventions

This manual uses the following convention.

	Note: provides additional information about a topic.
---	--

# Chapter 1

## Overview

---

### Table of Contents

Function.....	1
Compatibility.....	2

### 1.1 Function

The UniKits is a Web-based lightweight [O&M](#) tool for NETAŞ rack servers and [MEC](#) servers. It improves server provisioning efficiency and reduces O&M workload.

For the O&M functions of the UniKits, refer to [Table 1-1](#).

**Table 1-1 O&M Function Descriptions**

O&M Function	Sub-Function
Commissioning and deployment	<ul style="list-style-type: none"><li>● <a href="#">BMC</a> network configuration</li><li>● BMC configuration</li><li>● <a href="#">BIOS</a> configuration</li><li>● RAID configuration</li><li>● Configuration check</li><li>● Command configuration</li><li>● Power control</li><li>● <a href="#">PXE</a>-based batch configuration</li><li>● <a href="#">OS</a> installation</li></ul> <p>This function is an advanced function and requires a license.</p>
Firmware upgrade	<ul style="list-style-type: none"><li>● General firmware upgrade Supported firmware: BMC, BIOS, <a href="#">EPLD</a>, <a href="#">FRU</a>, and <a href="#">VR</a>.</li><li>● Standard card and hard disk firmware upgrade</li></ul>
Routine inspection	<ul style="list-style-type: none"><li>● Out-of-band inspection</li><li>● In-band inspection</li><li>● Asset collection</li></ul>
Troubleshooting	<ul style="list-style-type: none"><li>● Log collection</li><li>● Parts replacement</li><li>● Stress test</li><li>● UID setting</li></ul>

O&M Function	Sub-Function
	<ul style="list-style-type: none"><li>● Alarm clearing</li></ul>
Fault prediction	<ul style="list-style-type: none"><li>● This function is an advanced function and requires a license.<ul style="list-style-type: none"><li>→ Hard disk fault prediction</li><li>→ Memory fault prediction</li><li>→ Optical module fault prediction</li></ul></li></ul>

## 1.2 Compatibility

The following [OS](#)s support the UniKits:

- Windows 7 (64-bit)
- Windows 10 (64-bit)
- Windows 11 Pro (64-bit)
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

The UniKits supports the following types of devices:

- NCS6712 N4
- NCS6722 N4
- NCS6722 N3
- NCS6722 N4
- NCS6722A N3
- NCS6722A N4
- NCS6742 N4
- NCS6742G N4
- NCS6742 N4
- NCS6744 N4

# Chapter 2

# Tool Installation

---

## Table of Contents

Installation Preparations.....	3
Installing the UniKits.....	5

## 2.1 Installation Preparations

### Hardware Preparation

An installation **PC** with a specified Windows **OS** needs to be prepared. It is used to install the UniKits and acts as the client of the UniKits.



#### Note

For the supported Windows OSs, refer to "[1.2 Compatibility](#)".

The requirements on the hardware of the installation PC are as follows:

- **CPU**: 2 GHz or above
- Memory: 8 GB or above
- Free hard disk space: >10 GB

### Software Preparation

- On the **Tool Zone** page of the Web portal (<https://enterprise.NETAS.com.cn/>) for servers and storage products, download the Windows software installation package of the UniKits to the installation PC.
- On the installation PC, install any of the following browsers:
  - Google Chrome 70 or later
  - Firefox 70 or later
- If the OS of the installation PC is Windows Server 2012 R2, install the *Windows8.1KB2999226-x64.msu* patch package (download link: <https://www.microsoft.com/en-us/download/details.aspx?Id=49063>) before installing the UniKits.

**Note**

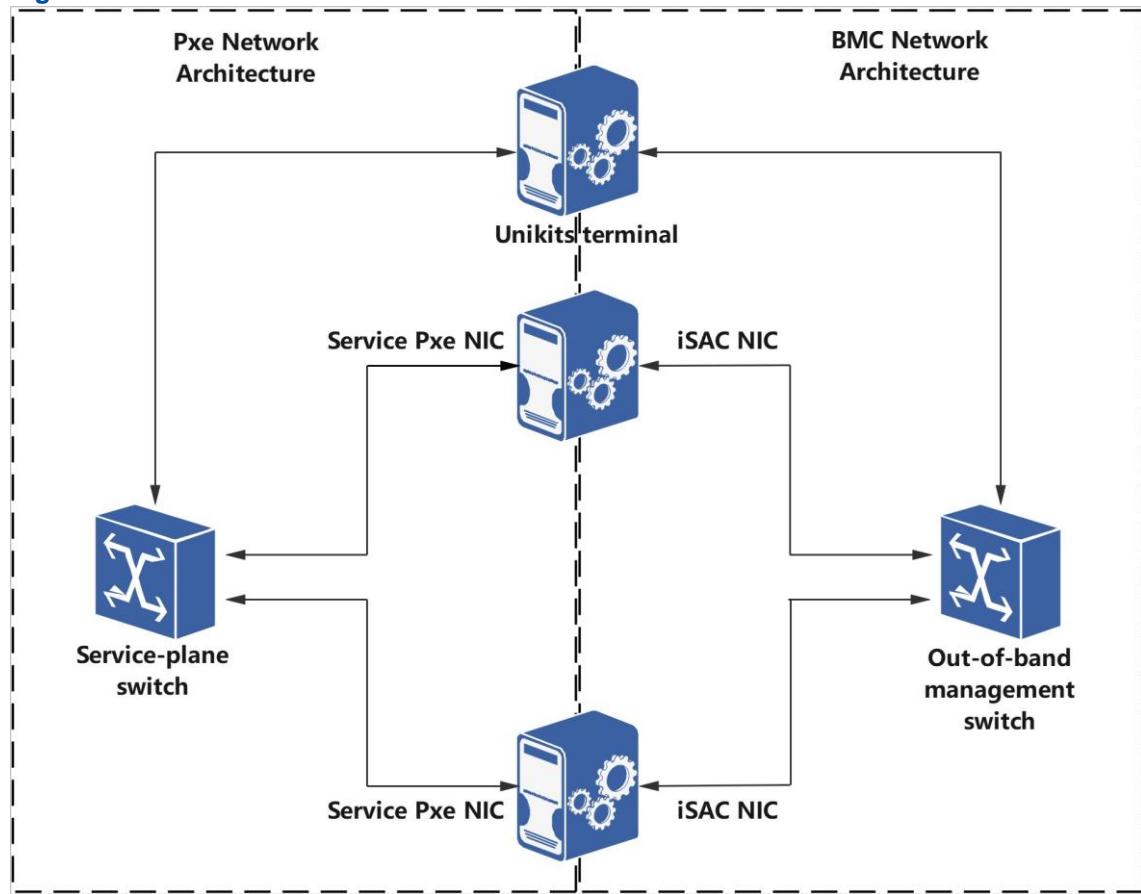
If the patch package is already installed, you can install the UniKits directly.

## Network Preparation

The **BMC** of each server to be maintained must be located in the same **LAN** as the client of the UniKits.

Figure 2-1 shows the network architecture of the UniKits.

**Figure 2-1 Network Architecture**



The network architecture of the UniKits is described as follows:

- If the **PXE**-based batch configuration function is not used, the client of the UniKits does not need to be connected to the service-plane switch. If the function is required, the client of the UniKits needs to be connected to the service-plane switch, and the PXE function needs to be enabled on the service PXE port.
- In the PXE network architecture, you must ensure that the client of the UniKits and the servers to be managed are in the same L2 network without crossing the L3 network.

- In the **BMC** network architecture, you must ensure that the client of the UniKits can access the servers to be maintained, the **IPMI**, **SSH**, **SNMP**, and Redfish links are proper, successfully ping the BMC **IP** address, and communication across the L3 network is supported (excluding the function of configuring a BMC IP address).  
For the default ports of the IPMI, SSH, SNMP, Redfish, **SMB**, and **CIFS** services, refer to **Table 2-1**.

**Table 2-1 Default Ports of Common Services**

Service	Default Port
IPMI	623
SSH	22
SNMP	161
BMC Web interface (Redfish)	443
SMB	139
CIFS	445

**Note**

On the Web portal of the BMC for the server to be maintained, you can view the valid port of each service on the page displayed after you select **Service > Port Services**.

- If **Configure the IP address in DHCP mode** is used, the UniKits starts a DHCPv6 server. The DHCPv6 server and the client (server to be configured) exchange DHCPv6 packets through **UDP**. The client uses UDP port 546 while the server uses UDP port 547.

## 2.2 Installing the UniKits

### Abstract

You can maintain servers through the client of the UniKits only after installing the UniKits on the installation PC.

### Steps

1. On the installation PC, extract UniKits the installation package.

---

2. Double-click the UniKits installation file. The installation dialog box is displayed, see [Figure 2-2](#).

**Figure 2-2 Installing the UniKits**



Before installation, the installer automatically detects the following items:

- **Hardware configuration**

For recommended configurations, refer to "[2.1 Installation Preparations](#)".

If the configuration requirements are not met, an exclamation mark is displayed before a detection item. The installation of the UniKits is not affected, but the user experience is affected.

- **Firewall**

If the firewall is not disabled, click **Close Firewall** in the displayed dialog box. If the firewall fails to be disabled automatically, the required permission may not be granted. In this case, you need to manually disable the firewall. If the firewall is not disabled, the installation of the UniKits is not affected, but the **PXE**-based batch configuration function is affected.

- **Port**

Port 9100 is used by default. If the default port is already used, the tool automatically selects an idle port ranging from 9100 through 10000.

- **Browser**

If the Firefox or Google browser is installed on the installation PC, the detection is passed.

**ZTE**

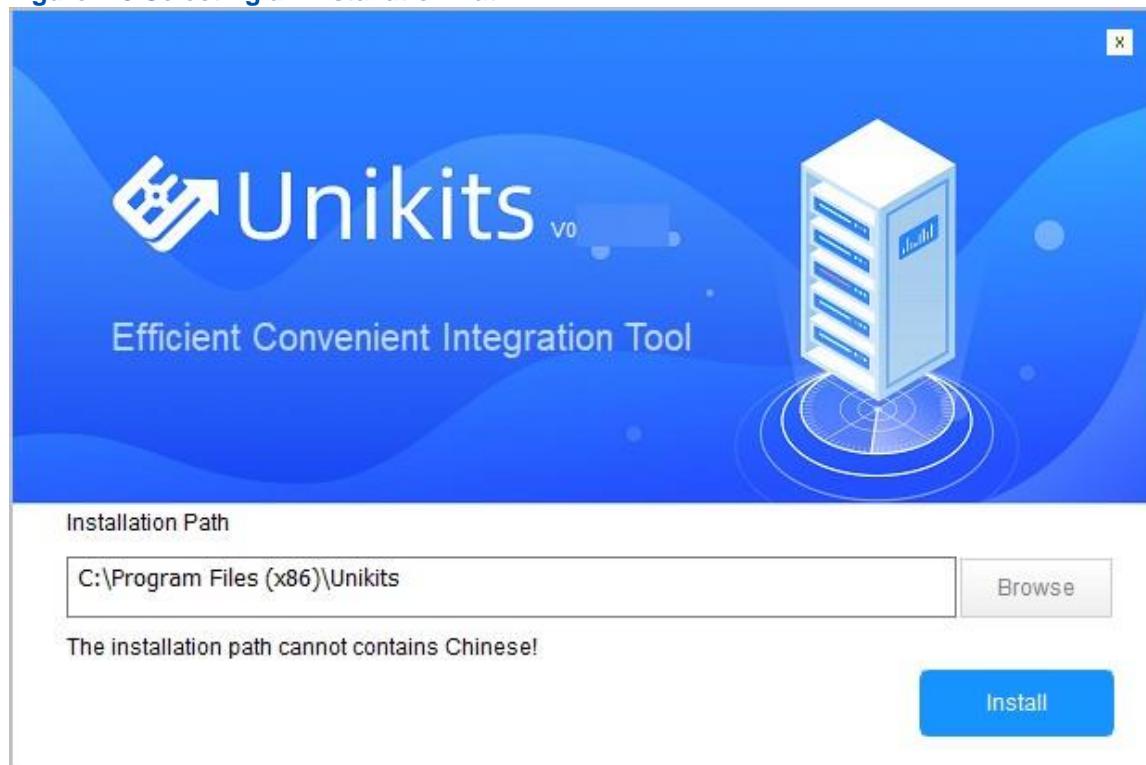
2 Tool Installation



A portable browser is not recommended.

3. Click **Next Step**. The dialog box for selecting an installation path is displayed, see [Figure 2-3](#).

**Figure 2-3 Selecting an Installation Path**



4. (Optional) Click **Browse** and then select the desired tool installation path.
5. Click **Install**.
6. Perform the following operations as required.

To...	Do...
Exit the installer	Click <b>Done</b> .
Start the UniKits	Click <b>Start</b> .

## Result

After the installation is completed, a shortcut icon like  is displayed on the desktop of the installation PC.

## Related Tasks

To upgrade or uninstall the UniKits, perform the following operations:

- Upgrading the UniKits
  1. Download the latest UniKits installation package.
  2. Upgrade the UniKits by referring to the UniKits installation procedure.



### Note

The installation path selected for upgrading the UniKits must be the same as that selected for installing the UniKits.

- Uninstalling the UniKits

1. In the **Start** menu on the installation PC, find the UniKits that is already installed.
2. Click the  icon.



### Note

If the UniKits is running, click **Confirm** in the displayed dialog box to close the UniKits and continue to uninstall it.

3. Click **Uninstall**.
4. Click **Finish**.

# Chapter 3

# Tool Usage

---

## Table of Contents

Logging In to the UniKits.....	9
Adding a BMC.....	14
Adding Hosts.....	30
Commissioning and Deployment.....	36
Firmware Upgrade.....	152
Routine Inspection.....	159
Troubleshooting.....	169
Fault Prediction.....	183
System Management.....	186
Task Center Management.....	197

## 3.1 Logging In to the UniKits

### Abstract

You can add a device and maintain it only after you log in to the UniKits.

### Context

Only users with the guest role can log in to the UniKits. Users with the administrator or operator role are not supported.

The default guest user is created by the UniKits automatically. The default username and password of the guest user are as follows:

- Username: guest
- Password: Superuser9!

If the UniKits is upgraded from a version earlier than V01.24.02.01 to V01.24.02.01 or later, and the guest user already exists in the previous version, the guest user is not automatically created by the UniKits. During login, if the guest user is not assigned the guest role in the previous version, after the correct password is entered, a message box is displayed, prompting the user to modify the corresponding permission.

## Steps

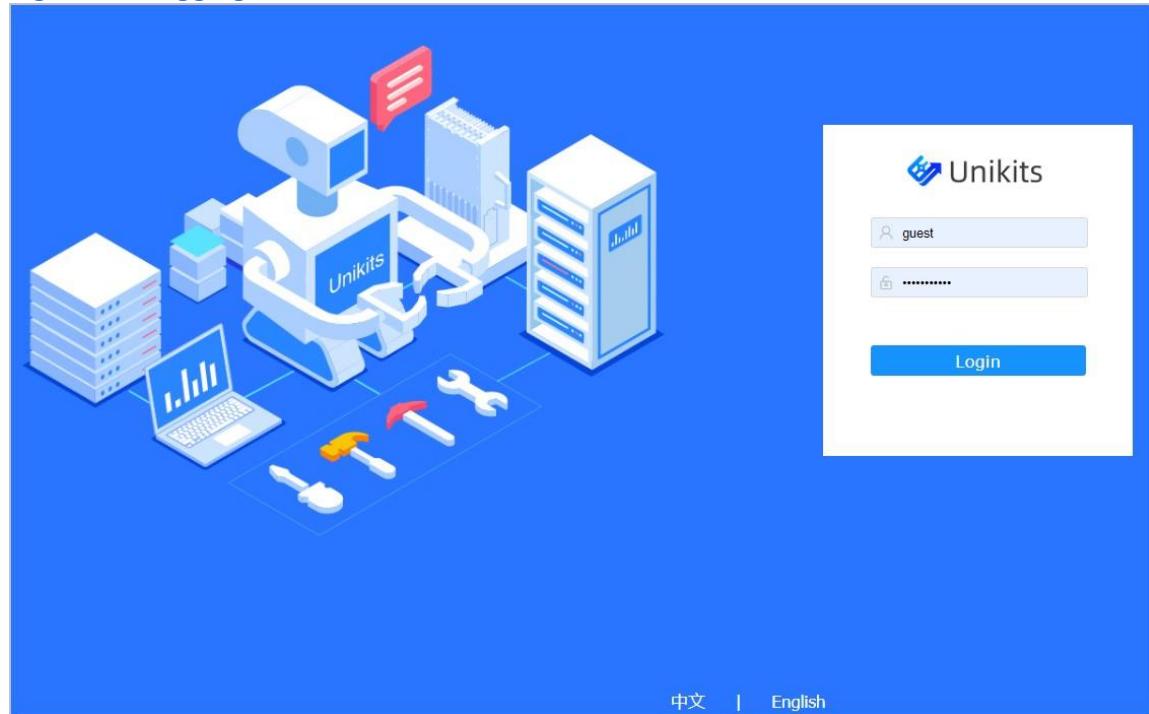
### Logging In to the UniKits as a Guest User

1. On the desktop of the PC, double-click  the icon. The page for logging in to the UniKits is displayed, see [Figure 3-1](#).



If you have logged in to the installation PC as a non-administrator user, right-click the  icon, and select **Run as administrator** from the shortcut menu.

**Figure 3-1 Logging In to the UniKits**



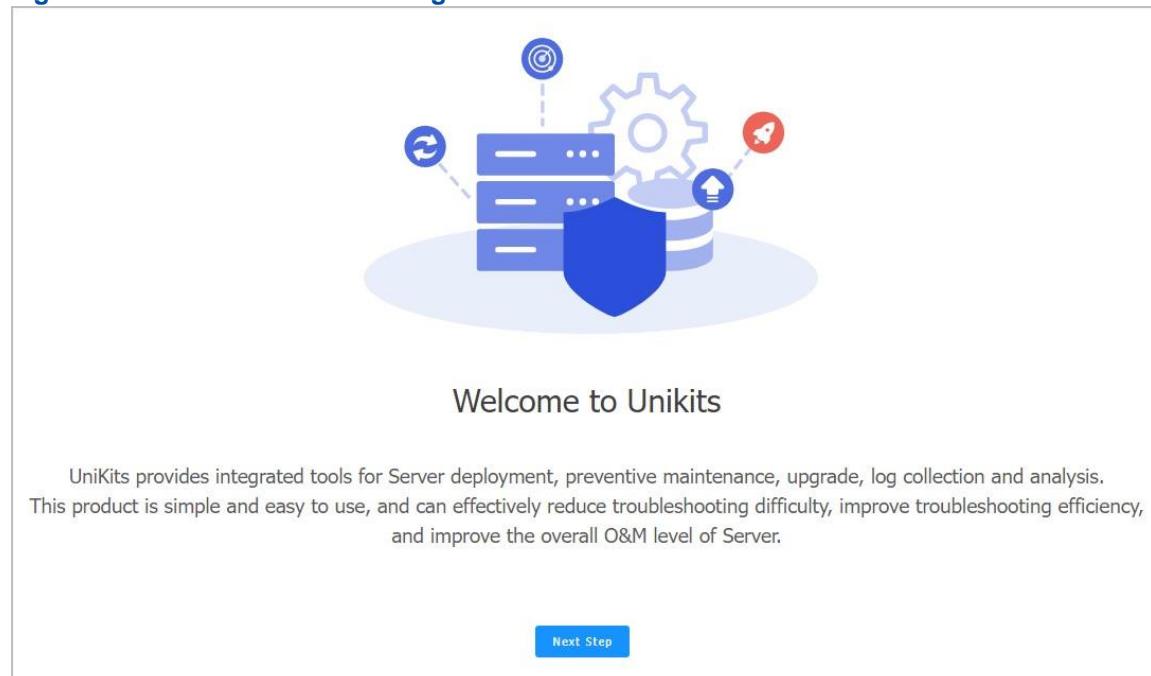
2. Enter your username and password.



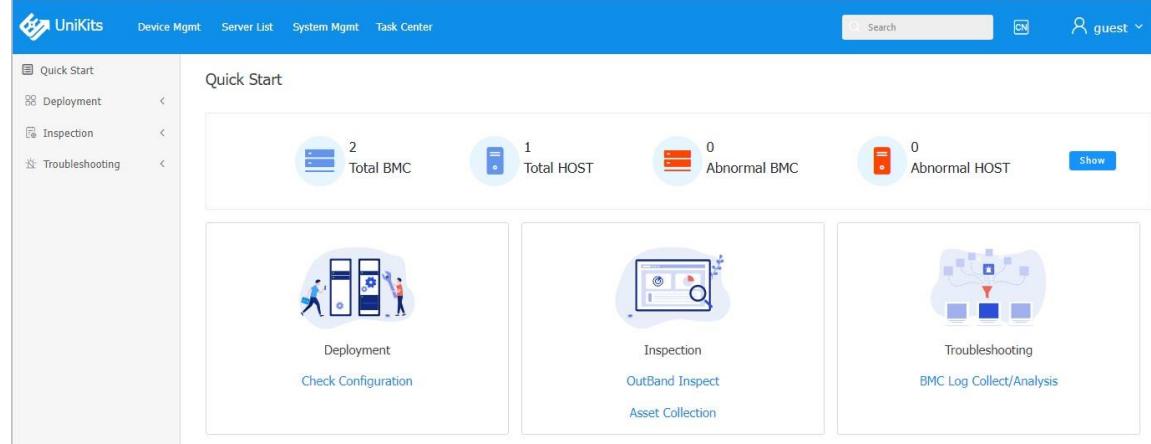
The default username and password of the guest user are as follows:

- Username: guest
- Password: Superuser9!

3. Click **Login**. The **Welcome to UniKits** page is displayed, see [Figure 3-2](#).

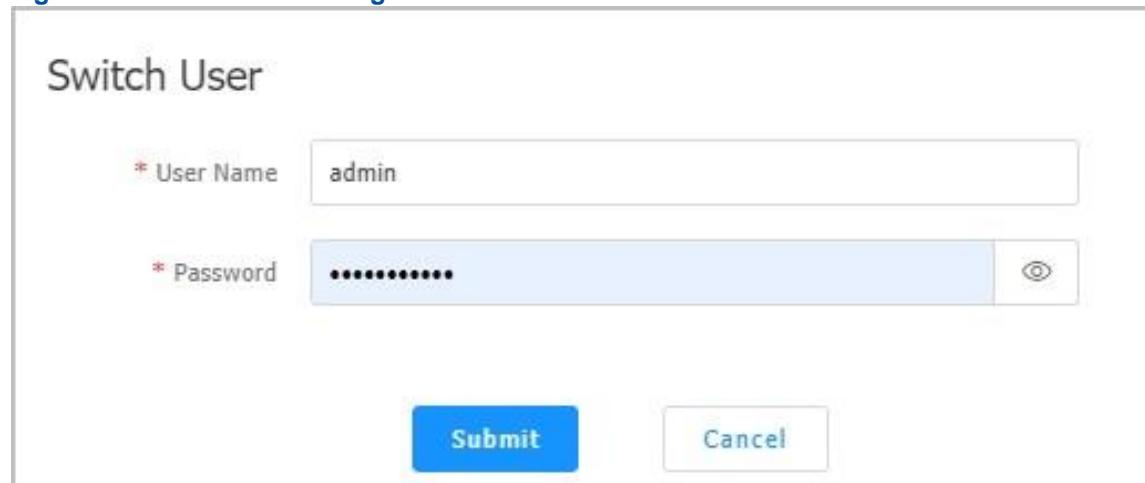
**Figure 3-2 Welcome to UniKits Page**

4. Click **Next Step** to log in to the UniKits. The **Quick Start** page is displayed, as shown in [Figure 3-3](#).

**Figure 3-3 Quick Start Page—Guest User**

### Switching to a User with the Administrator Role

5. Click **guest** in the upper right corner and select **Switch User** from the drop-down list. The **Switch User** dialog box is displayed, as shown in [Figure 3-4](#).

**Figure 3-4 Switch User Dialog Box**

---

**6. Set User Name and Password.**

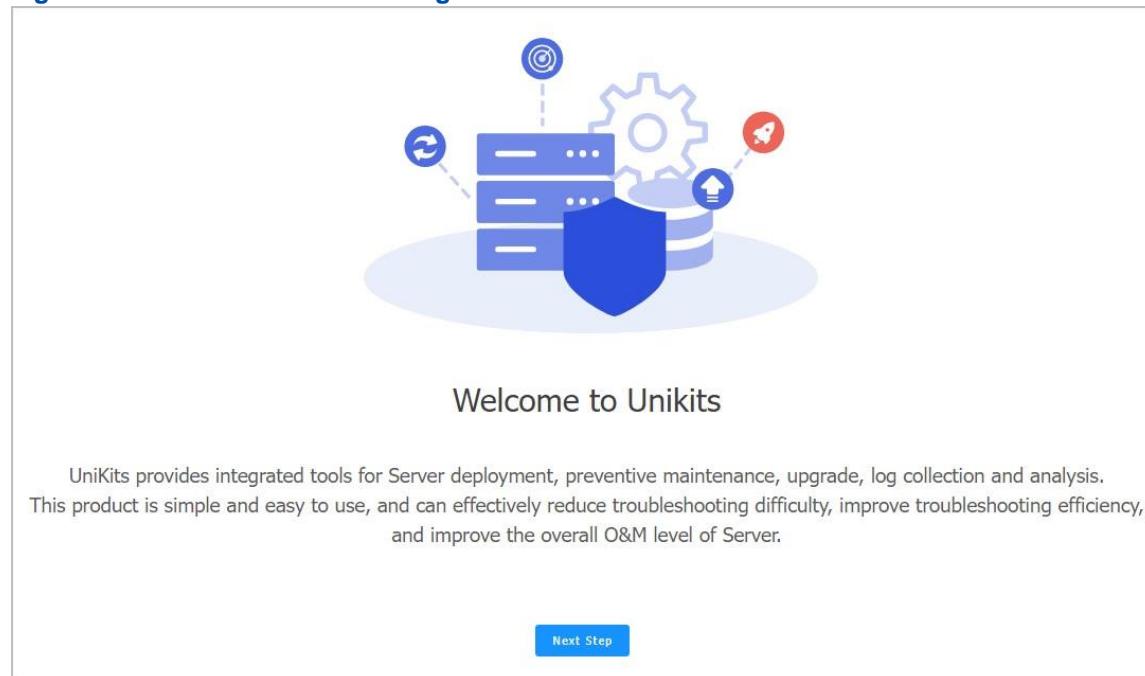
---

**Note**

The default username and password of the administrator are as follows:

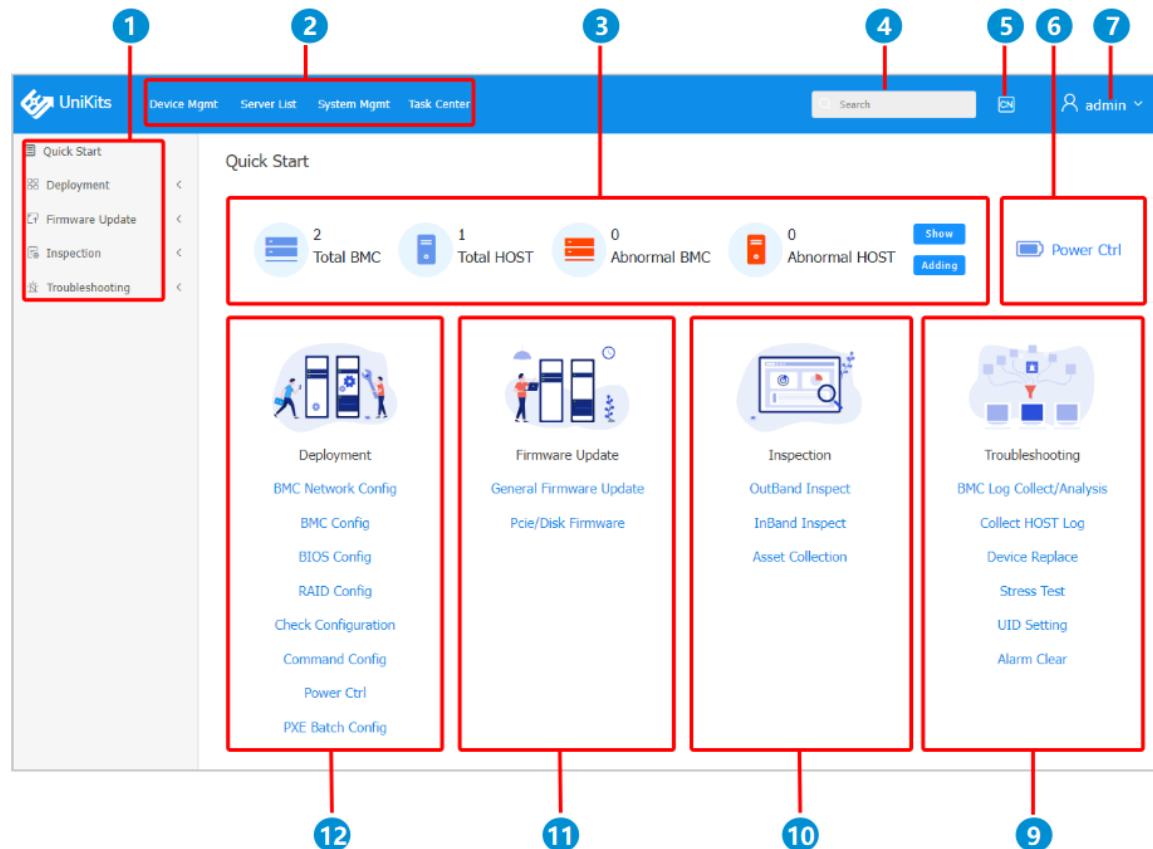
- Username: admin
- Password: Superuser9!

---

**7. Click Submit. The Welcome to UniKits page is displayed, as shown in Figure 3-5.****Figure 3-5 Welcome to UniKits Page**

---

**8. Click Next Step. The Quick Start page is displayed, as shown in Figure 3-6.**

**Figure 3-6 Quick Start Page—Administrator**

For a description of the **Quick Start** page, refer to [Table 3-1](#).

**Table 3-1 Quick Start Page Descriptions**

No.	Name	Description
1	Navigation tree	Displays the sub-menus under each main menu.
2	Menu bar	Main menus. Displays all the sub-menus in the format of a navigation tree in the left pane after you click any main menu on the menu bar.

3	Device overview area	<p>Displays the overview of all the devices maintained through the UniKits.</p> <ul style="list-style-type: none"> <li>• To view the details of all the devices, click <b>Show</b>. The <b>Server List</b> page is displayed, showing the device details.</li> <li>• To add a device, click <b>Adding</b> and select the desired option from the shortcut menu.</li> </ul> <p>The options in the shortcut menu include:</p> <ul style="list-style-type: none"> <li>→ <b>Adding BMC</b> For details, refer to "<a href="#">3.2 Adding a BMC</a>".</li> <li>→ <b>Add HOST</b> For details, refer to "<a href="#">3.3 Adding Hosts</a>".</li> </ul>
No.	Name	Description
4	Search box	Not supported.
5	Language button	Allows you to change the language.
6	Power control area	<p>Allows you to control the power supply of device after you click <b>Power Ctrl</b> and enter the <b>Power Ctrl</b> page.</p> <p>For details, refer to "<a href="#">3.4.8 Controlling Power Supply</a>".</p>
7	Current user	<p>Displays the currently logged-in user.</p> <ul style="list-style-type: none"> <li>• To view the details of the currently logged-in user, hover the mouse cursor over this button.</li> <li>• To change the password of the currently logged-in user, click <b>Modify Password</b> in the information box displayed after you hover the mouse cursor over this button.</li> <li>• To switch to another user, click <b>Switch User</b> in the information box displayed after you hover the mouse cursor over this button.</li> <li>• To log out the currently logged-in user, click <b>LogOut</b> in the information box displayed after you hover the mouse cursor over this button.</li> </ul>
8	Troubleshooting area	<p>Allows you to troubleshoot devices.</p> <p>For details, refer to "<a href="#">3.7 Troubleshooting</a>".</p>
9	Routine inspection area	<p>Allows you to inspect devices.</p> <p>For details, refer to "<a href="#">3.6 Routine Inspection</a>".</p>
10	Firmware upgrade area	<p>Allows you to upgrade firmware of devices.</p> <p>For details, refer to "<a href="#">3.5 Firmware Upgrade</a>".</p>
11	Deployment area	<p>Allows you to deploy devices.</p> <p>For details, refer to "<a href="#">3.4 Commissioning and Deployment</a>".</p>

## Related Tasks

To exit the UniKits that runs in the background, perform the following operations:

1. In the system tray on the desktop of the installation PC, right-click the  icon, and select **Exit** from the shortcut menu.
2. In the displayed message box, click **Yes**.

## 3.2 Adding a BMC

A **BMC** is the management module of a server. The **CPU**, bridge chip, **EPLD**, and sensors on the boards of the server are connected to the BMC through different channels for out-of-band management.

After a BMC is added, you can manage and maintain the out-of-band functions of the corresponding server through the UniKits.

One or more BMCs can be added through any of the following ways:

- Manually adding a BMC

Use this way if you add the BMC of a single server. For details, refer to "[3.2.1 Manually Adding a BMC](#)".

- Adding BMCs through auto-scan

Use this way if you add BMCs of multiple servers of the same model that are in the same network segment. For details, refer to "[3.2.2 Adding BMCs Through Auto Scan](#)".

- Adding BMCs in batches

Use this way if you add BMCs of a large number of servers. For details, refer to "[3.2.3 Adding BMCs in Batches Through a Configuration File](#)".



### Note

- When a BMC is manually added or BMCs are added through auto-scan, link diagnosis is automatically performed. If the diagnosis fails, the BMC(s) cannot be added. When BMCs are added in batches, whether link diagnosis is performed can be controlled through parameters.
- If the "Redfish error: get cpu model failed" message is displayed when the BMCs of the servers (for example, NCS6722A N3) that share the same mainboard, you need to check whether the hosts of the servers are powered on. If the hosts are not powered on, the **CPU** models cannot be obtained.

## 3.2.1 Manually Adding a BMC

### Abstract

This procedure describes how to manually configure the parameters for the **BMC** of a server so that the BMC of the server can be added.

## Prerequisite

The BMC IP address configured for the server before delivery is modified. For details, refer to "[3.4.1.1 Configuring a BMC IP Address](#)".

## Steps

1. Use either of the following methods to access the **Adding BMC** page.
  - Access it from the **Quick Start** page
    - a. Select **Device Mgmt > Quick Start**. The **Quick Start** page is displayed.
    - b. In the device overview area, click **Add Server** and select **Adding BMC** from the shortcut menu.
  - Access it from the **Server List** page
    - a. Select **Server List**. The **Server List** page is displayed.
    - b. On the **BMC** tab, click **Add Server**.

2. Set the parameters.

The parameters on the **Adding BMC** page vary with the selected server models and [SNMP](#) versions. Common configuration examples are as follows:

- [Figure 3-7](#) shows a configuration example of a G5 server.

**Figure 3-7 Manually Adding the BMC of a G5 Server**

Adding BMC

**Basic Parameters**

Adding Mode  Manual  Auto Scan  Batch Import

Server Name: R5300 G5

\* ISAC IP: 10.10.10.2

Group Name: Please enter group name, uniview is reserved

\* Server Type: R5300 G5E

When AutoDetect is selected, manual configuration is recommended.

**Setting Parameters**

Setting Type  Manual Mode  Default Mode

\* IPMI User Name: zteroot

\* IPMI password:  

SSH User Name: sysadmin

SSH Password:  

SSH Port: 22

**Buttons**

**Submit** **Cancel**

For a description of the parameters, refer to [Table 3-2](#).

**Table 3-2 Parameter Descriptions for Manually Adding the BMC of a G5 Server**

Parameter	Description
<b>Basic Parameters</b>	
Adding Mode	Select <b>Manual</b> .
Server Name	Enter the name of the server that you want to add.
iSAC IP	Enter the BMC IP address of the server.
Group Name	Set a group name for the server. In this way, you can filter servers by group name. <b>uniview</b> is the reserved group name and you cannot use it.
Parameter	Description
Server Type	Select the server type. For an <b>OEM</b> server, select <b>AutoDetect</b> . If <b>Server Type</b> is set to <b>AutoDetect</b> , it is recommended that <b>Setting Type</b> be set to <b>Manual Mode</b> .
<b>Setting Parameters</b>	
Setting Type	Select a configuration mode. Options: → <b>Default Mode</b> : The default configuration parameters of the server are used. It is recommended that this mode be used in the scenario where the parameters are not modified during commissioning. → <b>Manual Mode</b> : You need to manually set the parameters. It is recommended that this mode be used when parameters are already modified after commissioning.
IPMI User Name	The UniKits communicates with the server through the IPMI. Enter a username with the administrator or operator permissions. The usernames can be viewed on the Web portal of the BMC. It is recommended that you enter a username with the administrator permissions. For different server models, the paths for viewing the usernames are different: → For a server of the G5 model, select <b>User &amp; Security &gt; Local Users</b> . → For a server of other models, select <b>Settings &gt; Group Management &gt; Group Management Configuration</b> .
IPMI password	Enter the password of the IPMI user.

SSH User Name	The UniKits communicates with the server through SSH. Enter the BMC administrator username. Default: <code>sysadmin</code> .
SSH Password	<p>Enter the password of the SSH user. The default password depends on the BMC version.</p> <p>→ BMC V3: The default password is <code>superuser</code> for versions prior to V03.20.11.02, and that is <code>Superuser@123</code> for V03.20.11.02 and later.</p> <p>→ BMC V4: The default password is <code>superuser</code> for versions prior to V04.23.01.02, and that is <code>Superuser@123</code> for V04.23.01.02 and later.</p>
SSH Port	Enter the SSH port number of the server. Default: 22.

- Figure 3-8 shows an example of configuration in the SNMPv2 scenario.

**Figure 3-8 Manually Adding the BMC of a Server in the SNMPv2 Scenario**

Adding BMC

**Basic Parameters**

Adding Mode  Manual  Auto Scan  Batch Import

Server Name: R5300 G4

\* iSAC IP: 10.10.10.2

? Group Name: Please enter group name, uniview is reserved

\* ② Server Type: R5300 G4

When AutoDetect is selected, manual configuration is recommended...

**Setting Parameters**

② Setting Type  Default Mode  Manual Mode

\* IPMI User Name: zteroot

\* IPMI password:

SNMP Protocol  SNMP V2  SNMP V3

\* SNMP Read Community: zte\_public

\* SNMP Read/Write Community: platform

\* SNMP Port: 161

SSH User Name: sysadmin

SSH Password:

SSH Port: 22

For a description of the parameters, refer to [Table 3-3](#).

**Table 3-3 Parameter Descriptions for Manually Adding the BMC of a Server in the SNMPv2 Scenario**

Parameter	Description
<b>Basic Parameters</b>	
Adding Mode	Select <b>Manual</b> .
Server Name	Enter the name of the server that you want to add.
iSAC IP	Enter the BMC IP address of the server.
Group Name	Set a group name for the server. In this way, you can filter servers by group name. <b>uniview</b> is the reserved group name and you cannot use it.
Server Type	Select the server type.

Parameter	Description
	For an <b>OEM</b> server, select <b>AutoDetect</b> . If <b>Server Type</b> is set to <b>AutoDetect</b> , it is recommended that <b>Setting Type</b> be set to <b>Manual Mode</b> .
<b>Setting Parameters</b>	
Setting Type	Select a configuration mode. Options: → <b>Default Mode</b> : The default configuration parameters of the server are used. It is recommended that this mode be used in the scenario where the parameters are not modified during commissioning. → <b>Manual Mode</b> : You need to manually set the parameters. It is recommended that this mode be used when parameters are already modified after commissioning.
IPMI User Name	The UniKits communicates with the server through the IPMI. Enter a username with the administrator or operator permissions. The usernames can be viewed on the Web portal of the BMC. It is recommended that you enter a username with the administrator permissions. For different server models, the paths for viewing the usernames are different: → For a server of the G5 model, select <b>User &amp; Security &gt; Local Users</b> . → For a server of other models, select <b>Settings &gt; Group Management &gt; Group Management Configuration</b> .
IPMI password	Enter the password of the IPMI user.

SNMP Protocol	Select <b>SNMP V2</b> .
SNMP Read Community	<p>Enter the SNMP read-only community of the server. Default: <i>NETAS_public</i>.</p> <p>For different server models, the methods for viewing the SNMP readonly community are different.</p> <ul style="list-style-type: none"> <li>→ For a server of the G4X model, log in to the BMC of the server through SSH, and run the following command:</li> </ul> <pre># cat /conf/snmp_users.conf</pre> <p>In the command output, the character string displayed next to <b>rocommunity</b> is the read-only community.</p> <ul style="list-style-type: none"> <li>→ For a server of other models, log in to the Web portal of the BMC of the server, and select <b>Settings &gt; SNMP Configurations &gt; SNMP Community</b>.</li> </ul>
SNMP Read/Write Community	<p>Enter the SNMP read-write community of the server. Default: <i>platform</i>.</p> <p>For different server models, the methods for viewing the SNMP readwrite community are different.</p>
Parameter	<b>Description</b>
	<ul style="list-style-type: none"> <li>→ For a server of the G4X model, log in to the BMC of the server through SSH, and run the following command:</li> </ul> <pre># cat /conf/snmp_users.conf</pre> <p>In the command output, the character string displayed next to <b>rwcommunity</b> is the read-write community.</p> <ul style="list-style-type: none"> <li>→ For a server of other models, log in to the Web portal of the BMC of the server, and select <b>Settings &gt; SNMP Configurations &gt; SNMP Community</b>.</li> </ul>
SNMP Port	Enter the SNMP port number of the server. You can log in to the Web portal of the BMC, and select <b>Settings &gt; Services</b> to view the port number. Default: <i>161</i> .
SSH User Name	The UniKits communicates with the server through SSH. Enter the BMC administrator username. Default: <i>sysadmin</i> .
SSH Password	<p>Enter the password of the SSH user. The default password depends on the BMC version.</p> <ul style="list-style-type: none"> <li>→ BMC V3: The default password is <i>superuser</i> for versions prior to V03.20.11.02, and that is <i>Superuser@123</i> for V03.20.11.02 and later.</li> <li>→ BMC V4: The default password is <i>superuser</i> for versions prior to V04.23.01.02, and that is <i>Superuser@123</i> for V04.23.01.02 and later.</li> </ul>

SSH Port	Enter the SSH port number of the server. Default: 22.
----------	---

- [Figure 3-9](#) shows an example of configuration in the SNMPv3 scenario.

### Figure 3-9 Manually Adding the BMC of a Server in the SNMPv3 Scenario

Adding BMC

**Basic Parameters**

Adding Mode  Manual  Auto Scan  Batch Import

Server Name: R530 G4

\* iSAC IP: 10.10.10.2

① Group Name: Please enter group name, uniview is reserved

\* ② Server Type: R530 G4

When AutoDetect is selected, manual configuration is recommended.

**Setting Parameters**

① Setting Type  Default Mode  Manual Mode

\* IPMI User Name: zteroot

\* IPMI password:  

SNMP Protocol  SNMP V2  SNMP V3

\* SNMP User Name: zteroot

Ensure that the input user SNMP access level is read/write access. Otherwise, some configuration functions cannot be used.

\* SNMP Port: 161

Security Level: Authentication and encryption

\* SNMP authentication protocol: SHA

\* SNMP authentication protocol password:  

\* SNMP Private Protocol: AES

\* SNMP Private Protocol Password:  

SSH User Name: sysadmin

SSH Password:  

SSH Port: 22

**Buttons**

For a description of the parameters, refer to [Table 3-4](#).

**Table 3-4 Parameter Descriptions for Manually Adding the BMC of a Server in the SNMPv3 Scenario**

Parameter	Description
<b>Basic Parameters</b>	
Adding Mode	Select <b>Manual</b> .
Server Name	Enter the name of the server that you want to add.
iSAC IP	Enter the BMC IP address of the server.

Group Name	Set a group name for the server. In this way, you can filter servers by group name. <b>uniview</b> is the reserved group name and you cannot use it.
Server Type	Select the server type. For an <b>OEM</b> server, select <b>AutoDetect</b> .

Parameter	Description
	If <b>Server Type</b> is set to <b>AutoDetect</b> , it is recommended that <b>Setting Type</b> be set to <b>Manual Mode</b> .
<b>Setting Parameters</b>	
Setting Type	Select a configuration mode. Options: → <b>Default Mode</b> : The default configuration parameters of the server are used. It is recommended that this mode be used in the scenario where the parameters are not modified during commissioning. → <b>Manual Mode</b> : You need to manually set the parameters. It is recommended that this mode be used when parameters are already modified after commissioning.
IPMI User Name	The UniKits communicates with the server through the IPMI. Enter a username with the administrator or operator permissions. The usernames can be viewed on the Web portal of the BMC. It is recommended that you enter a username with the administrator permissions. For different server models, the paths for viewing the usernames are different: → For a server of the G5 model, select <b>User &amp; Security &gt; Local Users</b> . → For a server of other models, select <b>Settings &gt; Group Management &gt; Group Management Configuration</b> .
IPMI password	Enter the password of the IPMI user.
SNMP Protocol	Select <b>SNMP V3</b> .
SNMP User Name	Enter a username with the administrator permissions. You can log in to the Web portal of the BMC, and select <b>Settings &gt; Group Management &gt; Group Management Configuration</b> to view the usernames.
SNMP Port	Enter the SNMP port number of the server. You can log in to the Web portal of the BMC, and select <b>Settings &gt; Services</b> to view the port number. Default: 161.

Security Level	Default: <b>Authentication and encryption</b> , which does not need to be modified.
SNMP authentication protocol	Set the authentication protocol for SNMPv3. Options: <a href="#">MD5</a> and <a href="#">SHA</a> . You can log in to the Web portal of the BMC, and select <b>Settings &gt; Group Management &gt; Group Management Configuration</b> to view the authentication protocols. Note: You need to select the administrator user group for the view.
SNMP authentication protocol password	Enter the password of the SNMP user.
<b>Parameter</b>	<b>Description</b>
SNMP Private Protocol	Set the privacy protocol for SNMPv3. Options: <a href="#">DES</a> and <a href="#">AES</a> . You can log in to the Web portal of the BMC, and select <b>Settings &gt; Group Management &gt; Group Management Configuration</b> to view the privacy protocols. Note: You need to select the administrator user group for the view.
SNMP Private Protocol Password	Enter the password of the SNMP user.
SSH User Name	The UniKits communicates with the server through SSH. Enter the BMC administrator username. Default: <i>sysadmin</i> .
SSH Password	Enter the password of the SSH user. The default password depends on the BMC version. → BMC V3: The default password is <i>superuser</i> for versions prior to V03.20.11.02, and that is <i>Superuser@123</i> for V03.20.11.02 and later. → BMC V4: The default password is <i>superuser</i> for versions prior to V04.23.01.02, and that is <i>Superuser@123</i> for V04.23.01.02 and later.
SSH Port	Enter the SSH port number of the server. Default: 22.



### Note

If the IPMI username is the one with the administrator permissions, the following three passwords (namely, the password for the administrator to log in to the Web portal of the BMC) must be the same:

- IPMI password
- SNMP authentication protocol password → SNMP Private Protocol Password

---

### 3. Click **Submit**.

## Related Tasks

On the **BMC** tab of the **Server List** page, perform the following operations as required.

To...	Do...
View the information about abnormal BMCs	Click <b>Abnormal BMC</b> . The <b>Viewing the Abnormal List</b> dialog box is displayed.
Modify the information about a BMC	<ol style="list-style-type: none"> <li>1. Click <b>More</b> in the <b>Operation</b> column for the BMC, and select <b>Edit</b> from the shortcut menu. The <b>Update Server Info</b> dialog box is displayed.</li> <li>2. Modify the information about the BMC.</li> </ol>
To...	Do...
	<p>3. Click <b>Submit</b>.</p> <p>Note: If any parameter other than <b>Server Name</b> and <b>Group Name</b> is modified, link diagnosis for the server is automatically triggered and the diagnosis result is updated accordingly on the page.</p>
Refresh the information about a BMC	Click <b>More</b> in the <b>Operation</b> column for the BMC, and select <b>Refresh</b> from the shortcut menu.
Export BMC information	<ol style="list-style-type: none"> <li>1. Select the desired BMCs.</li> <li>2. Click <b>Export Server List</b>.</li> </ol>
Delete BMCs	<ol style="list-style-type: none"> <li>1. Select the desired BMCs.</li> <li>2. Click <b>Remove Server</b>.</li> </ol> <p>Note: After a BMC is deleted, the deletion operation cannot be rolled back. If the BMC is needed, you can only add it again.</p>

### 3.2.2 Adding BMCs Through Auto Scan

#### Abstract

This procedure describes how to add the **BMC**s of servers of the same model that are in the same network segment through auto scan.

#### Prerequisite

The BMC **IP** addresses configured for the servers before delivery are modified. For details, refer to "[3.4.1.1 Configuring a BMC IP Address](#)".

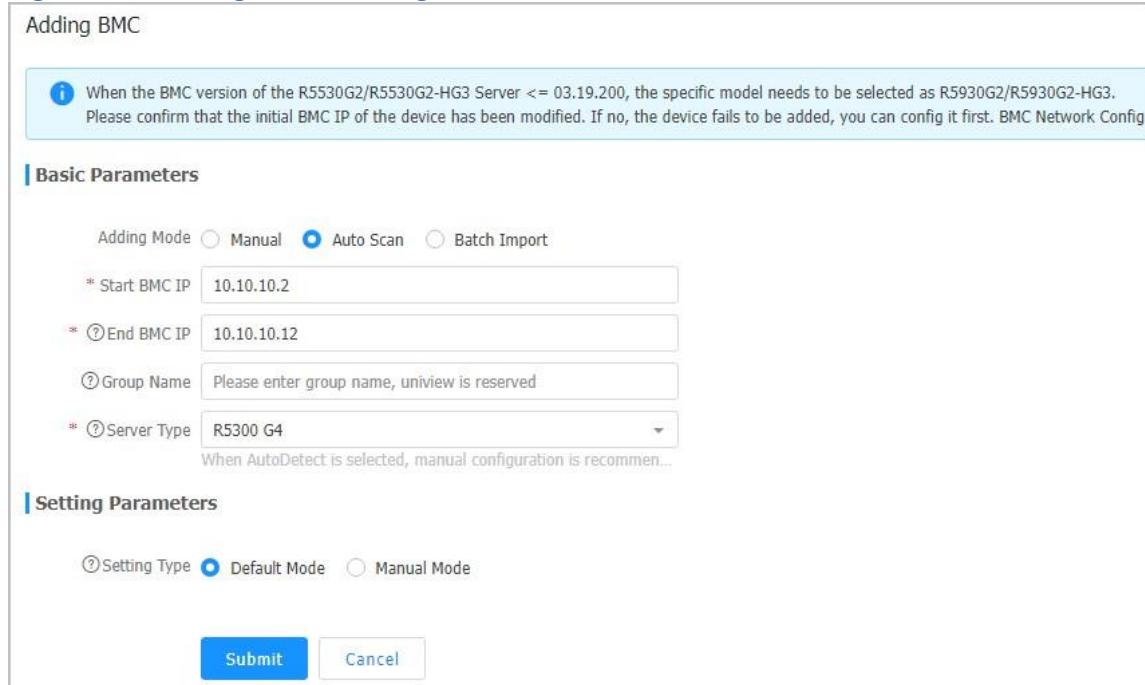
#### Steps

1. Use either of the following methods to access the **Adding BMC** page (see [Figure 3-10](#)):

- Access it from the **Quick Start** page

- a. Select **Device Mgmt > Quick Start**. The **Quick Start** page is displayed.
- b. In the device overview area, click **Adding** and select **Adding BMC** from the shortcut menu.
- Access it from the **Server List** page
  - a. Select **Server List**. The **Server List** page is displayed.
  - b. On the **BMC** tab, click **Add Server**.

**Figure 3-10 Adding BMCs Through Auto-Scan**



Adding BMC

**Basic Parameters**

Adding Mode  Manual  Auto Scan  Batch Import

\* Start BMC IP: 10.10.10.2

\* End BMC IP: 10.10.10.12

Group Name: Please enter group name, uniview is reserved

\* Server Type: R5300 G4

When AutoDetect is selected, manual configuration is recommended.

**Setting Parameters**

Setting Type  Default Mode  Manual Mode

**Submit** **Cancel**

2. Set the parameters. For a description of the parameters, refer to [Table 3-5](#).

**Table 3-5 Parameter Descriptions for Adding BMCs Through Auto-Scan**

Parameter	Description
<b>Basic Parameters</b>	
Adding Mode	Select <b>Auto Scan</b> .
Start BMC IP	Enter the start BMC IP address of the network segment to be scanned.
End BMC IP	Enter the end BMC IP address of the network segment to be scanned. <b>Start BMC IP</b> and <b>End BMC IP</b> must be in the same network segment, and <b>Start BMC IP</b> needs to be configured first.

Group Name	Set a group name for the newly added servers. In this way, you can filter servers by group name. <b>uniview</b> is the reserved group name and you cannot use it.
Server Type	Select the type of servers to be added. For an <b>OEM</b> server, select <b>AutoDetect</b> . If <b>Server Type</b> is set to <b>AutoDetect</b> , it is recommended that <b>Setting Type</b> be set to <b>Manual Mode</b> .



### Note

The parameters in the **Setting Parameters** area are configured in the same way as those configured for manually adding a BMC. For details, refer to "[3.2.1 Manually Adding a BMC](#)".

3. Click **Submit**.

## 3.2.3 Adding BMCs in Batches Through a Configuration File

### Abstract

This procedure describes how to add **BMCs** of servers in batches by importing a configuration file.

### Prerequisite

The BMC **IP** addresses configured for the servers before delivery are modified. For details, refer to "[3.4.1.1 Configuring a BMC IP Address](#)".

### Steps

1. Use either of the following methods to access the **Adding BMC** page (see [Figure 3-11](#)):

- Access it from the **Quick Start** page
  - a. Select **Device Mgmt > Quick Start**. The **Quick Start** page is displayed.
  - b. In the device overview area, click **Add Server** and select **Adding BMC** from the shortcut menu.
- Access it from the **Server List** page
  - a. Select **Server List**. The **Server List** page is displayed.
  - b. On the **BMC** tab, click **Add Server**.

### Figure 3-11 Adding BMCs in Batches

Adding BMC

**Basic Parameters**

Adding Mode  Manual  Auto Scan  Batch Import

Upload Server-List File  You can download it first [Config Template](#) and then perform the configuration.

2. (Optional) If there is no configuration file, click **Config Template** to download and fill in the configuration template. For a description of the parameters in the configuration template, refer to [Table 3-6](#).



The name of the configuration template downloaded to your local PC is *ImportServer.csv*.

**Table 3-6 Parameter Descriptions for the BMC Configuration Template**

Parameter	Description	Setting
Name	Server name.	Enter a server name, which can be customized.
IP	BMC IP address.	Enter a BMC IP address, which supports both <a href="#">IPv4</a> and <a href="#">IPv6</a> .
Group	Group name.	It is recommended that you enter a rack number. <b>uniview</b> (case insensitive) is the reserved group name and you cannot use it.
Type	Server type.	Enter a server type, which can be viewed on the Web portal of the BMC. For different server models, the methods for viewing the server types are different. <ul style="list-style-type: none"> <li>For a server of the G5 model, view the server type on the <b>Homepage</b>.</li> <li>For a server of other models, view the server type on the <b>Overview</b> page.</li> </ul>

ManageUser	IPMI username.	<p>Enter a username with the administrator or operator permissions. The usernames can be viewed on the Web portal of the BMC. It is recommended that you enter a username with the administrator permissions.</p> <p>For different server models, the paths for viewing the usernames are different:</p> <ul style="list-style-type: none"> <li>For a server of the G5 model, select <b>User &amp; Security &gt; Local Users</b>.</li> <li>For a server of other models, select <b>Settings &gt; Group Management &gt; Group Management Configuration</b>.</li> </ul> <p>If it is left blank, the default value is used in accordance with the server model.</p>
ManagePassword	IPMI password.	<p>Enter the password of the IPMI user.</p> <p>If the password contains a symbol, add the escape character "\\" before the symbol.</p> <p>If it is left blank, the default value is used in accordance with the server model.</p>

Parameter	Description	Setting
SshUser	SSH username.	<p>Enter the BMC administrator username.</p> <p>If it is left blank, the default value is used in accordance with the server model. Default: <i>sysadmin</i>.</p>
SshPassword	SSH password.	<p>Enter the password of the SSH user.</p> <p>If it is left blank, the default value is used in accordance with the server model. The default password depends on the BMC version.</p> <ul style="list-style-type: none"> <li><b>BMC V3:</b> <ul style="list-style-type: none"> <li>→ For versions prior to V03.20.11.02, the default password is <i>superuser</i>. → For V03.20.11.02 and later, the default password is <i>Superuser@123</i>.</li> </ul> </li> <li><b>BMC V4:</b> <ul style="list-style-type: none"> <li>→ For versions prior to V04.23.01.02, the default password is <i>superuser</i>. → For V04.23.01.02 and later, the default password is <i>Superuser@123</i>.</li> </ul> </li> </ul>
SshPort	SSH port number.	<p>Enter the SSH port number of a server.</p> <p>If it is left blank, the default value is used in accordance with the server model. Default: <i>22</i>.</p>

SnmpVersion	SNMP protocol type.	Enter the SNMP version. Options: V2 and V3. If it is left blank, the default value ( <i>v2</i> ) is used.
SnmpPort	SNMP port number.	Enter the SNMP port number of a server. You can log in to the Web portal of the BMC, and select <b>Settings &gt; Services</b> to view the port number. If it is left blank, the default value ( <i>161</i> ) is used.
SnmpReadCommunity	SNMP read-only community.	<p>It is valid for SNMPv2.</p> <p>Enter the SNMP read-only community of a server.</p> <p>For different server models, the methods for viewing the SNMP read-only community are different.</p> <ul style="list-style-type: none"> <li>For a server of the G4X model, log in to the BMC of the server through SSH, and run the following command:  <code># cat /conf/snmp_users.conf</code>  In the command output, the character string displayed next to <b>rocommunity</b> is the read-only community.</li> <li>For a server of other models, log in to the Web portal of the BMC of the server, and select <b>Settings &gt; SNMP Configurations &gt; SNMP Community</b>.</li> </ul> <p>If it is left blank, the default value (<i>NETAŞ_public</i>) is used.</p>

Parameter	Description	Setting
SnmpWriteCommunity	SNMP read-write community.	<p>It is valid for SNMPv2.</p> <p>Enter the SNMP read-write community of the server.</p> <p>For different server models, the methods for viewing the SNMP read-write community are different.</p> <ul style="list-style-type: none"> <li>For a server of the G4X model, log in to the BMC of the server through SSH, and run the following command:  <code># cat /conf/snmp_users.conf</code>  In the command output, the character string displayed next to <b>rwcommunity</b> is the read-write community.</li> <li>For a server of other models, log in to the Web portal of the BMC of the server, and select <b>Settings &gt; SNMP Configurations &gt; SNMP Community</b>.</li> </ul> <p>If it is left blank, the default value (<i>platform</i>) is used.</p>
SnmpUser	SNMP username.	<p>It is valid for SNMPv3 and required.</p> <p>Enter a username with the administrator permissions of the server. You can log in to the Web portal of the BMC, and select <b>Settings &gt; Group Management &gt; Group Management Configuration</b> to view the usernames.</p>

SecurityLevel	Security level.	It is valid for SNMPv3 and required. Use the default value ( <i>authPriv</i> ).
AuthProtocol	Authentication protocol.	It is valid for SNMPv3 and required. Set the authentication protocol for SNMPv3. Options: <a href="#">MD5</a> and <a href="#">SHA</a> . You can log in to the Web portal of the BMC, and select <b>Settings &gt; Group Management &gt; Group Management Configuration</b> to view the authentication protocols. Note: You need to select the administrator user group for the view.
AuthKey	Authorization protocol password.	It is valid for SNMPv3 and required. Enter the password of the SNMP user.
PrivProtocol	Privacy protocol.	It is valid for SNMPv3 and required. Set the privacy protocol for SNMPv3. Options: <a href="#">DES</a> and <a href="#">AES</a> . You can log in to the Web portal of the BMC, and select <b>Settings &gt; Group Management &gt; Group Management Configuration</b> to view the privacy protocols. Note: You need to select the administrator user group for the view.
PrivKey	Privacy protocol password.	It is valid for SNMPv3 and required. Enter the password of the SNMP user.
Parameter	Description	Setting
LinkDiag	Whether to diagnose links.	<p>This parameter is valid only when servers are imported in batches. Options:</p> <ul style="list-style-type: none"> <li>● yes: indicates to check whether links are operating properly.</li> <li>● no: indicates not to check whether links are operating properly.</li> </ul> <p>If it is set to <b>yes</b>, the link state is checked by default. If the link diagnosis fails, the involved BMC fails to be added.</p>



### Note

The SSH and SNMP users of each server must have the administrator permission. Otherwise, some functions may be affected.

For the BMC of a G5 server, the following SNMP-related parameters do not need to be set:

- SnmpVersion
- SnmpPort
- SnmpReadCommunity
- SnmpWriteCommunity
- SnmpUser

- SecurityLevel
- AuthProtocol
- AuthKey
- PrivProtocol
- PrivKey

---



In the configuration template, you need to remove the placeholder value \*\*\* from any fields that do not need to be filled in. Otherwise, the configuration file fails to be imported.

---

3. Click **Select File**, and select the edited configuration file.



After a configuration file is selected, the parameters in it are automatically verified. If a parameter is not properly set, the configuration file cannot be imported.

---

4. Click **Submit**.

### 3.3 Adding Hosts

After a host is added, you can manage and maintain the in-band functions of the corresponding server through the UniKits.

One or more hosts can be added through any of the following ways:

- Manually adding a host
  - Use this way if you add a single server. For details, refer to "[3.3.1 Manually Adding a Host](#)".
- Adding hosts through auto-scan
  - Use this way if you add multiple servers of the same model that are in the same network segment. For details, refer to "[3.3.2 Adding Hosts Through Auto Scan](#)".
- Adding hosts in batches
  - Use this way if you add a large number of servers. For details, refer to "[3.3.3 Adding Hosts in Batches Through a Configuration File](#)".



When a host is manually added or hosts are added through auto-scan, link diagnosis is automatically performed. If the link diagnosis fails, the involved host fails to be added. When hosts are added in batches, whether link diagnosis is performed can be controlled through parameters.

### 3.3.1 Manually Adding a Host

#### Abstract

This procedure describes how to manually configure the parameters for a server host so that the server host can be added.

#### Prerequisite

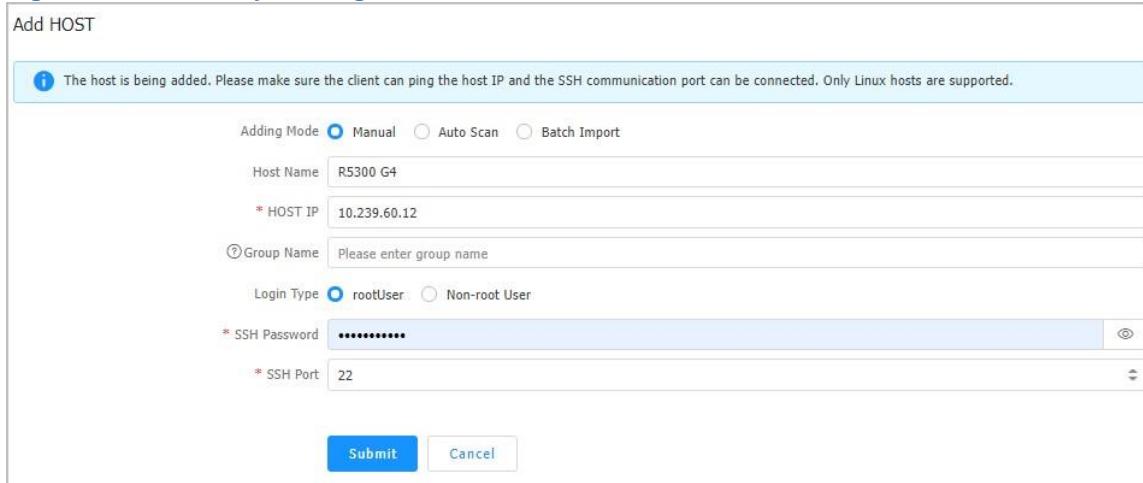
The host **IP** address can be successfully pinged from the installation **PC** and messages can be exchanged between them through the **SSH** port.

#### Steps

1. Use either of the following methods to access the **Add HOST** page (see [Figure 3-12](#)):

- Access it from the **Quick Start** page
  - a. Select **Device Mgmt > Quick Start**. The **Quick Start** page is displayed.
  - b. In the device overview area, click **Adding** and select **Add HOST** from the shortcut menu.
- Access it from the **Server List** page
  - a. Select **Server List**. The **Server List** page is displayed.
  - b. On the **HOST** tab, click **Add HOST**.

[Figure 3-12 Manually Adding a Host](#)



2. Set the parameters. For a description of the parameters, refer to [Table 3-7](#).

[Table 3-7 Parameter Descriptions for Manually Adding a Host](#)

Parameter	Description
Adding Mode	Select <b>Manual</b> .
Host Name	Enter the name of the host to be added.

HOST IP		Enter the host IP address.
Group Name		Set a group name for the host. In this way, you can filter hosts by group name. <b>uniview</b> is the reserved group name and you cannot use it.
Login Type		Select the way for logging in to the host. Options: <ul style="list-style-type: none"> <li>● <b>rootUser</b>: indicates to log in to the host as the <i>root</i> user.</li> <li>● <b>Non-root User</b>: indicates to log in to the host as a non-root user.</li> </ul>
rootUser	SSH Password	Enter the password to be used by the <i>root</i> user to log in to the host.
	SSH Port	Enter the SSH port number of the host. Default: 22.
Non-root User	SSH User Name	Enter the username used by a non-root user to log in to the host.
	SSH Password	Enter the password used by a non-root user to log in to the host.
	root User Password	Enter the password to be used by the <i>root</i> user to log in to the host.
	SSH Port	Enter the SSH port number of the host. Default: 22.

3. Click **Submit**.

### Related Tasks

On the **HOST** tab of the **Server List** page, perform the following operations as required.

To...	Do...
View the information about abnormal hosts	Click <b>Abnormal HOST</b> . The <b>Viewing the Abnormal List</b> dialog box is displayed.
Modify the information about a host	<ol style="list-style-type: none"> <li>1. Click <b>More</b> in the <b>Operation</b> column for the host, and select <b>Edit</b> from the shortcut menu. The <b>Update Server Info</b> dialog box is displayed.</li> <li>2. Modify the host information.</li> <li>3. Click <b>Submit</b>.</li> </ol> <p>Note: If any parameter other than <b>Host Name</b> and <b>Group Name</b> is modified, link diagnosis for the host is automatically triggered and the diagnosis result is updated accordingly.</p>

Refresh the information about a host	Click <b>More</b> in the <b>Operation</b> column for the host, and select <b>Refresh</b> from the shortcut menu.
Export host information	<ol style="list-style-type: none"> <li>1. Select the hosts that you want to export.</li> <li>2. Click <b>Export HOST List</b>.</li> </ol>
Delete hosts	<ol style="list-style-type: none"> <li>1. Select the hosts that you want to delete.</li> <li>2. Click <b>Remove HOST</b>.</li> </ol> <p>Note: After a host is deleted, the deletion operation cannot be rolled back. If the host is needed, you can only add it again.</p>

### 3.3.2 Adding Hosts Through Auto Scan

#### Abstract

This procedure describes how to add server hosts that are in the same network segment through auto scan.

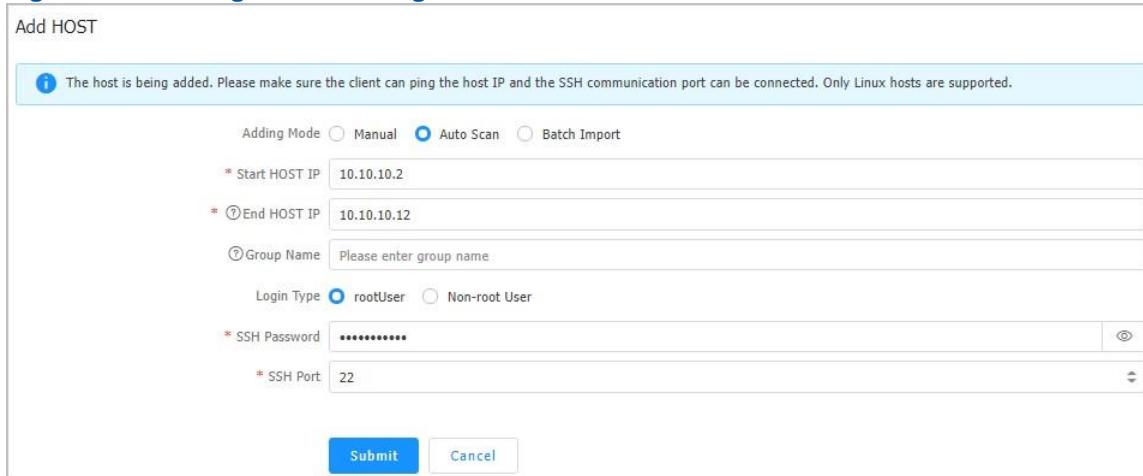
#### Prerequisite

The host **IP** addresses can be successfully pinged from the installation **PC** and messages can be exchanged through the **SSH** port.

#### Steps

1. Use either of the following methods to access the **Add HOST** page (see [Figure 3-13](#)):

- Access it from the **Quick Start** page
  - a. Select **Device Mgmt > Quick Start**. The **Quick Start** page is displayed.
  - b. In the device overview area, click **Adding** and select **Add HOST** from the shortcut menu.
- Access it from the **Server List** page
  - a. Select **Server List**. The **Server List** page is displayed.
  - b. On the **HOST** tab, click **Add HOST**.

**Figure 3-13 Adding Hosts Through Auto-Scan**


2. Set the parameters. For a description of the parameters, refer to **Table 3-8**.

**Table 3-8 Parameter Descriptions for Adding Hosts Through Auto-Scan**

Parameter	Description	
Adding Mode	Select <b>Auto Scan</b> .	
Start HOST IP	Enter the start host IP address of the network segment to be scanned.	
End HOST IP	Enter the end host IP address of the network segment to be scanned. <b>Start HOST IP</b> and <b>End HOST IP</b> must be in the same network segment, and <b>Start HOST IP</b> needs to be set first.	
Group Name	Set a group name for the hosts. In this way, you can filter hosts by group name. <b>uniview</b> is the reserved group name and you cannot use it.	
Login Type	Select the way for logging in to the hosts. Options: <ul style="list-style-type: none"> <li>• <b>rootUser</b>: indicates to log in to the hosts as the <i>root</i> user.</li> <li>• <b>Non-root User</b>: indicates to log in to the hosts as a nonroot user.</li> </ul>	
rootUser	SSH Password	Enter the password to be used by the <i>root</i> user to log in to the hosts.
	SSH Port	Enter the SSH port number of the hosts. Default: 22.
Non-root User	SSH User Name	Enter the username used by a non-root user to log in to the hosts.

Parameter	Description	
	SSH Password	Enter the password used by a non-root user to log in to the hosts.
	root User Password	Enter the password to be used by the <code>root</code> user to log in to the hosts.
	SSH Port	Enter the SSH port number of the hosts. Default: 22.

3. Click **Submit**.

### 3.3.3 Adding Hosts in Batches Through a Configuration File

#### Abstract

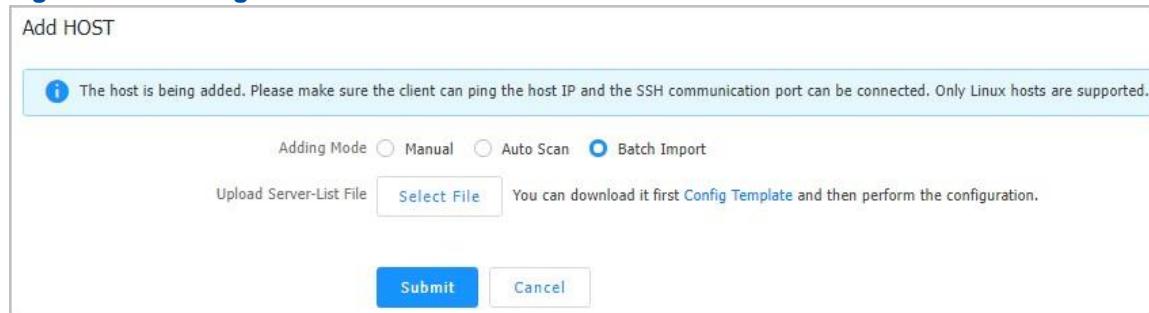
This procedure describes how to add server hosts in batches by importing a configuration file.

#### Steps

1. Use either of the following methods to access the **Add HOST** page (see [Figure 3-14](#)):

- Access it from the **Quick Start** page
  - a. Select **Device Mgmt > Quick Start**. The **Quick Start** page is displayed.
  - b. In the device overview area, click **Adding** and select **Add HOST** from the shortcut menu.
- Access it from the **Server List** page
  - a. Select **Server List**. The **Server List** page is displayed.
  - b. On the **HOST** tab, click **Add HOST**.

**Figure 3-14 Adding Hosts in Batches**



2. (Optional) If there is no configuration file, click **Config Template** to download and fill in the configuration template. For a description of the parameters in the configuration template, refer to [Table 3-9](#).

**Note**

The name of the configuration template downloaded to your local PC is *ImportHostServer.csv*.

**Table 3-9 Parameter Descriptions for the Host Configuration Template**

Parameter	Description	Setting
Name	Host name	You can customize the name.
IP	Host IP address	Options: <a href="#">IPv4</a> and <a href="#">IPv6</a> .
SshUser	SSH username	It must be set to <b>root</b> . Otherwise, functions are affected.
SshPassword	SSH password	Enter the password to be used by the <i>root</i> user to log in to the hosts.
SshPort	SSH port number	Enter the SSH port number of the hosts. Default: 22.
Group	Group name	It is recommended that you enter a rack number. <b>uniview</b> (case insensitive) is the reserved group name and you cannot use it.
LinkDiag	Whether to diagnose links	<p>It is valid only when hosts are imported in batches. Options:</p> <ul style="list-style-type: none"> <li>• yes: indicates to check whether links are operating properly.</li> <li>• no: indicates not to check whether links are operating properly.</li> </ul> <p>If it is set to <b>yes</b>, the link state is checked by default. If the link diagnosis fails, the involved host fails to be added.</p>

3. Click **Select File**, and select the edited configuration file.

**Note**

After a configuration file is selected, the parameters in it are automatically verified. If a parameter is not properly set, the configuration file cannot be imported.

4. Click **Submit**.

## 3.4 Commissioning and Deployment

### 3.4.1 BMC Network Parameter Configuration

BMC network parameters include:

- [IP](#) parameters

For how to configure IP parameters, refer to "[3.4.1.1 Configuring a BMC IP Address](#)".

- Port parameters

For how to configure port parameters, refer to "[3.4.1.2 Configuring Network Port Parameters](#)".

- Network port bonding parameters

For how to configure network port bonding parameters, refer to "[3.4.1.3 Configuring Network Port Bonding Parameters](#)".

- DNS parameters

For how to configure DNS parameters, refer to "[3.4.1.4 Configuring DNS Parameters](#)".

### 3.4.1.1 Configuring a BMC IP Address

#### Abstract

The following scenarios involve **BMC IP** configuration:

- **Modify the default IP address of a single equipment**



#### Note

In this scenario, two IP addresses need to be configured for the installation **PC**. One IP address must be in the same network segment with the default IP address (192.168.5.7), and the other must be in the same network segment with the destination IP address. Otherwise, the configuration will fail. (For details, refer to [Related Tasks](#)).

For example, if the destination IP address is 10.235.238.11 and the subnet mask is 255.255.255.0, the two IP addresses of the installation PC are 192.168.5.100 and 10.235.238.100 and their subnet masks are both 255.255.255.0.

- **Configure the IP address in DHCP mode**
- **Add/Modify IP address according to current IP address**
- **Configure the IP address with SSDP**



#### Note

The G5 series servers (for example, the NCS6722 N4) only support the configuration of IP addresses in SSDP mode.

#### Context

For a description of the BMC IP configuration scenarios, refer to [Table 3-10](#).

**Table 3-10 Descriptions of BMC IP Configuration Scenarios**

Scenario	Description
----------	-------------

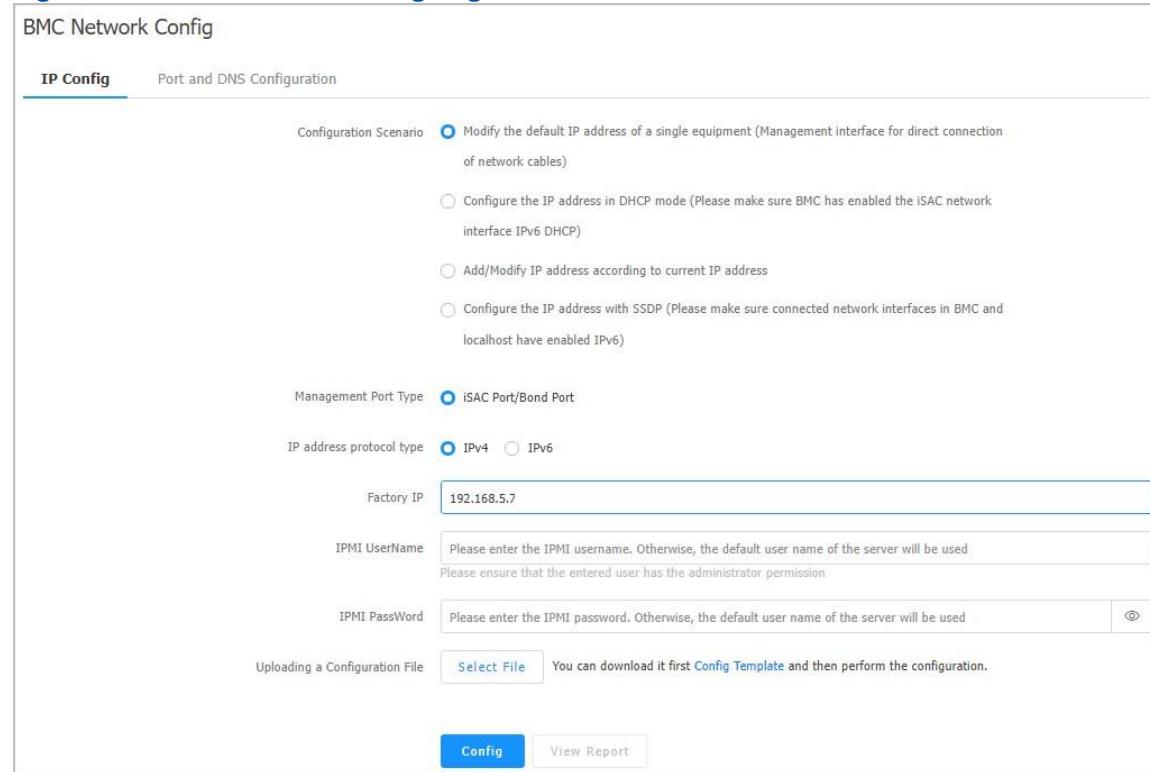
<b>Modify the default IP address of a single equipment</b>	<ul style="list-style-type: none"> <li>The iSAC network ports of all servers to be configured must have the same factory default IP address, <b>IPMI</b> username and IPMI password.</li> <li>The installation <b>PC</b> must be directly connected to the iSAC network port of a server rather than being connected to the server through a switch or router.</li> <li>The installation PC is connected to only one server at a time.</li> <li>The installation PC can successfully ping the factory default IP address of a server.</li> </ul>
--	--

Scenario	Description
	<ul style="list-style-type: none"> <li>During configuration, network cables are plugged and unplugged manually.</li> <li>When the following message is displayed, you need to insert the network cable into the iSAC network port on another server to be configured and repeat the steps until all servers are configured. Please insert the lan cable into the x server</li> <li>If the factory default IP address of a server cannot be pinged successfully, the serial number of a server fails to be obtained, or the serial number of a server is not in the configuration list within 20 minutes, the configuration flow times out.</li> </ul>
<b>Configure the IP address in DHCP mode</b>	<ul style="list-style-type: none"> <li>All servers to be configured must have the same IPMI username and IPMI password.</li> <li><b>IPv6</b> DHCP is enabled on the iSAC network ports of all servers to be configured.</li> <li>The iSAC network ports of all servers to be configured and the network port of the installation PC are in the same LAN. Communication across the L3 network is not supported, and no more than 200 servers are allowed to be configured.</li> <li>The shared network port cannot be in the same LAN as the iSAC network port.</li> <li>There is only one DHCPv6 server in the LAN.</li> <li>If no server needs to be allocated a temporary IPv6 address within 20 minutes, the configuration flow times out.</li> <li>If both <b>IPv4</b> and IPv6 addresses need to be configured for the iSAC network port of a server, the IPv4 address must be configured first. After the IPv4 address configuration flow is complete, you need to wait for 10 minutes before configuring the IPv6 address.</li> <li>An IP address to be configured in the configuration file must be in the same network segment as that of the installation PC.</li> </ul>

<b>Add/Modify IP address according to current IP address</b>	<ul style="list-style-type: none"> <li>The iSAC network ports of all servers to be configured and the network port of the installation PC are in the same LAN.</li> <li>If the server to be configured is in the device list, you need to add it to the device list when its IP address is modified.</li> <li>The username and password in the configuration file must be correct.</li> </ul>
<b>Configure the IP address with SSDP</b>	<ul style="list-style-type: none"> <li>Applicable to G5 series servers with BMC version V04.23.01.02 or later.</li> <li>Applicable to G4 series servers with BMC version V03.20.02.00 or later.</li> <li>IPv6 is enabled on network ports for connection between the installation PC and a BMC.</li> <li>If IPv6 is configured on both the iSAC network port and shared port of a BMC, they cannot be connected to the installation PC at the same time.</li> <li>In the configuration file, the serial number of each server must be valid.</li> </ul>
<b>Scenario</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>The iSAC network ports of all servers to be configured and the network port of the installation PC are in the same LAN. Communication across the L3 network is not supported, and no more than 200 servers are allowed to be configured.</li> <li>It is recommended that you enable IPv6 only on the network port of the installation PC connected to the servers to be configured, and disable IPv6 on other network ports.</li> <li>The G4 series servers only support the configuration of IP addresses in SSDP mode when the BMC network interface is in normal mode.</li> </ul>

### Steps

1. Select **Device Mgmt > Deployment > BMC Network Config**. The **BMC Network Config** page is displayed, see [Figure 3-15](#).

**Figure 3-15 BMC Network Config Page**


BMC Network Config

**IP Config** **Port and DNS Configuration**

Configuration Scenario  Modify the default IP address of a single equipment (Management interface for direct connection of network cables)  
 Configure the IP address in DHCP mode (Please make sure BMC has enabled the iSAC network interface IPv6 DHCP)  
 Add/Modify IP address according to current IP address  
 Configure the IP address with SSDP (Please make sure connected network interfaces in BMC and localhost have enabled IPv6)

Management Port Type  iSAC Port/Bond Port

IP address protocol type  IPv4  IPv6

Factory IP

IPMI UserName   
Please enter the IPMI username. Otherwise, the default user name of the server will be used  
 Please ensure that the entered user has the administrator permission

IPMI PassWord   
Please enter the IPMI password. Otherwise, the default user name of the server will be used

Uploading a Configuration File  You can download it first [Config Template](#) and then perform the configuration.

**Config** **View Report**

2. Set the parameters. For a description of the parameters, refer to [Table 3-11](#).

**Table 3-11 IP Configuration Parameter Descriptions**

Parameter	Description	
Configuration Scenario	Select a configuration scenario. Options: <ul style="list-style-type: none"> <li>● <b>Modify the default IP address of a single equipment</b></li> <li>● <b>Configure the IP address in DHCP mode</b></li> </ul>	
	<ul style="list-style-type: none"> <li>● <b>Add/Modify IP address according to current IP address</b></li> <li>● <b>Configure the IP address with SSDP</b></li> </ul>	
Modify the default IP address of a single equipment	Management Port Type	Select <b>iSAC Port/Bond Port</b> .
	IP address protocol type	Select the BMC IP version. Options: <ul style="list-style-type: none"> <li>● <b>IPv4</b></li> <li>● <b>IPv6</b></li> </ul>
	Factory IP	Enter the factory default BMC IP address of the server. Default: 192.168.5.7.

	IPMI UserName	Enter the IPMI username of the server. This user must have the administrator permissions. If it is left blank, the default username ( <b>NETAŞroot</b> ) of the server is used.
	IPMI Password	Enter the IPMI password of the server. If it is left blank, the default password ( <b>superuser9!</b> ) of the server is used.
	Uploading a Configuration File	If there is no configuration file, click <b>Config Template</b> to download and fill in the configuration template. For how to fill in the configuration template, refer to <a href="#">Table 3-12</a> . The name of the configuration template downloaded to your local PC is <i>ImportIPConfiguration.xls</i> . Click <b>Select File</b> , and select the edited configuration file.
Configure the IP address in DHCP mode	Management Port Type	Select <b>iSAC Port/Bond Port</b> .
	IP address protocol type	Select the BMC IP version. Options: <ul style="list-style-type: none"><li>● <b>IPv4</b></li><li>● <b>IPv6</b></li></ul> If both an IPv4 address and an IPv6 address need to be configured, configure the IPv4 address first and then the IPv6 address.
	IPMI UserName	Enter the IPMI username of the server. This user must have the administrator permissions. If it is left blank, the default username ( <b>NETAŞroot</b> ) of the server is used.
	IPMI Password	Enter the IPMI password of the server. If it is left blank, the default password ( <b>superuser9!</b> ) of the server is used.
Parameter	Description	
	Uploading a Configuration File	If there is no configuration file, click <b>Config Template</b> to download and fill in the configuration template. For how to fill in the configuration template, refer to <a href="#">Table 3-12</a> . The name of the configuration template downloaded to your local PC is <i>ImportIPConfiguration.xls</i> . Click <b>Select File</b> , and select the edited configuration file.
Add/Modify IP address according	Management Port Type	Select <b>iSAC Port/Bond Port</b> .

to current IP address	Uploading a Configuration File	If there is no configuration file, click <b>Config Template</b> to download and fill in the configuration template. For how to fill in the configuration template, refer to <a href="#">Table 3-12</a> . The name of the configuration template downloaded to your local PC is <i>ImportIPConfiguration.xls</i> . Click <b>Select File</b> , and select the edited configuration file.
Configure the IP address with SSDP	Uploading a Configuration File	If there is no configuration file, click <b>Config Template</b> to download and fill in the configuration template. For how to fill in the configuration template, refer to <a href="#">Table 3-12</a> . The name of the configuration template downloaded to your local PC is <i>ImportIPConfiguration.xls</i> . Click <b>Select File</b> , and select the edited configuration file.

**Table 3-12 Configuration Template Descriptions**

Scenario	Description
<b>Modify the default IP address of a single equipment</b>	<ul style="list-style-type: none"> <li>When configuring an IPv4 address, you need to set the following parameters: Serial Number, IPv4 Address, IPv4 Mask, and IPv4 Gateway.</li> <li>When configuring an IPv6 address, you need to set the following parameters: Serial Number, IPv6 Address, IPv6 Prefix, and IPv6 Gateway.</li> <li>No blank line is allowed between adjacent lines.</li> <li>The serial number or IPv4/IPv6 address must be unique.</li> <li>In the same line, the IPv4/IPv6 address and the gateway must be in the same network segment.</li> </ul>
<b>Configure the IP address in DHCP mode</b>	<ul style="list-style-type: none"> <li>When configuring an IPv4 address, you need to set the following parameters: Serial Number, IPv4 Address, IPv4 Mask, and IPv4 Gateway.</li> <li>When configuring an IPv6 address, you need to set the following parameters: Serial Number, IPv6 Address, IPv6 Prefix, and IPv6 Gateway.</li> <li>No blank line is allowed between adjacent lines.</li> <li>The serial number or IPv4/IPv6 address must be unique.</li> </ul>
Scenario	Description
	<ul style="list-style-type: none"> <li>In the same line, the IPv4/IPv6 address and the gateway must be in the same network segment.</li> </ul>

<b>Add/Modify IP address according to current IP address</b>	<ul style="list-style-type: none"> <li>When configuring an IPv4 address, you need to set the following parameters: Current IP, UserName, Password, IPv4 Address, IPv4 Mask, and IPv4 Gateway.</li> <li>When configuring an IPv6 address, you need to set the following parameters: Current IP, UserName, Password, IPv6 Address, IPv6 Prefix, and IPv6 Gateway.</li> <li>No blank line is allowed between adjacent lines.</li> <li>The current IP address or the IPv4/IPv6 address must be unique.</li> <li>In the same line, the IPv4/IPv6 address and the gateway must be in the same network segment.</li> </ul>
<b>Configure the IP address with SSDP</b>	<ul style="list-style-type: none"> <li>When configuring an IPv4 address, you need to set the following parameters: Serial Number, UserName, Password, IPv4 Address, IPv4 Mask, and IPv4 Gateway.</li> <li>When configuring an IPv6 address, you need to set the following parameters: Serial Number, UserName, Password, IPv6 Address, IPv6 Prefix, and IPv6 Gateway.</li> <li>No blank line is allowed between adjacent lines.</li> <li>The serial number or IPv4/IPv6 address must be unique.</li> <li>In the same line, the IPv4/IPv6 address and the gateway must be in the same network segment.</li> <li>Both IPv4 and IPv6 addresses can be configured.</li> </ul>

- Click **Config**. A confirmation message box is displayed.
- Verify the related information as prompted, and click **Submit**.



#### Note

- Before the configuration, the UniKits checks whether the BMC IP address is correct. The IP address is configured only after the check is passed.
- During the configuration, the UniKits configures the IP addresses in accordance with the sequence of servers in the configuration file and displays the IP address configuration results. If you need to terminate the configuration, click **Terminate**.
- After the configuration, a message indicating that the configuration is completed is displayed.

#### Related Tasks

To configure the IP addresses on the installation PC (using Windows 10 as an example), perform the following operations:

- Select **Settings > Network & Internet > Change adapter options**. The **Network Connections** window is displayed.
- Right-click the desired Ethernet, and select **Properties** from the shortcut menu. The **Ethernet Properties** dialog box is displayed.

3. In the **This connection uses the following items** area, double-click **Internet Protocol Version 4 (TCP/IPv4)**. The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box is displayed.
4. Click **Advanced** in the lower right corner. The **Advanced TCP/IP Settings** dialog box is displayed.
5. Click **Add**. A dialog box is displayed. Configure the IP addresses and subnet masks.
6. Click **OK**.

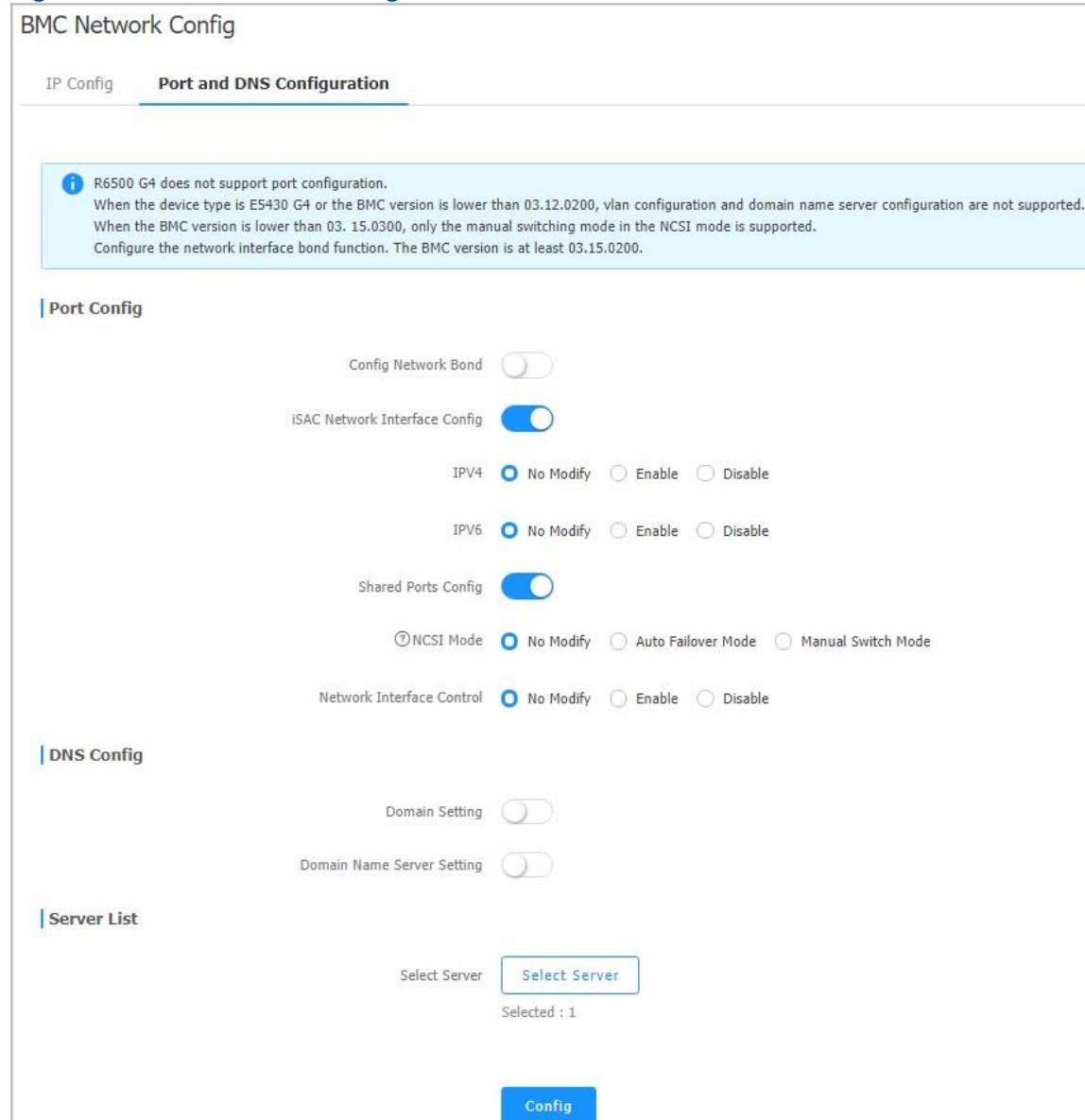
### 3.4.1.2 Configuring Network Port Parameters

#### Abstract

This procedure describes how to configure the network port parameters of the specified server. For example, you can enable or disable **IPv4/IPv6** on the **iSAC** network port, and configure the **NCSI** mode of the shared network port.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Network Config**. The **BMC Network Config** page is displayed.
2. Click **Port and DNS Configuration**. The **Port and DNS Configuration** tab is displayed, see [Figure 3-16](#).

**Figure 3-16 Port and DNS Configuration Tab**

3. Set the parameters in the **Port Config** area. For a description of the parameters, refer to [Table 3-13](#).

**Table 3-13 Parameter Descriptions for Configuring a Network Port**

Parameter	Description
Config Network Bond	Turn off the <b>Config Network Bond</b> switch.
iSAC Network Interface Config	If you need to configure the iSAC network port parameters, turn on the <b>iSAC Network Interface Config</b> switch, and select whether to enable IPv4/IPv6 on the iSAC network port. <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configuration.</li> <li>● <b>Enable:</b> indicates to enable IPv4/IPv6 on the iSAC network port.</li> <li>● <b>Disable:</b> indicates to disable IPv4/IPv6 on the iSAC network port.</li> </ul>

Parameter	Description
	You cannot disable IPv4 and IPv6 at the same time.
Shared Ports Config	<p>If you need to configure the shared network port parameters, turn on the <b>Shared Ports Config</b> switch and set the following parameters:</p> <ul style="list-style-type: none"> <li>● <b>NCSI Mode: No Modify</b> indicates not to modify the original server configuration. <b>Auto Failover Mode</b> indicates to automatically switch to a shared network port when the iSAC network port fails. In this case, you need to set <b>Channel Index</b>, which indicates that the shared network port of the server is provided preferentially. <b>Manual Switch Mode</b> indicates to manually switch to a shared network port when the iSAC network port fails. In this case, you need to set <b>Channel Index</b>.</li> <li>● <b>Channel Index</b>: enter a channel ID, range: 0–3.</li> <li>● <b>Network Interface Control</b>: select whether to enable network control. After network port control is enabled, the shared network port is allocated to the VLAN of the BMC.</li> <li>● <b>VLAN</b>: select whether to enable VLAN. If this parameter is set to <b>Enable</b>, you need to configure a VLAN ID.</li> <li>● <b>VLAN ID</b>: enter a VLAN ID, range: 1–4094.</li> </ul> <p>Note: If there is no requirement for enabling VLAN and configuring a VLAN ID on site, it is recommended that you select <b>No Modify</b>.</p>

4. In the **Server List** area, click **Select Server**, and select the server that you want to configure.
5. Click **Config**.

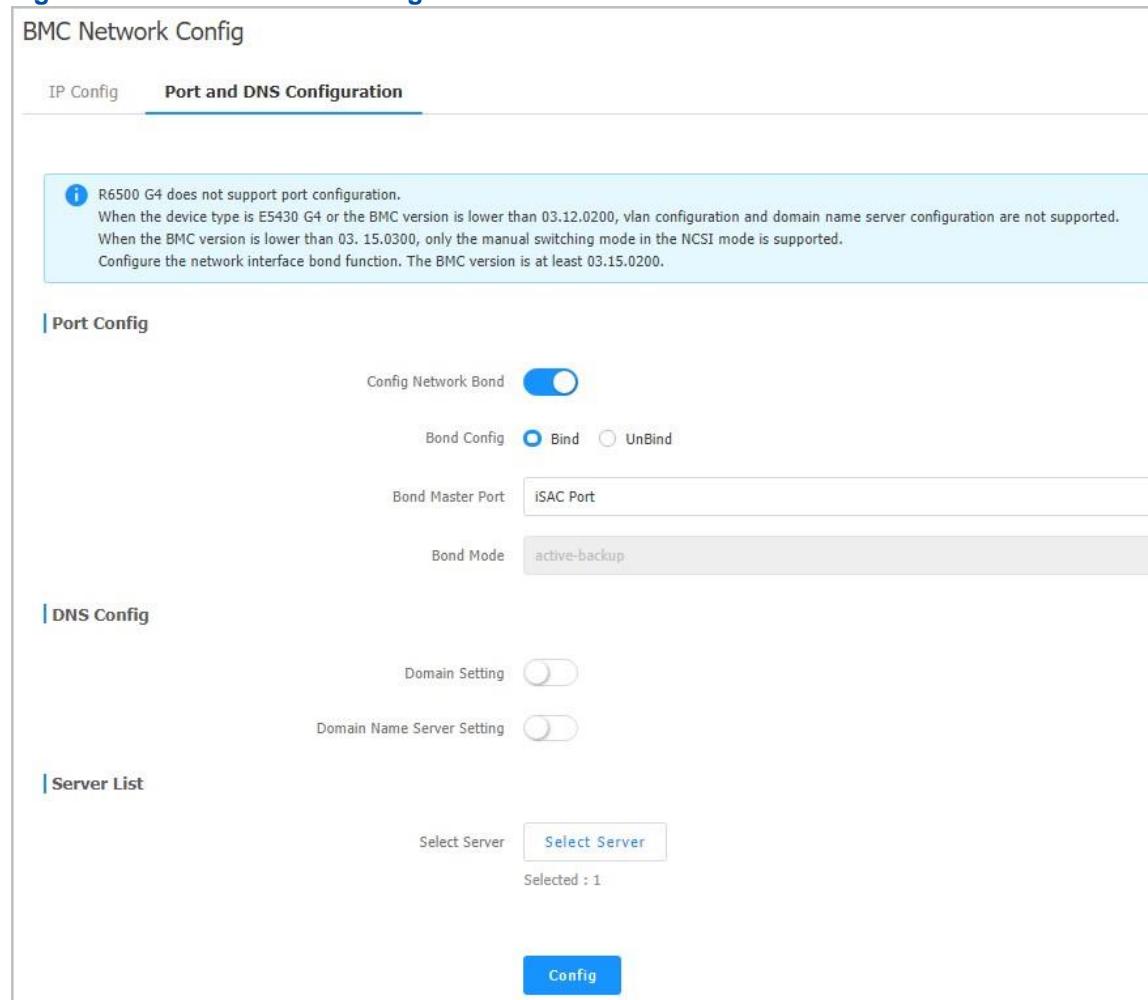
### 3.4.1.3 Configuring Network Port Bonding Parameters

#### Abstract

After an **iSAC** network port and a shared network port are bound, a new IP address is generated. If either of the ports is connected, you can access the **BMC** through the new **IP** address that is bound.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Network Config**. The **BMC Network Config** page is displayed.
2. Click **Port and DNS Configuration**. The **Port and DNS Configuration** tab is displayed, see [Figure 3-17](#).

**Figure 3-17 Port and DNS Configuration Tab**

3. Set the parameters in the **Port Config** area. For a description of the parameters, refer to [Table 3-14](#).

**Table 3-14 Parameter Descriptions for Network Port Bonding**

Parameter	Description
Config Network Bond	Turn on the <b>Config Network Bond</b> switch.
Bond Config	Select whether to bind a network port.
Bond Master Port	Select the master network port.

4. In the **Server List** area, click **Select Server**, and select the server that you want to configure.

5. Click **Config**.

### 3.4.1.4 Configuring DNS Parameters

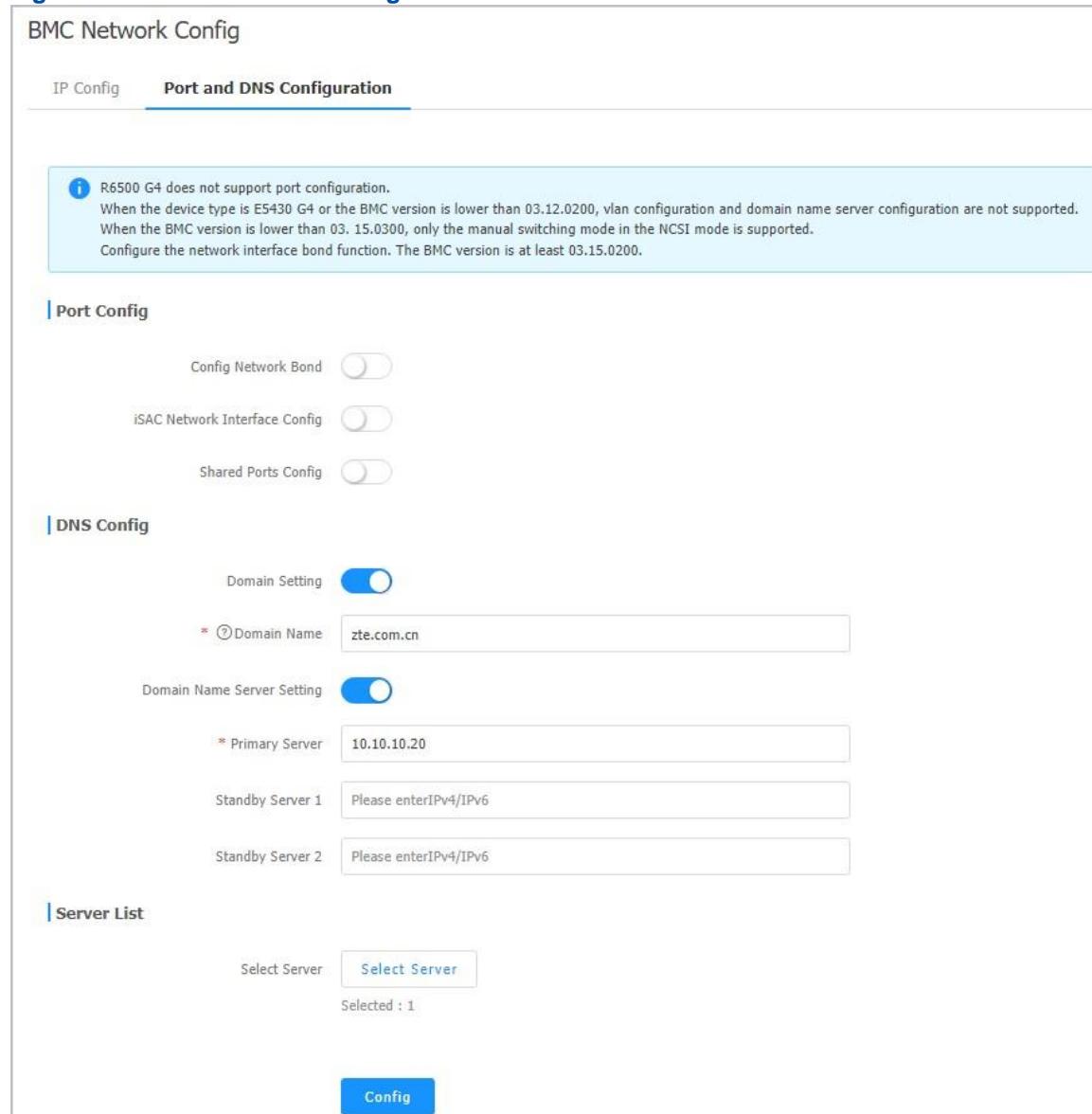
#### Abstract

This procedure describes how to configure the **DNS** parameters for a server to access the Web portal of the **BMC** through a **FQDN**.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Network Config**. The **BMC Network Config** page is displayed.
2. Click **Port and DNS Configuration**. The **Port and DNS Configuration** tab is displayed, see [Figure 3-18](#).

**Figure 3-18 Port and DNS Configuration Tab**



BMC Network Config

IP Config Port and DNS Configuration

**Note:** R6500 G4 does not support port configuration.  
When the device type is E5430 G4 or the BMC version is lower than 03.12.0200, vlan configuration and domain name server configuration are not supported.  
When the BMC version is lower than 03.15.0300, only the manual switching mode in the NCSI mode is supported.  
Configure the network interface bond function. The BMC version is at least 03.15.0200.

**Port Config**

Config Network Bond

iSAC Network Interface Config

Shared Ports Config

**DNS Config**

Domain Setting

\* Domain Name: zte.com.cn

Domain Name Server Setting

\* Primary Server: 10.10.10.20

Standby Server 1: Please enterIPv4/IPv6

Standby Server 2: Please enterIPv4/IPv6

**Server List**

Select Server:

Selected : 1

**Config**

3. Set the parameters in the **DNS Config** area. For a description of the parameters, refer to [Table 3-15](#).

**Table 3-15 DNS Parameter Descriptions**

Parameter	Description
Domain Setting	Turn on the <b>Domain Setting</b> switch.
Domain Name	<p>Enter the domain name, which consists of digits, uppercase and lowercase letters, hyphens (-), and dots (.).</p> <p>A domain name cannot start or end with a hyphen.</p> <p>The length of a domain name cannot exceed 63 characters per label, and the length of a FQDN cannot exceed 255 characters.</p>
Domain Name Server Setting	<p>Select whether to set DNS servers.</p> <ul style="list-style-type: none"> <li>• If you need to set DNS servers, turn on the <b>Domain Name Server Setting</b> switch, and set <b>Primary Server</b>, <b>Standby Server 1</b>, and <b>Standby Server 2</b>. The <b>Primary Server</b> parameter is required, while others are optional. The values of <b>Primary Server</b>, <b>Standby Server 1</b>, and <b>Standby Server 2</b> must be different.</li> <li>• If you do not need to set DNS servers, turn off the <b>Domain Name Server Setting</b> switch.</li> </ul>

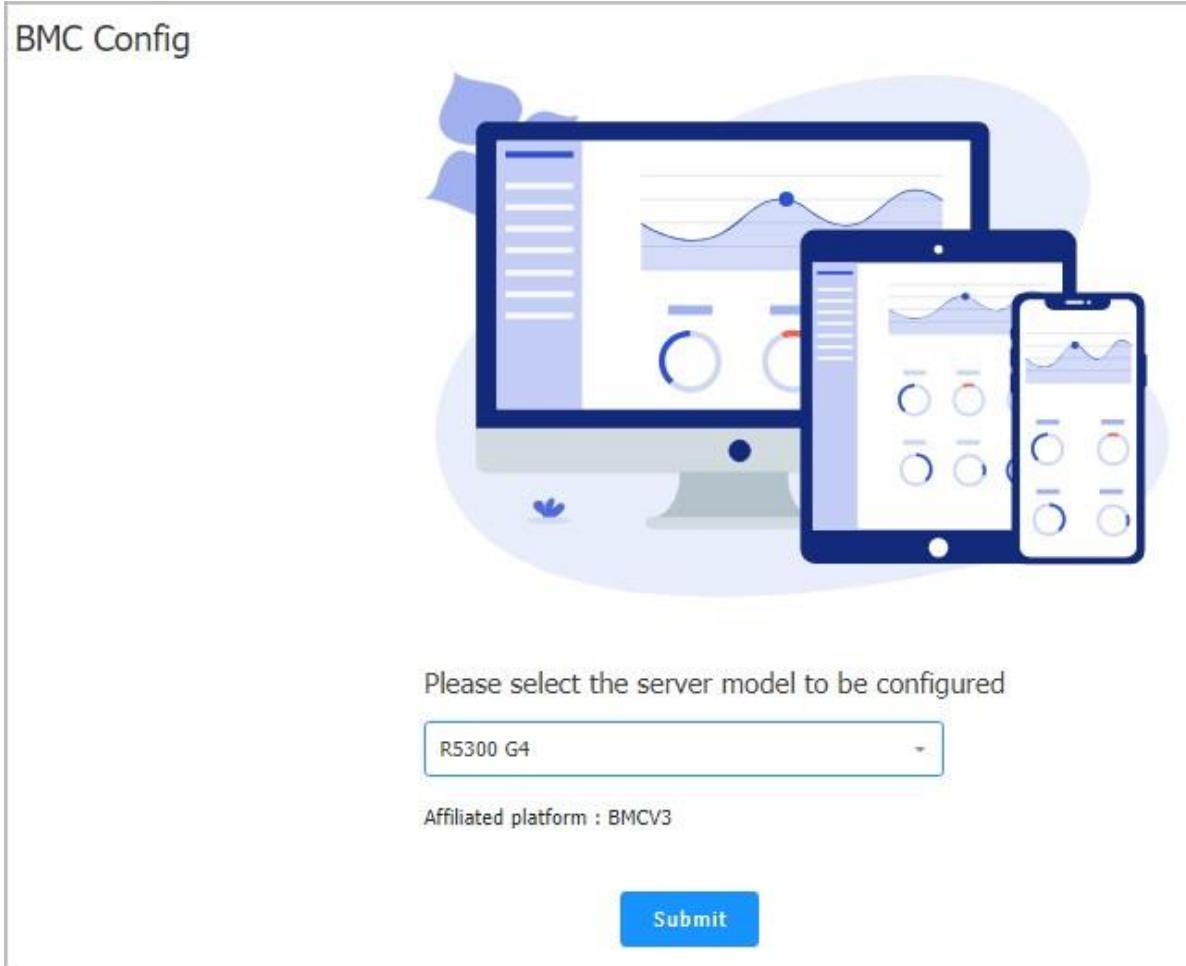
4. In the **Server List** area, click **Select Server**, and select the server that you want to configure.

5. Click **Config**.

### 3.4.2 BMC (V3) Configuration

The **BMC** versions of the servers maintained through the UniKits include V3 and V4. After a server model is selected on the **BMC Config** page, the content related to the corresponding BMC version is automatically displayed on the UniKits.

For example, after NCS6722 N4 (Gen 4) is selected on the **BMC Config** page, the content corresponding to BMC V3 is automatically displayed on the UniKits, as shown in [Figure 3-19](#).

**Figure 3-19 BMC Config Page**

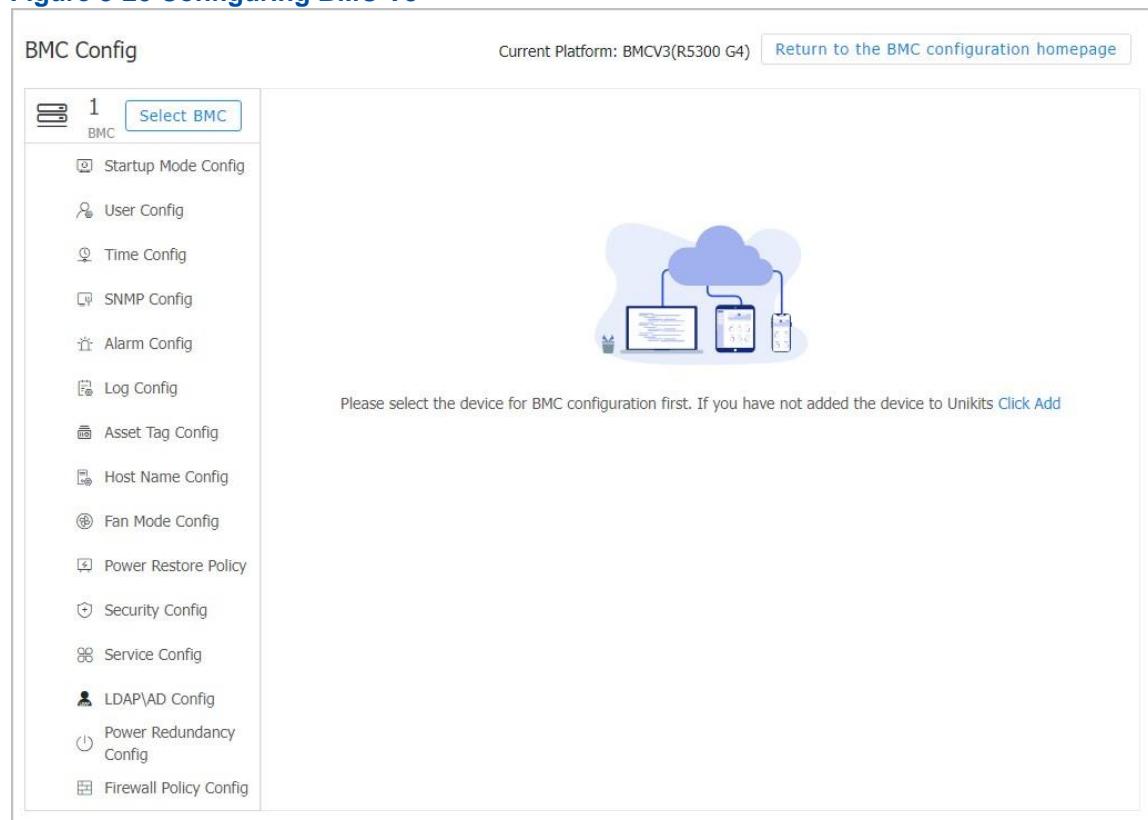
### 3.4.2.1 Configuring Boot Options

#### Abstract

This procedure describes how to configure boot options, including the boot device and application mode.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-20](#).

**Figure 3-20 Configuring BMC V3**


BMC Config

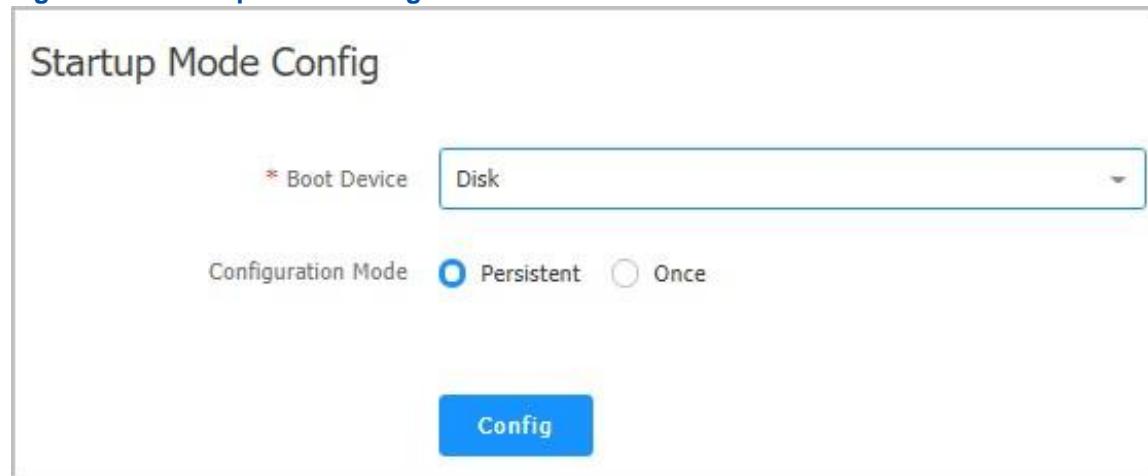
Current Platform: BMCV3(R5300 G4) [Return to the BMC configuration homepage](#)

1 BMC [Select BMC](#)

- Startup Mode Config
- User Config
- Time Config
- SNMP Config
- Alarm Config
- Log Config
- Asset Tag Config
- Host Name Config
- Fan Mode Config
- Power Restore Policy
- Security Config
- Service Config
- LDAP\AD Config
- Power Redundancy Config
- Firewall Policy Config

Please select the device for BMC configuration first. If you have not added the device to Unikits [Click Add](#)

- Click **Select BMC**, and select the BMC for which you want to configure boot options.
- In the left pane on the **BMC Config** page, click **Startup Mode Config**. The **Startup Mode Config** area is displayed, see [Figure 3-21](#).

**Figure 3-21 Startup Mode Config Area**


Startup Mode Config

\* Boot Device

Configuration Mode  Persistent  Once

**Config**

- Set the parameters. For a description of the parameters, refer to [Table 3-16](#).

**Table 3-16 Boot Option Parameter Descriptions**

Parameter	Description

Boot Device	Select the hardware device used to boot the OS of the server. Options: <ul style="list-style-type: none"> <li>● <b>No Override:</b> The first boot device is not set. The default boot mode set in <b>BIOS</b> is used, which is not controlled by the <b>BMC</b>.</li> <li>● <b>Network:</b> The OS is forcibly started through a network.</li> <li>● <b>Disk:</b> The OS is forcibly started through a hard disk.</li> <li>● <b>USB:</b> The OS is forcibly booted through a <b>USB</b> flash drive.</li> <li>● <b>CD Rom:</b> The OS is forcibly booted through a CD/DVD-ROM drive.</li> <li>● <b>BIOS:</b> After the server is booted, the BIOS menu is displayed.</li> </ul>
Configuration Mode	Select whether the reconfigured server boot option is applied to the current restart only. <ul style="list-style-type: none"> <li>● <b>Once:</b> only effective for the current restart.</li> <li>● <b>Persistent:</b> permanently effective.</li> </ul>

7. Click **Config** to deliver the configurations.



#### Note

- During boot option configuration, the progress bar is displayed on the page.
- After boot option configuration is completed, the configuration result is displayed on the page.

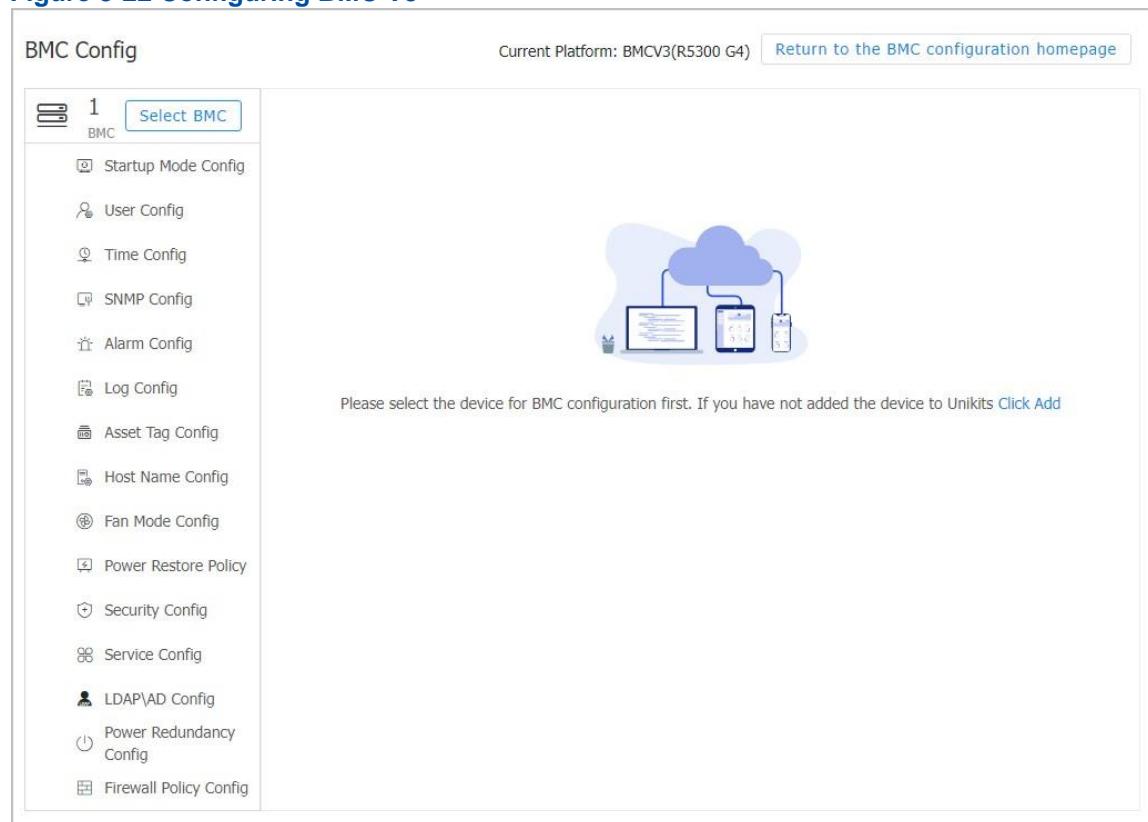
### 3.4.2.2 Configuring a User

#### Abstract

This procedure describes how to configure a **BMC** user for BMC configuration and management.

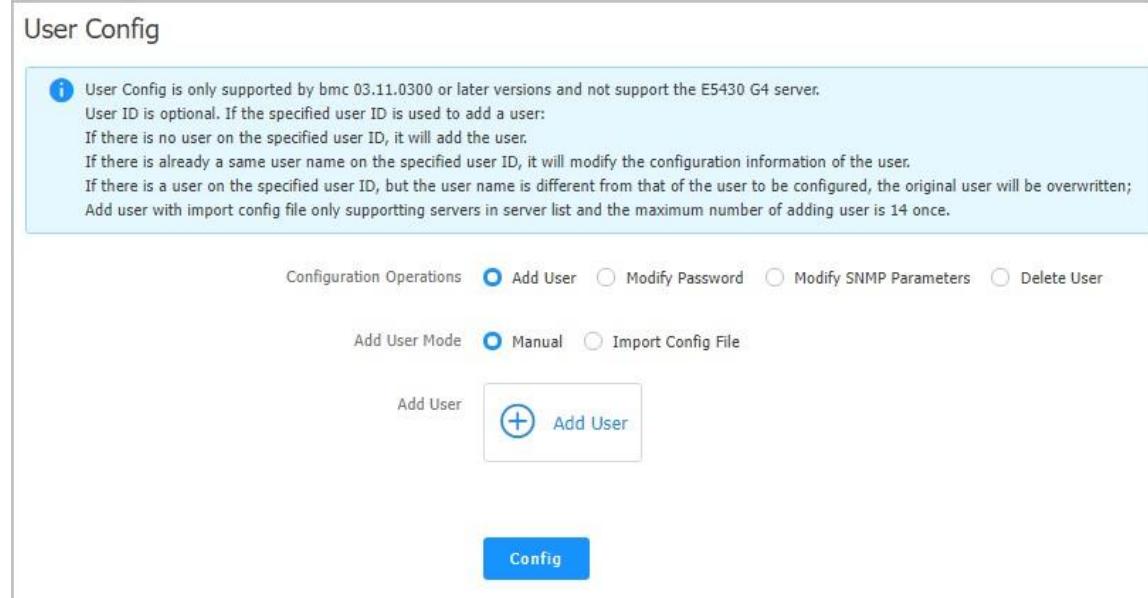
#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-22](#).

**Figure 3-22 Configuring BMC V3**


The screenshot shows the 'BMC Config' page. At the top left is a sidebar with a 'BMC' icon and the number '1'. Next to it is a 'Select BMC' button. The main area contains a list of configuration items with corresponding icons: Startup Mode Config (key), User Config (key), Time Config (key), SNMP Config (key), Alarm Config (key), Log Config (key), Asset Tag Config (key), Host Name Config (key), Fan Mode Config (key), Power Restore Policy (key), Security Config (key), Service Config (key), LDAP\AD Config (key), Power Redundancy Config (key), and Firewall Policy Config (key). To the right of the list is a blue cloud icon with three devices (laptop, smartphone, tablet) connected to it. Below the list is a message: 'Please select the device for BMC configuration first. If you have not added the device to Unikits [Click Add](#)'. At the top right of the main area is a 'Current Platform: BMCV3(R5300 G4)' label and a 'Return to the BMC configuration homepage' link.

4. Click **Select BMC**, and select the BMC for which you want to configure a user.
5. In the left pane on the **BMC Config** page, click **User Config**. The **User Config** area is displayed, see [Figure 3-23](#).

**Figure 3-23 User Config Area**


The screenshot shows the 'User Config' area. At the top left is a note: 'User Config is only supported by bmc 03.11.0300 or later versions and not support the E5430 G4 server. User ID is optional. If the specified user ID is used to add a user: If there is no user on the specified user ID, it will add the user. If there is already a same user name on the specified user ID, it will modify the configuration information of the user. If there is a user on the specified user ID, but the user name is different from that of the user to be configured, the original user will be overwritten; Add user with import config file only supporting servers in server list and the maximum number of adding user is 14 once.' Below the note are two rows of configuration operations: 'Configuration Operations' (radio buttons for Add User, Modify Password, Modify SNMP Parameters, and Delete User) and 'Add User Mode' (radio buttons for Manual and Import Config File). In the center is an 'Add User' button with a plus sign. At the bottom is a 'Config' button.

6. Perform the following operations as required.

To...	Do...
Manually add a user	<ol style="list-style-type: none"> <li>Set <b>Configuration Operations</b> to <b>Add User</b>.</li> <li>Set <b>Add User Mode</b> to <b>Manual</b>.</li> <li>Click <b>Add User</b>. The <b>Add User</b> dialog box is displayed.</li> <li>Set the parameters.</li> <li>Click <b>Submit</b>.</li> <li>Click <b>Config</b> to deliver the configurations.</li> </ol>
Add users in batches	<ol style="list-style-type: none"> <li>Set <b>Configuration Operations</b> to <b>Add User</b>.</li> <li>Set <b>Add User Mode</b> to <b>Import Config File</b>.</li> <li>Click <b>Select File</b>, and select a configuration file.</li> <li>Click <b>Config</b> to deliver the configurations.</li> </ol>
Manually modify a password	<ol style="list-style-type: none"> <li>Set <b>Configuration Operations</b> to <b>Modify Password</b>.</li> <li>Set <b>Modify Type</b> to <b>Manual Modify</b>.</li> <li>Enter the username for which you want to modify the password.</li> <li>Select the password size.</li> <li>Enter a new password.</li> <li>Click <b>Config</b> to deliver the configurations.</li> </ol>
Modify passwords in batches	<ol style="list-style-type: none"> <li>Set <b>Configuration Operations</b> to <b>Modify Password</b>.</li> <li>Set <b>Modify Type</b> to <b>Import Config File</b>.</li> <li>Click <b>Select File</b>, and select a configuration file.</li> <li>Click <b>Config</b> to deliver the configurations.</li> </ol>
Modify SNMP parameters	<ol style="list-style-type: none"> <li>Set <b>Configuration Operations</b> to <b>Modify SNMP Parameters</b>.</li> <li>Enter the username for which you want to modify SNMP parameters. This user must have the administrator permissions.</li> <li>Modify the SNMP parameters.</li> <li>Click <b>Config</b> to deliver the configurations.</li> </ol>
Delete a user	<ol style="list-style-type: none"> <li>Set <b>Configuration Operations</b> to <b>Delete User</b>.</li> <li>Enter the username that you want to delete.</li> <li>Click <b>Config</b> to deliver the configurations.</li> </ol>



### Note

- The ID of the user to be added cannot be a user ID that has already been added to the UniKits.
- Batch operations performed through a configuration file do not support the **Configures only failed servers** function.
- During user configuration, the progress bar is displayed on the page.
- After user configuration is completed, the configuration result is displayed on the page.

### 3.4.2.3 Configuring Time Parameters

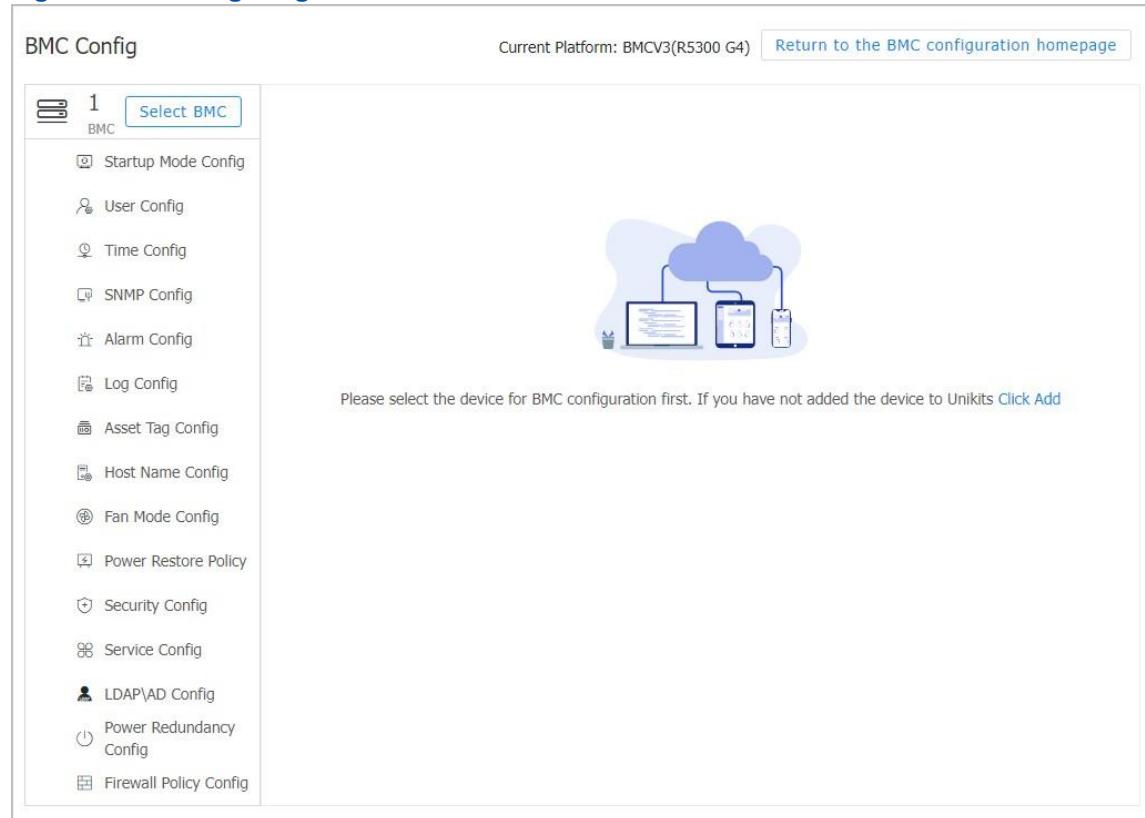
#### Abstract

This procedure describes how to configure time parameters, so that the **BMC** can obtain the correct time.

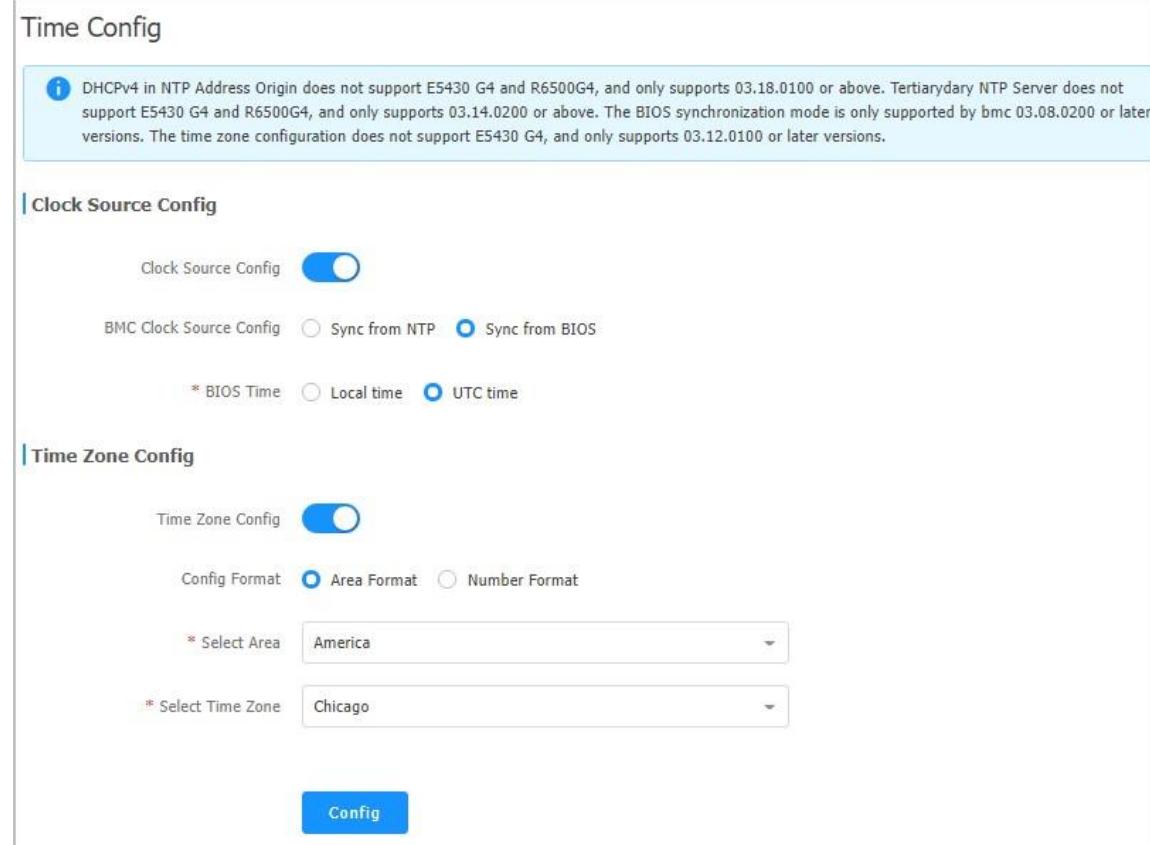
#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-24](#).

**Figure 3-24 Configuring BMC V3**



4. Click **Select BMC**, and select the BMC for which you want to configure the time synchronization mode and time zone.
5. In the left pane on the **BMC Config** page, click **Time Config**. The **Time Config** area is displayed, see [Figure 3-25](#).

**Figure 3-25 Time Config Area**


**Clock Source Config**

Clock Source Config

BMC Clock Source Config  Sync from NTP  Sync from BIOS

\* BIOS Time  Local time  UTC time

**Time Zone Config**

Time Zone Config

Config Format  Area Format  Number Format

\* Select Area: America

\* Select Time Zone: Chicago

**Config**

6. In the **Clock Source Config** area, select the BMC time synchronization mode and set the corresponding parameters.

To...	Do...
Synchronize time from an NTP server	<ol style="list-style-type: none"> <li>Turn on the <b>Clock Source Config</b> switch.</li> <li>Set <b>BMC Clock Source Config</b> to <b>Sync from NTP</b>.</li> <li>Set <b>NTP Address Origin</b> to <b>Static</b>.</li> <li>Configure the following parameters: <ul style="list-style-type: none"> <li><b>Primary NTP Server</b>: Enter the IP address or <b>FQDN</b> of NTP server 1, with the length not exceeding 127 characters. Required.</li> <li><b>Secondary NTP Server</b>: Enter the IP address or <b>FQDN</b> of NTP server 2, with the length not exceeding 127 characters. Optional.</li> <li><b>Tertiary NTP Server</b>: Enter the IP address or <b>FQDN</b> of NTP server 3, with the length not exceeding 127 characters. Optional.</li> <li><b>Sync Period</b>: Enter the time synchronization period in seconds, range: 60–65535.</li> </ul> </li> </ol>
Synchronize time from an NTP server over DHCP	<ol style="list-style-type: none"> <li>Turn on the <b>Clock Source Config</b> switch.</li> <li>Set <b>BMC Clock Source Config</b> to <b>Sync from NTP</b>.</li> <li>Set <b>NTP Address Origin</b> to <b>DHCPv4</b>.</li> </ol>
To...	Do...

Synchronize time from the BIOS	<ol style="list-style-type: none"> <li>Turn on the <b>Clock Source Config</b> switch.</li> <li>Set <b>BMC Clock Source Config</b> to <b>Sync from BIOS</b>.</li> <li>Set <b>BIOS Time</b>.           <ul style="list-style-type: none"> <li>If the server runs the Linux OS, select <b>UTC time</b>.</li> <li>If the server runs the Windows OS, select <b>Local time</b>.</li> </ul> <p><b>UTC</b> time is the universal time coordinated, and UTC time = local time - time zone difference. For example, if Beijing time is 08:00, the UTC time is 00:00.</p> </li></ol>
--------------------------------	--



### Note

If NTP-based time synchronization is enabled, the BMC first synchronizes time from **Primary NTP Server**. If the synchronization fails, it synchronizes time from **Secondary NTP Server** and **Tertiary NTP Server** in turn.

- Set the parameters in the **Time Zone Config** area. For a description of the parameters, refer to [Table 3-17](#).

**Table 3-17 Time Zone Parameter Descriptions**

Parameter	Description	
Time Zone Config	Turn on the <b>Time Zone Config</b> switch.	
Config Format	Select a time zone format. Options: <ul style="list-style-type: none"> <li><b>Area Format</b></li> <li><b>Number Format</b></li> </ul>	
Area Format	Select Area	Select an area.
	Select Time Zone	Select a time zone identified by location.
Number Format	Select Time Zone	Select a numeric time zone.

- Click **Config** to deliver the configurations.



### Note

- During time configuration, the progress bar is displayed on the page.
- After time configuration is completed, the configuration result is displayed on the page.

### 3.4.2.4 Configuring SNMP Parameters

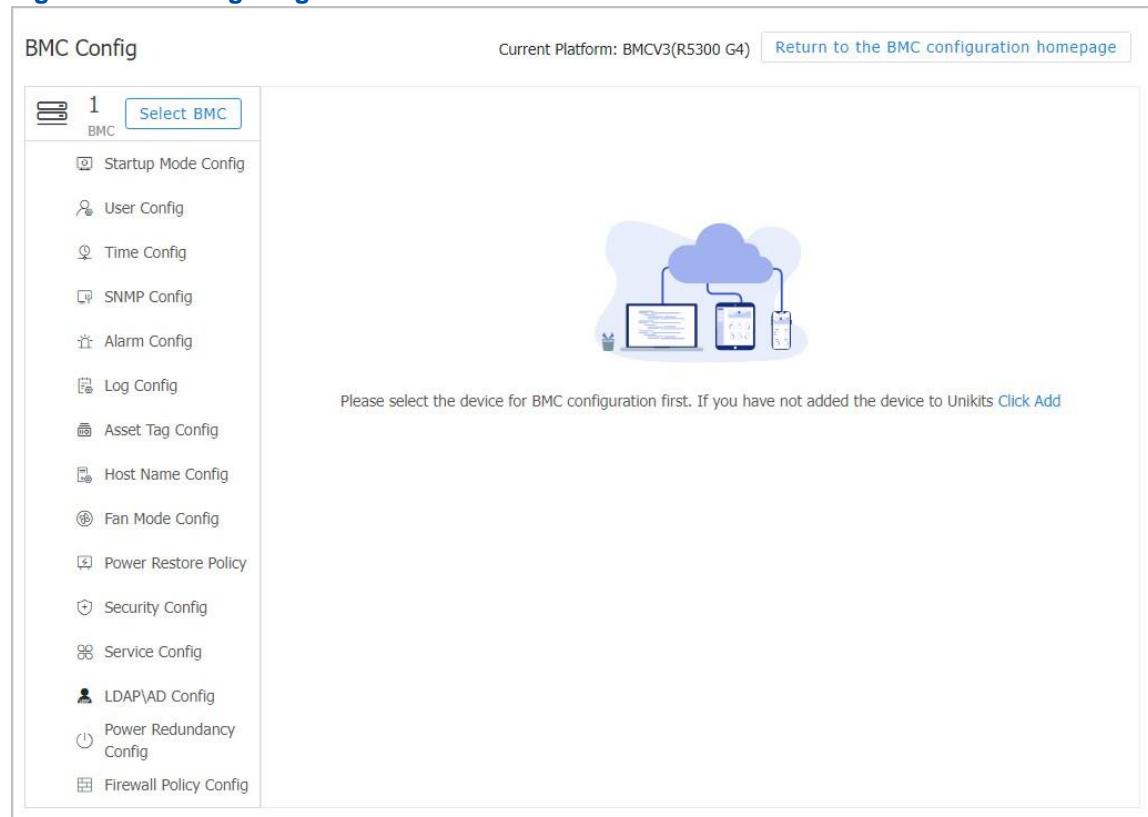
#### Abstract

This procedure describes how to configure **SNMP** parameters for communication between a **BMC** and a third-party **NMS**.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-26](#).

[Figure 3-26 Configuring BMC V3](#)



4. Click **Select BMC**, and select the BMC for which you want to configure SNMP parameters.
5. In the left pane on the **BMC Config** page, click **SNMP Config**. The **SNMP Config** area is displayed, see [Figure 3-27](#).

**Figure 3-27 SNMP Config Area**

SNMP Config

**Info** For the trap enable, trap community name, and trap destination address in domain name format configuration, the BMC version must be 03.14.0200 or above.  
The above configurations are not supported on the E5430 G4 server.  
R6500G4 server does not support that the trap destination is specified by domain name.  
If the SNMP service is set as disabled, the outband inspection, asset collection, and asset acceptance functions in the Unikits are unavailable, and the server cannot be re-managed after being removed from the BMC list.

Config SNMP Service	<input type="radio"/> Unchanged <input checked="" type="radio"/> Enable <input type="radio"/> Disable												
Config SNMP Port	<input type="radio"/> Unchanged <input checked="" type="radio"/> Modify												
* SNMP Port	<input type="text" value="161"/>												
Config Read-Only Community	<input type="radio"/> Unchanged <input checked="" type="radio"/> Modify												
* ②SNMP Read Community	<input type="text" value="zte_public"/>												
Config Read-Write Community	<input type="radio"/> Unchanged <input checked="" type="radio"/> Modify												
* ②SNMP Read/Write Community	<input type="text" value="platform"/>												
Config Trap Enable	<input type="radio"/> Unchanged <input checked="" type="radio"/> Modify												
* ②Trap Enable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable												
Config Trap Community Name	<input checked="" type="radio"/> Unchanged <input type="radio"/> Modify												
②Trap Destination	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>ID</th> <th>Dest Address</th> <th>Trap Port</th> <th>Protocol Type</th> <th>Trap User</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td>0</td> <td><input type="text" value="10.10.10.20"/></td> <td><input type="text" value="161"/></td> <td><input type="text" value="V2"/></td> <td><input type="text" value="Enter trap user"/></td> <td></td> </tr> </tbody> </table> <a href="#">+ Trap Destination</a>	ID	Dest Address	Trap Port	Protocol Type	Trap User	Delete	0	<input type="text" value="10.10.10.20"/>	<input type="text" value="161"/>	<input type="text" value="V2"/>	<input type="text" value="Enter trap user"/>	
ID	Dest Address	Trap Port	Protocol Type	Trap User	Delete								
0	<input type="text" value="10.10.10.20"/>	<input type="text" value="161"/>	<input type="text" value="V2"/>	<input type="text" value="Enter trap user"/>									

**Config**

6. Set the parameters. For a description of the parameters, refer to [Table 3-18](#).

**Table 3-18 SNMP Parameter Descriptions**

Parameter	Description
<b>Config SNMP Service</b>	<ul style="list-style-type: none"> <li>To keep the original SNMP service configuration of the server, select <b>Unchanged</b>.</li> <li>To enable the SNMP service, select <b>Enable</b>.</li> <li>To disable the SNMP service, select <b>Disable</b>.</li> </ul> <p>If the SNMP service is disabled, some functions are unavailable, for example, out-of-band management, asset collection, and asset acceptance. When a server is removed from the device list, the server cannot be managed.</p>
<b>Config SNMP Port</b>	<ul style="list-style-type: none"> <li>To keep the original SNMP port of the server, select <b>Unchanged</b>.</li> <li>To modify the SNMP port of the server, select <b>Modify</b> and set <b>SNMP Port</b>.</li> </ul>

<b>Config Read-Only Community</b>	<ul style="list-style-type: none"> <li>To keep the original read-only community of the server, select <b>Unchanged</b>.</li> </ul>
<b>Parameter</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>To modify the read-only community of the server, select <b>Modify</b> and set <b>SNMP Read Community</b>.</li> </ul>
<b>Config Read-Write Community</b>	<ul style="list-style-type: none"> <li>To keep the original read-write community of the server, select <b>Unchanged</b>.</li> <li>To modify the read-write community of the server, select <b>Modify</b> and set <b>SNMP Read/Write Community</b>.</li> </ul>
<b>Config Trap Enable</b>	<ul style="list-style-type: none"> <li>To keep the original trap enabling status of the server, select <b>Disable</b>.</li> <li>To modify the trap enabling status of the server, select <b>Modify</b> and set <b>Trap Enable</b>.</li> </ul>
<b>Config Trap Community Name</b>	<ul style="list-style-type: none"> <li>To keep the original trap community name of the server, select <b>Unchanged</b>.</li> <li>To modify the trap community name of the server, select <b>Modify</b> and set <b>Trap Community Name</b>.</li> </ul>
<b>Trap Destination</b>	<p>Configure trap destinations. A maximum of 15 trap destinations can be configured.</p> <p>Click  <b>Trap Destination</b> to add another trap destination.</p> <ul style="list-style-type: none"> <li><b>ID</b>: range: 0–14.</li> <li><b>Dest Address</b>: SNMP destination <b>IP</b> address.</li> <li><b>Trap Port</b>: range: 1–65535.</li> <li><b>Protocol Type</b>: SNMP version, including V1, V2, and V3.</li> <li><b>Trap User</b>: valid and required when <b>Protocol Type</b> is set to <b>V3</b>. You must enter an existing SNMP trap username with administrator permissions.</li> </ul>

7. Click **Config** to deliver the configurations.



- During SNMP parameter configuration, the progress bar is displayed on the page.
- After SNMP parameter configuration is completed, the configuration result is displayed on the page.

### 3.4.2.5 Configuring Alarm Parameters

#### Abstract

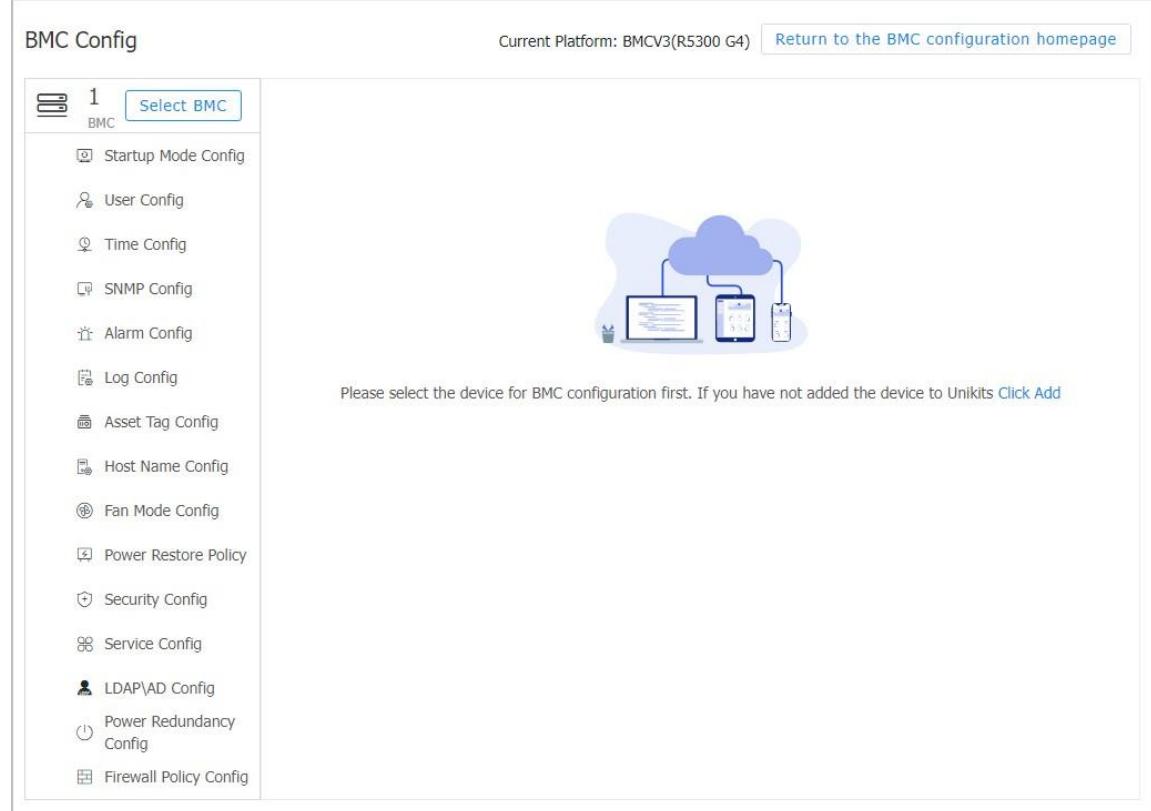
Alarm parameters include alarm source parameters and pre-alarm parameters.

This procedure describes how to configure alarm parameters to send notifications or alarms when alarms occur on servers or the number of alarms reaches the threshold, so that maintenance personnel can locate and handle faults in a timely manner.

## Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-28](#).

**Figure 3-28 Configuring BMC V3**



4. In the left pane on the **BMC Config** page, click **Alarm Config**. The **Alarm Config** area is displayed, see [Figure 3-29](#).

**Figure 3-29 Alarm Config Area**

### Alarm Config

Alarm Config

Select the Template Server Server

Selected : 10.239.226.145 (N/A)

Alarm Item Config	Slot	NetPort	Power Supply No.												
	<input type="button" value="Batch Enable"/>	<input type="button" value="Batch Disable"/>	<input type="button" value="Batch Unchanged"/>												
	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th style="padding: 2px;">Slot</th> <th style="padding: 2px;">Operation</th> </tr> </thead> <tbody> <tr><td style="padding: 2px;"><input type="checkbox"/></td><td style="padding: 2px;">Slot0</td></tr> <tr><td style="padding: 2px;"><input type="checkbox"/></td><td style="padding: 2px;">Slot1</td></tr> <tr><td style="padding: 2px;"><input type="checkbox"/></td><td style="padding: 2px;">Slot2</td></tr> <tr><td style="padding: 2px;"><input type="checkbox"/></td><td style="padding: 2px;">Slot3</td></tr> <tr><td style="padding: 2px;"><input type="checkbox"/></td><td style="padding: 2px;">Slot4</td></tr> </tbody> </table>			Slot	Operation	<input type="checkbox"/>	Slot0	<input type="checkbox"/>	Slot1	<input type="checkbox"/>	Slot2	<input type="checkbox"/>	Slot3	<input type="checkbox"/>	Slot4
Slot	Operation														
<input type="checkbox"/>	Slot0														
<input type="checkbox"/>	Slot1														
<input type="checkbox"/>	Slot2														
<input type="checkbox"/>	Slot3														
<input type="checkbox"/>	Slot4														
	Total 14 <span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 5px; margin: 0 5px;">&lt;&lt;</span> <span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 5px; margin: 0 5px;">&lt;</span> <span style="border: 1px solid #0072bc; border-radius: 5px; padding: 2px 5px; color: white;">1</span> <span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 5px; margin: 0 5px;">2</span> <span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 5px; margin: 0 5px;">3</span> <span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 5px; margin: 0 5px;">&gt;</span> <span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 5px; margin: 0 5px;">&gt;&gt;</span> <span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 5px; margin: 0 5px;">5 / Page</span> <span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 5px; margin: 0 5px;">&gt;</span>														

Pre-alarm Config

CPU PreAlarm  No Modify  Disable  Alarms  
 Notification

Memory PreAlarm  No Modify  Disable  Alarms  
 Notification

PCIe PreAlarm  No Modify  Disable  Alarms  
 Notification

Select Server Select Server

Selected : 1

Config

5. Set the parameters. For a description of the parameters, refer to [Table 3-19](#).

**Table 3-19 Alarm Configuration Parameter Descriptions**

Parameter	Description
Alarm Config	<ul style="list-style-type: none"> <li>To configure an alarm source, turn on the <b>Alarm Config</b> switch.</li> <li>To not configure an alarm source, turn off the <b>Alarm Config</b> switch.</li> </ul>

Parameter	Description
Select the Template Server	Click <b>Server</b> , and select a server. The <b>Slot</b> , <b>NetPort</b> , and <b>Power Supply No.</b> of the server are obtained and used as the template to configure alarm sources.
Alarm Item Config	<p>In the <b>Operation</b> column, click <b>Enable</b>, <b>Disable</b>, and <b>Unchanged</b> for the desired alarm source to configure whether to report alarms.</p> <ul style="list-style-type: none"> <li>● <b>Enable</b>: indicates to report alarms.</li> <li>● <b>Disable</b>: indicates not to report alarms.</li> <li>● <b>No Modify</b>: indicates not to modify the original server configurations. If you select multiple alarm sources, click <b>Batch Enable</b>, <b>Batch Disable</b>, or <b>Batch Unchanged</b> to set whether to report alarms.</li> </ul>
Pre-alarm Config	<ul style="list-style-type: none"> <li>● To configure the pre-alarm function, turn on the <b>Pre-alarm Config</b> switch.</li> <li>● To not configure the pre-alarm function, turn off the <b>Pre-alarm Config</b> switch.</li> </ul>
CPU PreAlarm	<p>Select whether to configure the CPU pre-alarm function. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configurations.</li> <li>● <b>Disable</b>: indicates to disable the CPU pre-alarm function.</li> <li>● <b>Alarms</b>: indicates to send an alarm if the CPU usage reaches the threshold.</li> <li>● <b>Notification</b>: indicates to send a notification if the CPU usage reaches the threshold.</li> </ul> <p>If <b>Alarms</b> or <b>Notification</b> is selected, set <b>Pre-alarm Threshold</b> (range: 1–100).</p>
Memory PreAlarm	<p>Select whether to configure the memory pre-alarm function. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configurations.</li> <li>● <b>Disable</b>: indicates to disable the memory pre-alarm function.</li> <li>● <b>Alarms</b>: indicates to send an alarm if the memory usage reaches the threshold.</li> </ul> <p>If <b>Alarms</b> is selected, set <b>Alarm Type</b>. Options:</p> <ul style="list-style-type: none"> <li>● <b>Accumulate Policy</b>: If the number of alarms reaches <b>CE Accumulate Alarm Threshold</b> within <b>CE Accumulate Alarm Window</b>, an alarm indicating memory alarm accumulation is raised.</li> <li>● <b>Accumulate&amp;Storm Policy</b>: indicates to use both the alarm accumulation policy and alarm storm policy. <ul style="list-style-type: none"> <li>→ If the number of alarms reaches <b>CE Accumulate Alarm Threshold</b> within <b>CE Accumulate Alarm Window</b>, an alarm indicating memory alarm accumulation is raised.</li> <li>→ If the number of alarms reaches <b>CE Storm Alarm Time Threshold</b> within <b>CE Storm Alarm Time Window</b>, an alarm indicating too many memory alarms generated within a short time is raised.</li> </ul> </li> </ul> <p><b>CE Storm Alarm Time Window</b> is less than <b>CE Accumulate Alarm Window</b>, and <b>CE Storm Alarm Time Threshold</b> is less than <b>CE Accumulate Alarm Threshold</b>.</p>

PCIe PreAlarm	Select whether to configure the PCIe pre-alarm function. Options: ● <b>No Modify</b> : indicates not to modify the original server configurations.
<b>Parameter</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>● <b>Disable</b>: indicates to disable the PCIe pre-alarm function.</li> <li>● <b>Alarms</b>: indicates to send an alarm if the PCIe usage reaches the threshold.</li> <li>● <b>Notification</b>: indicates to send a notification if the PCIe usage reaches the threshold.</li> </ul> <p>If <b>Alarms</b> or <b>Notification</b> is selected, set <b>Pre-alarm Threshold</b> (range: 1–100).</p>
Select Server	Click <b>Select Server</b> to select the servers for which you want to configure alarm parameters.

6. Click **Config** to deliver the configurations.



#### Note

- During alarm parameter configuration, the progress bar is displayed on the page.
- After alarm parameter configuration is completed, the configuration result is displayed on the page.

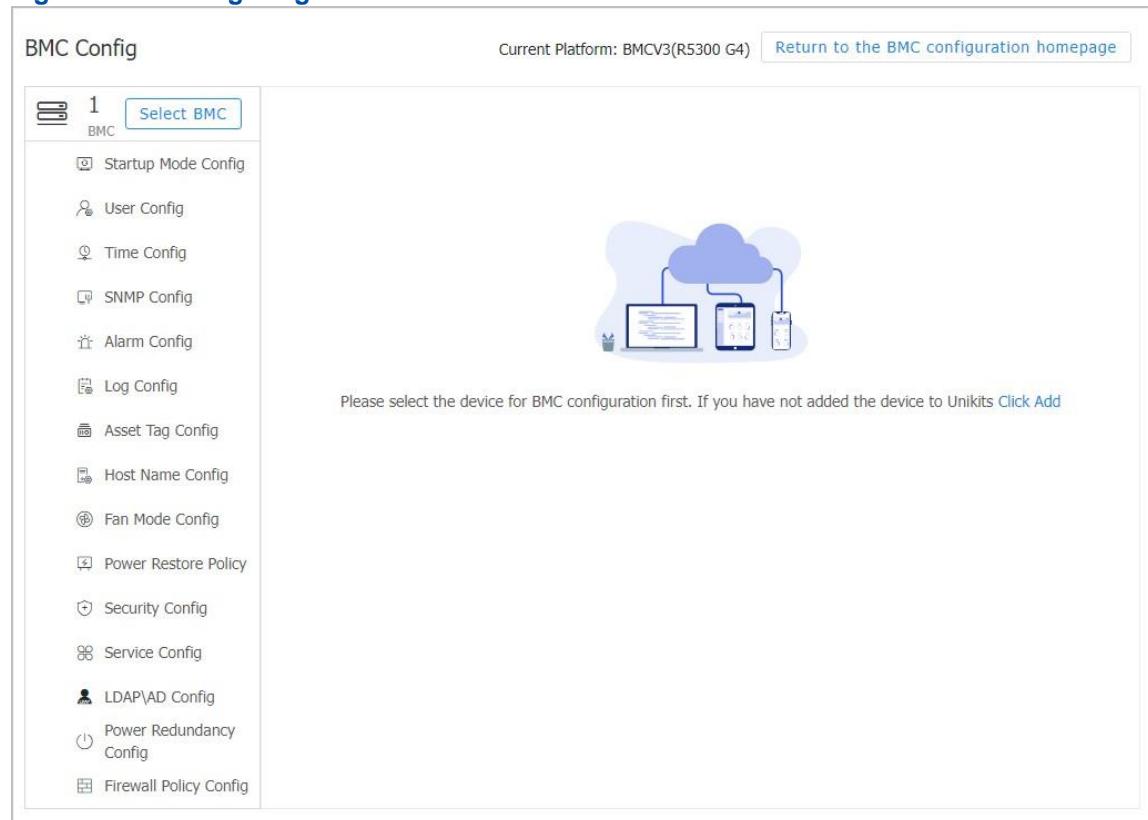
### 3.4.2.6 Configuring Syslog Parameters

#### Abstract

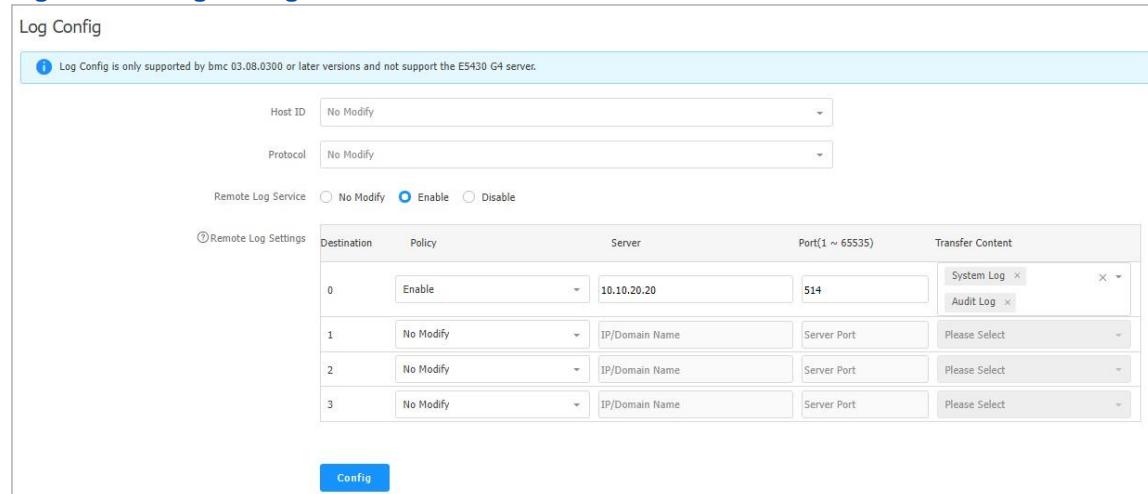
This procedure describes how to configure syslog parameters to upload local logs (including audit logs, operation logs, and system logs) of a server to a syslog server.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-30](#).

**Figure 3-30 Configuring BMC V3**

4. Click **Select BMC**, and select the BMC for which you want to configure syslog parameters.
5. In the left pane on the **BMC Config** page, click **Log Config**. The **Log Config** area is displayed, see [Figure 3-31](#).

**Figure 3-31 Log Config Area**


Destination	Policy	Server	Port(1 ~ 65535)	Transfer Content
0	Enable	10.10.20.20	514	<input type="checkbox"/> System Log <input type="checkbox"/> Audit Log
1	No Modify	IP/Domain Name	Server Port	<input type="checkbox"/> Please Select
2	No Modify	IP/Domain Name	Server Port	<input type="checkbox"/> Please Select
3	No Modify	IP/Domain Name	Server Port	<input type="checkbox"/> Please Select

6. Set the parameters. For a description of the parameters, refer to [Table 3-20](#).

**Table 3-20 Log Parameter Descriptions**

Parameter	Description
-----------	-------------

Host ID	Select the host ID to be uploaded to server logs. Options: <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original configurations.</li> <li>● <b>Board serial number</b>: indicates to use the board serial number.</li> <li>● <b>Asset label</b>: indicates to use the asset tag.</li> <li>● <b>Host Name</b>: indicates to use the host name.</li> </ul>
Protocol	Select the log transmission protocol. Options: <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original configurations.</li> <li>● <b>UDP</b>: indicates to use UDP.</li> <li>● <b>TCP</b>: indicates to use TCP.</li> </ul>
Remote Log Service	Set the parameters of the log server that logs are to be synchronized with: <ul style="list-style-type: none"> <li>● <b>Policy</b>: select whether to enable the configuration policy. Options include <b>No Modify</b>, <b>Enable</b>, and <b>Disable</b>. If the configuration policy is disabled, the corresponding configurations on the selected BMC are cleared.</li> <li>● <b>Server</b>: enter the <b>IP</b> address of the log server.</li> <li>● <b>Port</b>: enter the port number of the log server. Range: 1–65535.</li> <li>● <b>Transfer Content</b>: select at least one type of logs to be transmitted, including system logs, operation logs, and audit logs.</li> </ul> <p>Note: Only two remote log servers can be configured.</p>

7. Click **Config** to deliver the configurations.



#### Note

- During remote log parameter configuration, the progress bar is displayed on the page.
- After remote log parameter configuration is completed, the configuration result is displayed on the page.

After the configuration is completed, if the following message is displayed, the Redfish service of the server is not started. For how to enable the Redfish service, refer to "[3.4.2.12 Configuring Services](#)".

Redfish service unavailable, please config again after redfish service is open.

### 3.4.2.7 Configuring Asset Tags

#### Abstract

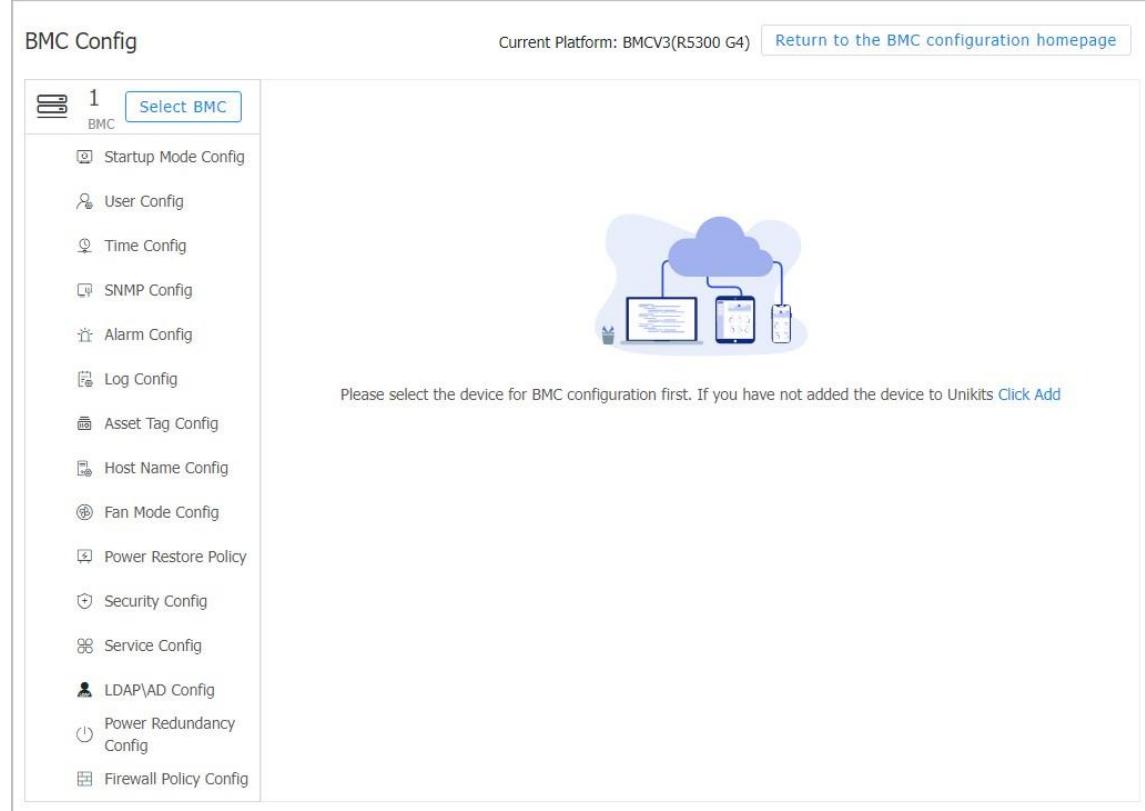
This procedure describes how to modify the asset tags of servers when they need to be updated in batches.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.

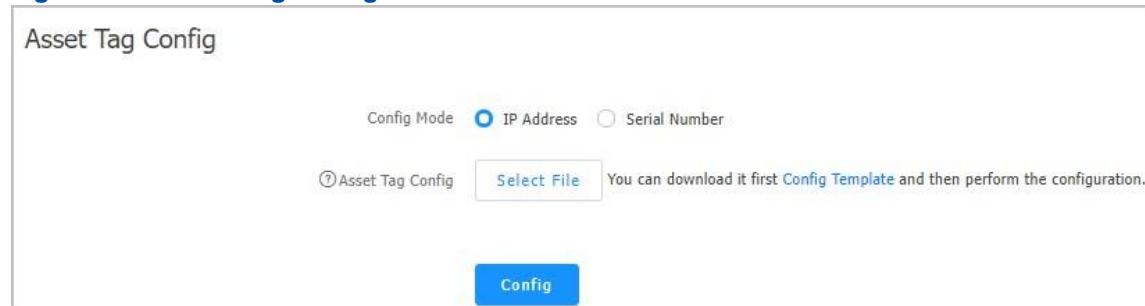
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-32](#).

**Figure 3-32 Configuring BMC V3**



4. In the left pane on the **BMC Config** page, click **Asset Tag Config**. The **Asset Tag Config** area is displayed, see [Figure 3-33](#).

**Figure 3-33 Asset Tag Config Area**



5. Set the parameters. For a description of the parameters, refer to [Table 3-21](#).

**Table 3-21 Asset Tag Parameter Descriptions**

Parameter	Description
-----------	-------------

Config Mode	<ul style="list-style-type: none"> <li>To match servers based on <b>BMC IP</b> addresses and then configure asset tags, select <b>IP Address</b>. In this mode, you do not need to select a BMC.</li> <li>To match servers based on serial numbers and then configure asset tags, select <b>Serial Number</b>. In this mode, you need to select a BMC.</li> </ul>
Asset Tag Config	<ol style="list-style-type: none"> <li>(Optional) If there is no asset tag configuration file, click <b>Config Template</b> to download and fill in the configuration template.             <ul style="list-style-type: none"> <li>If <b>Config Mode</b> is set to <b>IP Address</b>, the name of the configuration template downloaded to your local PC is <i>ImportAssetTag.csv</i>.</li> <li>If <b>Config Mode</b> is set to <b>Serial Number</b>, the name of the configuration template downloaded to your local PC is <i>ImportAssetTagWithSN.csv</i>.</li> </ul> </li> <li>Click <b>Select File</b>, and select the edited configuration file. After a file is selected, the tool automatically verifies the file. If the check fails, the error lines and causes are displayed.</li> </ol>

6. Click **Config** to deliver the configurations.



#### Note

- During asset tag configuration, the progress bar is displayed on the page.
- After asset tag configuration is completed, the configuration result is displayed on the page.

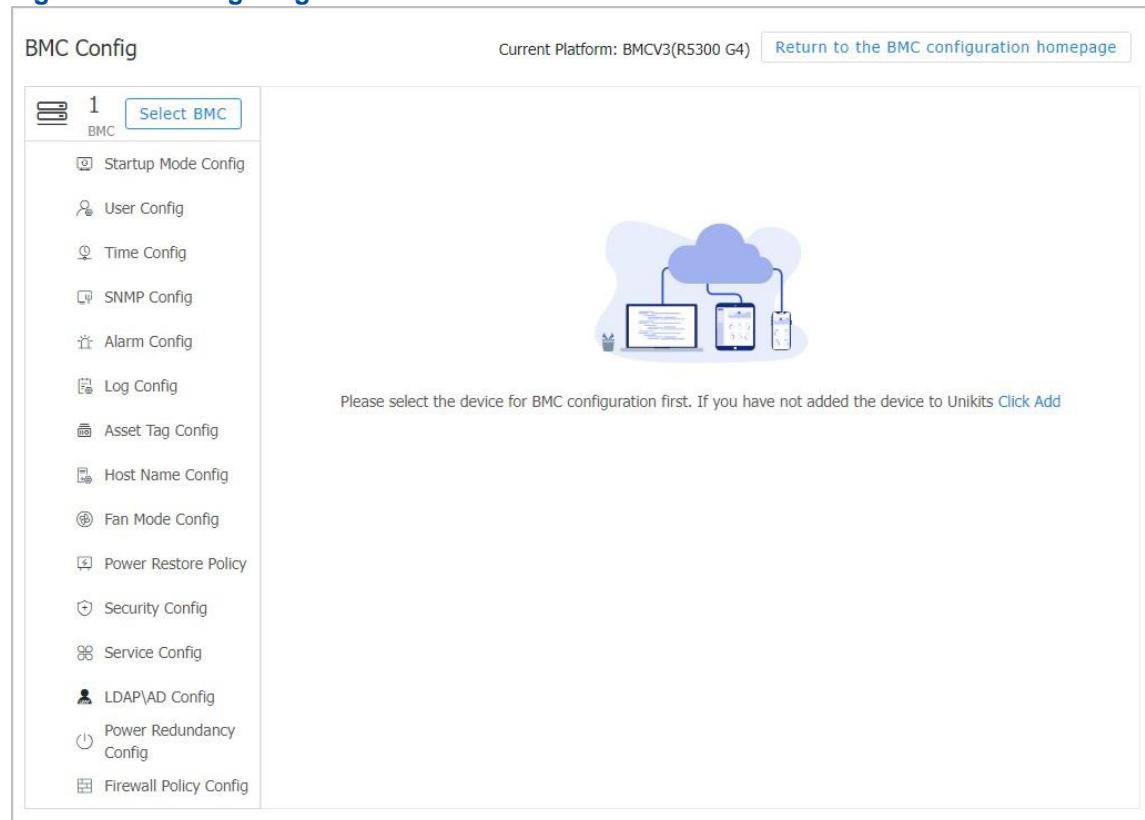
### 3.4.2.8 Configuring a Host Name

#### Abstract

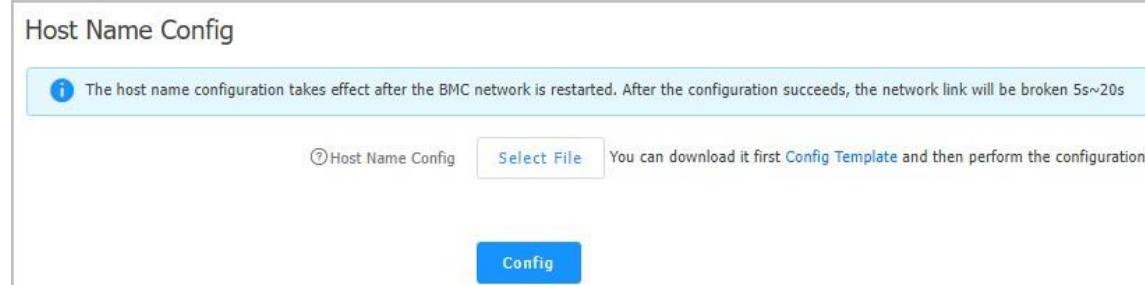
This procedure describes how to configure a host name to identify the corresponding server.

#### Steps

- Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
- From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
- Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-34](#).

**Figure 3-34 Configuring BMC V3**


4. In the left pane on the **BMC Config** page, click **Host Name Config**. The **Host Name Config** area is displayed, see [Figure 3-35](#).

**Figure 3-35 Host Name Config Area**


5. (Optional) If there is no host name configuration file, click **Config Template** to download and fill in the configuration template.



The name of the configuration template downloaded to your local PC is *ImportHostname.csv*.

6. Click **Select File**, and select the edited configuration file.



After a file is selected, the tool automatically verifies the file. If the check fails, the error lines and causes are displayed.

---

7. Click **Config** to deliver the configurations.

---



- During host name configuration, the progress bar is displayed on the page.
- After host name configuration is completed, the configuration result is displayed on the page.

---

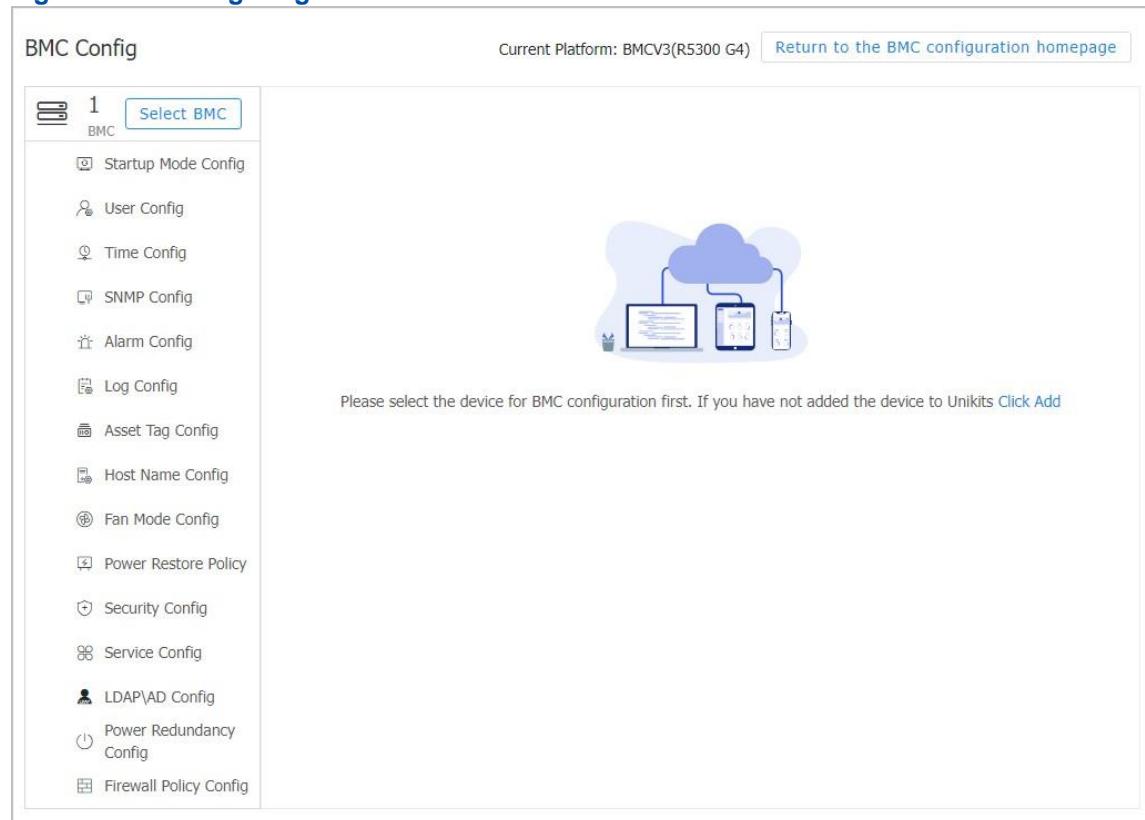
### 3.4.2.9 Configuring a Heat Dissipation Mode

#### Abstract

A heat dissipation mode is configured in accordance with the environment where a server is held to ensure the performance and stability of the server.

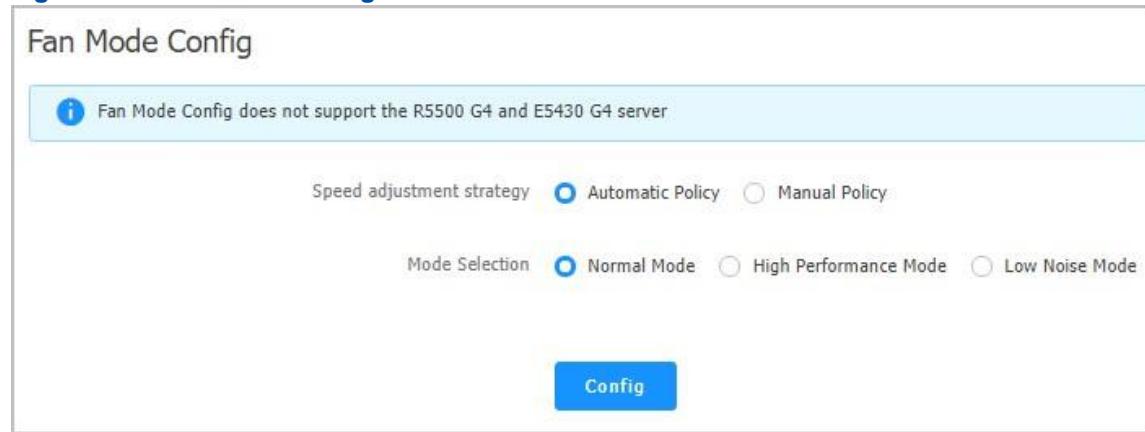
#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-36](#).

**Figure 3-36 Configuring BMC V3**


The screenshot shows the 'BMC Config' page. At the top, it says 'Current Platform: BMCV3(R5300 G4)' and 'Return to the BMC configuration homepage'. On the left, a sidebar lists various configuration options: Startup Mode Config, User Config, Time Config, SNMP Config, Alarm Config, Log Config, Asset Tag Config, Host Name Config, Fan Mode Config, Power Restore Policy, Security Config, Service Config, LDAP\AD Config, Power Redundancy Config, and Firewall Policy Config. On the right, there is a cloud icon with three devices (laptop, smartphone, tablet) connected to it, and a message: 'Please select the device for BMC configuration first. If you have not added the device to Unikits [Click Add](#)'.

4. Click **Select BMC**, and select the BMC for which you want to configure the heat dissipation mode.
5. In the left pane on the **BMC Config** page, click **Fan Mode Config**. The **Fan Mode Config** area is displayed, see [Figure 3-37](#).

**Figure 3-37 Fan Mode Config Area**


The screenshot shows the 'Fan Mode Config' area. At the top, a message says 'Fan Mode Config does not support the R5500 G4 and E5430 G4 server'. Below this, there are two sections: 'Speed adjustment strategy' with radio buttons for 'Automatic Policy' (selected) and 'Manual Policy', and 'Mode Selection' with radio buttons for 'Normal Mode' (selected), 'High Performance Mode', and 'Low Noise Mode'. At the bottom is a blue 'Config' button.

6. Set the parameters. For a description of the parameters, refer to [Table 3-22](#).

**Table 3-22 Parameter Descriptions for Heat Dissipation Mode**

Parameter	Description
-----------	-------------

Speed adjustment strategy	Select the speed regulation policy. Options: <ul style="list-style-type: none"> <li>● <b>Automatic Policy</b></li> <li>● <b>Manual Policy</b></li> </ul>
Mode Selection	This parameter is required when <b>Speed adjustment strategy</b> is set to <b>Automatic Policy</b> .  Select an automatic speed regulation mode. Options: <ul style="list-style-type: none"> <li>● <b>Normal Mode</b>: selected when there is clearance above the top surface of the server and the server is insensitive to noise.</li> <li>● <b>High Performance Mode</b>: selected when servers are stacked together and there is no clearance between them.</li> <li>● <b>Low Noise Mode</b>: selected when servers are placed in an office or other areas that are sensitive to noise.</li> </ul>
Speed Percentage	This parameter is required when <b>Speed adjustment strategy</b> is set to <b>Manual Policy</b> .  Speed percentage indicates the ratio of the current speed of a fan to its maximum speed.  Enter the speed percentage (range: 10%–100%).

7. Click **Config** to deliver the configurations.



- During heat dissipation mode configuration, the progress bar is displayed on the page.
- After heat dissipation mode configuration is completed, the configuration result is displayed on the page.

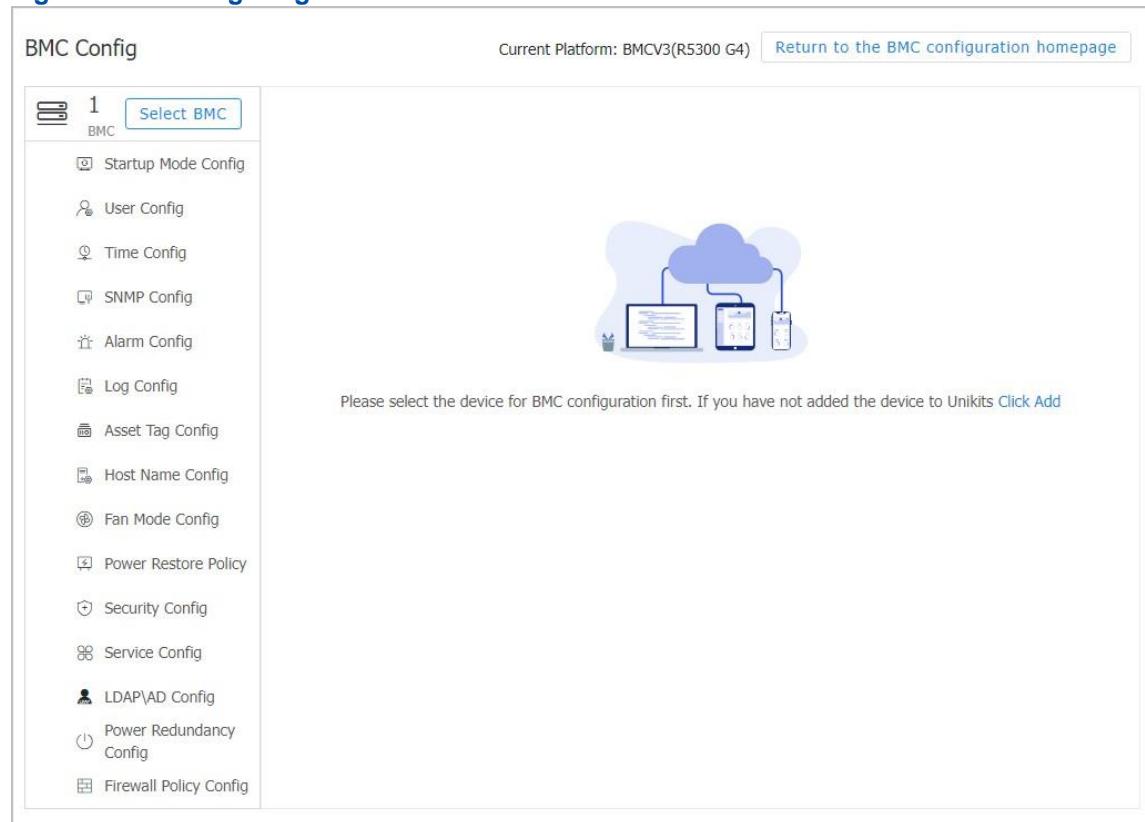
### 3.4.2.10 Configuring the Host Startup Policy

#### Abstract

This procedure describes how to configure the host startup policy to specify the power status after the server power is restored.

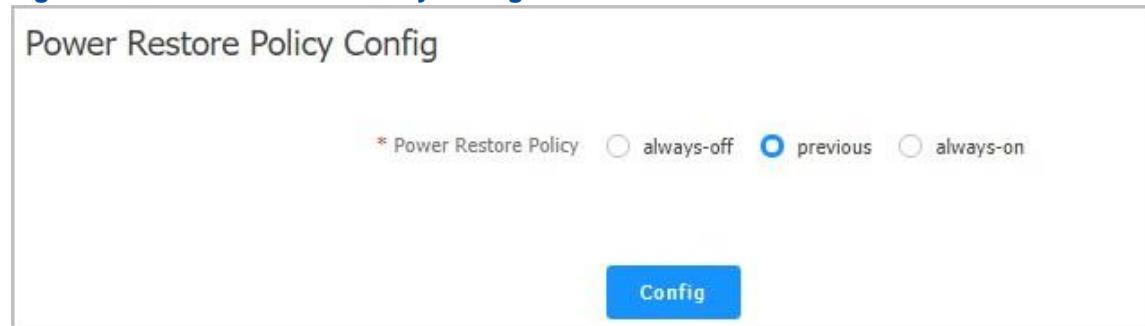
#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-38](#).

**Figure 3-38 Configuring BMC V3**


The screenshot shows the 'BMC Config' page. At the top, it says 'BMC Config' and 'Current Platform: BMCV3(R5300 G4)'. There is a 'Return to the BMC configuration homepage' link. On the left, a sidebar lists various configuration options: Startup Mode Config, User Config, Time Config, SNMP Config, Alarm Config, Log Config, Asset Tag Config, Host Name Config, Fan Mode Config, Power Restore Policy, Security Config, Service Config, LDAP\AD Config, Power Redundancy Config, and Firewall Policy Config. A blue cloud icon with a network connection is displayed in the center. A message at the bottom of the sidebar says: 'Please select the device for BMC configuration first. If you have not added the device to Unikits [Click Add](#)'.

4. Click **Select BMC**, and select the BMC for which you want to configure the host startup policy.
5. In the left pane on the **BMC Config** page, click **Power Restore Policy**. The **Power Restore Policy Config** area is displayed, see [Figure 3-39](#).

**Figure 3-39 Power Restore Policy Config Area**


The screenshot shows the 'Power Restore Policy Config' area. It features a radio button selection for the 'Power Restore Policy'. The options are: \* Power Restore Policy (radio button is not selected), always-off (radio button is not selected), previous (radio button is selected), and always-on (radio button is not selected). A blue 'Config' button is located at the bottom right.

6. Select host startup policy. Options:
  - **always-off**: When the server is powered off and then restores power, the host is in the power-off status.
  - **previous**: When the server is powered off and then restores power, the host is in the status the same as that before the power-off.

- **always-on:** When the server is powered off and then restores power, the host is in the power-on status.

7. Click **Config** to deliver the configurations.

---



#### Note

- During host startup policy configuration, the progress bar is displayed on the page.
- After host startup policy configuration is completed, the configuration result is displayed on the page.

---

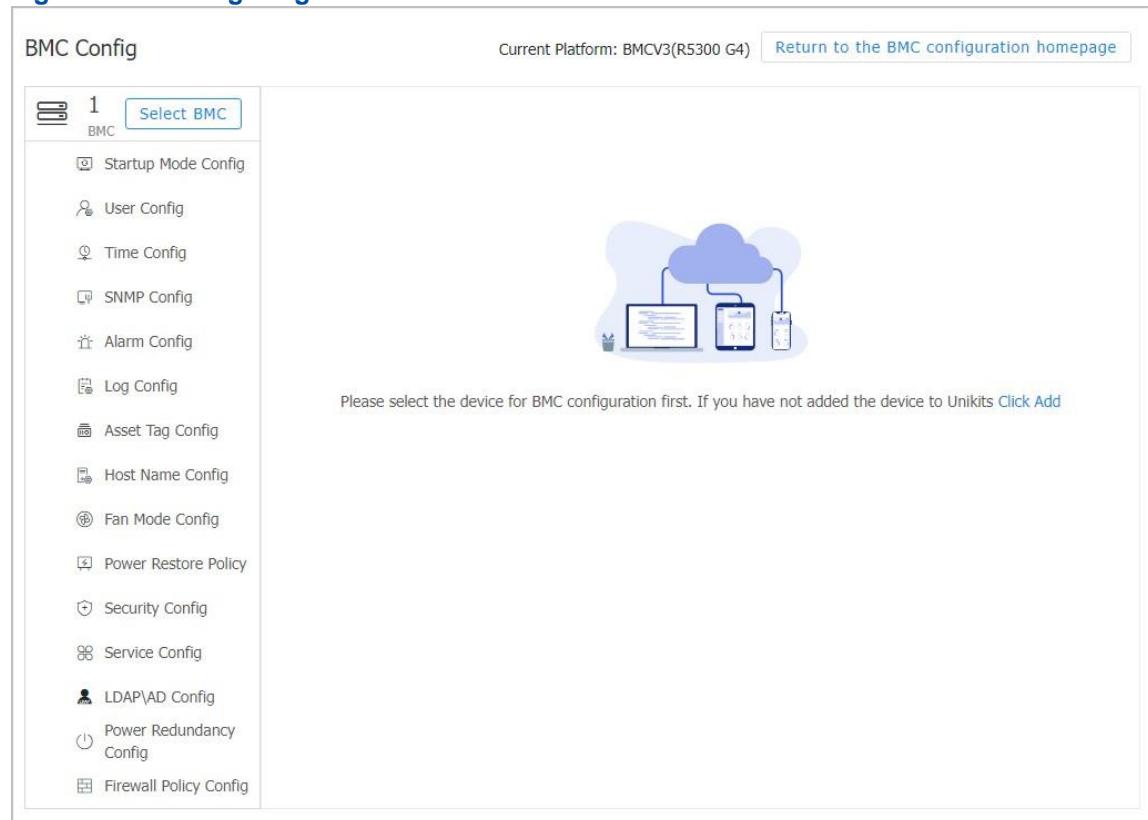
### 3.4.2.11 Configuring Security Parameters

#### Abstract

This procedure describes how to configure security parameters to ensure the security of servers during remote operations.

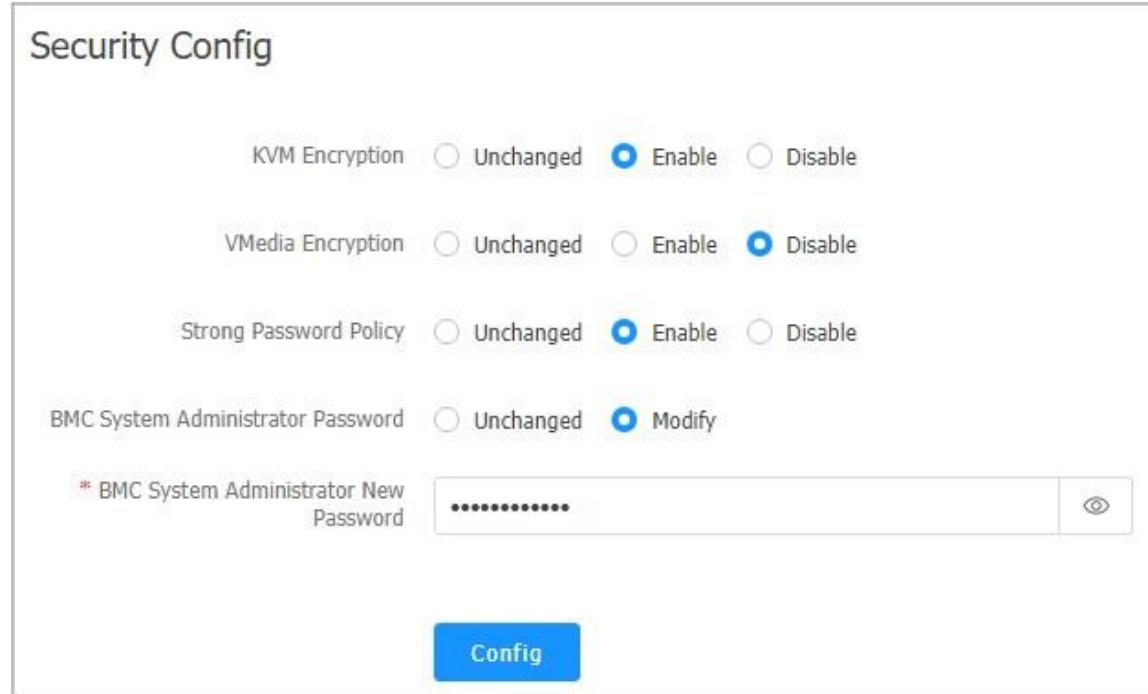
#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-40](#).

**Figure 3-40 Configuring BMC V3**


The screenshot shows the 'BMC Config' page. At the top, it says 'BMC Config' and 'Current Platform: BMCV3(R5300 G4)'. There is a link to 'Return to the BMC configuration homepage'. On the left, a sidebar lists various configuration options: Startup Mode Config, User Config, Time Config, SNMP Config, Alarm Config, Log Config, Asset Tag Config, Host Name Config, Fan Mode Config, Power Restore Policy, Security Config, Service Config, LDAP\AD Config, Power Redundancy Config, and Firewall Policy Config. On the right, there is a cloud icon with three devices (laptop, smartphone, tablet) connected to it, and a message: 'Please select the device for BMC configuration first. If you have not added the device to Unikits [Click Add](#)'.

4. Click **Select BMC**, and select the BMC for which you want to configure security parameters.
5. In the left pane on the **BMC Config** page, click **Security Config**. The **Security Config** area is displayed, see [Figure 3-41](#).

**Figure 3-41 Security Config Area**


The screenshot shows the 'Security Config' area. It includes the following settings:

- KVM Encryption: Radio buttons for 'Unchanged' (selected), 'Enable', and 'Disable'.
- VMedia Encryption: Radio buttons for 'Unchanged' (selected), 'Enable', and 'Disable'.
- Strong Password Policy: Radio buttons for 'Unchanged' (selected), 'Enable', and 'Disable'.
- BMC System Administrator Password: Radio buttons for 'Unchanged' (selected) and 'Modify'. Below it is a password input field with the placeholder '\* BMC System Administrator New Password' and a visibility icon.

At the bottom is a large blue 'Config' button.

6. Set the parameters. For a description of the parameters, refer to [Table 3-23](#).

**Table 3-23 Security Parameter Descriptions**

Parameter	Description
KVM Encryption	Select whether to enable KVM encryption. After <b>KVM Encryption</b> is set to <b>Enable</b> , encryption is implemented during KVM-based remote operations on the server. You cannot enable KVM encryption if you have enabled application support on the KVM service port.
VMedia Encryption	Select whether to enable VMedia encryption. After <b>VMedia Encryption</b> is set to <b>Enable</b> , files remotely uploaded to the server through the KVM are encrypted.
Strong Password Policy	Select whether to enable the strong password policy. Options: <ul style="list-style-type: none"><li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li><li>● <b>Enable</b>: indicates to enable the strong password policy.</li><li>● <b>Disable</b>: indicates to disable the strong password policy.</li></ul>
BMC System Administrator Password	Password for logging in to the server through <a href="#">SSH</a> . Select whether to modify the original BMC system administrator password of the server. Options: <ul style="list-style-type: none"><li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li><li>● <b>Modify</b>: indicates to modify the original password. Enter the new password in the <b>BMC System Administrator New Password</b> text box.</li></ul>

7. Click **Config** to deliver the configurations.



- During security parameter configuration, the progress bar is displayed on the page.
- After security parameter configuration is completed, the configuration result is displayed on the page.

### 3.4.2.12 Configuring Services

#### Abstract

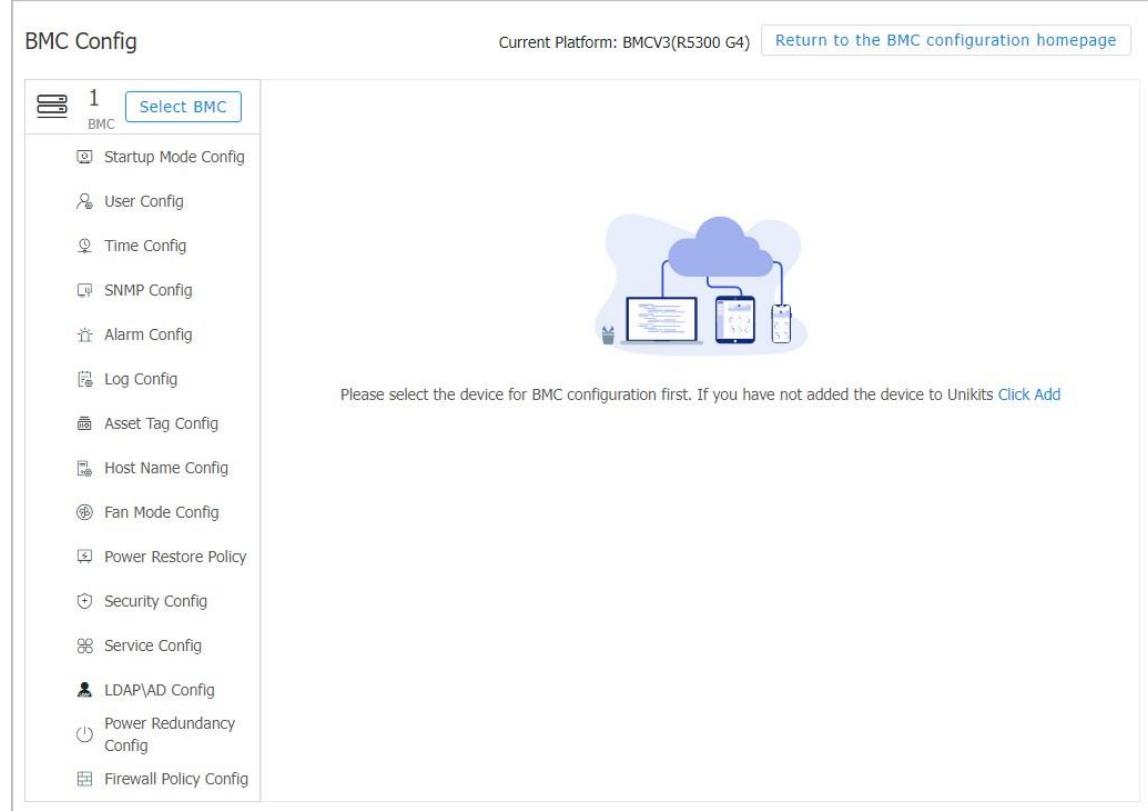
This procedure describes how to configure the status, secure port, non-secure port, and timeout for each service of a [BMC](#).

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.

2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-42](#).

**Figure 3-42 Configuring BMC V3**



BMC Config

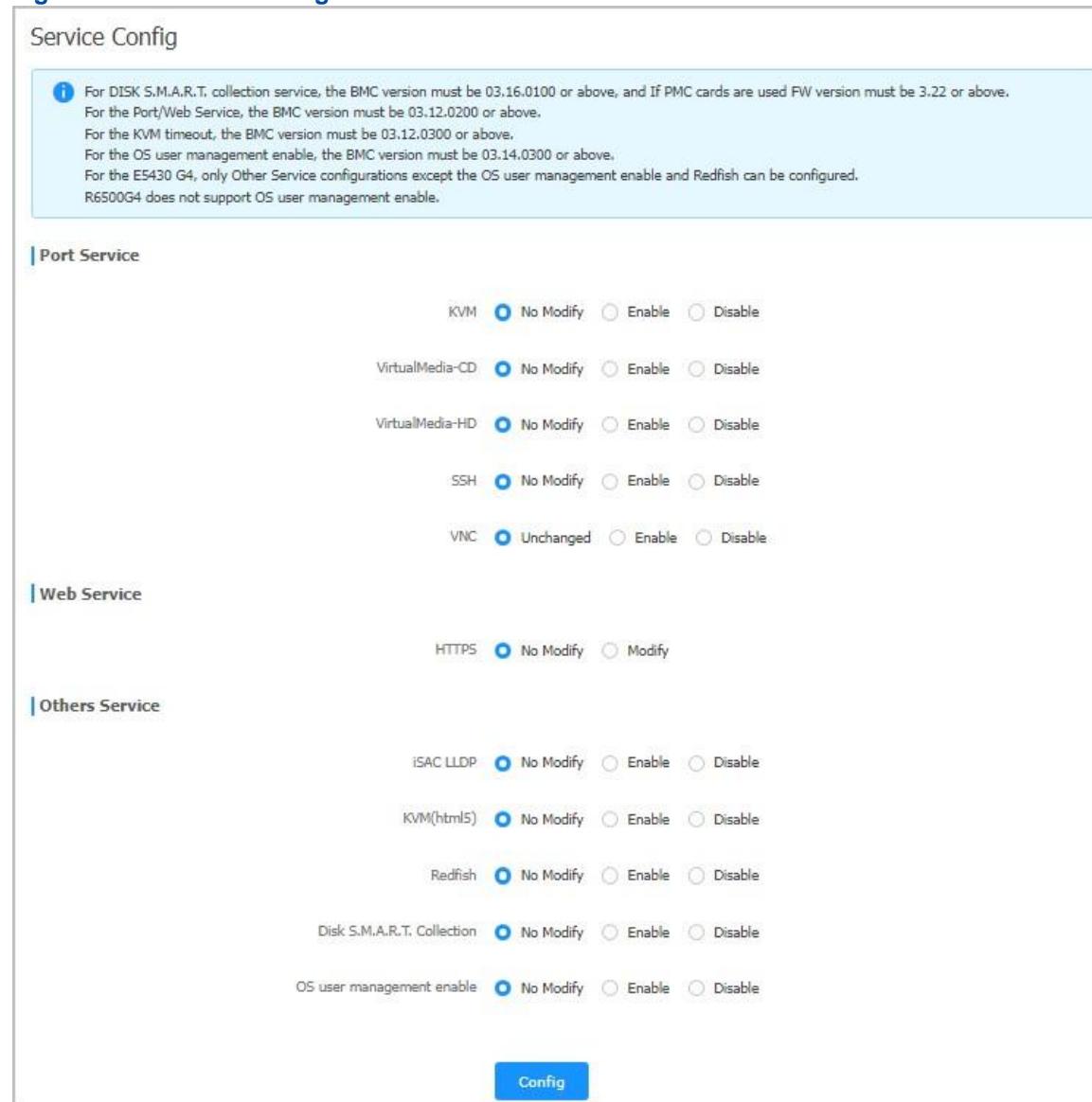
Current Platform: BMCV3(R5300 G4) [Return to the BMC configuration homepage](#)

1 Select BMC

- Startup Mode Config
- User Config
- Time Config
- SNMP Config
- Alarm Config
- Log Config
- Asset Tag Config
- Host Name Config
- Fan Mode Config
- Power Restore Policy
- Security Config
- Service Config
- LDAP\AD Config
- Power Redundancy Config
- Firewall Policy Config

Please select the device for BMC configuration first. If you have not added the device to UniKits [Click Add](#)

4. Click **Select BMC**, and select the BMC for which you want to configure services.
5. In the left pane on the **BMC Config** page, click **Service Config**. The **Service Config** area is displayed, see [Figure 3-43](#).

**Figure 3-43 Service Config Area**


**Service Config**

**Port Service**

- KVM:  No Modify  Enable  Disable
- VirtualMedia-CD:  No Modify  Enable  Disable
- VirtualMedia-HD:  No Modify  Enable  Disable
- SSH:  No Modify  Enable  Disable
- VNC:  Unchanged  Enable  Disable

**Web Service**

- HTTPS:  No Modify  Modify

**Others Service**

- iSAC LLDP:  No Modify  Enable  Disable
- KVM(html5):  No Modify  Enable  Disable
- Redfish:  No Modify  Enable  Disable
- Disk S.M.A.R.T. Collection:  No Modify  Enable  Disable
- OS user management enable:  No Modify  Enable  Disable

**Config**

6. Set the parameters. For a description of the parameters, refer to [Table 3-24](#).

**Table 3-24 Service Parameter Descriptions**

Parameter	Description
<b>Port Service</b>	
KVM	Select the KVM service configuration mode. Options: <ul style="list-style-type: none"> <li>• <b>No Modify</b>: indicates not to modify the original server configurations.</li> <li>• <b>Enable</b>: indicates to enable the KVM service.</li> </ul>
Parameter	Description

	<ul style="list-style-type: none"> <li>● <b>Disable</b>: indicates to disable the KVM service.</li> </ul> <p>After enabling the KVM service, you need to configure the following parameters:</p> <ul style="list-style-type: none"> <li>● <b>KVM Port</b>: security port (default: 7582) in KVM encryption mode and non-security port (default: 7578) in KVM non-encryption mode. Port number range: 1–65535.</li> <li>● <b>KVM TimeOut</b>: KVM service timeout period, range: 5–30 minutes.</li> </ul>
VirtualMedia-CD	<p>Select the VirtualMedia-CD service mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configurations.</li> <li>● <b>Enable</b>: indicates to enable the VirtualMedia-CD service.</li> <li>● <b>Disable</b>: indicates to disable the VirtualMedia-CD service.</li> </ul> <p>After enabling the VirtualMedia-CD service, you need to configure the following parameter:</p> <p><b>VirtualMedia-CD Port</b>: security port (default: 5124) in VMedia encryption mode and non-security port (default: 5120) in VMedia non-encryption mode. Port number range: 1–65535.</p>
VirtualMedia-HD	<p>Select the VirtualMedia-HD service mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configurations.</li> <li>● <b>Enable</b>: indicates to enable the VirtualMedia-HD service.</li> <li>● <b>Disable</b>: indicates to disable the VirtualMedia-HD service.</li> </ul> <p>After enabling the VirtualMedia-HD service, you need to configure the following parameter:</p> <p><b>VirtualMedia-HD Port</b>: security port (default: 5127) in VMedia encryption mode and non-security port (default: 5123) in VMedia non-encryption mode. Port number range: 1–65535.</p>
SSH	<p>Select the SSH service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configurations.</li> <li>● <b>Enable</b>: indicates to enable the SSH service.</li> <li>● <b>Disable</b>: indicates to disable the SSH service.</li> </ul> <p>After enabling the SSH service, you need to configure the following parameter:</p> <p><b>SSH Port</b>: default: 22. Port number range: 1–65535.</p>
VNC	<p>Select the VNC service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li> <li>● <b>Enable</b>: indicates to enable the VNC service.</li> <li>● <b>Disable</b>: indicates to disable the VNC service.</li> </ul> <p>After enabling the VNC service, you need to configure the following parameters:</p> <ul style="list-style-type: none"> <li>● <b>VNC Nonsecure Port</b>: Enter a non-secure port number. Default: 5900, range: 1–65535.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>● <b>VNC Secure Port:</b> Enter a secure port number. Default: 5901, range: 1–65535.</li> <li>● <b>VNC Service Password:</b> Select <b>Modify</b> and enter the new VNC password.</li> </ul>
<b>Web Service</b>	
HTTPS	<p>Select the HTTPS service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original port number.</li> <li>● <b>Modify:</b> indicates not to modify the original port number.</li> </ul> <p>After <b>Modify</b> is selected, the following parameter needs to be set:</p> <p><b>HTTPS Port:</b> security port (default: 443). Port number range: 1–65535.</p>
<b>Others Service</b>	
iSAC LLDP	<p>Select the iSAC LLDP service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configurations.</li> <li>● <b>Enable:</b> indicates to enable the iSAC LLDP service.</li> <li>● <b>Disable:</b> indicates to disable the iSAC LLDP service.</li> </ul>
KVM(html5)	<p>Select the KVM(html5) service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configurations.</li> <li>● <b>Enable:</b> indicates to enable the KVM(html5) service.</li> <li>● <b>Disable:</b> indicates to disable the KVM(html5) service.</li> </ul>
Redfish	<p>Select the Redfish service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configurations.</li> <li>● <b>Enable:</b> indicates to enable the Redfish service.</li> <li>● <b>Disable:</b> indicates to disable the Redfish service.</li> </ul>
DISK S.M.A.R.T. Collection	<p>Select the DISK S.M.A.R.T. Collection service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configurations.</li> <li>● <b>Enable:</b> indicates to enable the DISK S.M.A.R.T. Collection service.</li> <li>● <b>Disable:</b> indicates to disable the DISK S.M.A.R.T. Collection service.</li> </ul> <p>The collection period ranges from 1 through 360 days.</p>
OS user management enable	<p>Select the configuration mode of the user management service. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configurations.</li> <li>● <b>Enable:</b> indicates to the enable the user management service in the BIOS/OS. That is, BMC users can be configured in the BIOS/OS.</li> <li>● <b>Disable:</b> indicates to the disable the user management service in the BIOS/OS. That is, BMC users cannot be configured in the BIOS/OS.</li> </ul>

7. Click **Config** to deliver the configurations.

**Note**

- During service configuration, the progress bar is displayed on the page.
- After service configuration is completed, the configuration result is displayed on the page.

### 3.4.2.13 Configuring LDAP/AD Parameters

#### Abstract

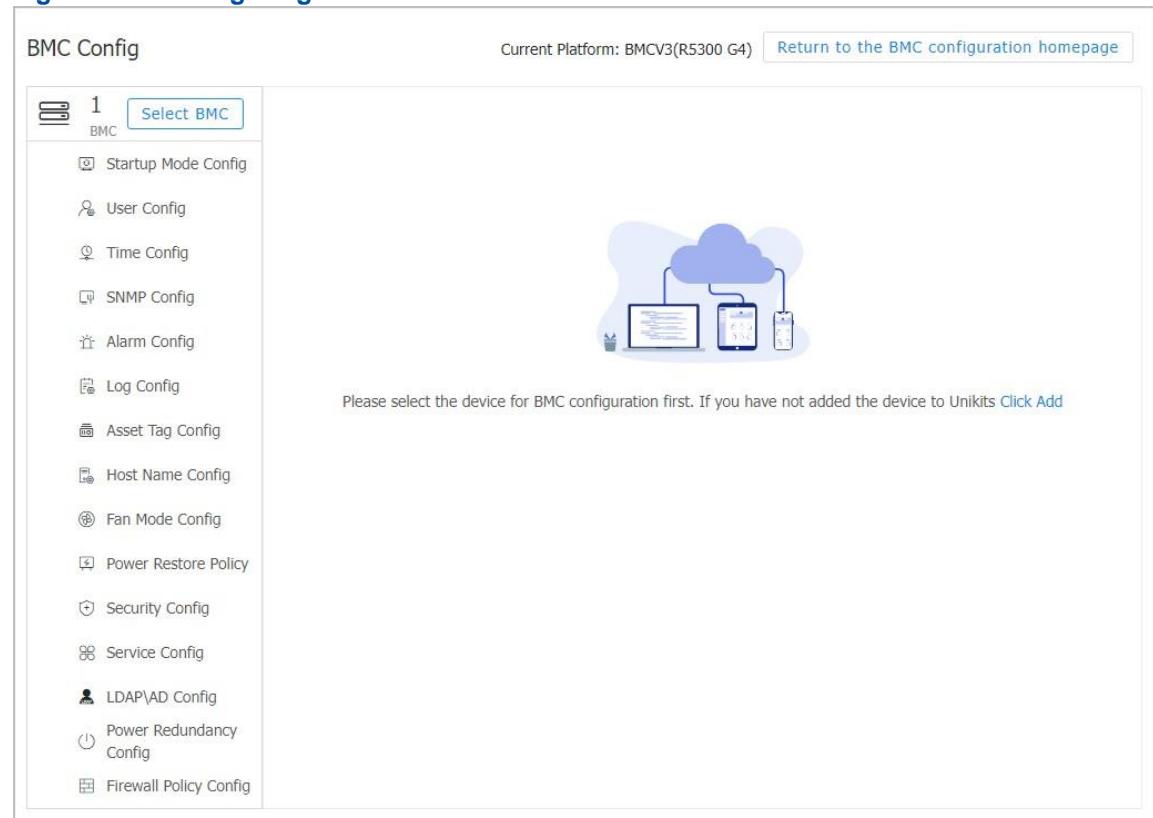
This procedure describes how to configure LDAP/AD parameters to authenticate external users through an [LDAP](#) server or [AD](#) server.

**Note**

External users refer to non-BMC users.

#### Steps

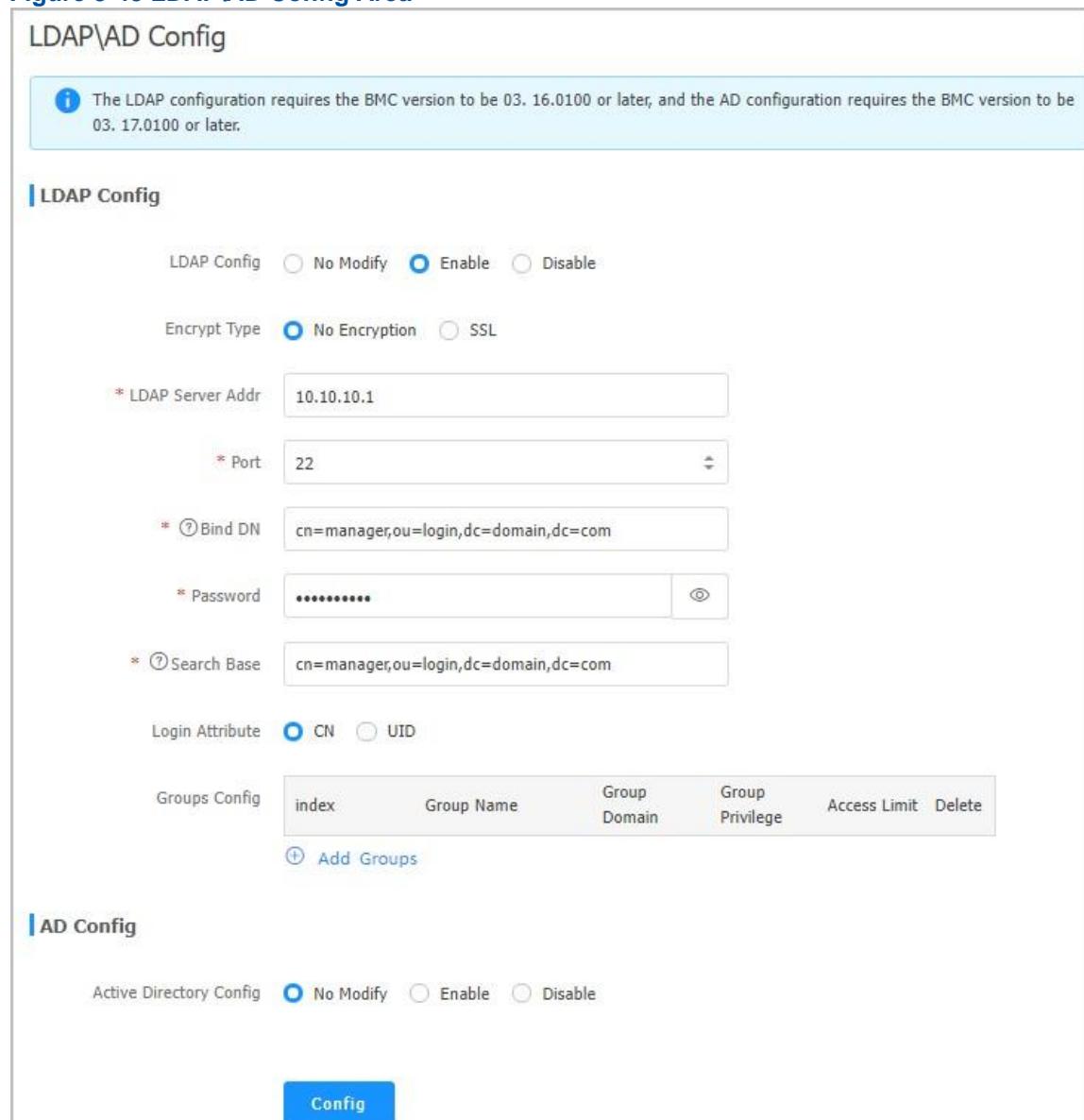
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-44](#).

**Figure 3-44 Configuring BMC V3**

The screenshot shows the 'BMC Config' page. At the top left, there is a list of BMCs with '1' selected. A 'Select BMC' button is highlighted in blue. To the right, the text 'Current Platform: BMCV3(R5300 G4)' is displayed, along with a 'Return to the BMC configuration homepage' link. The main content area contains a list of configuration options: Startup Mode Config, User Config, Time Config, SNMP Config, Alarm Config, Log Config, Asset Tag Config, Host Name Config, Fan Mode Config, Power Restore Policy, Security Config, Service Config, LDAP\AD Config, Power Redundancy Config, and Firewall Policy Config. To the right of the list is a network diagram showing a central cloud connected to a laptop, a smartphone, and a tablet. Below the diagram, a message reads: 'Please select the device for BMC configuration first. If you have not added the device to Unikits [Click Add](#)'.

4. Click **Select BMC**, and select the BMC for which you want to configure LDAP\AD parameters.
5. In the left pane on the **BMC Config** page, click **LDAP\AD Config**. The **LDAP\AD Config** area is displayed, see [Figure 3-45](#).

Figure 3-45 LDAP\AD Config Area



**LDAP\AD Config**

**LDAP Config**

The LDAP configuration requires the BMC version to be 03.16.0100 or later, and the AD configuration requires the BMC version to be 03.17.0100 or later.

LDAP Config  No Modify  Enable  Disable

Encrypt Type  No Encryption  SSL

\* LDAP Server Addr: 10.10.10.1

\* Port: 22

\* Bind DN: cn=manager,ou=login,dc=domain,dc=com

\* Password: \*\*\*\*\* (i)

\* Search Base: cn=manager,ou=login,dc=domain,dc=com

Login Attribute  CN  UID

Groups Config	index	Group Name	Group Domain	Group Privilege	Access Limit	Delete
<a href="#">(i) Add Groups</a>						

**AD Config**

Active Directory Config  No Modify  Enable  Disable

**Config**

6. Set the parameters. For a description of the parameters, refer to [Table 3-25](#).

Table 3-25 LDAP/AD Parameter Descriptions

Parameter	Description
<b>LDAP Config</b>	
LDAP Config	Select the LDAP configuration mode. Options: <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configuration.</li> </ul>
Parameter	Description

	<ul style="list-style-type: none"> <li>● <b>Enable</b>: indicates to enable LDAP authentication.</li> <li>● <b>Disable</b>: indicates to disable LDAP authentication.</li> </ul> <p>After <b>LDAP Config</b> is set to <b>Enable</b>, LDAP parameters are activated.</p>
Encrypt Type	<p>Select the encryption type. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Encryption</b>: indicates that no encryption is used.</li> <li>● <b>SSL</b>: indicates that <a href="#">SSL</a> encryption is used.</li> </ul>
LDAP Server Addr	Enter the IP address of the LDAP server in <a href="#">IPv4</a> or <a href="#">IPv6</a> format.
Port	Enter the port number. Range: 1–65535. Default: 389. If <b>Encrypt Type</b> is set to <b>SSL</b> , enter port number 636.
Bind DN	Enter the bind DN for logging in to the LDAP server. The name consists of 4–64 letters and digits, and must start with a letter. Allowed special characters include dots (.), commas (,), hyphens (-), underscores (_), and equal signs (=). For example, <i>cn=manager,ou=login,dc=domain,dc=com</i> .
Password	Enter the password for logging in to the LDAP server. It cannot be left blank. Range: 1–47 characters.
Search Base	Enter the directory on the LDAP server where the information about external users is stored. For example, <i>ou=login,dc=domain,dc=com</i> .
Login Attribute	Select the attribute used by the LDAP server to identify users.
Groups Config	Click <b>Add Groups</b> to add a group and set the corresponding parameters.
<b>AD Config</b>	
Active Directory Config	<p>Select the AD configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configurations.</li> <li>● <b>Enable</b>: indicates to enable AD authentication.</li> <li>● <b>Disable</b>: indicates to disable AD authentication.</li> </ul> <p>After <b>Active Directory Config</b> is set to <b>Enable</b>, AD parameters are activated.</p>
Encrypt Type	<p>Select the encryption type. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Encryption</b>: indicates that no encryption is used.</li> <li>● <b>SSL</b>: indicates that <a href="#">SSL</a> encryption is used.</li> </ul>

User Name	Enter the username for logging in to the AD server. <ul style="list-style-type: none"> <li>• The username is a string of 1–64 characters consisting of letters and digits.</li> <li>• The username must start with an alphabetic character.</li> <li>• Letters are case-sensitive.</li> <li>• Special characters are not allowed.</li> </ul>
<b>Parameter</b>	<b>Description</b>
	If the username and password are not required, leave this parameter blank.
Password	Enter the password for logging in to the AD server. Range: 6–127 characters. If the username and password are not required, leave this parameter blank.
User Domain	Enter the domain name of the AD server, for example, <i>MyDomain.com</i> .
Domain Controller 1	Enter the IP address 1 of the AD server, which supports IPv4 and IPv6 formats, and is required.
Domain Controller 2	Enter the IP address 2 of the AD server, which supports IPv4 and IPv6 formats, and is optional.
Domain Controller 3	Enter the IP address 3 of the AD server, which supports IPv4 and IPv6 formats, and is optional.
Groups Config	Click <b>Add Groups</b> to add a group and set the corresponding parameters.

7. Click **Config** to download the configuration.



#### Note

- During LDAP/AD parameter configuration, the progress bar is displayed on the page.
- After LDAP/AD parameter configuration is completed, the configuration result is displayed on the page.

### 3.4.2.14 Migrating Configurations

#### Abstract

Configuration migration is an advanced function, which requires a license.

Configuration migration is to import the **BMC** configurations in a configuration file or the **BMC** configurations in a template server to the specified **BMC**.

**Note**

BMC configurations do not involve personalized configurations, such as the IP address, version number, serial number, and host name.

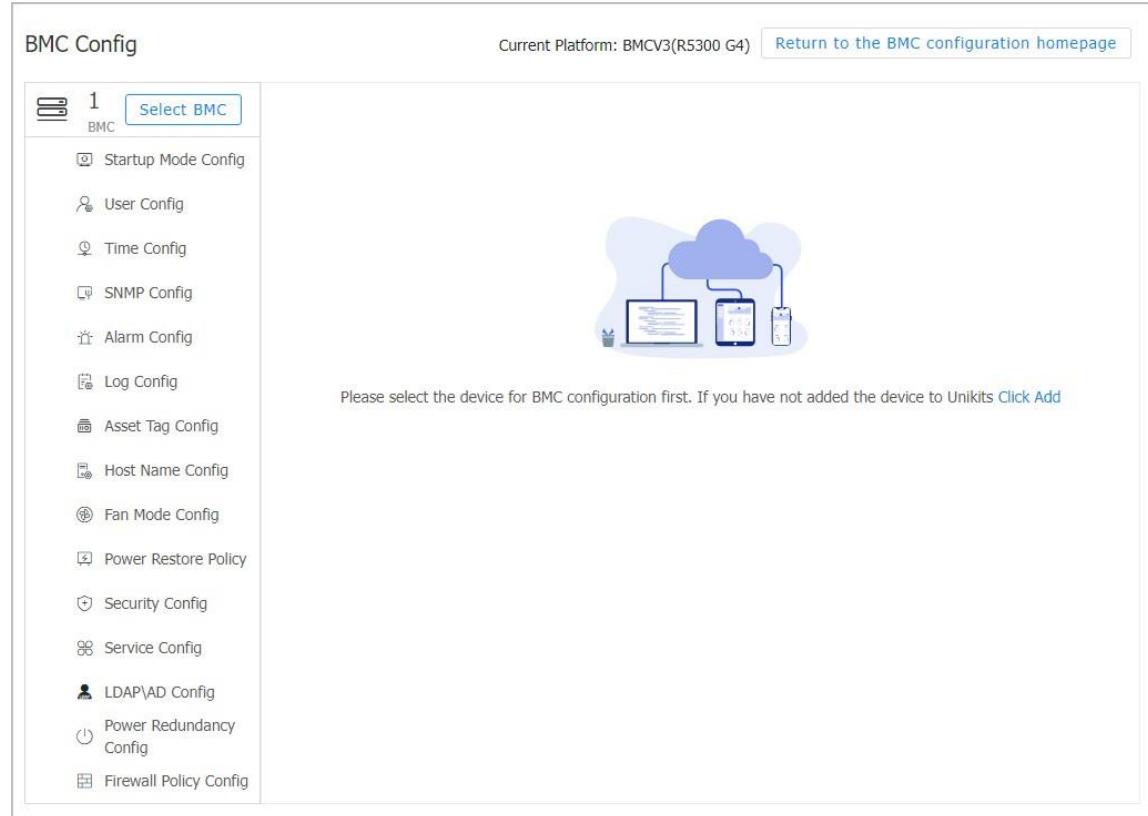
**Prerequisite**

The license is already imported. For how to import a license, refer to "[3.9.4 Importing a License](#)".

**Steps**

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-46](#).

**Figure 3-46 Configuring BMC V3**



BMC Config

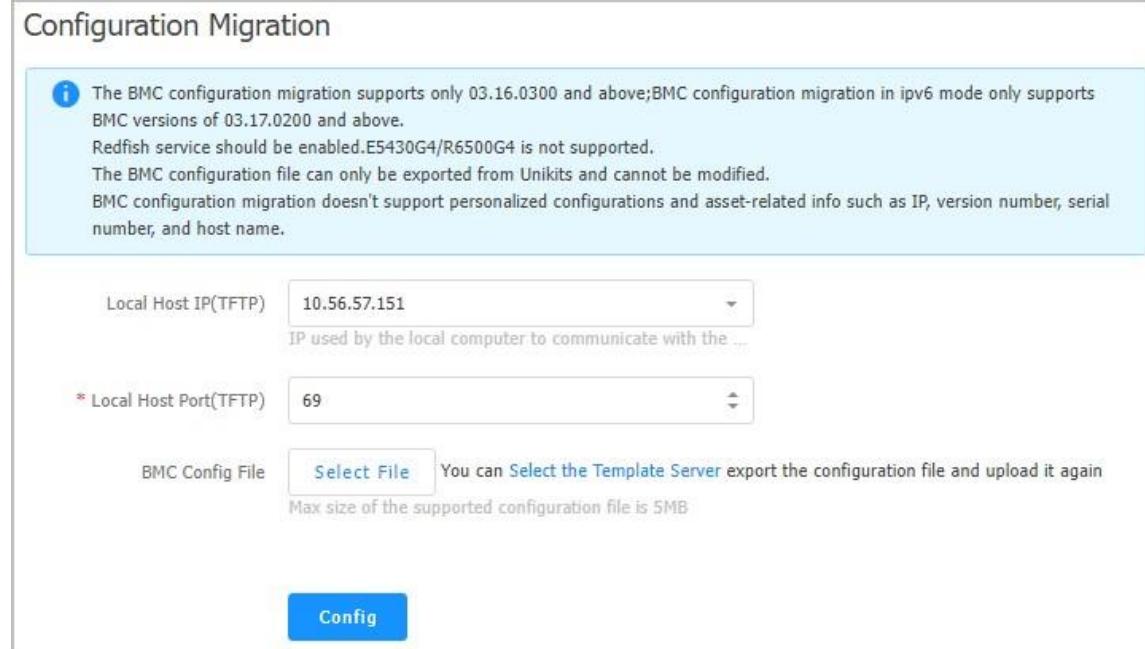
Current Platform: BMCV3(R5300 G4) [Return to the BMC configuration homepage](#)

1 Select BMC

- Startup Mode Config
- User Config
- Time Config
- SNMP Config
- Alarm Config
- Log Config
- Asset Tag Config
- Host Name Config
- Fan Mode Config
- Power Restore Policy
- Security Config
- Service Config
- LDAP\AD Config
- Power Redundancy Config
- Firewall Policy Config

Please select the device for BMC configuration first. If you have not added the device to UniKits [Click Add](#)

4. Click **Select BMC**, and select the BMC for which you want to migrate configurations.
5. In the left pane on the **BMC Config** page, click **Configuration Migration**. The **Configuration Migration** area is displayed, see [Figure 3-47](#).

**Figure 3-47 Configuration Migration Area**


**Configuration Migration**

**Note:** The BMC configuration migration supports only 03.16.0300 and above; BMC configuration migration in ipv6 mode only supports BMC versions of 03.17.0200 and above. Redfish service should be enabled. E5430G4/R6500G4 is not supported. The BMC configuration file can only be exported from Unikits and cannot be modified. BMC configuration migration doesn't support personalized configurations and asset-related info such as IP, version number, serial number, and host name.

Local Host IP(TFTP): 10.56.57.151  
IP used by the local computer to communicate with the ...

\* Local Host Port(TFTP): 69

BMC Config File: **Select File** You can **Select the Template Server** export the configuration file and upload it again. Max size of the supported configuration file is 5MB

**Config**

6. Set the parameters. For a description of the parameters, refer to [Table 3-26](#).

**Table 3-26 Configuration Migration Parameter Descriptions**

Parameter	Description
Local Host IP	To use the configuration migration function, you need to enable the local TFTP service function. Select the IP address for the local TFTP service. This IP address must be in the same network as that of the BMC to be configured.
Local Host Port	Enter the port number for the local TFTP service. Range: 1–65535, default: 69.
BMC Config File	<ul style="list-style-type: none"> <li>If there is a local configuration file, click <b>Select File</b>, and select the configuration file.</li> <li>If there is no local configuration file, click <b>Select the Template Server</b>, and select the corresponding template server to use the configuration file exported from the template server.</li> </ul>

7. Click **Config**. A warning dialog box is displayed.

**Note**

- During migration configuration, the progress bar is displayed on the page.
- After migration configuration is completed, the configuration result is displayed on the page.

8. Enter **yes** in the text box, and select **I have read it and know the influence**.

9. Click **Submit**.

**Note**

- During configuration migration, the progress bar is displayed on the page.
- After configuration migration is completed, the migration result is displayed on the page.

### 3.4.2.15 Configuring the Power Mode

**Abstract**

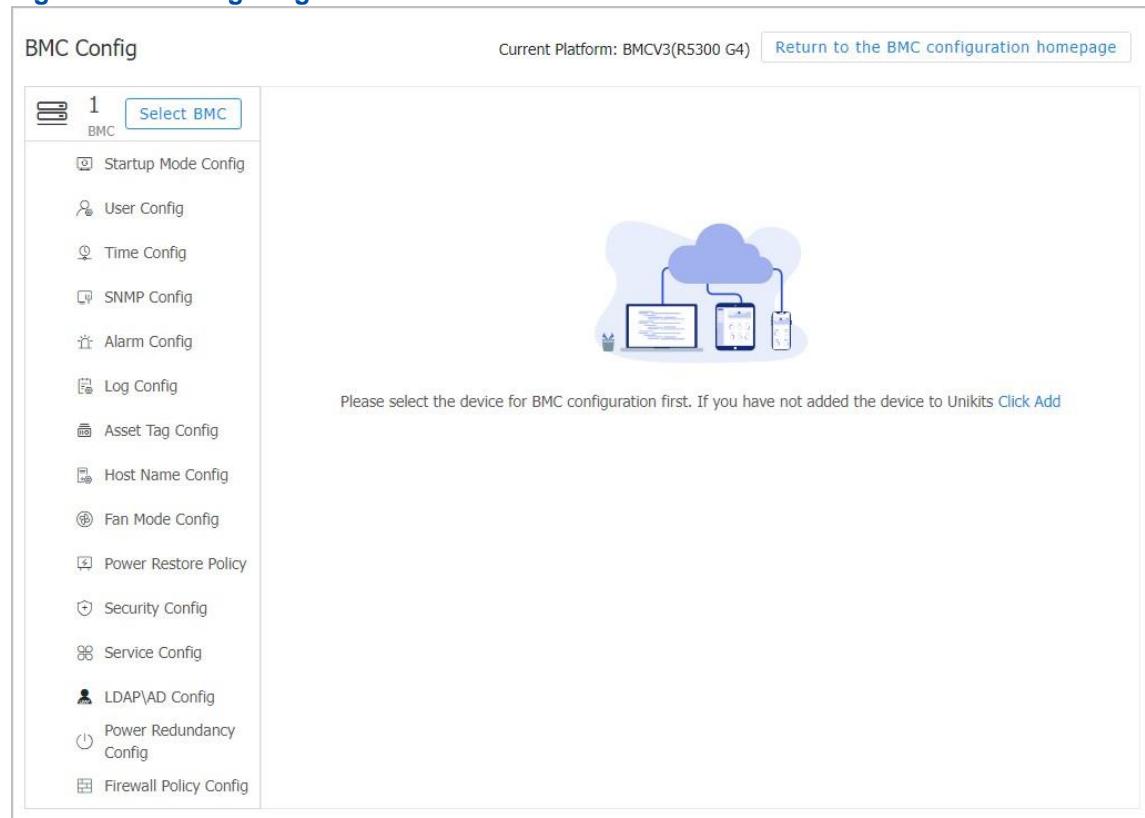
The server power modes include:

- **Sharing:** The power modules supply power in load-balancing mode.
- **Failover:** The power modules supply power in active/standby mode.

A proper power mode enables the power modules to supply power to servers in a reasonable manner.

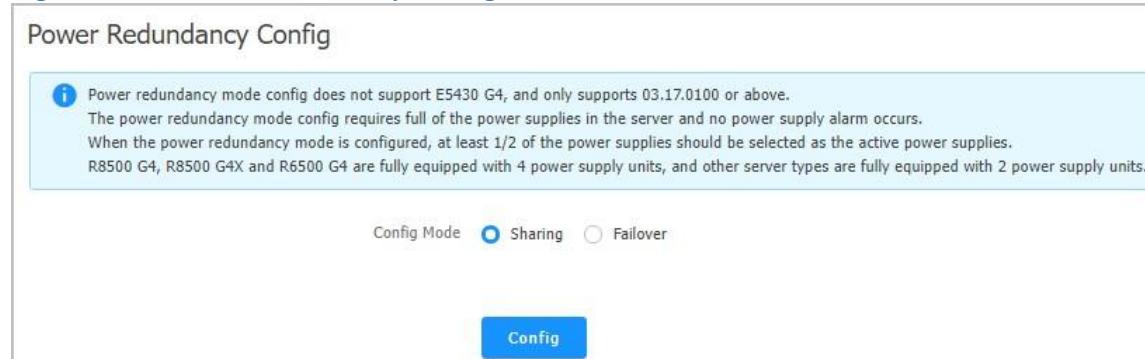
**Steps**

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-48](#).

**Figure 3-48 Configuring BMC V3**


The screenshot shows the 'BMC Config' page with a sidebar containing 16 configuration items. The items are: Startup Mode Config, User Config, Time Config, SNMP Config, Alarm Config, Log Config, Asset Tag Config, Host Name Config, Fan Mode Config, Power Restore Policy, Security Config, Service Config, LDAP\AD Config, Power Redundancy Config, and Firewall Policy Config. A central panel displays a cloud icon with three devices (laptop, smartphone, tablet) connected to it, and a message: 'Please select the device for BMC configuration first. If you have not added the device to Unikits [Click Add](#)'. The top right corner shows 'Current Platform: BMCV3(R5300 G4)' and a 'Return to the BMC configuration homepage' link.

4. Click **Select BMC**, and select the BMC for which you want to configure the power mode.
5. In the left pane on the **BMC Config** page, click **Power Redundancy Config**. The **Power Redundancy Config** area is displayed, see [Figure 3-49](#).

**Figure 3-49 Power Redundancy Config Area**


The screenshot shows the 'Power Redundancy Config' area. It includes a note: 'Power redundancy mode config does not support E5430 G4, and only supports 03.17.0100 or above. The power redundancy mode config requires full of the power supplies in the server and no power supply alarm occurs. When the power redundancy mode is configured, at least 1/2 of the power supplies should be selected as the active power supplies. R8500 G4, R8500 G4X and R6500 G4 are fully equipped with 4 power supply units, and other server types are fully equipped with 2 power supply units.' Below the note are two radio buttons: 'Sharing' (selected) and 'Failover'. At the bottom is a 'Config' button.

6. Select the operation mode of the power modules. Options:
  - **Sharing**: The power modules supply power in load-balancing mode.
  - **Failover**: The power modules supply power in active/standby mode.
 If **Failover** is selected, the active power module needs to be selected.
7. Click **Config** to deliver the configurations.

**Note**

- During power mode configuration, the progress bar is displayed on the page.
- After power mode configuration is completed, the configuration result is displayed on the page.

### 3.4.2.16 Configuring Firewall Parameters

#### Abstract

By configuring firewall parameters, you can add blacklists and whitelists to control access to the **BMC**.

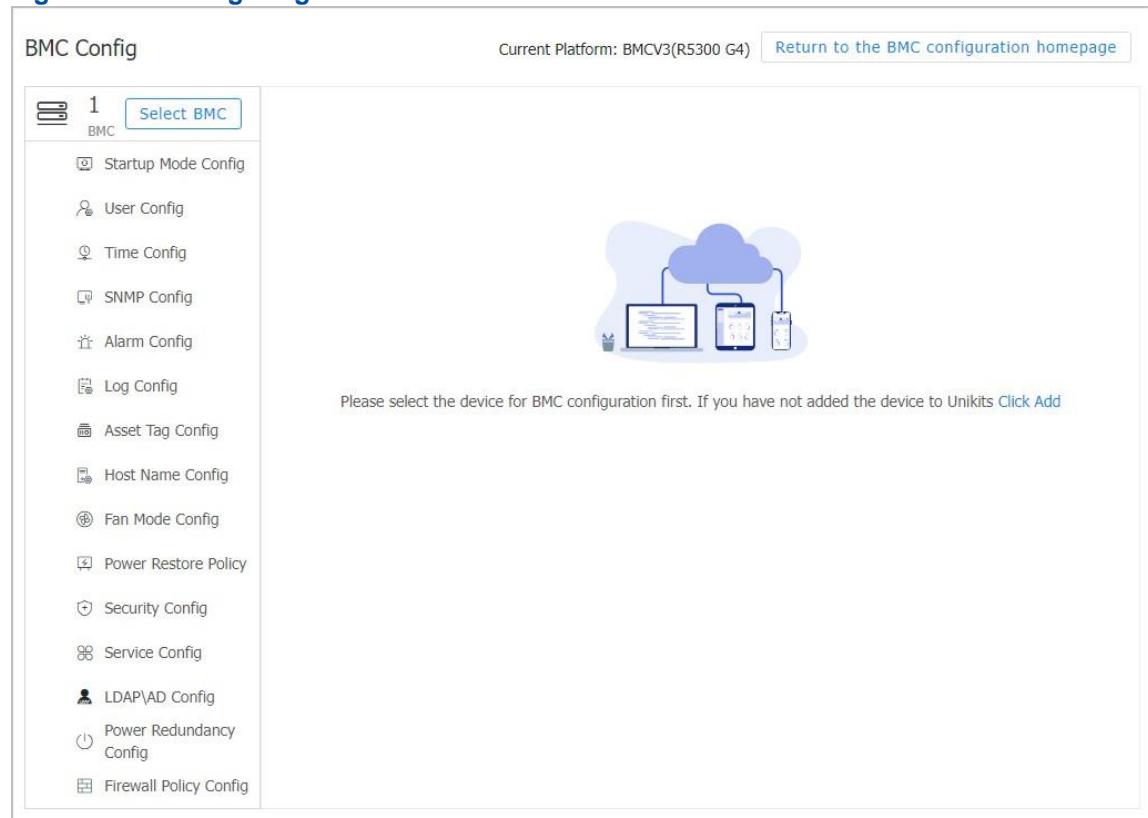
- The devices in a blacklist are forbidden to access the BMC.
- Only the devices in a whitelist are allowed to access the BMC.

When adding a whitelist, you must first add the **IP** address of your local **PC** (acting as a client PC) to the whitelist to ensure that your local PC can access the Web portal of the BMC.

This procedure describes how to configure firewall parameters.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content of the corresponding BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in [Figure 3-50](#).

**Figure 3-50 Configuring the BMC V3**

The screenshot shows the 'BMC Config' page. At the top, it displays 'Current Platform: BMCV3(R5300 G4)' and a 'Return to the BMC configuration homepage' link. On the left, a sidebar lists various configuration options: 'Select BMC' (highlighted in blue), 'Startup Mode Config', 'User Config', 'Time Config', 'SNMP Config', 'Alarm Config', 'Log Config', 'Asset Tag Config', 'Host Name Config', 'Fan Mode Config', 'Power Restore Policy', 'Security Config', 'Service Config', 'LDAP\AD Config', 'Power Redundancy Config', and 'Firewall Policy Config'. To the right of the sidebar is a network icon showing a cloud connected to a laptop, a smartphone, and a tablet. Below the icon, a message reads: 'Please select the device for BMC configuration first. If you have not added the device to Unikits [Click Add](#)'. The 'Firewall Policy Config' option is the last item in the list.

4. Click **Select BMC**, and select the BMC for which you want to configure firewall parameters.
5. From the left pane of the BMC V3 configuration page, select **Firewall Policy Config**. The **Firewall Policy Config** page is displayed, as shown in [Figure 3-51](#).

### Figure 3-51 Firewall Policy Config Page

Firewall Policy Config

**White list:** Only devices that meet the rules are allowed to access BMC. No address other than the white list can access the BMC. Please operate with caution.  
When adding white list rules, please first add the local IP address or MAC address to ensure normal access to BMC.  
**Black list:** Only devices that meet the rules are prohibited from accessing BMC.  
**IP segment:** support a single IP or IP segment, support IPv4 and IPv6, and the format of the start IP address and end IP address must be consistent. 127.0.0.1 is not allowed to be configured for single IP.

IPv4 Firewall Policy Config	<input type="radio"/> Unchanged	<input checked="" type="radio"/> White List Enable	<input type="radio"/> Black List Enable								
IPv6 Firewall Policy Config	<input type="radio"/> Unchanged	<input checked="" type="radio"/> White List Enable	<input type="radio"/> Black List Enable								
White List Policy	<input type="radio"/> Unchanged	<input checked="" type="radio"/> Modify									
White List Rule	<input checked="" type="radio"/> IP <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th style="width: 15%;">Operate</th> <th style="width: 35%;">Start IP</th> <th style="width: 35%;">End IP</th> <th style="width: 15%;">Delete</th> </tr> </thead> <tbody> <tr> <td>Add</td> <td>10.56.57.151</td> <td>10.56.57.159</td> <td></td> </tr> </tbody> </table> <input type="button" value="Add List"/>			Operate	Start IP	End IP	Delete	Add	10.56.57.151	10.56.57.159	
Operate	Start IP	End IP	Delete								
Add	10.56.57.151	10.56.57.159									
Black List Policy	<input checked="" type="radio"/> Unchanged	<input type="radio"/> Modify									

**Config**

6. Set the parameters. For a description of the parameters, refer to [Table 3-27](#).

**Table 3-27 Firewall Parameter Descriptions**

Parameter	Description
<b>IPv4 Firewall Policy Config</b>	Select the IPv4 firewall policy. Options: <ul style="list-style-type: none"> <li>● <b>Unchanged:</b> indicates not to modify the original server configurations.</li> <li>● <b>White List Enable:</b> indicates that only the devices in a whitelist are allowed to access the Web portal of the BMC.</li> <li>● <b>Black List Enable:</b> indicates that the devices in a blacklist are not allowed to access the Web portal of the BMC.</li> </ul>
<b>IPv6 Firewall Policy Config</b>	Select the IPv6 firewall policy. Options: <ul style="list-style-type: none"> <li>● <b>Unchanged:</b> indicates not to modify the original server configurations.</li> <li>● <b>White List Enable:</b> indicates that only the devices in a whitelist are allowed to access the Web portal of the BMC.</li> <li>● <b>Black List Enable:</b> indicates that only the devices in a blacklist are not allowed to access the Web portal of the BMC.</li> </ul>
<b>White List Policy</b>	Select whether to modify the whitelist. Options: <ul style="list-style-type: none"> <li>● <b>Unchanged:</b> indicates not to modify the original server whitelist.</li> <li>● <b>Modify:</b> indicates to modify the original whitelist of the server, and adds or deletes IP address segments in <b>White List Config</b>.</li> </ul>

<b>Black List Policy</b>	Select whether to modify the blacklist. Options: <ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server blacklist.</li> </ul>
<b>Parameter</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>● <b>Modify</b>: indicates to modify the original blacklist of the server, and adds or deletes IP address segments in <b>Black List Config</b>.</li> </ul>

7. Click **Config** to deliver the configuration.



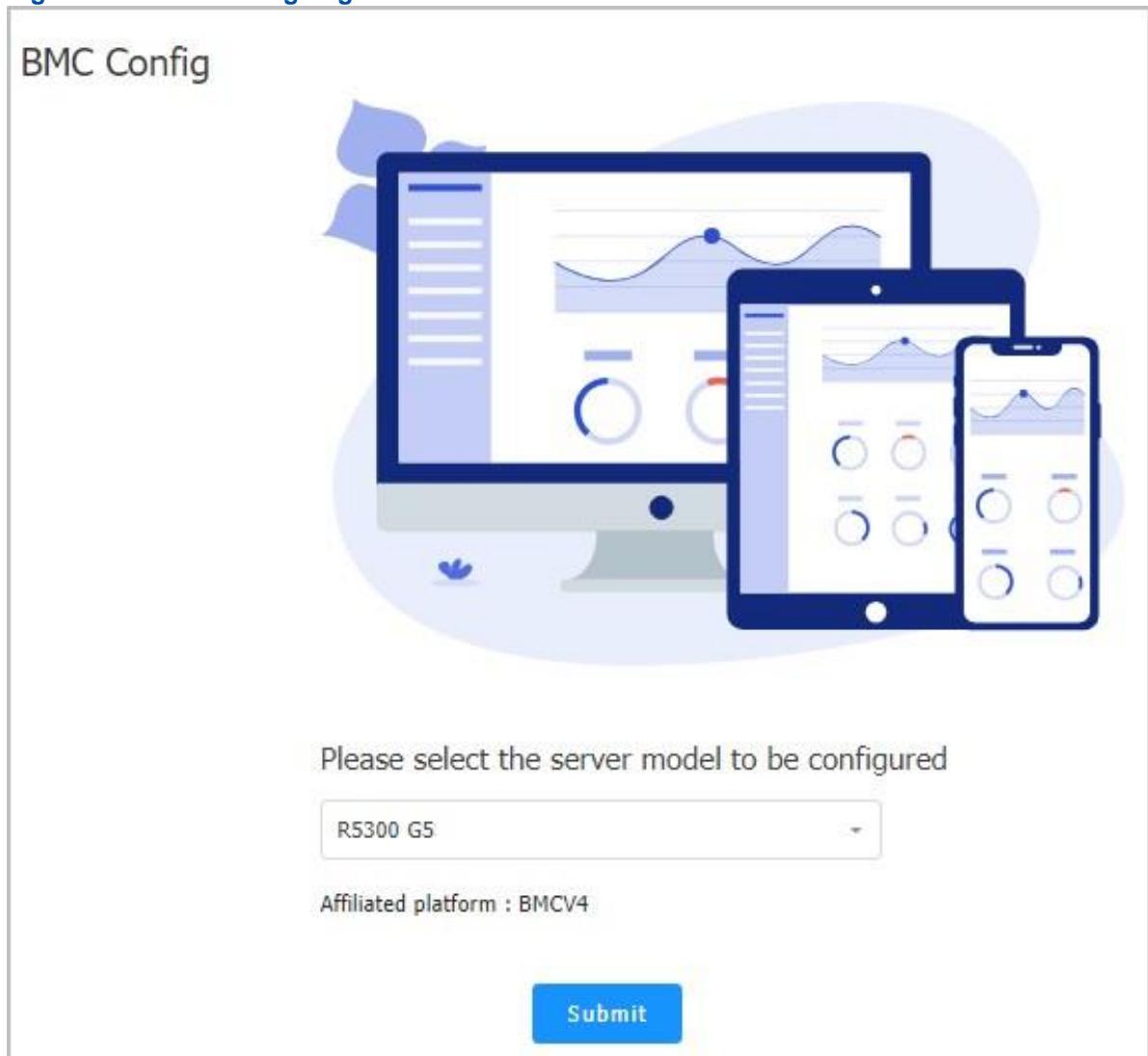
#### Note

- During firewall parameter configuration, the progress bar is displayed on the page.
- After firewall parameter configuration is completed, the configuration result is displayed on the page.

### 3.4.3 BMC (V4) Configuration

The **BMC** versions of the servers maintained through the UniKits include V3 and V4. After a server model is selected on the **BMC Config** page, the content related to the corresponding BMC version is automatically displayed on the UniKits.

For example, after NCS6722 N4 is selected on the **BMC Config** page, the content corresponding to BMC V4 is automatically displayed on the UniKits, as shown in [Figure 3-52](#).

**Figure 3-52 BMC Config Page**

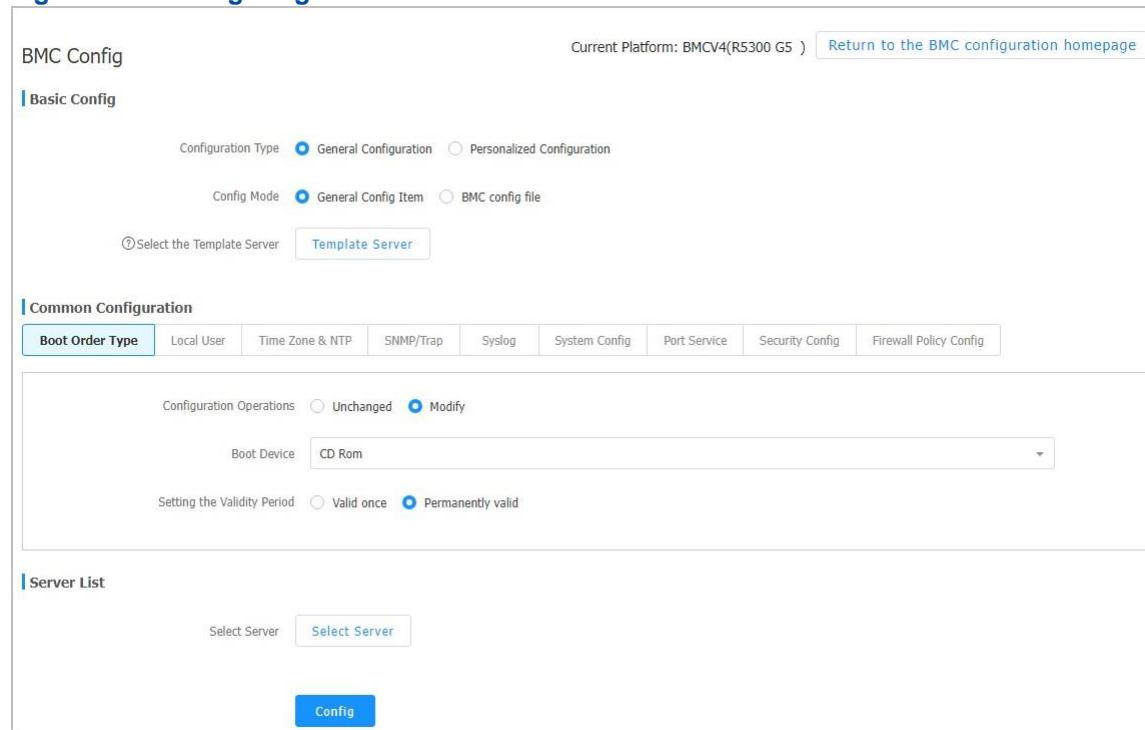
### 3.4.3.1 Configuring Boot Options

#### Abstract

This procedure describes how to configure boot options, including the boot device and application mode.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V4 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V4 is displayed, as shown in [Figure 3-53](#).

**Figure 3-53 Configuring BMC V4**


The screenshot shows the BMC Config interface. At the top, it says 'BMC Config' and 'Current Platform: BMCV4(R5300 G5 )'. There is a link to 'Return to the BMC configuration homepage'. The 'Basic Config' section is visible, showing 'Configuration Type' (set to 'General Configuration') and 'Config Mode' (set to 'General Config Item'). Below this, there is a note to 'Select the Template Server' with a 'Template Server' button. The 'Common Configuration' section is expanded, showing tabs for 'Boot Order Type', 'Local User', 'Time Zone & NTP', 'SNMP/Trap', 'Syslog', 'System Config', 'Port Service', 'Security Config', and 'Firewall Policy Config'. The 'Boot Order Type' tab is selected. It contains fields for 'Configuration Operations' (set to 'Modify'), 'Boot Device' (set to 'CD Rom'), and 'Setting the Validity Period' (set to 'Permanently valid'). The 'Server List' section is also visible, with a 'Select Server' button and a 'Config' button.

4. In the **Common Configuration** area, click **Boot Order Type** to switch to the **Boot Order Type** tab.
5. Set the parameters. For a description of the parameters, refer to [Table 3-28](#).

**Table 3-28 Boot Option Parameter Descriptions**

Parameter	Configuration Description
Configuration Type	Select <b>General Configuration</b> .
Config Mode	Select a configuration mode. Options: <ul style="list-style-type: none"> <li>● <b>General Config Item</b> → To import the configurations from a template server, click <b>Template Server</b>, and select a server as the template server in the displayed dialog box. After the import, the configurations in the template server are automatically displayed in the <b>Common Configuration</b> area, and can be modified.               <ul style="list-style-type: none"> <li>→ To not import the configurations from a template server, do not select this option.</li> </ul> </li> <li>● <b>BMC config file</b> <ul style="list-style-type: none"> <li>→ To import the configurations in a BMC configuration file, click <b>Select File</b>, and select the BMC configuration file in the displayed dialog box. After the import, the configurations in the BMC configuration file are automatically displayed in the <b>Common Configuration</b> area, and can be modified.                   <ul style="list-style-type: none"> <li>→ To not import a BMC configuration file, do not select this option.</li> </ul> </li> </ul> </li> </ul>

Configuration Operations	Select whether to modify the original server configurations. ● <b>Unchanged</b> : indicates not to modify the original server configurations.
<b>Parameter</b>	<b>Configuration Description</b>
	● <b>Modify</b> : indicates to modify the original server configurations. After selecting <b>Modify</b> , you also need to set <b>Boot Device</b> and <b>Setting the Validity Period</b> .
Boot Device	Select the device used to boot the <b>OS</b> of the server. Options: ● <b>Unconfigured</b> : The first boot device is not set. The default boot device set in the <b>BIOS</b> prevails, which is not controlled by the <b>BMC</b> . ● <b>Disk</b> : The OS is forcibly booted through a hard disk. ● <b>Network</b> : The OS is forcibly booted through a network. ● <b>CD Rom</b> : The OS is forcibly booted through a CD/DVD-ROM drive. ● <b>BIOS Config</b> : The BIOS menu is displayed after the server is booted. ● <b>Floppy drive/pluggable mobile device</b> : The OS is forcibly booted from a floppy drive or removable device.
Setting the Validity Period	Select whether the reconfigured server boot options are applied to the current restart only. ● <b>One-time</b> : only effective for the current restart. ● <b>Permanent</b> : permanently effective.
Select Server	Click <b>Select Server</b> , and select the servers to be configured in the displayed dialog box.

6. Click **Config** to deliver the configurations.



- During boot option configuration, the progress bar is displayed on the page.
- After boot option configuration is completed, the configuration result is displayed on the page.

### 3.4.3.2 Configuring a User

#### Abstract

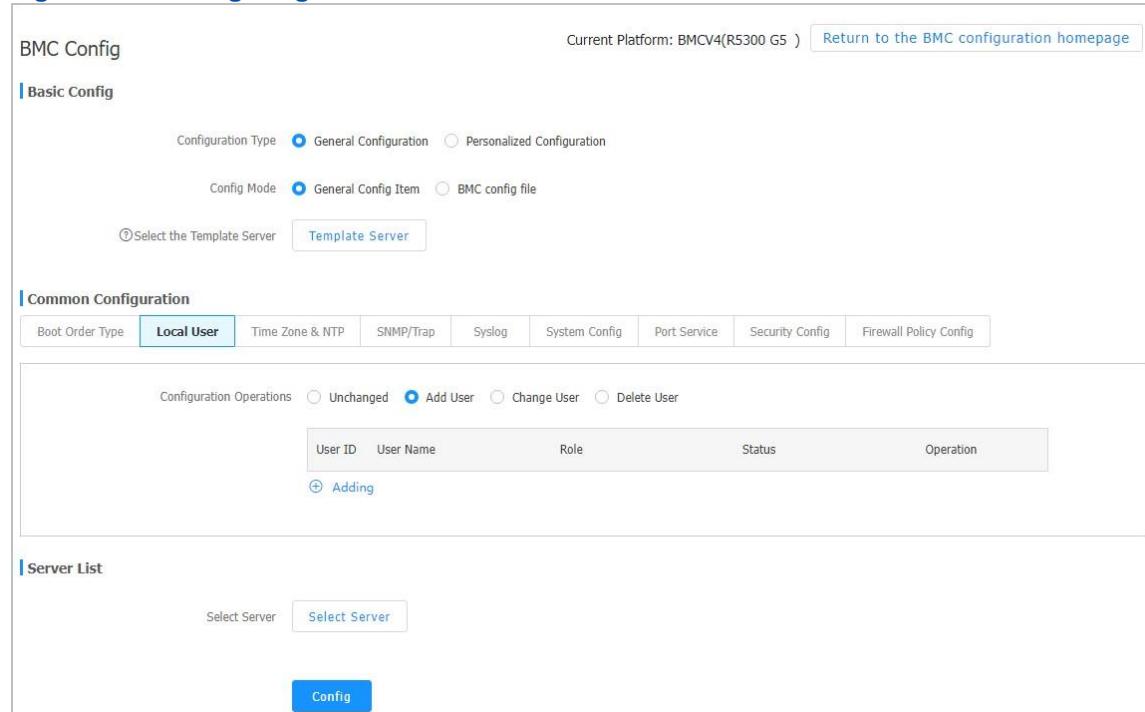
This procedure describes how to configure a **BMC** user for BMC configuration and management.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V4 is automatically displayed on the UniKits.

3. Click **Submit**. The page for configuring BMC V4 is displayed, as shown in Figure 3-54.

**Figure 3-54 Configuring BMC V4**



The screenshot shows the BMC Config interface. At the top, it says "BMC Config" and "Current Platform: BMCV4(R5300 G5)". There is a "Return to the BMC configuration homepage" link. Below this, the "Basic Config" section is visible with configuration type and mode settings. The "Common Configuration" section is selected, showing tabs for Boot Order Type, Local User, Time Zone & NTP, SNMP/Trap, Syslog, System Config, Port Service, Security Config, and Firewall Policy Config. The "Local User" tab is selected. Under "Common Configuration", there is a table for managing users. The table has columns for User ID, User Name, Role, Status, and Operation. A button labeled "Adding" is visible. The "Server List" section is also shown with a "Select Server" button and a "Config" button.

4. In the **Common Configuration** area, click **Local User** to switch to the **Local User** tab.  
 5. Set the parameters. For a description of the parameters, refer to Table 3-29.

**Table 3-29 Local User Parameter Descriptions**

Parameter	Description
Configuration Type	Select <b>General Configuration</b> .
Config Mode	User configuration does not support import or export. Therefore, this parameter does not need to be configured.
Configuration Operations	<p>Select whether to add, modify, or delete a BMC user.</p> <ul style="list-style-type: none"> <li>To not modify the original user configurations, select <b>Unchanged</b>.</li> <li>To add a BMC user, select <b>Add User</b>. After <b>Add User</b> is selected, the <b>Adding</b> button is activated. Click <b>Adding</b>, and set the user parameters in the displayed dialog box.</li> <li>To modify a BMC user, select <b>Change User</b>. After <b>Change User</b> is selected, the <b>Select User</b> button is activated. Click <b>Select User</b>, and modify the user parameters in the displayed dialog box.</li> <li>To delete a BMC user, select <b>Delete User</b>. After <b>Delete User</b> is selected, the <b>Adding</b> button is activated. Click <b>Adding</b>, and enter the BMC username that you want to delete.</li> </ul>

Select Server	Click <b>Select Server</b> , and select the servers to be configured in the displayed dialog box.
---------------	---

6. Click **Config** to deliver the configurations.



#### Note

- During user configuration, the progress bar is displayed on the page.
- After user configuration is completed, the configuration result is displayed on the page.

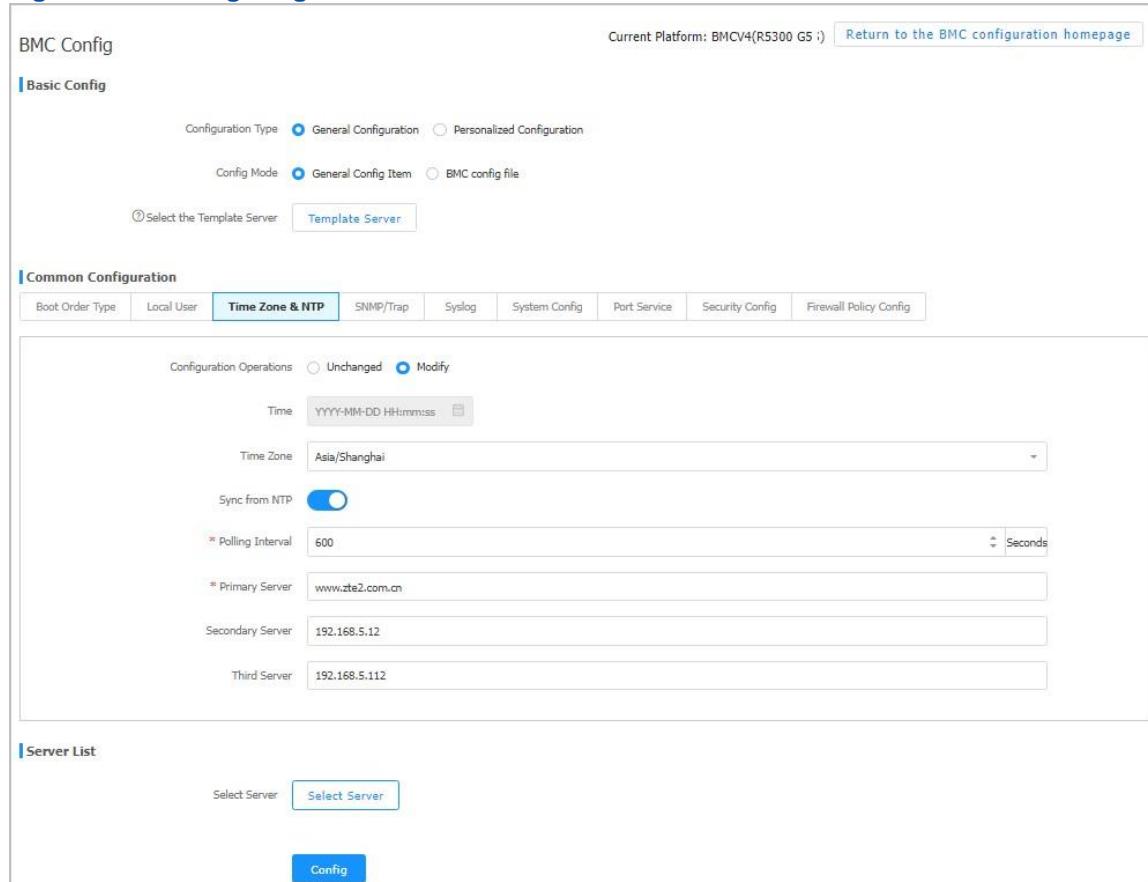
### 3.4.3.3 Configuring Time Parameters

#### Abstract

This procedure describes how to configure time parameters, so that the **BMC** of a server can obtain the correct time.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V4 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V4 is displayed, as shown in [Figure 3-55](#).

**Figure 3-55 Configuring BMC V4**


The screenshot shows the BMC Config interface with the following details:

- Basic Config** tab is selected.
- Configuration Type**:  General Configuration  Personalized Configuration
- Config Mode**:  General Config Item  BMC config file
- Select the Template Server**:
- Common Configuration** tab is selected.
- Time Zone & NTP** sub-tab is selected.
- Configuration Operations**:  Unchanged  Modify
- Time**: YYYY-MM-DD HHmmss
- Time Zone**: Asia/Shanghai
- Sync from NTP**:
- \* Polling Interval**: 600
- \* Primary Server**: www.zte2.com.cn
- Secondary Server**: 192.168.5.12
- Third Server**: 192.168.5.112
- Server List** tab is present.
- Select Server**:
- Config** button is present.

4. In the **Common Configuration** area, click **Time Zone & NTP** to switch to the **Time Zone & NTP** tab.
5. Set the parameters. For a description of the parameters, refer to [Table 3-30](#).

**Table 3-30 Time Zone & NTP Parameter Descriptions**

Parameter	Description
Configuration Type	Select <b>General Configuration</b> .

Config Mode	<p>Select a configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>General Config Item</b> → To import the configurations from a template server, click <b>Template Server</b>, and select a server as the template server in the displayed dialog box. After the import, the configurations in the template server are automatically displayed in the <b>Common Configuration</b> area, and can be modified.</li> <li>→ To not import the configurations from a template server, do not select this option.</li> <li>● <b>BMC config file</b></li> <li>→ To import the configurations in a BMC configuration file, click <b>Select File</b>, and select the BMC configuration file in the displayed dialog box. After the import, the configurations in the BMC configuration file are automatically displayed in the <b>Common Configuration</b> area, and can be modified.</li> <li>→ To not import a BMC configuration file, do not select this option.</li> </ul>
Configuration Operations	<p>Select whether to modify the original server configurations.</p> <ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li> <li>● <b>Modify</b>: indicates to modify the original server configurations.</li> </ul> <p>After selecting <b>Modify</b>, you also need to set the following parameters:</p> <ul style="list-style-type: none"> <li>● <b>Time</b></li> <li>● <b>Time Zone</b></li> <li>● <b>Sync from NTP</b> ● <b>Polling Interval</b></li> <li>● <b>Primary Server</b></li> <li>● <b>Secondary Server</b></li> <li>● <b>Third Server</b></li> </ul>
Time	<ul style="list-style-type: none"> <li>● This parameter can be set when <b>Sync from NTP</b> is disabled. Click  and then set the time.</li> <li>● This parameter cannot be set when <b>Sync from NTP</b> is enabled.</li> </ul>
Time Zone	Select a time zone identified by location.
Sync from NTP	<ul style="list-style-type: none"> <li>● To synchronize time with an NTP server, enable <b>Sync from NTP</b>. After <b>Sync from NTP</b> is enabled, the following parameters are activated: <ul style="list-style-type: none"> <li>→ <b>Polling Interval</b></li> <li>→ <b>Primary Server</b></li> <li>→ <b>Secondary Server</b></li> <li>→ <b>Third Server</b></li> </ul> </li> <li>● To not synchronize time with an NTP server, disable <b>Sync from NTP</b>.</li> </ul>
Parameter	<b>Description</b>
	<ul style="list-style-type: none"> <li>→ <b>Third Server</b></li> <li>● To not synchronize time with an NTP server, disable <b>Sync from NTP</b>.</li> </ul>
Polling Interval	Enter the time synchronization interval in seconds, range: 60–65535.

Primary Server	Enter the IP address or <a href="#">FQDN</a> of the primary NTP server. It cannot exceed 127 characters. This parameter is required.
Secondary Server	Enter the IP address or <a href="#">FQDN</a> of the secondary NTP server. It cannot exceed 127 characters. This parameter is optional.
Third Server	Enter the IP address or <a href="#">FQDN</a> of the tertiary NTP server. It cannot exceed 127 characters. This parameter is optional.
Select Server	Click <b>Select Server</b> , and select the servers to be configured in the displayed dialog box.

6. Click **Config** to deliver the configurations.



- During time zone and NTP configuration, the progress bar is displayed on the page.
- After time zone and NTP configuration is completed, the configuration result is displayed on the page.

### 3.4.3.4 Configuring SNMP Parameters

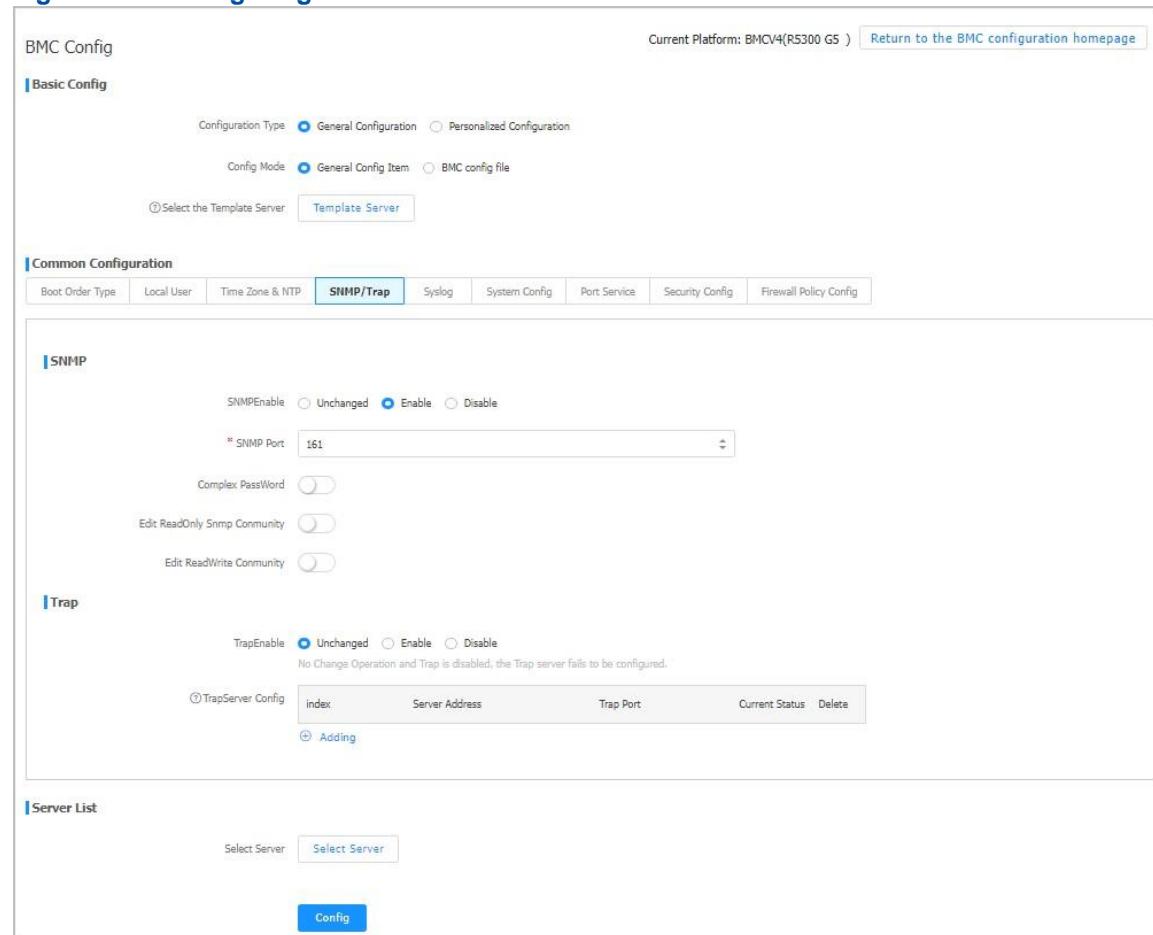
#### Abstract

This procedure describes how to configure [SNMP](#) parameters for communication between the **BMC** of a server and other devices or systems.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V4 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V4 is displayed, as shown in [Figure 3-56](#).

### Figure 3-56 Configuring BMC V4



The screenshot shows the BMC Config interface for BMC V4. The 'Basic Config' tab is selected. In the 'Common Configuration' area, the 'SNMP/Trap' tab is selected. The 'SNMP' section contains fields for 'SNMPEnable' (set to 'Enable'), 'SNMP Port' (set to '161'), and 'Complex PassWord' (disabled). The 'Trap' section contains fields for 'TrapEnable' (set to 'Unchanged') and a table for 'TrapServer Config' with a single row for 'Adding'. The 'Server List' section at the bottom has a 'Select Server' button. A 'Config' button is located at the bottom right of the configuration area.

4. In the **Common Configuration** area, click **SNMP/Trap** to switch to the **SNMP/Trap** tab.
5. Set the parameters. For a description of the parameters, refer to [Table 3-31](#).

**Table 3-31 SNMP Parameter Descriptions**

Parameter	Description
Configuration Type	Select <b>General Configuration</b> .

Configuration Mode	<p>Select a configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>General Config Item</b> → To import the configurations from a template server, click <b>Template Server</b>, and select a server as the template server in the displayed dialog box. After the import, the configurations in the template server are automatically displayed in the <b>Common Configuration</b> area, and can be modified.</li> <li>→ To not import the configurations from a template server, do not select this option.</li> <li>● <b>BMC config file</b></li> <li>→ To import the configurations in a BMC configuration file, click <b>Select File</b>, and select the BMC configuration file in the displayed dialog box. After the import, the configurations in the BMC configuration file are automatically displayed in the <b>Common Configuration</b> area, and can be modified.</li> </ul>
--------------------	--

Parameter	Description
	<p>→ To not import a BMC configuration file, do not select this option. SNMP community names cannot be imported or exported.</p>
SNMPEnable	<p>Select whether to enable the SNMP function. Options:</p> <ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li> <li>● <b>Enable</b>: indicates to enable the SNMP function.</li> <li>● <b>Disable</b>: indicates to disable the SNMP function.</li> </ul> <p>After enabling the SNMP function, you also need to set the following parameters:</p> <ul style="list-style-type: none"> <li>● <b>SNMP Port</b></li> <li>● <b>Complex PassWord</b></li> <li>● <b>Edit ReadOnly Snmp Community</b></li> <li>● <b>Edit ReadWrite Community</b></li> </ul>
SNMP Port	<p>Enter the non-secure port number of the SNMP service. Range: 1–65535, default: 161.</p>
Complex PassWord	<ul style="list-style-type: none"> <li>● To use a strong password, enable <b>Complex PassWord</b>. After this function is enabled, the read-only community name and read-write community name must comply with the password strength rules.</li> <li>● To not use a strong password, disable <b>Complex PassWord</b>.</li> </ul>
Edit ReadOnly Snmp Community	<ul style="list-style-type: none"> <li>● To edit the read-only community name, enable <b>Edit ReadOnly Snmp Community</b> and then enter the read-only community name (default: roAdmin9!).</li> <li>● To not edit the read-only community name, disable <b>Edit ReadOnly Snmp Community</b>.</li> </ul>

Edit ReadWrite Community	<ul style="list-style-type: none"> <li>To edit the read-write community name, enable <b>Edit ReadWrite Community</b> and then enter the read-write community name (default: rwAdmin9!).</li> <li>To not edit the read-write community name, disable <b>Edit ReadWrite Community</b>.</li> </ul>
TrapEnable	<p>Select whether to enable the trap function. Options:</p> <ul style="list-style-type: none"> <li><b>Unchanged</b>: indicates not to modify the original server configurations.</li> <li><b>Enable</b>: indicates to enable the trap function.</li> <li><b>Disable</b>: indicates to disable the trap function.</li> </ul> <p>After enabling the trap function, you also need to set the following parameters:</p> <ul style="list-style-type: none"> <li><b>Trap Version</b></li> <li><b>Select V3 User</b></li> <li><b>Community</b></li> <li><b>Confirm Community</b></li> <li><b>TrapHost ID</b></li> <li><b>TrapAlarm Severity</b></li> <li><b>TrapServer Config</b></li> </ul>
Trap Version	Select the <b>SNMP</b> version for traps. Options: <b>V1</b> , <b>V2C</b> , and <b>V3</b> .
Parameter	Description
Select V3 User	<p>This parameter is required when <b>Trap Version</b> is set to <b>V3</b>.</p> <p>Select an SNMPv3 user as the alarm sender.</p>
Community	<p>This parameter is required when <b>Trap Version</b> is set to <b>V1</b> or <b>V2C</b>.</p> <p>Enter the trap community name.</p>
Confirm Community	<p>This parameter is required when <b>Trap Version</b> is set to <b>V1</b> or <b>V2C</b>.</p> <p>Enter the trap community name, which must be the same as that in <b>Community</b>.</p>
TrapHost ID	Select the identifier of the host that reports alarms.
TrapAlarm Severity	<p>Select the level of events to be reported.</p> <p>For example, if <b>TrapAlarm Severity</b> is set to <b>Critical</b>, only critical alarms are reported.</p>
TrapServer Config	<p>Click <b>Adding</b> to add trap servers. A maximum of four trap servers can be added.</p> <p>After adding a trap server, you need to set the following parameters:</p> <ul style="list-style-type: none"> <li><b>index</b>: Select the sequence of the trap server. Range: 1–4.</li> <li><b>Server Address</b>: Enter the address of the server that receives alarms. An <b>IPv4</b> address, <b>IPv6</b> address, or domain name is supported.</li> <li><b>Trap Port</b>: Enter the port number of the server that receives alarms. Range: 1–65535.</li> <li><b>Current Status</b>: Select whether to enable the current server to receive alarms.</li> </ul>

Select Server	Click <b>Select Server</b> , and select the servers to be configured in the displayed dialog box.
6. Click <b>Config</b> to deliver the configurations.	



- During SNMP parameter configuration, the progress bar is displayed on the page.
- After SNMP parameter configuration is completed, the configuration result is displayed on the page.

### 3.4.3.5 Configuring Syslog Parameters

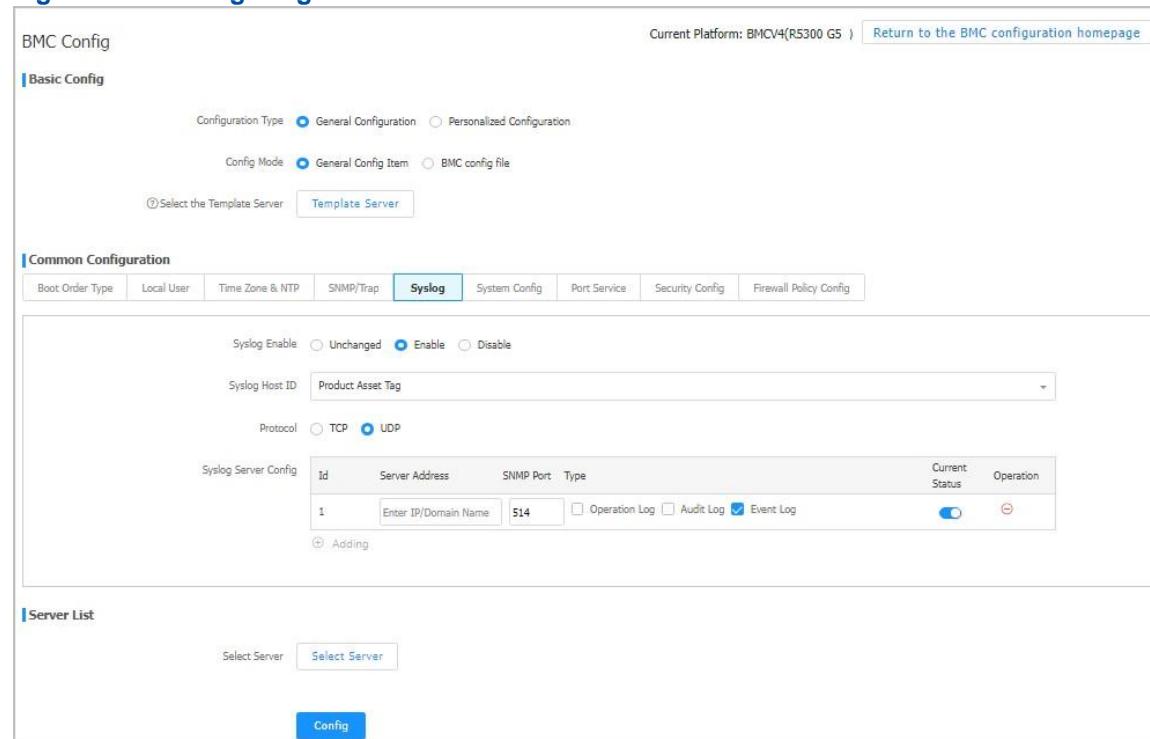
#### Abstract

This procedure describes how to configure syslog parameters to upload local logs (including audit logs, operation logs, and event logs) of a server to a syslog server.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V4 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V4 is displayed, see [Figure 3-57](#).

### Figure 3-57 Configuring BMC V4



- In the **Common Configuration** area, click **Syslog** to switch to the **Syslog** tab.
- Set the parameters. For a description of the parameters, refer to [Table 3-32](#).

**Table 3-32 Syslog Parameter Descriptions**

Parameter	Description
Configuration Type	Select <b>General Configuration</b> .
Config Mode	Select a configuration mode. Options: <ul style="list-style-type: none"> <li><b>General Config Item</b> → To import the configurations from a template server, click <b>Template Server</b>, and select a server as the template server in the displayed dialog box. After the import, the configurations in the template server are automatically displayed in the <b>Common Configuration</b> area, and can be modified.               <ul style="list-style-type: none"> <li>→ To not import the configurations from a template server, do not select this option.</li> </ul> </li> <li><b>BMC config file</b> <ul style="list-style-type: none"> <li>→ To import the configurations in a BMC configuration file, click <b>Select File</b>, and select the BMC configuration file in the displayed dialog box. After the import, the configurations in the BMC configuration file are automatically displayed in the <b>Common Configuration</b> area, and can be modified.</li> </ul> </li> </ul>
Parameter	Description
	→ To not import a BMC configuration file, do not select this option.

Syslog Enable	Select whether to enable the syslog function. <ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li> <li>● <b>Enable</b>: indicates to enable the syslog function.</li> <li>● <b>Disable</b>: indicates to disable the syslog function.</li> </ul> <p>After <b>Enable</b> is selected, the following parameters also need to be set:</p> <ul style="list-style-type: none"> <li>● <b>Syslog Host ID</b></li> <li>● <b>Protocol</b></li> <li>● <b>Syslog Server Config</b></li> </ul>
Syslog Host ID	Select how to identify the host in a log file. Options: <ul style="list-style-type: none"> <li>● <b>Host Name</b>: identified by host name.</li> <li>● <b>Product Asset Tag</b>: identified by asset tag.</li> <li>● <b>Board serial number</b>: identified by board SN.</li> </ul>
Protocol	Select the log transmission protocol. Options: <ul style="list-style-type: none"> <li>● <b>UDP</b></li> <li>● <b>TCP</b></li> </ul>
Syslog Server Config	Set the parameters related to the syslog server. <ul style="list-style-type: none"> <li>● <b>Server Address</b>: enter the <b>IP</b> address of the syslog server.</li> <li>● <b>SNMP Port</b>: enter the port number of the syslog server. Range: 1–65535.</li> <li>● <b>Type</b>: select the types of logs to be transmitted. Options: Operation Log, Audit Log, and Event Log. At least one log type needs to be selected.</li> </ul>
Select Server	Click <b>Select Server</b> , and select the servers to be configured in the displayed dialog box.

6. Click **Config** to deliver the configurations.



- During syslog parameter configuration, the progress bar is displayed on the page.
- After syslog parameter configuration is completed, the configuration result is displayed on the page.

### 3.4.3.6 Configuring System Parameters

#### Abstract

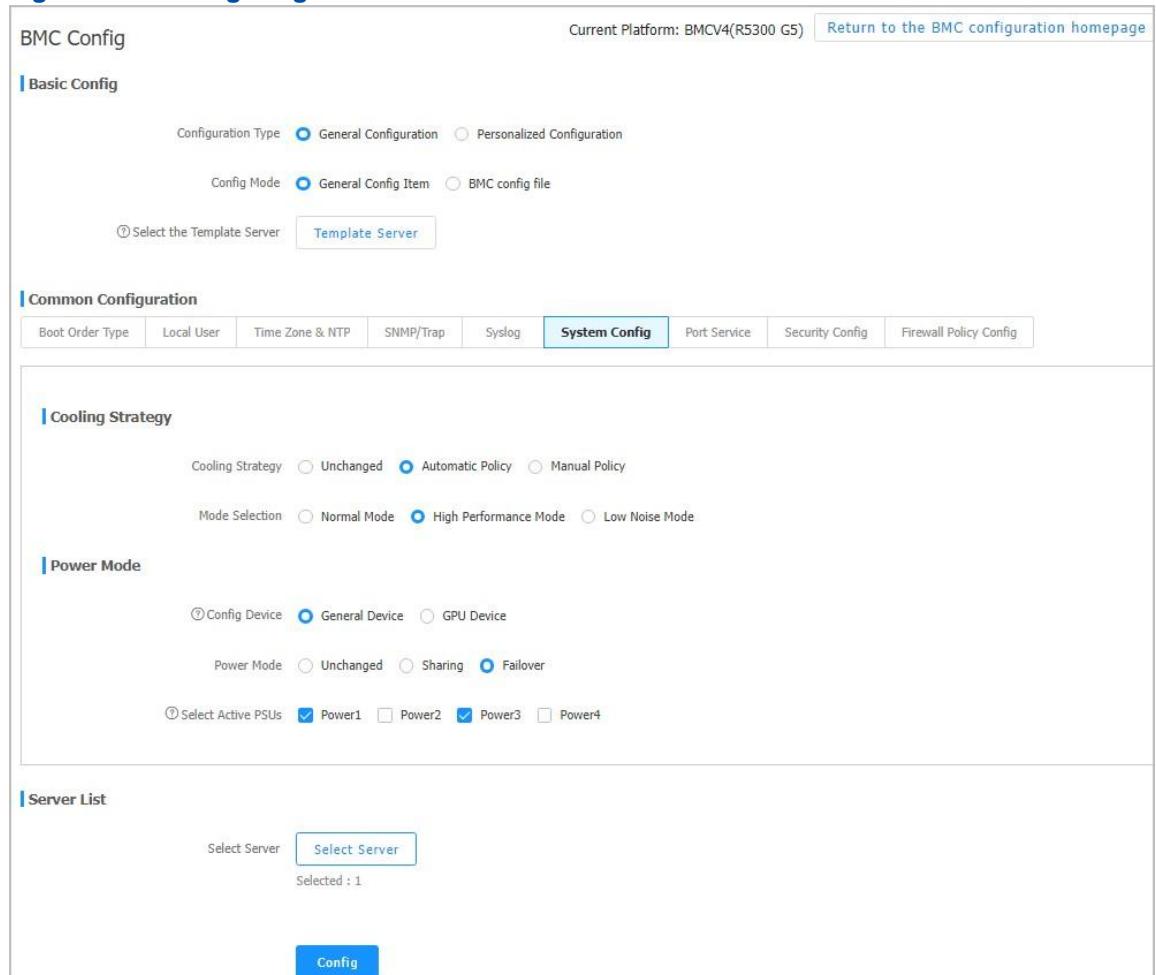
System parameters include the cooling policy and power mode.

- A cooling policy is configured in accordance with the environment where a server is placed to ensure the performance and stability of the server.
- A proper power mode enables the power modules to supply power to the server in a reasonable manner.

## Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V4 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V4 is displayed, as shown in [Figure 3-58](#).

**Figure 3-58 Configuring BMC V4**



BMC Config

Current Platform: BMCV4(R5300 G5) [Return to the BMC configuration homepage](#)

**Basic Config**

Configuration Type:  General Configuration  Personalized Configuration

Config Mode:  General Config Item  BMC config file

② Select the Template Server [Template Server](#)

**Common Configuration**

Boot Order Type Local User Time Zone & NTP SNMP/Trap Syslog **System Config** Port Service Security Config Firewall Policy Config

**Cooling Strategy**

Cooling Strategy:  Unchanged  Automatic Policy  Manual Policy

Mode Selection:  Normal Mode  High Performance Mode  Low Noise Mode

**Power Mode**

② Config Device:  General Device  GPU Device

Power Mode:  Unchanged  Sharing  Failover

② Select Active PSUs:  Power1  Power2  Power3  Power4

**Server List**

Select Server [Select Server](#)  
Selected : 1

**Config**

4. In the **Common Configuration** area, click **System Config** to switch to the **System Config** tab.
5. Set the parameters. For a description of the parameters, refer to [Table 3-33](#).

**Table 3-33 System Configuration Parameter Descriptions**

Parameter	Description
Configuration Type	Select <b>General Configuration</b> .
Config Mode	Select a configuration mode. Options: ● <b>General Config Item</b>

Parameter	Description
	<ul style="list-style-type: none"> <li>→ To import the configurations from a template server, click <b>Template Server</b>, and select a server as the template server in the displayed dialog box. After the import, the configurations in the template server are automatically displayed in the <b>Common Configuration</b> area, and can be modified.</li> <li>→ To not import the configurations from a template server, do not select this option.</li> <li>● <b>BMC config file</b> <ul style="list-style-type: none"> <li>→ To import the configurations in a BMC configuration file, click <b>Select File</b>, and select the BMC configuration file in the displayed dialog box. After the import, the configurations in the BMC configuration file are automatically displayed in the <b>Common Configuration</b> area, and can be modified.</li> <li>→ To not import a BMC configuration file, do not select this option.</li> </ul> </li> </ul>
Cooling Strategy	<p>Select a cooling policy. Options:</p> <ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li> <li>● <b>Automatic Policy</b>: indicates to automatically regulate the rotational speed of fan units. After selecting <b>Automatic Policy</b>, you also need to set <b>Mode Selection</b>.</li> <li>● <b>Manual Policy</b>: indicates to manually regulate the rotational speed of fan units. After selecting <b>Manual Policy</b>, you also need to set <b>Speed Percentage</b>.</li> </ul>
Mode Selection	<p>This parameter is required when <b>Cooling Strategy</b> is set to <b>Automatic Policy</b>. Select an automatic speed regulation mode.</p> <ul style="list-style-type: none"> <li>● <b>Normal Mode</b>: selected when there is clearance above the top surface of a server and the server is insensitive to noise.</li> <li>● <b>High Performance Mode</b>: selected when servers are stacked together and there is no clearance between them.</li> <li>● <b>Low Noise Mode</b>: selected when servers are placed in an office or other areas that are sensitive to noise. <b>Low Noise Mode</b> is not available for the NCS6742G N4 servers.</li> </ul>
Speed Percentage	<p>This parameter is required when <b>Cooling Strategy</b> is set to <b>Manual Policy</b>. The speed ratio is the ratio of the current speed of a fan to the maximum speed of the fan.</p> <p>Enter a percentage, range: 10%–100%.</p>
Config Device	<p>Select a server model to be configured. Options:</p> <ul style="list-style-type: none"> <li>● <b>General Device</b>: a model without GPU modules.</li> <li>● <b>GPU Device</b>: a model configured with GPU modules.</li> </ul>

Power Mode/Main-Board Power Mode	When <b>Config Device</b> is set to <b>General Device</b> , the <b>Power Mode</b> parameter is displayed. When <b>Config Device</b> is set to <b>GPU Device</b> , the <b>MainBoard Power Mode</b> parameter is displayed. Select a power mode. Options:
<b>Parameter</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li> <li>● <b>Sharing</b>: The power modules operate in load-balancing mode. Multiple power modules supply power to the server simultaneously, and the power consumption of the server is shared equally. In this mode, the overall power supply capability is strong, and the failure of a single power module has a small impact on the other power modules. However, the power supply efficiency is low, and the power consumption is high.</li> <li>● <b>Failover</b>: The power modules operate in active/standby mode. One or more power modules are active power modules for supplying power to the server, and the other power modules are standby ones. In this mode, the power supply efficiency is high, and the service life of the power modules is long. The <b>Failover</b> mode can be selected only when two or more power modules are present and operating properly. If <b>Power Mode</b> is set to <b>Failover</b>, you also need to set the <b>Select Active PSUs</b> parameter to select the active power modules.</li> </ul>
Select Active PSUs	<p>This parameter is required when <b>Power Mode</b> is set to <b>Failover</b>.</p> <p>Select the active power modules.</p> <p>For a dual-power-module server, you can select <b>Power1</b> and <b>Power2</b> only.</p>
GPU Power Mode	<p>This parameter is required when <b>Config Device</b> is set to <b>GPU Device</b>.</p> <p>Select the power mode of the GPU module. Options:</p> <ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li> <li>● <b>Sharing</b>: The power modules operate in load-balancing mode. Multiple power modules supply power to the server simultaneously, and the power consumption of the server is shared equally. In this mode, the overall power supply capability is strong, and the failure of a single power module has a small impact on other power modules. However, the power supply efficiency is low, and the power consumption is high.</li> <li>● <b>Failover</b>: The power modules operate in active or standby mode. One or more power modules are active power modules for supplying power to the server, and other power modules are standby ones. In this mode, the power supply efficiency is high, and the service life of the power modules is long. The <b>Failover</b> mode can be selected only when two or more power modules are present and operating properly. If <b>Power Mode</b> is set to <b>Failover</b>, you also need to set the <b>Select Active PSUs</b> parameter to select the active power modules.</li> </ul>

Select Active PSUs	This parameter is required when <b>GPU Power Mode</b> is set to <b>Failover</b> . Select the active power modules of the GPU module.
Select Server	Click <b>Select Server</b> , and select the servers to be configured in the displayed dialog box.

6. Click **Config** to deliver the configurations.



- During system parameter configuration, the progress bar is displayed on the page.
- After system parameter configuration is completed, the configuration result is displayed on the page.

### 3.4.3.7 Configuring Service Parameters

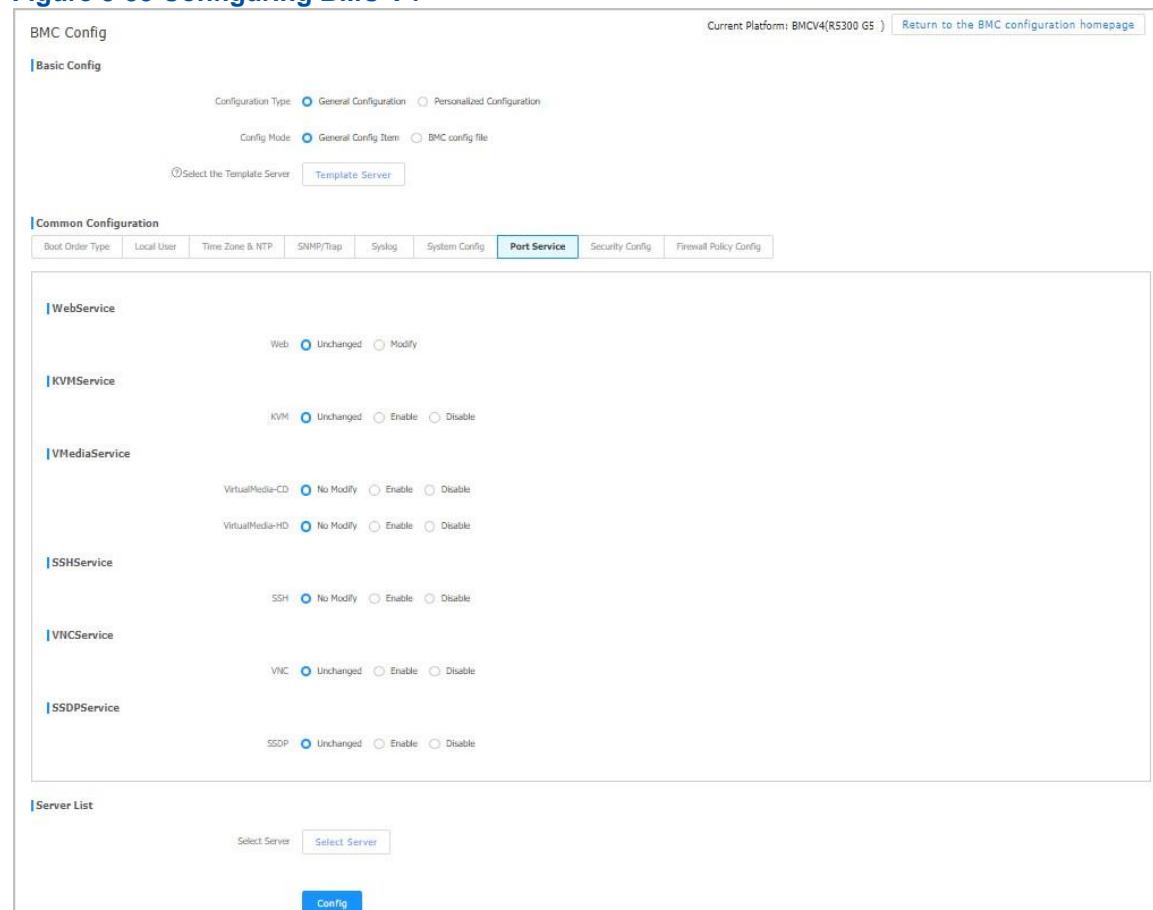
#### Abstract

This procedure describes how to configure the service parameters for the **BMC**, including the service status, secure port, non-secure port, and timeout period.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V4 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V4 is displayed, as shown in [Figure 3-59](#).

### Figure 3-59 Configuring BMC V4



The screenshot shows the BMC Config interface for a BMCV4(RS300 G5) platform. The 'Port Service' tab is selected. The interface includes sections for WebService, KVMService, VMediaService, SSHService, VNCService, and SSDPService, each with configuration options like 'Unchanged', 'Modify', 'Enable', and 'Disable'. A 'Server List' section at the bottom allows selecting a template server. A 'Config' button is located at the bottom center.

4. In the **Common Configuration** area, click **Port Service** to switch to the **Port Service** tab.
5. Set the parameters. For a description of the parameters, refer to [Table 3-34](#).

**Table 3-34 Port Service Parameter Descriptions**

Parameter	Description
Configuration Type	Select <b>General Configuration</b> .

Config Mode	<p>Select a configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>General Config Item</b> → To import the configurations from a template server, click <b>Template Server</b>, and select a server as the template server in the displayed dialog box. After the import, the configurations in the template server are automatically displayed in the <b>Common Configuration</b> area, and can be modified.</li> <li>→ To not import the configurations from a template server, do not select this option.</li> <li>● <b>BMC config file</b> <ul style="list-style-type: none"> <li>→ To import the configurations in a BMC configuration file, click <b>Select File</b>, and select the BMC configuration file in the displayed dialog box. After the import, the configurations in the BMC configuration file are automatically displayed in the <b>Common Configuration</b> area, and can be modified.</li> <li>→ To not import a BMC configuration file, do not select this option.</li> </ul> </li> </ul>
Web	<p>Select the <b>HTTPS</b> service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li> <li>● <b>Modify</b>: indicates to modify the original server configurations.</li> </ul> <p>After <b>Modify</b> is selected, the following parameters need to be set:</p> <ul style="list-style-type: none"> <li>● <b>HTTPS Port</b>: Enter a secure port number. Default: 443.</li> <li>● <b>HTTPS TimeOut</b>: Enter the timeout period. Range: 1–60, unit: minutes.</li> </ul>
KVM	<p>Select the <b>KVM</b> service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li> <li>● <b>Enable</b>: indicates to enable the KVM service.</li> <li>● <b>Disable</b>: indicates to disable the KVM service.</li> </ul> <p>After enabling the KVM service, you need to configure the following parameters:</p> <ul style="list-style-type: none"> <li>● <b>KVM Port</b>: Enter a secure port number (default: 7582) in KVM encryption mode or a non-secure port number (default: 7578) in KVM non-encryption mode. Range: 1–65535.</li> <li>● <b>KVM TimeOut</b>: Enter the timeout period. Range: 1–60, unit: minutes.</li> </ul>
VirtualMedia-CD	<p>Select the VirtualMedia-CD service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configurations.</li> <li>● <b>Enable</b>: indicates to enable the VirtualMedia-CD service.</li> <li>● <b>Disable</b>: indicates to disable the VirtualMedia-CD service.</li> </ul> <p>After enabling the VirtualMedia-CD service, you need to configure the following parameter:</p>

Parameter	Description

	<p><b>VirtualMedia-CD Port:</b> Enter a secure port number (default: 5124) in VMedia encryption mode or a non-secure port number (default: 5120) in VMedia non-encryption mode. Range: 1–65535.</p>
VirtualMedia-HD	<p>Select the VirtualMedia-HD service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configurations.</li> <li>● <b>Enable:</b> indicates to enable the VirtualMedia-HD service.</li> <li>● <b>Disable:</b> indicates to disable the VirtualMedia-HD service.</li> </ul> <p>After enabling the VirtualMedia-HD service, you need to configure the following parameter:</p> <p><b>VirtualMedia-HD Port:</b> Enter a secure port number (default: 5127) in VMedia encryption mode or a non-secure port number (default: 5123) in VMedia non-encryption mode. Range: 1–65535.</p>
SSH	<p>Select the SSH service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configurations.</li> <li>● <b>Enable:</b> indicates to enable the SSH service.</li> <li>● <b>Disable:</b> indicates to disable the SSH service.</li> </ul> <p>After enabling the SSH service, you need to configure the following parameter:</p> <p><b>SSH Port:</b> Enter a secure port number. Default: 22, range: 1–65535.</p>
VNC	<p>Select the VNC service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>Unchanged:</b> indicates not to modify the original server configurations.</li> <li>● <b>Enable:</b> indicates to enable the VNC service.</li> <li>● <b>Disable:</b> indicates to disable the VNC service.</li> </ul> <p>After enabling the VNC service, you need to configure the following parameters:</p> <ul style="list-style-type: none"> <li>● <b>Nonsecure Port:</b> Enter a non-secure port number. Default: 5900, range: 1–65535.</li> <li>● <b>Secure Port:</b> Enter a secure port number. Default: 5901, range: 1–65535.</li> <li>● <b>VNC Service Password:</b> Select whether to change the original VNC service password. To change the password, select <b>Modify</b> and then enter a new password in the <b>VNC Service New Password</b> text box.</li> </ul>
SSDP	<p>Select the SSDP service configuration mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>Unchanged:</b> indicates not to modify the original server configurations.</li> <li>● <b>Enable:</b> indicates to enable the SSDP service.</li> <li>● <b>Disable:</b> indicates to disable the SSDP service.</li> </ul> <p>After enabling the SSDP service, you need to configure the following parameters:</p> <ul style="list-style-type: none"> <li>● <b>SSDPPort:</b> Enter a port number. Default: 1900, range: 1–65535.</li> <li>● <b>SSDP Notify:</b> Select whether to enable the SSDP multicast function.</li> <li>● <b>SSDP Multicast Interval:</b> Enter the multicast interval. Range: 0–1800, unit: seconds.</li> <li>● <b>SSDP IPv6 Scope:</b> Select the IPv6 multicast scope.</li> </ul>

Parameter	Description
Select Server	Click <b>Select Server</b> , and select the servers to be configured in the displayed dialog box.

6. Click **Config** to deliver the configurations.



- During service parameter configuration, the progress bar is displayed on the page.
- After service parameter configuration is completed, the configuration result is displayed on the page.

### 3.4.3.8 Configuring Security Parameters

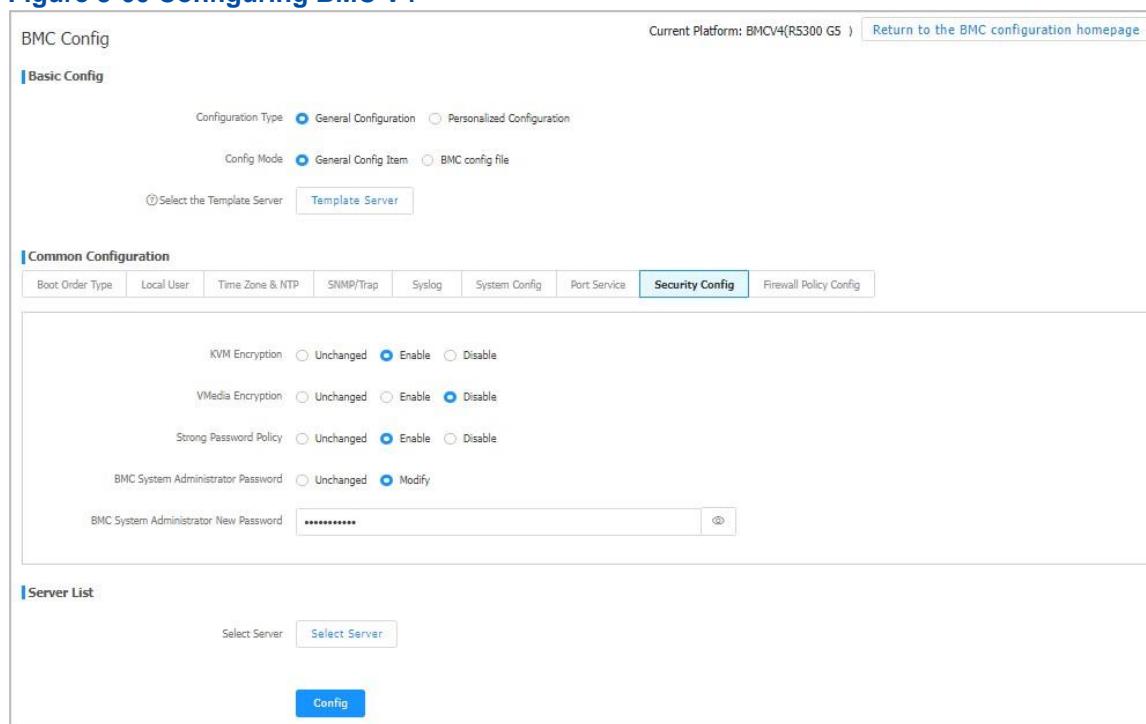
#### Abstract

This procedure describes how to configure security parameters to ensure the security of a server during remote operations.

#### Step

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V4 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V4 is displayed, as shown in [Figure 3-60](#).

[Figure 3-60 Configuring BMC V4](#)



The screenshot shows the BMC Config page with the following details:

- Header:** Current Platform: BMCV4(R5300 G5) | [Return to the BMC configuration homepage](#)
- Basic Config:**
  - Configuration Type:  General Configuration  Personalized Configuration
  - Config Mode:  General Config Item  BMC config file
  - Select the Template Server: [Template Server](#)
- Common Configuration:**
  - KVM Encryption:  Unchanged  Enable  Disable
  - VMedia Encryption:  Unchanged  Enable  Disable
  - Strong Password Policy:  Unchanged  Enable  Disable
  - BMC System Administrator Password:  Unchanged  Modify
  - BMC System Administrator New Password:  (Redacted)
- Server List:**
  - Select Server: [Select Server](#)
  - Config: [Config](#)

4. In the **Common Configuration** area, click **Security Config** to switch to the **Security Config** tab.
5. Set the parameters. For a description of the parameters, refer to [Table 3-35](#).

**Table 3-35 Security Parameter Descriptions**

Parameter	Description
Configuration Type	Select <b>General Configuration</b> .
Config Mode	Select a configuration mode. Options: <ul style="list-style-type: none"> <li>● <b>General Config Item</b> → To import the configurations from a template server, click <b>Template Server</b>, and select a server as the template server in the displayed dialog box. After the import, the configurations in the template server are automatically displayed in the <b>Common Configuration</b> area, and can be modified.               <ul style="list-style-type: none"> <li>→ To not import the configurations from a template server, do not select this option.</li> </ul> </li> <li>● <b>BMC config file</b> <ul style="list-style-type: none"> <li>→ To import the configurations in a BMC configuration file, click <b>Select File</b>, and select the BMC configuration file in the displayed dialog box. After the import, the configurations in the BMC configuration file are automatically displayed in the <b>Common Configuration</b> area, and can be modified.               <ul style="list-style-type: none"> <li>→ To not import a BMC configuration file, do not select this option.</li> </ul> </li> </ul> </li> </ul>
KVM Encryption	Select whether to enable the <b>KVM</b> encryption function. Options: <ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li> </ul>
Parameter	Description
	<ul style="list-style-type: none"> <li>● <b>Enable</b>: indicates to enable the KVM encryption function.</li> <li>● <b>Disable</b>: indicates to disable the KVM encryption function.</li> </ul> After the function is enabled, encryption is implemented during KVM-based remote operations on the servers. You cannot enable KVM encryption if you have enabled application support on the KVM service port.
VMedia Encryption	Select whether to enable the VMedia encryption function. Options: <ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li> <li>● <b>Enable</b>: indicates to enable the VMedia encryption function.</li> <li>● <b>Disable</b>: indicates to disable the VMedia encryption function.</li> </ul> After the function is enabled, files remotely uploaded to the servers through the KVM are encrypted.

Strong Password Policy	Select whether to enable the strong password policy. Options: <ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li> <li>● <b>Enable</b>: indicates to enable the strong password policy.</li> <li>● <b>Disable</b>: indicates to disable the strong password policy.</li> </ul>
BMC System Administrator Password	Password for logging in to the server through <a href="#">SSH</a> . Select whether to modify the original BMC system administrator password of the server. Options: <ul style="list-style-type: none"> <li>● <b>Unchanged</b>: indicates not to modify the original server configurations.</li> <li>● <b>Modify</b>: indicates to modify the original password. Enter the new password in the <b>BMC System Administrator New Password</b> text box.</li> </ul>
Select Server	Click <b>Select Server</b> , and select the servers to be configured in the displayed dialog box.

6. Click **Config** to deliver the configurations.



- During security parameter configuration, the progress bar is displayed on the page.
- After security parameter configuration is completed, the configuration result is displayed on the page.

### 3.4.3.9 Configuring Firewall Parameters

#### Abstract

By configuring firewall parameters, you can add blacklists and whitelists to control access to the [BMC](#).

- The devices in a blacklist are forbidden to access the BMC.
- Only the devices in a whitelist are allowed to access the BMC.

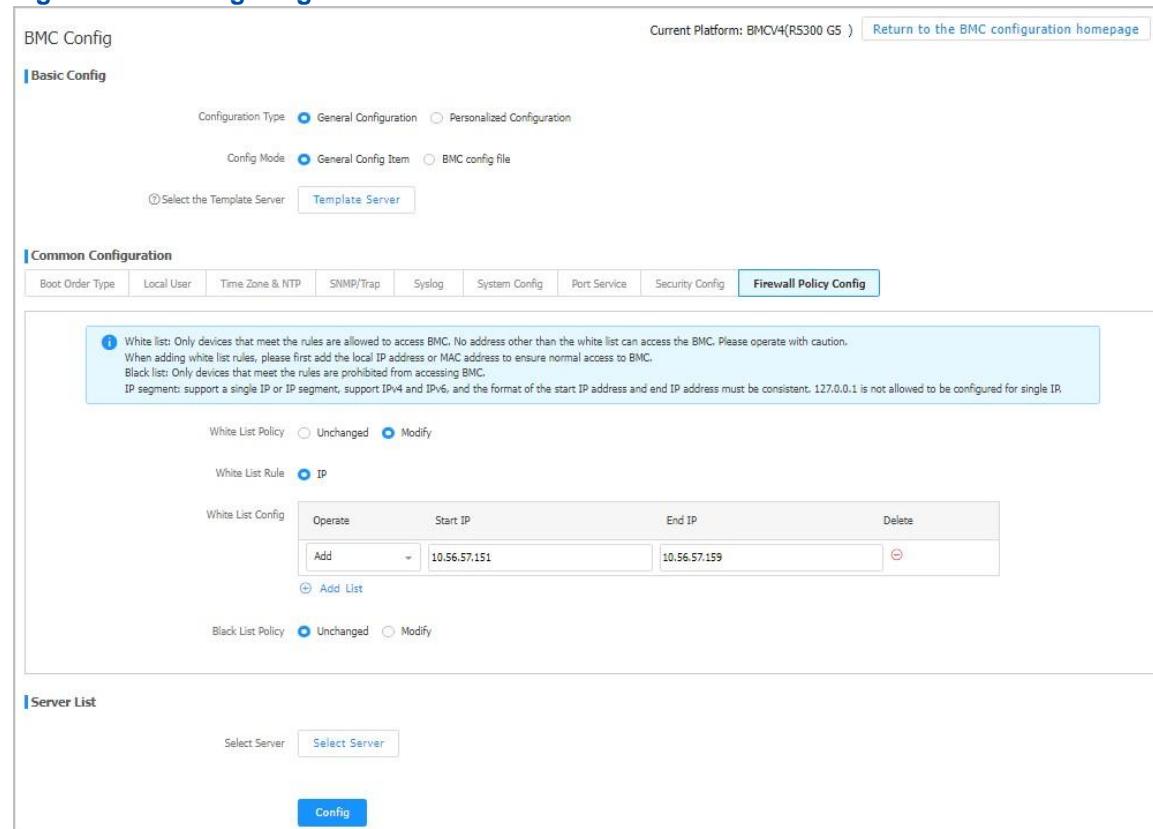
When adding a whitelist, you must first add the [IP](#) address of your local [PC](#) (acting as a client PC) to the whitelist to ensure that your local PC can access the Web portal of the BMC.

This procedure describes how to configure firewall parameters.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content of the corresponding BMC V4 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V4 is displayed, as shown in [Figure 3-61](#).

### Figure 3-61 Configuring the BMC V4



The screenshot shows the BMC Config interface. At the top, there are tabs for 'BMC Config' and 'Return to the BMC configuration homepage'. Below this, the 'Basic Config' section is visible. The 'Common Configuration' section is active, with the 'Firewall Policy Config' tab selected. A note in this section states: 'White list: Only devices that meet the rules are allowed to access BMC. No address other than the white list can access the BMC. Please operate with caution. When adding white list rules, please first add the local IP address or MAC address to ensure normal access to BMC. Black list: Only devices that meet the rules are prohibited from accessing BMC. IP segment: support a single IP or IP segment, support IPv4 and IPv6, and the format of the start IP address and end IP address must be consistent. 127.0.0.1 is not allowed to be configured for single IP.' Below this note, there are sections for 'White List Policy' (radio buttons for 'Unchanged' and 'Modify', with 'Modify' selected), 'White List Rule' (radio button for 'IP', selected), and a table for 'White List Config' with columns for 'Operate', 'Start IP', 'End IP', and 'Delete'. The table shows an entry for '10.56.57.151'. There is also a 'Black List Policy' section with similar options. The 'Server List' section at the bottom includes a 'Select Server' button and a 'Config' button.

- In the **Common Configuration** area, click **Firewall Policy Config** to switch to the **Firewall Policy Config** tab.
- Set the parameters. For a description of the parameters, refer to [Table 3-36](#).

**Table 3-36 Firewall Parameter Descriptions**

Parameter	Description
<b>White List Policy</b>	Select whether to modify the whitelist. Options: <ul style="list-style-type: none"> <li><b>Unchanged</b>: indicates not to modify the original server whitelist.</li> </ul>
<b>Parameter</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li><b>Modify</b>: indicates to modify the original whitelist of the server, and adds or deletes IP address segments in <b>White List Config</b>.</li> </ul>
<b>Black List Policy</b>	Select whether to modify the blacklist. Options: <ul style="list-style-type: none"> <li><b>Unchanged</b>: indicates not to modify the original server blacklist.</li> <li><b>Modify</b>: indicates to modify the original blacklist of the server, and adds or deletes IP address segments in <b>Black List Config</b>.</li> </ul>
<b>Select Server</b>	Click <b>Select Server</b> . In the displayed dialog box, select a server to be configured.

- Click **Config** to deliver the configurations.

**Note**

- During firewall parameter configuration, the progress bar is displayed on the page.
- After firewall parameter configuration is completed, the configuration result is displayed on the page.

### 3.4.3.10 Configuring Asset Tags

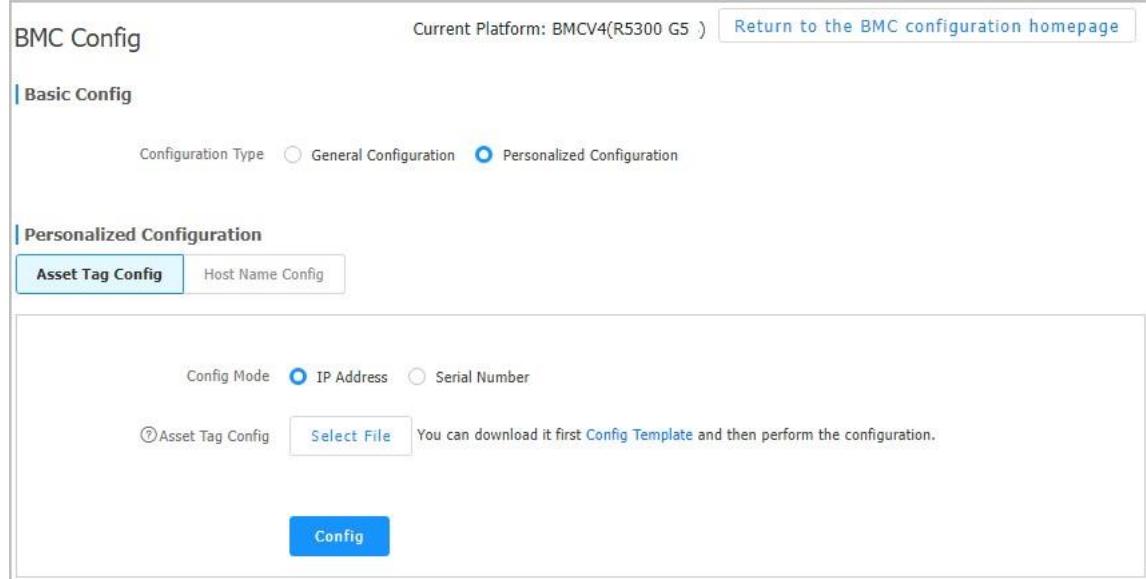
#### Abstract

This procedure describes how to modify the asset tags of servers in batches when their asset tags need to be updated.

#### Steps

1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V4 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V4 is displayed, as shown in [Figure 3-62](#).

[Figure 3-62 Configuring BMC V4](#)



BMC Config

Current Platform: BMCV4(R5300 G5 ) [Return to the BMC configuration homepage](#)

Configuration Type:  General Configuration  Personalized Configuration

Asset Tag Config Host Name Config

Personalized Configuration

Asset Tag Config [Select File](#) You can download it first Config Template and then perform the configuration.

Config

4. In the **Personalized Configuration** area, click **Asset Tag Config** to switch to the **Asset Tag Config** tab.
5. Set the parameters. For a description of the parameters, refer to [Table 3-37](#).

[Table 3-37 Asset Tag Parameter Descriptions](#)

Parameter	Description
-----------	-------------

Configuration Type	Select <b>Personalized Configuration</b> .
Config Mode	<ul style="list-style-type: none"> <li>To match servers based on <b>BMC IP</b> addresses and then configure asset tags, select <b>IP Address</b>. In this mode, you do not need to select a BMC.</li> <li>To match servers based on serial numbers and then configure asset tags, select <b>Serial Number</b>. In this mode, you need to select a BMC.</li> </ul>
Asset Tag Config	<ol style="list-style-type: none"> <li>(Optional) If there is no asset tag configuration file, click <b>Config Template</b> to download and fill in the configuration template.           <ul style="list-style-type: none"> <li>If <b>Config Mode</b> is set to <b>IP Address</b>, the name of the configuration template downloaded to your local PC is <i>ImportAssetTag.csv</i>.</li> <li>If <b>Config Mode</b> is set to <b>Serial Number</b>, the name of the configuration template downloaded to your local PC is <i>ImportAssetTagWithSN.csv</i>.</li> </ul> </li> <li>Click <b>Select File</b>, and select the edited configuration file. The selected file is automatically verified. If it fails the verification, the error lines and causes are displayed.</li> </ol>

6. Click **Config** to deliver the configurations.



#### Note

- During asset tag configuration, the progress bar is displayed on the page.
- After asset tag configuration is completed, the configuration result is displayed on the page.

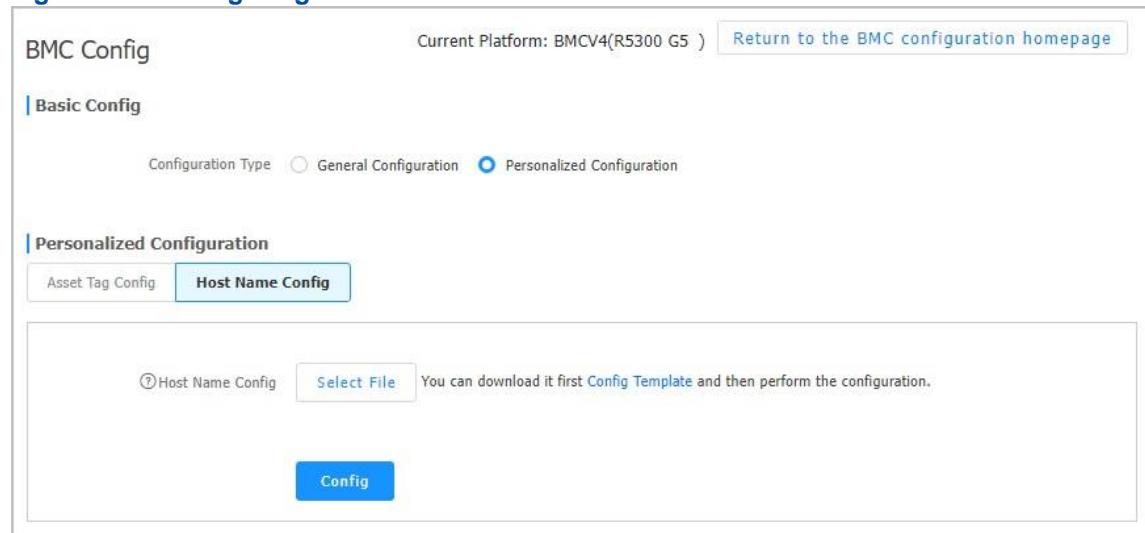
### 3.4.3.11 Configuring a Host Name

#### Abstract

This procedure describes how to configure a host name to identify a server.

#### Steps

- Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
- From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V4 is automatically displayed on the UniKits.
- Click **Submit**. The page for configuring BMC V4 is displayed, as shown in [Figure 3-63](#).

**Figure 3-63 Configuring BMC V4**

4. In the **Personalized Configuration** area, click **Host Name Config** to switch to the **Host Name Config** tab.
5. Set the parameters. For a description of the parameters, refer to [Table 3-38](#).

**Table 3-38 Host Name Parameter Descriptions**

Parameter	Description
Configuration Type	Select <b>Personalized Configuration</b> .
Host Name Config	<p>a. (Optional) If there is no host name configuration file, click <b>Config Template</b> to download and fill in the configuration template. The name of the configuration template downloaded to your local PC is <i>ImportHostname.csv</i>.</p> <p>b. Click <b>Select File</b>, and select the edited configuration file. The selected file is automatically verified. If it fails the verification, the error lines and causes are displayed.</p>

6. Click **Config** to deliver the configurations.



- During host name configuration, the progress bar is displayed on the page.
- After host name configuration is completed, the configuration result is displayed on the page.

### 3.4.4 BIOS Configuration

In the UniKits, you can configure the **BIOS** parameters of servers in batches.

You can configure the BIOS through either of the following ways:

- Configuring the BIOS through general configuration items

For details, refer to "[3.4.4.1 Configuring the BIOS Through General Configuration Items](#)".

- Configuring the BIOS through a configuration file

For details, refer to "[3.4.4.2 Configuring the BIOS Through a Configuration File](#)".

### 3.4.4.1 Configuring the BIOS Through General Configuration Items

#### Abstract

This procedure describes how to configure the BIOS through general configuration items.

#### Steps

1. Select **Device Mgmt > Deployment > BIOS Config**. The **BIOS Config** page is displayed, see [Figure 3-64](#).

**Figure 3-64 BIOS Config Page—General Configuration Items**
**Note**

The **BIOS Config** page is long, and only some contents are displayed in the above figure.

2. Set the parameters. For a description of the parameters, refer to [Table 3-39](#).

**Table 3-39 BIOS Parameter Descriptions—General Configuration Items**

Parameter	Description
<b>Basic Config</b>	
Config Mode	Select <b>General Config Item</b> .

Select the Template Server	Click <b>Template Server</b> , and select a server as the template. After a template server is selected, all the BIOS configuration items below are those on the template server.
<b>Parameter</b>	
<b>Boot Config</b>	
Boot Type	Select the server boot mode. Options: <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configuration.</li> <li>● <b>Legacy</b>: indicates to boot the server in Legacy mode.</li> <li>● <b>UEFI</b>: indicates to boot the server in <b>UEFI</b> mode.</li> </ul>
Boot Order	Select whether to modify the boot order of the server. Options: <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configuration.</li> <li>● <b>Modify Boot Order</b>: indicates to modify the boot order. In this case, you need to set the boot devices in sequence in <b>Boot Order Type</b>.</li> </ul>
<b>Pxe Config</b>	
Network Stack Config	Select whether to enable the PXE function. Options: <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configuration.</li> <li>● <b>Enable</b>: indicates to enable the PXE function.</li> <li>● <b>Disable</b>: indicates to disable the PXE function.</li> </ul> After the PXE function is enabled, you need to set <b>Protocol Stack</b> and <b>Embedded NIC</b> .
<b>Virtual Config</b>	
VT-D	Select whether to enable the virtualization function. Options: <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configuration.</li> <li>● <b>Enable</b>: indicates to enable the virtualization function.</li> <li>● <b>Disable</b>: indicates to disable the virtualization function.</li> </ul>
VMX(VT-X)	Select whether to enable the Vanderpool technology. Options: <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configuration.</li> <li>● <b>Enable</b>: indicates to enable the Vanderpool technology.</li> <li>● <b>Disable</b>: indicates to disable the Vanderpool technology.</li> </ul>
PCIe SR-IOV	Select whether to enable the SR-IOV function. Options: <ul style="list-style-type: none"> <li>● <b>No Modify</b>: indicates not to modify the original server configuration.</li> <li>● <b>Enable</b>: indicates to enable the SR-IOV function.</li> <li>● <b>Disable</b>: indicates to disable the SR-IOV function.</li> </ul>

Power Config	
Custom Power Policy	<p>Select the energy efficiency mode of power modules. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configuration.</li> <li>● <b>Efficiency:</b> energy-saving mode. This mode is applicable to most common scenarios. In this mode, the server enables energy saving with minimal performance compromise and puts some CPU cores to sleep at a low load, to increase energy savings while delivering good performance.</li> <li>● <b>Performance:</b> performance mode.</li> </ul>

Parameter	Description
	<p>This mode is applicable to high-performance scenarios characterized by high load, multiple threads and low latency. In this mode, the CPU usage and memory usage are high and energy saving is automatically disabled, and therefore the overall power consumption is increased.</p> <ul style="list-style-type: none"> <li>● <b>Custom:</b> user-defined mode. This mode is applicable to the scenarios where you need to customize the power management policy as required.</li> <li>● <b>Load Balance:</b> IEM-driven load-balancing mode. This mode is developed by NETAŞ and is applicable to the scenarios where power consumption and performance need to be balanced. In this mode, the server enables power saving to reduce power consumption, and dynamically adjusts the load of non-core areas in accordance with the core load, to balance power consumption and performance and maximize the performance per unit power consumption.</li> <li>● <b>IEM Power:</b> IEM-driven energy-saving mode. This mode is developed by NETAŞ and is applicable to the scenarios where the overall power consumption of the server needs to be controlled. In this mode, the server enables power saving, and dynamically adjusts the load of non-core areas in accordance with the core load to reduce the overall power consumption of non-core areas.</li> <li>● <b>Latency Performance:</b> low-latency mode. This mode is applicable to the scenarios with strict requirements for latency and jitter, for example, the real-time operating system. In this mode, the server disables energy saving and other management functions that may cause latency, and keeps idle CPUs at their highest frequency for faster response.</li> </ul>

<p><b>Turbo Mode</b></p> <p>Select whether to enable the dynamic CPU acceleration function. Options:</p> <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configuration.</li> <li>● <b>Enable:</b> indicates to enable the dynamic CPU acceleration function.</li> <li>● <b>Disable:</b> indicates to disable the dynamic CPU acceleration function.</li> </ul>	
<b>Processor Config</b>	
CPU Hyper Thread	Select whether to enable the CPU hyper-threading function. Options: <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configuration.</li> <li>● <b>Enable:</b> indicates to enable the CPU hyper-threading function.</li> <li>● <b>Disable:</b> indicates to disable the CPU hyper-threading function.</li> </ul>
<b>Memory Config</b>	
NUMA	Select whether to enable the NUMA function. Options: <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configuration.</li> </ul>
<b>Parameter</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>● <b>Enable:</b> indicates to enable the NUMA function.</li> <li>● <b>Disable:</b> indicates to disable the NUMA function.</li> </ul>
<b>Console Config</b>	
Serial Port Redirection	Select whether to enable the serial port redirection function. Options: <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configuration.</li> <li>● <b>Enable:</b> indicates to enable the serial port redirection function.</li> <li>● <b>Disable:</b> indicates to disable the serial port redirection function.</li> </ul> After the serial port redirection function is enabled, you need to set <b>Serial Port BaudRate</b> .
<b>Security Config</b>	
BIOS Password Operation	Select the BIOS password configuration mode. Options: <ul style="list-style-type: none"> <li>● <b>No Modify:</b> indicates not to modify the original server configuration.</li> <li>● <b>Add/Modify:</b> indicates to create a new BIOS password or modify the existing BIOS password.                In this case, you also need to set <b>Current BIOS Password</b>, <b>New BIOS Password</b>, and <b>Confirm New Password</b>.             </li> <li>● <b>Delete:</b> indicates to delete the BIOS password.                In this case, you also need to set <b>Current BIOS Password</b>.             </li> </ul>
<b>Configuration Mode</b>	

Effective Mode	Select the validation mode. Options: <ul style="list-style-type: none"> <li>● <b>Manual Mode:</b> After the configurations are completed, you must manually restart the related host to apply the configurations.</li> <li>● <b>Immediately Effect:</b> After the configurations are completed, the related hosts are automatically restarted to apply the configurations.</li> </ul>
<b>Server List</b>	
Select Server	Click <b>Select Server</b> and select the server for which you want to configure the BIOS.

3. Click **Config**. A confirmation message box is displayed.
4. Click **Submit** to deliver the configuration command.



#### Note

- During BIOS configuration, the progress bar is displayed on the page.
- After BIOS configuration is completed, the configuration result is displayed on the page.

### 3.4.4.2 Configuring the BIOS Through a Configuration File

#### Abstract

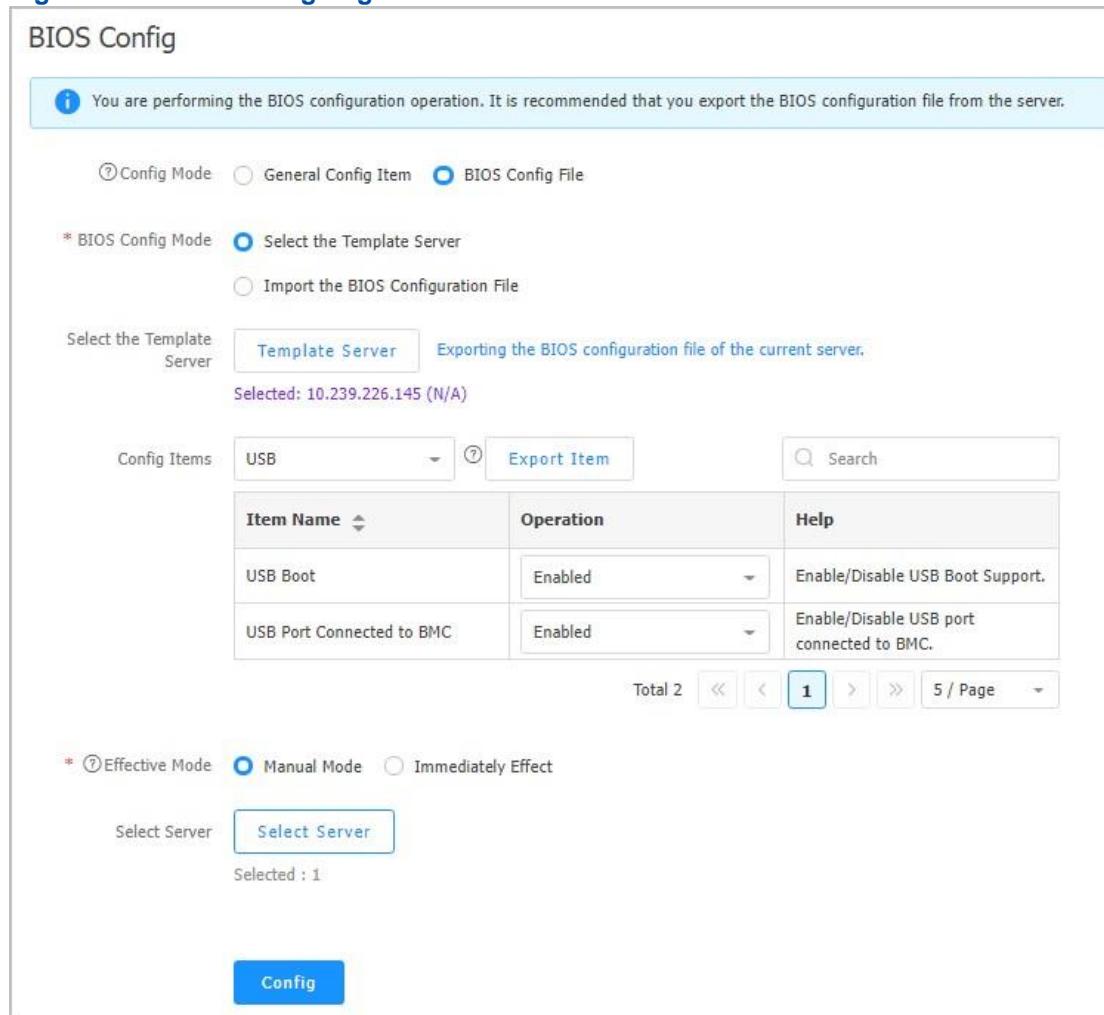
You can use either of the following methods for configuring the **BIOS** through a configuration file:

- **Select the Template Server:** select a server as the template server, export the BIOS configurations from the server, and configure the target server based on the exported BIOS configurations.
- **Import the BIOS Configuration File:** import an edited BIOS configuration file, and configure the target server based on the BIOS configuration file.

#### Steps

- Selecting a Template Server
  1. Select **Device Mgmt > Deployment > BIOS Config**. The **BIOS Config** page is displayed, see [Figure 3-65](#).

Figure 3-65 BIOS Config Page



The screenshot shows the BIOS Config page with the following interface elements:

- Header:** BIOS Config
- Information Bar:** You are performing the BIOS configuration operation. It is recommended that you export the BIOS configuration file from the server.
- Mode Selection:**
  - Config Mode
  - General Config Item
  - BIOS Config File
- BIOS Config Mode:**
  - BIOS Config Mode
  - Select the Template Server
  - Import the BIOS Configuration File
- Select the Template Server:**
  - Template Server (selected): Exporting the BIOS configuration file of the current server.
  - Selected: 10.239.226.145 (N/A)
- Config Items:** USB (selected)
  - Export Item** button
  - Search** input field

Item Name	Operation	Help
USB Boot	Enabled	Enable/Disable USB Boot Support.
USB Port Connected to BMC	Enabled	Enable/Disable USB port connected to BMC.
- Page Navigation:** Total 2, 1, 5 / Page
- Mode Selection:**
  - Effective Mode
  - Manual Mode
  - Immediately Effect
- Select Server:**
  - Select Server (selected)
  - Selected : 1
- Config Button:** A large blue button labeled "Config".

2. Set the parameters. For a description of the parameters, refer to [Table 3-40](#).

Table 3-40 Parameter Descriptions for Selecting a Template Server

Parameter	Description
Config Mode	Select <b>BIOS Config File</b> .
BIOS Config Mode	Select <b>Select the Template Server</b> .
Select the Template Server	Click <b>Template Server</b> , and select a server as the template.
Config Items	After a template server is selected, all the BIOS configuration items are those on the template server. To modify a configuration item, modify it in accordance with the help information in the <b>Help</b> column.
Effective Mode	Select the validation mode. Options: → <b>Manual</b> : After the configurations are completed, you must manually restart the related hosts to apply the configurations.

Parameter	Description
	→ <b>Immediately Effect:</b> After the configurations are completed, the related hosts are automatically restarted to apply the configurations.
Select Server	Click <b>Select Server</b> to select the server for which you want to configure the BIOS.

3. Click **Config**. A confirmation message box is displayed.
4. Click **Submit** to deliver the configuration command.



### Note

→ During BIOS configuration, the progress bar is displayed on the page. → After BIOS configuration is completed, the configuration result is displayed on the page.

- Importing a BIOS Configuration File

1. Select **Device Mgmt > Deployment > BIOS Config**. The **BIOS Config** page is displayed, see [Figure 3-66](#).

**Figure 3-66 BIOS Config Page**

### BIOS Config

i You are performing the BIOS configuration operation. It is recommended that you export the BIOS configuration file from the server.

Config Mode  
  General Config Item  
  BIOS Config File

\* BIOS Config Mode  
  Select the Template Server  
  Import the BIOS Configuration File

BIOS Config File  
 
  
 bios-config-file.xml 33412 B X

Config Items	USB	?	Export Item	Search
Item Name	USB	?	Operation	Help
USB Boot	Enabled		Enable/Disable USB Boot Support.	
USB Port Connected to BMC	Enabled		Enable/Disable USB port connected to BMC.	

Total 2  
 <<  
 <  
 1  
 >  
 >>  
 5 / Page  
 ▼

\*  Effective Mode  
  Manual Mode  
  Immediately Effect

Select Server  
 
  
 Selected : 1

2. Set the parameters. For a description of the parameters, refer to [Table 3-41](#).

**Table 3-41 Parameter Descriptions for Importing a BIOS Configuration File**

Parameter	Description
Config Mode	Select <b>BIOS Config File</b> .
BIOS Config Mode	Select <b>Import the BIOS Configuration File</b> .
BIOS Config File	Click <b>Select File</b> , and select the desired BIOS configuration file.
Config Items	After a BIOS configuration file is selected, each BIOS configuration item is that in the configuration file. To modify a configuration item, modify it in accordance with the help information in the <b>Help</b> column.
Effective Mode	Select the validation mode. Options: → <b>Manual Mode</b> : After the configurations are completed, you must manually restart the related hosts to apply the configurations. → <b>Immediately Effect</b> : After the configurations are completed, the related hosts are automatically restarted to apply the configurations.
Select Server	Click <b>Select Server</b> to select the server for which you want to configure the BIOS.

3. Click **Config**. A confirmation message box is displayed.
4. Click **Submit** to deliver the configuration command.



→ During BIOS configuration, the progress bar is displayed on the page. → After BIOS configuration is completed, the configuration result is displayed on the page.

### 3.4.5 RAID Configuration

You can configure **RAID** parameters in batches for a server through the UniKits.

RAID configuration modes include:

- Out-of-band RAID configuration

For details, refer to "[3.4.5.1 Performing Out-of-Band RAID Configuration](#)".

- In-band RAID configuration

For details, refer to "[3.4.5.2 Performing In-band RAID Configuration](#)".

### 3.4.5.1 Performing Out-of-Band RAID Configuration

#### Abstract

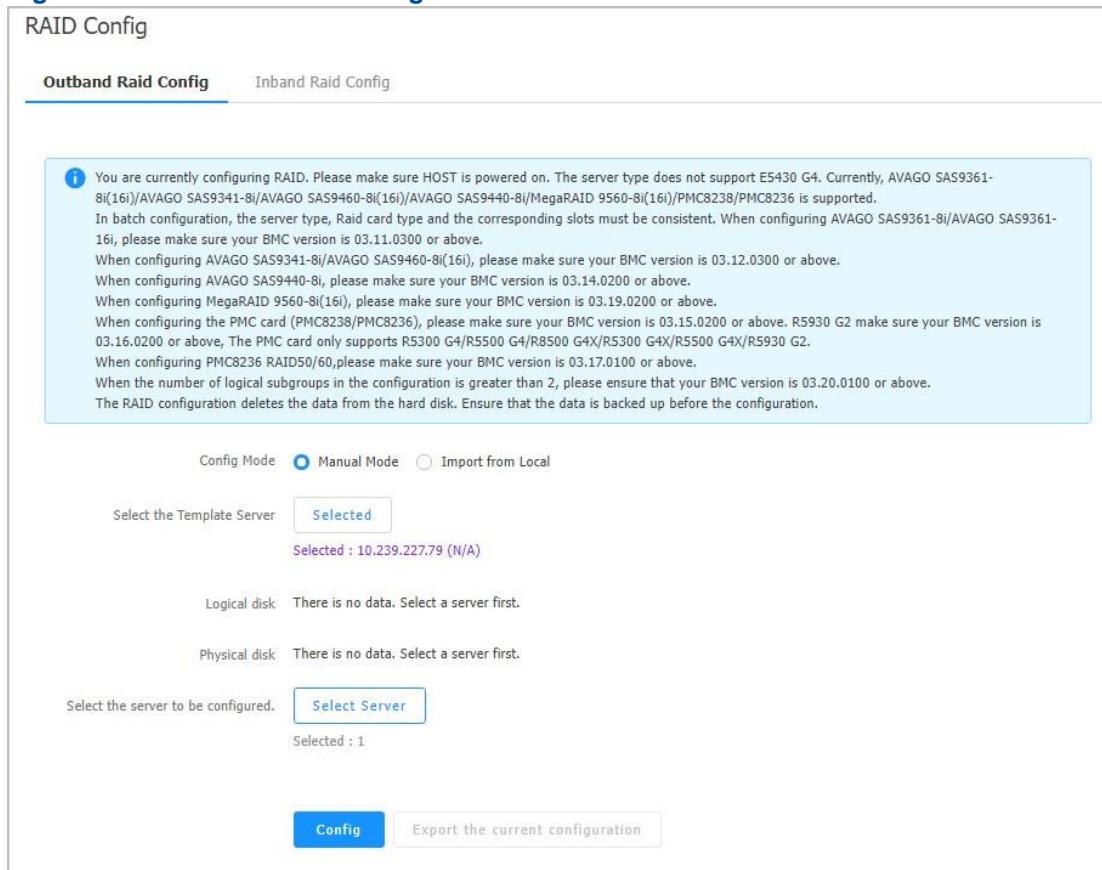
You can use either of the following methods for performing out-of-band **RAID** configuration:

- **Manual Mode:** select a server as the template server, export the RAID configurations from the server, and configure the target server based on the exported RAID configurations.
- **Import from Local:** import an edited RAID configuration file, and configure the target server based on the RAID configuration file.

#### Steps

- Manually Performing Out-of-Band RAID Configuration
  1. Select **Device Mgmt > Deployment > RAID Config**. The **RAID Config** page is displayed.
  2. Click **Outband Raid Config**. The **Outband Raid Config** tab is displayed, see [Figure 3-67](#).

**Figure 3-67 Outband Raid Config Tab—Manual Mode**



RAID Config

**Outband Raid Config** **Inband Raid Config**

**RAID Configuration Requirements:**

**Config Mode:**  **Manual Mode**  **Import from Local**

Select the Template Server: **Selected**  
Selected : 10.239.227.79 (N/A)

Logical disk: There is no data. Select a server first.

Physical disk: There is no data. Select a server first.

Select the server to be configured: **Select Server**  
Selected : 1

**Config** **Export the current configuration**

3. Set the parameters. For a description of the parameters, refer to [Table 3-42](#).

**Table 3-42 Parameter Descriptions for Manually Performing Out-of-Band RAID Configuration**

Parameter	Description
Config Mode	Select <b>Manual Mode</b> .
Parameter	Description
Select the Template Server	Click <b>Select Server</b> , and select a server as the template. After a template server is selected, all the RAID configuration items are those on the template server.
Logical disk	Perform the following operations as required. → To add a logical disk, click <b>Add VD</b> . → To modify a logical disk, click <b>Modify</b> in the <b>Operation</b> column for the logical disk. → To delete a logical disk, click <b>Delete</b> in the <b>Operation</b> column for the logical disk. → To clear a logical disk, click <b>Clear</b> . → To enable forcible reconfiguration, turn on the <b>Forced reconfiguration</b> switch. In this case, the original member disks of the logical disk are deleted and then the logical disk is reconfigured. Each controller corresponds to a <b>Forced reconfiguration</b> switch.
Select the server to be configured	Click <b>Select Server</b> to select the server for which you want to configure RAID.

4. (Optional) To export the configured logical disk information to a configuration file, click **Export the current configuration**.



**Note**

The number of exported configuration files is the same as the number of controllers.

5. Click **Config**. A confirmation message box is displayed.  
6. Click **Submit** to deliver the configuration command.



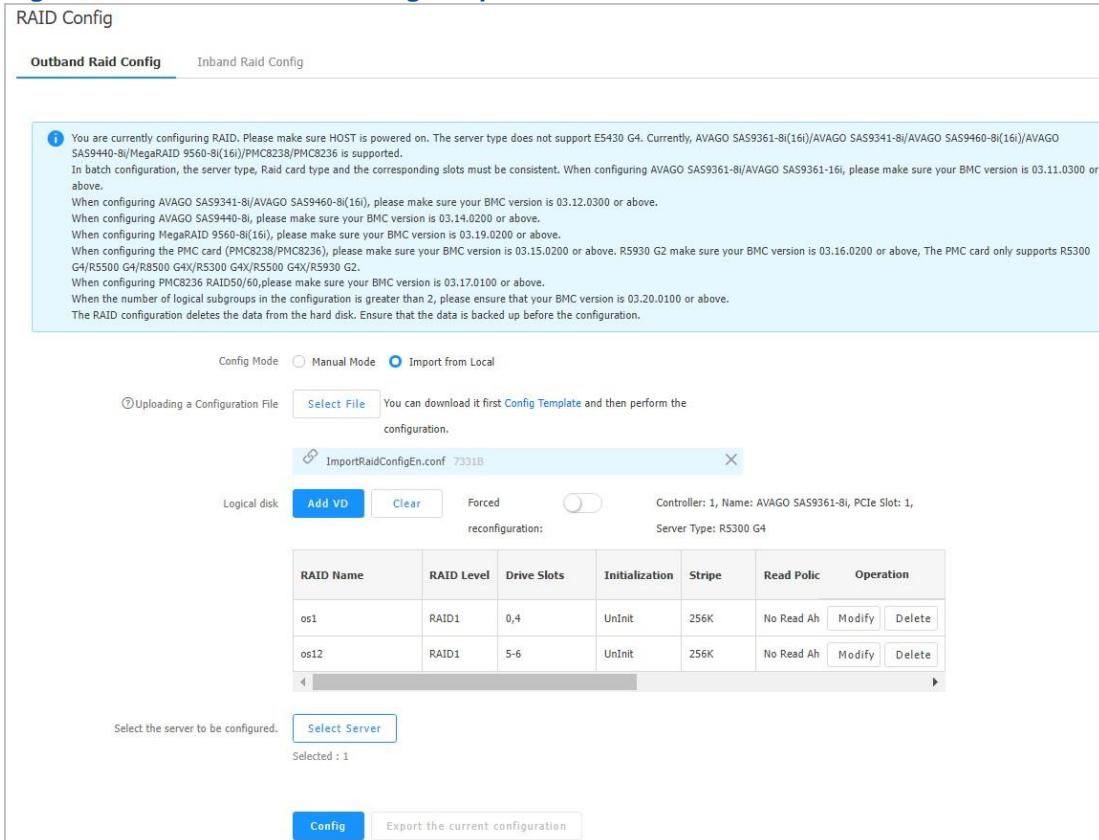
**Note**

→ During RAID configuration, the progress bar is displayed on the page. → After RAID configuration is completed, the configuration result is displayed on the page.

- Importing a Local Configuration File
  1. Select **Device Mgmt > Deployment > RAID Config**. The **RAID Config** page is displayed.

2. Click **Outband Raid Config**. The **Outband Raid Config** tab is displayed, see [Figure 3-68](#).

**Figure 3-68 Outband Raid Config—Import from Local**



3. Set the parameters. For a description of the parameters, refer to [Table 3-42. Table 3-43 Parameter Descriptions for Importing a Local Configuration File](#)

Parameter	Description
Config Mode	Select <b>Import from Local</b> .
Uploading a Configuration File	Click <b>Select File</b> , and select the desired RAID configuration file. After a RAID configuration file is selected, each RAID configuration item is that in the configuration file.

Logical Disk	<p>Perform the following operations as required.</p> <ul style="list-style-type: none"> <li>→ To add a logical disk, click <b>Add VD</b>.</li> <li>→ To modify a logical disk, click <b>Modify</b> in the <b>Operation</b> column for the logical disk. → To delete a logical disk, click <b>Delete</b> in the <b>Operation</b> column for the logical disk.</li> <li>→ To clear a logical disk, click <b>Clear</b>.</li> <li>→ To enable forcible reconfiguration, turn on the <b>Forced reconfiguration</b> switch. In this case, the original member disks of the logical disk are deleted and then the logical disk is reconfigured.</li> </ul> <p>Each controller corresponds to a <b>Forced reconfiguration</b> switch.</p>
Parameter	<b>Description</b>
Select the server to be configured	Click <b>Select Server</b> to select the server for which you want to configure RAID.

4. (Optional) To export the configured logical disk information to a configuration file, click **Export the current configuration**.



The number of exported configuration files is the same as the number of controllers.

5. Click **Config**. A confirmation message box is displayed.  
 6. Click **Submit** to deliver the configuration command.



→ During RAID configuration, the progress bar is displayed on the page. → After RAID configuration is completed, the configuration result is displayed on the page.

### 3.4.5.2 Performing In-band RAID Configuration

#### Abstract

In-band RAID configuration depends on the CIFS file sharing service on the PC (namely, the installation PC) where the UniKits is running. Therefore, you also need to set the sharing service parameters.

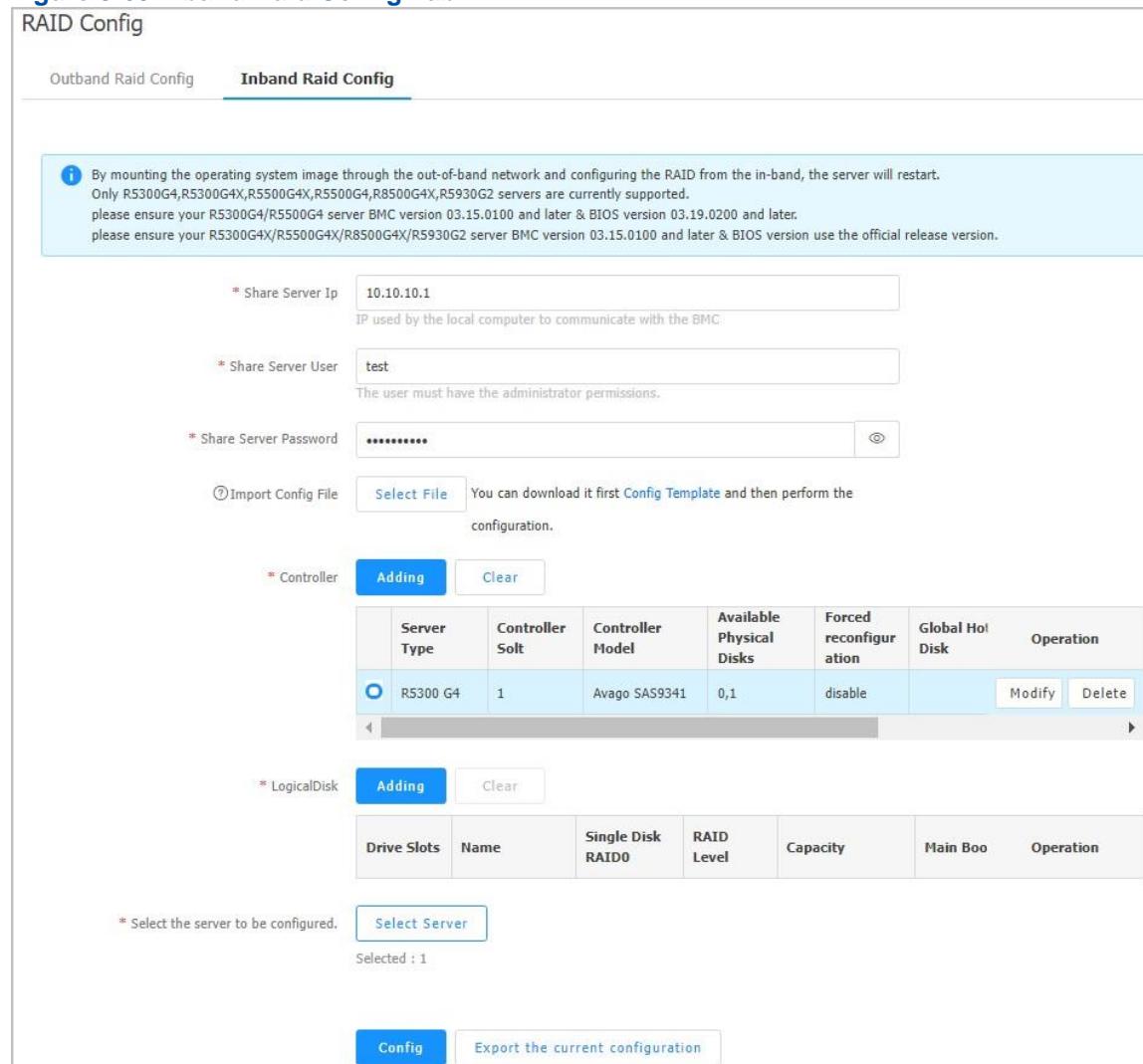
#### Prerequisite

The CIFS sharing function is already enabled on the installation PC. For details, refer to "[5 Reference: Enabling the SMB/CIFS File Sharing Function](#)".

## Steps

1. Select **Device Mgmt > Deployment > RAID Config**. The **RAID Config** page is displayed.
2. Click **Inband Raid Config**. The **Inband Raid Config** tab is displayed, see [Figure 3-69](#).

**Figure 3-69 Inband Raid Config Tab**



RAID Config

**Inband Raid Config**

By mounting the operating system image through the out-of-band network and configuring the RAID from the in-band, the server will restart. Only R5300G4,R5300G4X,R5500G4X,R5500G4,R8500G4X,R5930G2 servers are currently supported. please ensure your R5300G4/R5500G4 server BMC version 03.15.0100 and later & BIOS version 03.19.0200 and later. please ensure your R5300G4X/R5500G4X/R8500G4X/R5930G2 server BMC version 03.15.0100 and later & BIOS version use the official release version.

\* Share Server Ip: 10.10.10.1  
IP used by the local computer to communicate with the BMC

\* Share Server User: test  
The user must have the administrator permissions.

\* Share Server Password: \*\*\*\*\* (eye icon)

Import Config File:  You can download it first [Config Template](#) and then perform the configuration.

\* Controller:

	Server Type	Controller Slot	Controller Model	Available Physical Disks	Forced reconfiguration	Global Hot Disk	Operation
<input checked="" type="radio"/>	R5300 G4	1	Avago SAS9341	0,1	disable	<input type="button" value="Modify"/>	<input type="button" value="Delete"/>

\* LogicalDisk:

Drive Slots	Name	Single Disk RAID0	RAID Level	Capacity	Main Boo	Operation

\* Select the server to be configured.   
Selected : 1

3. Set the parameters. For a description of the parameters, refer to [Table 3-44](#).

**Table 3-44 Parameter Descriptions for Performing In-band RAID Configuration**

Parameter	Description
Share Server Ip	Enter the IP address of the installation PC.
Share Server User	Enter the username (with administrator permissions) of the installation PC.
Share Server Password	Enter the password corresponding to the specified username.

Select the server to be configured	Click <b>Select Server</b> , and select the server for which you want to configure RAID.
4. Use either of the following methods for adding a controller and logical disk.	
<ul style="list-style-type: none"> <li>● Importing a configuration file             <ul style="list-style-type: none"> <li>a. (Optional) If there is no RAID configuration file, click <b>Config Template</b> to download and fill in the configuration template.</li> <li>b. Click <b>Select File</b>, and select the edited RAID configuration file.</li> <li>c. Click <b>Submit</b>.</li> </ul> </li> </ul>	

**Note**

After a RAID configuration file is selected, each RAID configuration item is that in the configuration file.

- Manually adding a controller and logical disk
  - a. Click **Adding** next to **Controller**. The **Controller and Global Configuration Information** dialog box is displayed.
  - b. Enter the controller information and global configuration information.
  - c. Click **Submit**.
  - d. Click **Adding** next to **LogicalDisk**. The **Logical Disk Info** dialog box is displayed.
  - e. Set the parameters of the logical disk.
  - f. Click **Submit**.

**Note**

The above two methods support mixed use.

---

5. (Optional) To export the configured configuration information to a configuration file, click **Export the current configuration**.

---

**Note**

The number of exported configuration files is the same as the number of controllers.

---

6. Click **Config**. A confirmation message box is displayed.

7. Click **Submit** to deliver the configuration command.

---

**Note**

- During RAID configuration, the progress bar is displayed on the page.
- After RAID configuration is completed, the configuration result is displayed on the page.

## 3.4.6 Configuration Check

In the UniKits, you can check the **BMC**, **BIOS**, and **RAID** configurations in batches for a server.

Configuration check involves the following two scenarios:

- General check
  - For details, refer to "[3.4.6.1 Checking General Configurations](#)".
- Customized check
  - For details, refer to "[3.4.6.2 Checking Customized Configurations](#)".



### Note

For a server with BMC V3, both general and customized configurations can be checked. For a server with BMC V4, only general configurations can be checked.

### 3.4.6.1 Checking General Configurations

#### Abstract

By using the general check function, you can check whether the **BMC**, **BIOS**, and **RAID** configurations on a target server are the same as those on a template server or in a check file. You can check general configurations through either of the following ways:

- **Select the Template Server:** select a server as the template server, export the BMC, BIOS, and RAID configurations from the server, and configure the target server based on the exported configurations.
- **Import Check File:** import an edited check file, and configure the target server based on the check file.

#### Steps

- Selecting a Template Server
  1. Select **Device Mgmt > Deployment > Check Configuration**. The **Check Configuration** page is displayed, see [Figure 3-70](#).

### Figure 3-70 Check Configuration Page

Check Configuration

**Check Configuration**

To check the BIOS configuration, ensure that the BIOS configuration has been restarted and takes effect, and the BMC version is 03.07.0100 or above.  
To check the BMC configuration, ensure that the BMC version is 03.16.0300 or above.

**Basic Information**

Configuration Check Scenario  General Check  Customization Check

Config Template Type  Select the Template Server  Import Check File

Select the Template Server  Template Server Exporting the configuration file of the current server: BIOS/BMC/RAID  
Selected: 10.239.226.145 (N/A)

**BIOS Config**

BIOS Configuration Check  Yes  No

BIOS Check Item	USB	Virtual	iSAC	Boot	Memory	Processor	Console	Misc	Power	Security	POST
Item Name	Current Configuration										
USB Boot	Enabled										
USB Port Connected to BMC	Enabled										

**BMC Config**

BMC Config Check  Yes  No

**RAID Config**

RAID Configuration Check  Yes  No

**Confirm Check Item**

Selected Checked Items  Selected Checked Items

**Server List**

Select Server  Select Server  
Selected : 1

**Check** **View Report**

2. Set the parameters. For a description of the parameters, refer to [Table 3-45](#).

**Table 3-45 Parameter Descriptions for Configuration Check Through a Template Server**

Parameter	Description
<b>Basic Information</b>	
Configuration Check Scenario	Select <b>General Check</b> .
Config Template Type	Select <b>Select the Template Server</b> .

Select the Template Server	Select a template server that is used as the check criteria. To do this, perform the following operations:
----------------------------	--

Parameter	Description
	<ol style="list-style-type: none"> <li>Click <b>Template Server</b>. The <b>Select the exported configuration</b> dialog box is displayed.</li> <li>Select the configurations to be exported, including <b>BIOS Config</b>, <b>BMC Config</b>, and <b>RAID Config</b>.</li> <li>Click <b>Next Step</b>. The <b>Select Server</b> dialog box is displayed.</li> <li>Select a server as the template server, and click <b>Export</b>. After <b>Export</b> is clicked, the configuration parameters of the current server are obtained from the template server.</li> </ol> <p>After the configurations of the template server are successfully exported, the <b>Exporting the configuration file of the current server: BIOS/BMC/RAID</b> button is activated. To export the configurations from the template server to a local *.json file, click <b>Exporting the configuration file of the current server: BIOS/BMC/RAID</b>.</p>
<b>BIOS Config</b>	
BIOS Configuration Check	Select whether to check BIOS configurations.
BIOS Check Item	<ul style="list-style-type: none"> <li>→ If <b>BIOS Configuration Check</b> is set to <b>Yes</b>, the current BIOS configurations on the template server are displayed.</li> <li>→ If <b>BIOS Configuration Check</b> is set to <b>No</b>, this parameter is not displayed.</li> </ul>
<b>BMC Config</b>	
BMC Config Check	Select whether to check BMC configurations.
BMC Check Item	<ul style="list-style-type: none"> <li>→ If <b>BMC Config Check</b> is set to <b>Yes</b>, the current BMC configurations on the template server are displayed.</li> <li>→ If <b>BMC Config Check</b> is set to <b>No</b>, this parameter is not displayed.</li> </ul>
<b>RAID Config</b>	
RAID Configuration Check	Select whether to check RAID configurations.
RAID Check Item	<ul style="list-style-type: none"> <li>→ If <b>RAID Configuration Check</b> is set to <b>Yes</b>, the current RAID configurations on the template server are displayed.</li> <li>→ If <b>RAID Configuration Check</b> is set to <b>No</b>, this parameter is not displayed.</li> </ul>
<b>Confirm Check Item</b>	

Selected Checked Items	Confirm the items to be checked. To do this, perform the following operations: a. Click <b>Selected Checked Items</b> . The <b>Selected Checked Items</b> dialog box is displayed. b. Confirm the items to be checked, and click <b>Submit</b> .
<b>Server List</b>	
<b>Parameter</b>	<b>Description</b>
Select Server	Click <b>Select Server</b> to select the target server whose configurations are to be checked.

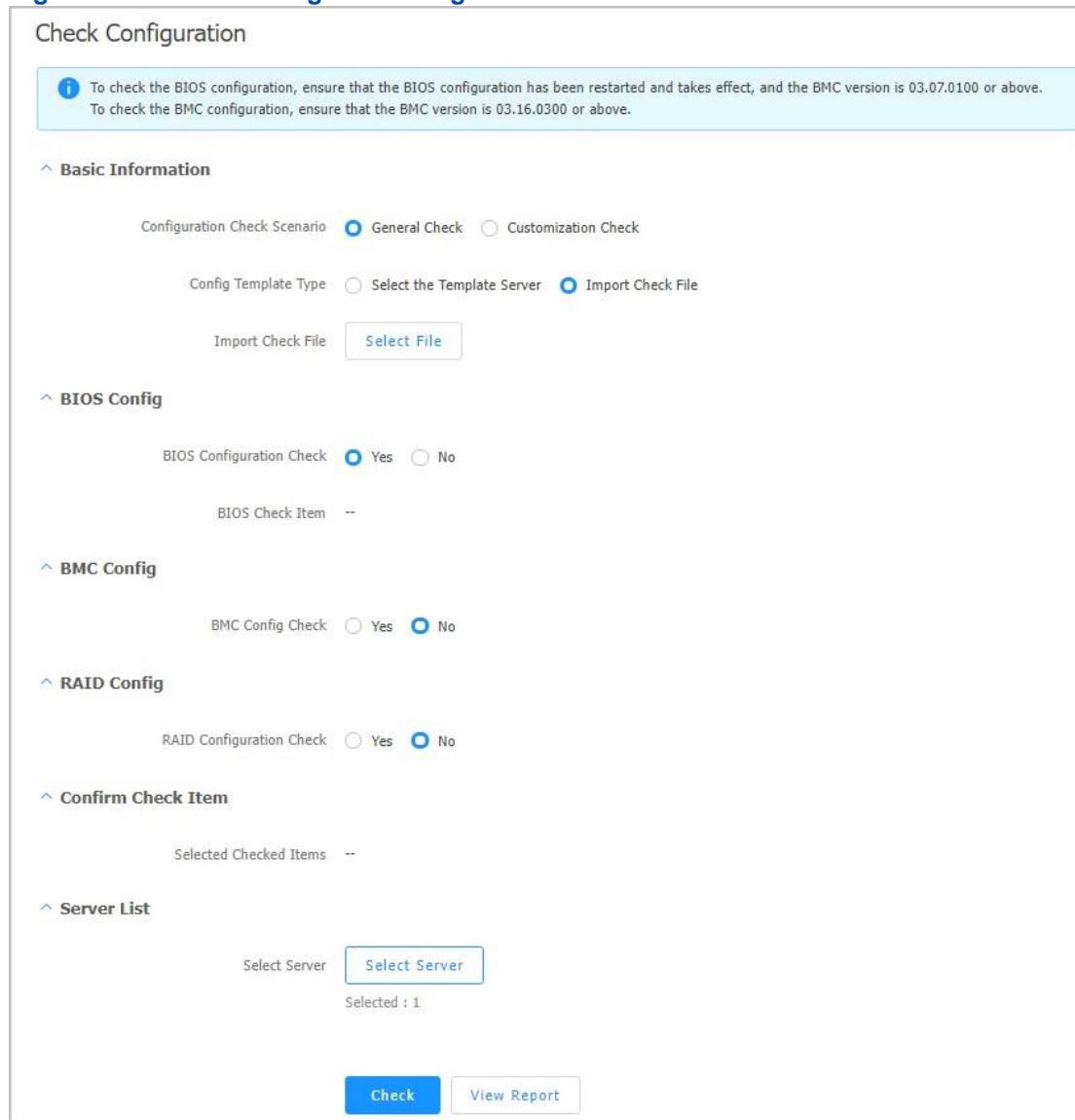
3. Click **Check**.



#### Note

→ During the check, the progress bar is displayed on the page. → After the check is completed, the configuration result is displayed on the page.

- Importing a Check File
  1. Select **Device Mgmt > Deployment > Check Configuration**. The **Check Configuration** page is displayed, see [Figure 3-71](#).

**Figure 3-71 Check Configuration Page**


**Check Configuration**

**1** To check the BIOS configuration, ensure that the BIOS configuration has been restarted and takes effect, and the BMC version is 03.07.0100 or above.  
To check the BMC configuration, ensure that the BMC version is 03.16.0300 or above.

**Basic Information**

Configuration Check Scenario  General Check  Customization Check

Config Template Type  Select the Template Server  Import Check File

Import Check File

**BIOS Config**

BIOS Configuration Check  Yes  No

BIOS Check Item --

**BMC Config**

BMC Config Check  Yes  No

**RAID Config**

RAID Configuration Check  Yes  No

**Confirm Check Item**

Selected Checked Items --

**Server List**

Select Server   
Selected : 1

2. Set the parameters. For a description of the parameters, refer to [Table 3-46](#).

**Table 3-46 Parameter Descriptions for Performing a Configuration Check Based on a Check File**

Parameter	Description
<b>Basic Information</b>	
Configuration Check Scenario	Select <b>General Check</b> .
Config Template Type	Select <b>Import Check File</b> .
Import Check File	Click <b>Select File</b> , and select the desired check file.

BIOS Config	
Parameter	Description
BIOS Configuration Check	Select whether to check BIOS configurations.
BIOS Check Item	<ul style="list-style-type: none"> <li>→ If <b>BIOS Configuration Check</b> is set to <b>Yes</b>, the current BIOS configurations on the template server are displayed.</li> <li>→ If <b>BIOS Configuration Check</b> is set to <b>No</b>, this parameter is not displayed.</li> </ul>
BMC Config	
BMC Config Check	Select whether to check BMC configurations.
BMC Check Item	<ul style="list-style-type: none"> <li>→ If <b>BMC Config Check</b> is set to <b>Yes</b>, the current BMC configurations on the template server are displayed.</li> <li>→ If <b>BMC Config Check</b> is set to <b>No</b>, this parameter is not displayed.</li> </ul>
RAID Config	
RAID Configuration Check	Select whether to check RAID configurations.
RAID Check Item	<ul style="list-style-type: none"> <li>→ If <b>RAID Configuration Check</b> is set to <b>Yes</b>, the current RAID configurations on the template server are displayed.</li> <li>→ If <b>RAID Configuration Check</b> is set to <b>No</b>, this parameter is not displayed.</li> </ul>
Confirm Check Item	
Selected Checked Items	<p>Confirm the items to be checked. To do this, perform the following operations:</p> <ol style="list-style-type: none"> <li>a. Click <b>Selected Checked Items</b>. The <b>Selected Checked Items</b> dialog box is displayed.</li> <li>b. Confirm the items to be checked, and click <b>Submit</b>.</li> </ol>
Server List	
Select Server	Click <b>Select Server</b> to select the target server whose configurations are to be checked.

3. Click **Check**.



→ During the check, the progress bar is displayed on the page. → After the check is completed, the configuration result is displayed on the page.

## Related Tasks

Perform the following operations as required on the check result page.

To...	Do...
Recheck the configurations	<ol style="list-style-type: none"> <li>1. Click <b>ReCheck</b>. A dialog box is displayed.</li> <li>2. Click <b>Submit</b> to return to the <b>Check Configuration</b> page.</li> <li>3. Reconfigure the check parameters.</li> <li>4. Click <b>Check</b>.</li> </ol>
Perform a secondary check	<ol style="list-style-type: none"> <li>1. Select the server for which you want to perform a secondary check.</li> <li>2. Click <b>Second Check</b>.</li> </ol>
Export the check report	Click <b>Exporting Check Summary Result</b> to export the configuration report to a local *.csv file.
Export the details of the comparison between a server and the template server	<ol style="list-style-type: none"> <li>1. Select the server that you want to compare with the template server.</li> <li>2. Click <b>Exporting Check Summary Details</b>.</li> </ol>

### 3.4.6.2 Checking Customized Configurations

#### Abstract

If you only need to check some specific configurations of a server, you can customize a check file.

Through the customization check function, you can check whether the configurations on the target server are the same as those in the customized check file.

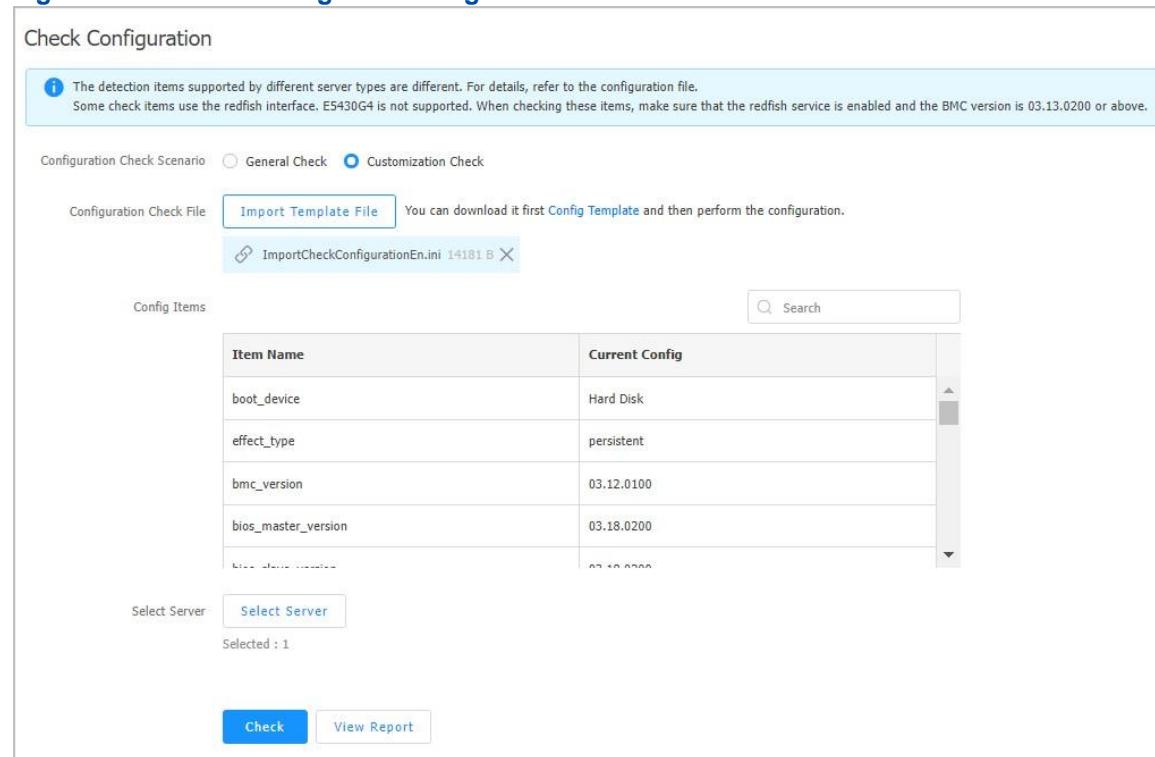


#### Note

You can modify the downloaded template file as required to create a customized check file.

#### Steps

1. Select **Device Mgmt > Deployment > Check Configuration**. The **Check Configuration** page is displayed, see [Figure 3-72](#).

**Figure 3-72 Check Configuration Page**


The detection items supported by different server types are different. For details, refer to the configuration file.

Some check items use the redfish interface. E5430G4 is not supported. When checking these items, make sure that the redfish service is enabled and the BMC version is 03.13.0200 or above.

Configuration Check Scenario  General Check  Customization Check

Configuration Check File  You can download it first [Config Template](#) and then perform the configuration.

Config Items

Item Name	Current Config
boot_device	Hard Disk
effect_type	persistent
bmc_version	03.12.0100
bios_master_version	03.18.0200

Search

2. Set the parameters. For a description of the parameters, refer to [Table 3-47](#).

**Table 3-47 Parameter Descriptions for Performing a Configuration Check Based on a Customized File**

Parameter	Description
Configuration Check Scenario	Select <b>Customization Check</b> .
Configuration Check File	Select a file that is used as the check criteria. To do this, perform the following operations: a. (Optional) If there is no configuration file, click <b>Config Template</b> to download and fill in the configuration template. b. Click <b>Select File</b> , and select the desired check file. c. Click <b>Submit</b> .
Config Items	After the check file is selected, the configuration items in the file are displayed in the configuration item list.
Select Server	Click <b>Select Server</b> to select the target server whose configurations are to be checked.

3. Click **Check**.



- During the check, the progress bar is displayed on the page.

- After the check is completed, the configuration result is displayed on the page.

### Related Tasks

Perform the following operations as required on the check result page.

To...	Do...
Recheck the configurations	<ol style="list-style-type: none"><li>Click <b>ReCheck</b>. A dialog box is displayed.</li><li>Click <b>Submit</b> to return to the <b>Check Configuration</b> tab.</li><li>Reconfigure the check parameters.</li><li>Click <b>Check</b>.</li></ol>
Export the check report	Click the <b>Export Report</b> button to export the configuration report to a local *.csv file.

## 3.4.7 Configuring Commands

### Abstract

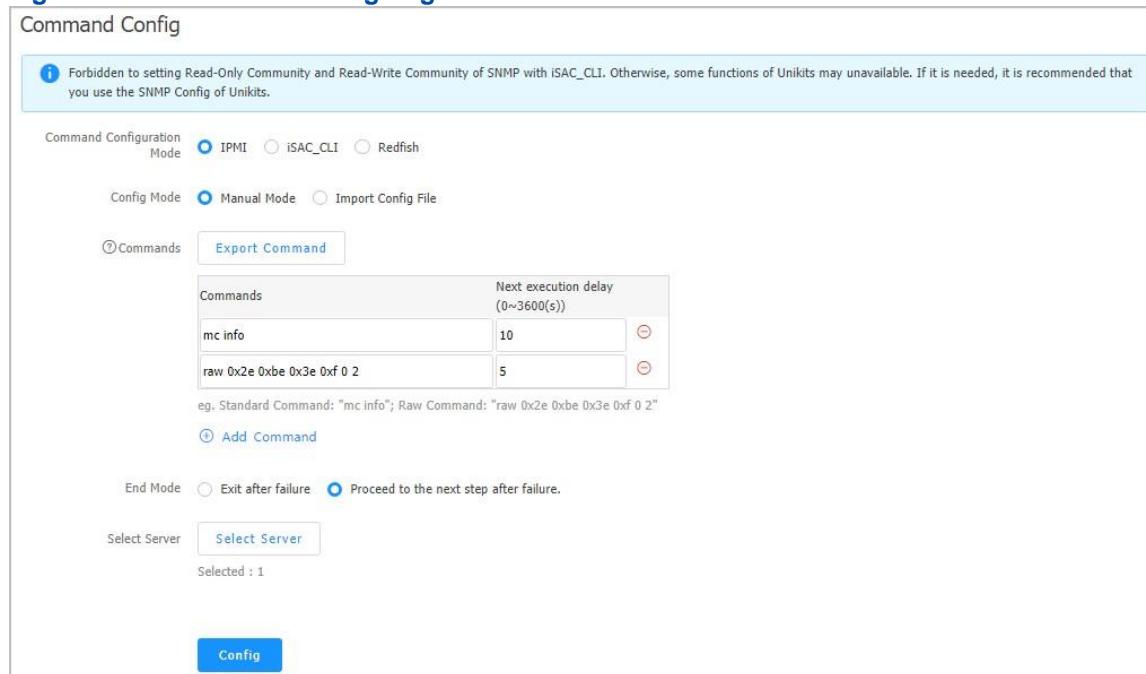
The command configuration function allows you to directly send IPMI commands, iSAC-CLI commands, or Redfish commands to operate a server.



This function does not support interactive commands.

### Steps

- Select **Device Mgmt > Deployment > Command Config**. The **Command Config** page is displayed, as shown in [Figure 3-73](#).

**Figure 3-73 Command Config Page**


The screenshot shows the 'Command Config' page. At the top, a note states: 'Forbidden to setting Read-Only Community and Read-Write Community of SNMP with iSAC\_CLI. Otherwise, some functions of Unikits may unavailable. If it is needed, it is recommended that you use the SNMP Config of Unikits.' Below this, 'Command Configuration Mode' is set to 'IPMI'. Under 'Config Mode', 'Manual Mode' is selected. A table lists commands with their next execution delays:

Commands	Next execution delay (0~3600(s))
mc info	10
raw 0x2e 0xbe 0x3e 0xf 0 2	5

Below the table, a note says: 'eg. Standard Command: "mc info"; Raw Command: "raw 0x2e 0xbe 0x3e 0xf 0 2"'.

Other settings include 'End Mode' (selected: 'Proceed to the next step after failure') and 'Select Server' (selected: 1). A 'Config' button is at the bottom.

2. Set the parameters. For a description of the parameters, refer to [Table 3-48](#).

**Table 3-48 Command Parameter Descriptions**

Parameter	Description
Command Configuration Mode	<p>Select a command type. Options:</p> <ul style="list-style-type: none"> <li><b>IPMI:</b> indicates to execute IPMI commands on a server. IPMI commands support two forms: raw commands and standard commands. It is forbidden to send IPMI commands to modify the <b>SNMP</b> read-only community or read-write community.</li> <li><b>iSAC_CLI:</b> indicates to execute iSAC-CLI commands on a server. It is recommended that you execute iSAC-CLI commands on the servers whose BMC version is 03.14.0200 or later. It is forbidden to send iSAC-CLI commands to modify the SNMP readonly community or read-write community.</li> <li><b>Redfish:</b> indicates to execute Redfish commands on a server. Redfish commands support four request methods: Get, Post, Patch, and Delete.</li> </ul>
Config Mode	<p>Select a command configuration mode. Options:</p> <ul style="list-style-type: none"> <li><b>Manual Mode:</b> A maximum of 10 commands can be configured manually. In this case, you need to set <b>Commands</b> and <b>Next execution delay</b>. For Redfish commands, you also need to set <b>Request Mode</b> and <b>Request Body</b>. The <b>Next execution delay</b> parameter sets the time interval between two commands. It is used to prevent command execution failure be-</li> </ul>

Parameter	Description
	<p>cause two mutually associated commands need to be executed at the specified interval. Range: 0–3600, unit: seconds.</p> <p>The <b>Request Body</b> parameter supports the JSON format only.</p> <ul style="list-style-type: none"> <li>● <b>Import Config File:</b> Commands are imported through a command script file. If there is no command script file, click <b>Config Template</b> to download the template, edit the template, and import it. Click <b>Select File</b>, and select the command configuration file.</li> </ul>
End Mode	<p>Select a command termination mode. Options:</p> <ul style="list-style-type: none"> <li>● <b>Exit after failure:</b> If a command fails to be executed, the command execution process stops immediately and the execution result is returned.</li> <li>● <b>Proceed to the next step after failure:</b> If a command fails to be executed, the command execution process of the next command continues and the execution result is returned after all other commands are executed.</li> </ul> <p>The termination mode is valid for only a single server. For example, when <b>Exit after failure</b> is selected, if a command is configured for multiple servers and fails to be executed on one server, the command execution process stops on that server only and the command execution process on other servers is not affected.</p>
Select Server	Click <b>Select Server</b> , and select the servers to be configured in the displayed dialog box.

3. Click **Config** to deliver the configurations.



- During command configuration, the progress bar is displayed on the page.
- After command configuration is completed, the configuration result is displayed on the page.

### 3.4.8 Controlling Power Supply

#### Abstract

If you are not on the customer site, you can control the power supply of a server through the UniKits as follows:

- Host power-on
- Host power-off
- Host restart
- **BMC** restart



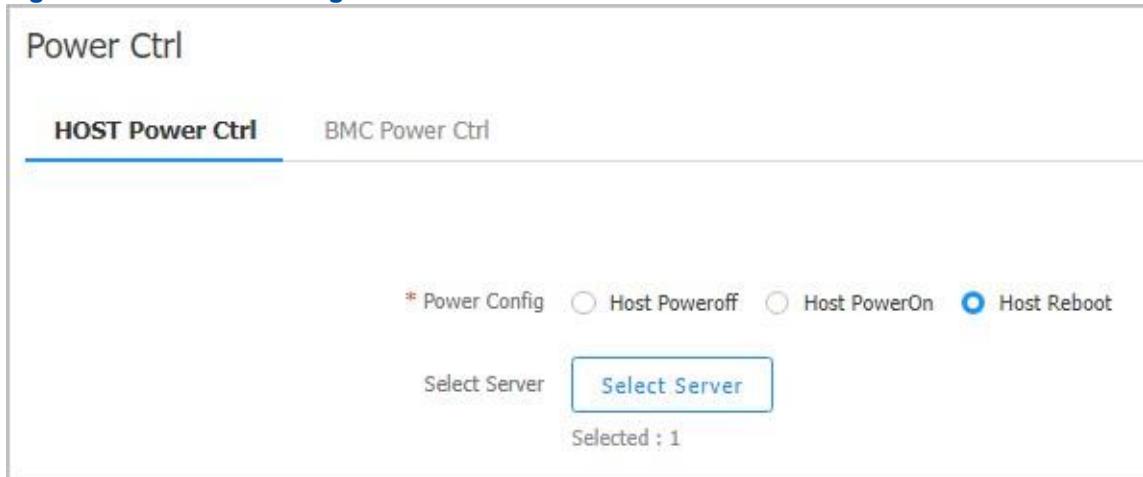
### Notice

After a host is powered off or restarted, services are interrupted and data is lost. Before powering off or restarting a host, you must migrate services and save data.

### Steps

1. Select **Device Mgmt > Deployment > Power Ctrl**. The **Power Ctrl** page is displayed, see [Figure 3-74](#).

**Figure 3-74 Power Ctrl Page**



2. Perform the following operations as required.

To...	Do...
Power off hosts	<ol style="list-style-type: none"> <li>Select <b>Host Poweroff</b>.</li> <li>Click <b>Select Server</b> and select the servers to be powered off.</li> <li>(Optional) If the selected servers are of different models, enter <b>yes</b> in the displayed dialog box and select <b>I have read it and know the influence</b>.</li> <li>Click <b>Config</b>. In the displayed dialog box, enter <b>yes</b> and select <b>I have read it and know the influence</b>.</li> <li>Click <b>Submit</b>.</li> </ol>
Power on hosts	<ol style="list-style-type: none"> <li>Select <b>HOST PowerOn</b>.</li> <li>Click <b>Select Server</b> and select the servers to be powered on.</li> <li>(Optional) If the selected servers are of different models, enter <b>yes</b> in the displayed dialog box and select <b>I have read it and know the influence</b>.</li> <li>Click <b>Config</b>. In the displayed dialog box, click <b>Submit</b>.</li> </ol>

Restart hosts	<ol style="list-style-type: none"> <li>Select <b>Host Reboot</b>.</li> <li>Click <b>Select Server</b> and select the servers to be restarted.</li> </ol>
To...	<b>Do...</b>
	<ol style="list-style-type: none"> <li>(Optional) If the selected servers are of different models, enter <b>yes</b> in the displayed dialog box and select <b>I have read it and know the influence</b>.</li> <li>Click <b>Config</b>. In the displayed dialog box, enter <b>yes</b> and select <b>I have read it and know the influence</b>.</li> <li>Click <b>Submit</b>.</li> </ol>
Restart the BMC	<ol style="list-style-type: none"> <li>Click <b>BMC Power Ctrl</b>. The <b>BMC Power Ctrl</b> tab is displayed.</li> <li>Select <b>BMC Reboot</b>.</li> <li>Click <b>Select Server</b> and select the BMCs to be restarted.</li> <li>(Optional) If the selected BMCs are of different models, enter <b>yes</b> in the displayed dialog box and select <b>I have read it and know the influence</b>.</li> <li>Click <b>Config</b>. In the displayed dialog box, enter <b>yes</b> and select <b>I have read it and know the influence</b>.</li> <li>Click <b>Submit</b>.</li> </ol>



### Note

- During power supply control, the progress bar is displayed on the page.
- After power supply control is completed, the configuration result is displayed on the page.

## Related Tasks

Perform the following operations as required after power supply control is completed.

To...	Do...
View execution results	Click <b>View Report</b> .
Re-execute the configuration operations	Click <b>Reconfiguration</b> , and reselect a configuration parameter to deliver the command.
Re-execute the configuration operation for failed servers only	Click <b>Configures only failed servers</b> to re-deliver the command.
Export the report	Click <b>Export Report</b> . The exported configuration results can be directly opened in a file or saved in <b>*.csv</b> format.

### 3.4.9 Perform PXE-Based Batch Configuration for a Server

#### Abstract

The **PXE**-based batch configuration function enables the local PXE tool to configure parameters for servers in batches.



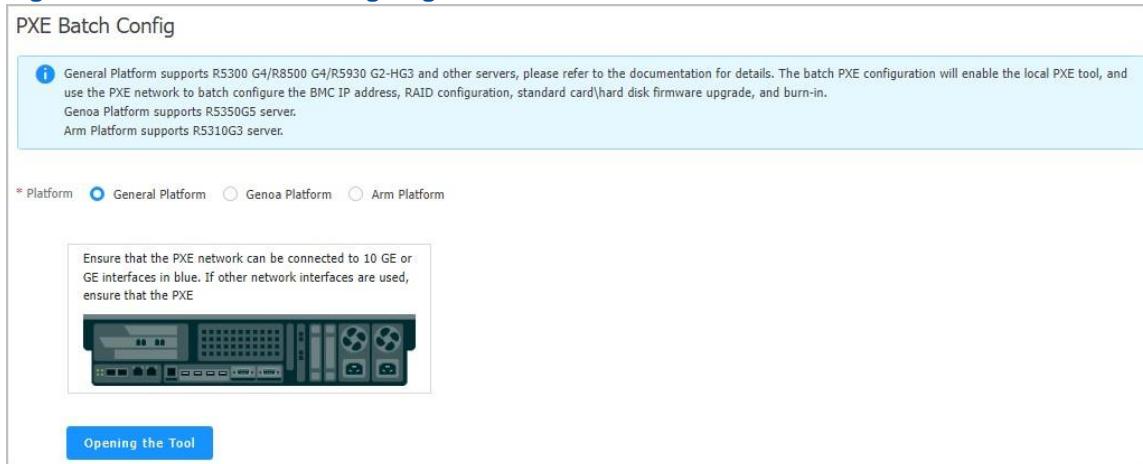
#### Notice

The use of the PXE-based batch configuration function automatically restarts the system, causing service interruption and loss of unsaved data. Therefore, you must save the data before using this function.

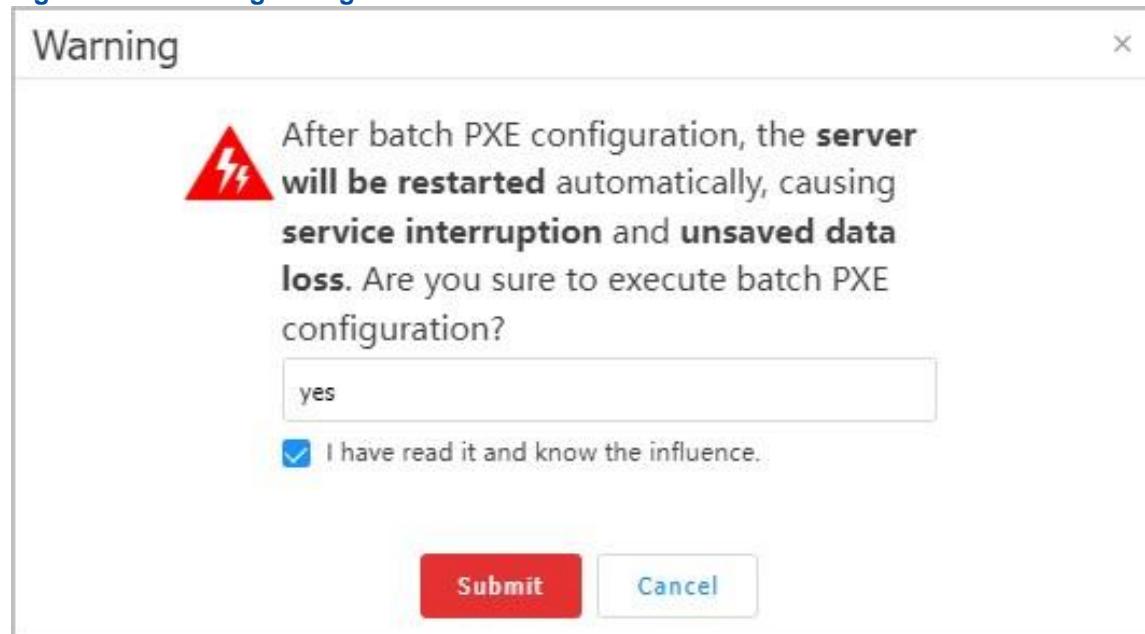
#### Steps

1. Select **Device Mgmt > Deployment > PXE Batch Config**. The **PXE Batch Config** page is displayed, see [Figure 3-75](#).

**Figure 3-75 PXE Batch Config Page**



2. Select the corresponding platform.
  - **General Platform:** Select this option if the server model that you want to configure is NCS6722 N4 (Gen 4)
  - **Genoa Platform:** Select this option if the server model that you want to configure is NCS6722A N4.
  - **Arm Platform:** Select this option if the server model that you want to configure is
3. Click **Open the Tool**. The **Warning** dialog box is displayed, see [Figure 3-76](#).

**Figure 3-76 Warning Dialog Box**

4. Enter **yes** in the text box, and select **I have read it and know the influence**.
5. Click **Submit**. The PXE tool is started.
6. Configure the servers in batches through the PXE tool.

### 3.4.10 OS Installation

OS installation is an advanced function and requires a license. For how to import a license file, refer to "[3.9.4 Importing a License](#)".

#### 3.4.10.1 Installing a Linux OS

##### Abstract

Through the UniKits, you can install a Linux OS for a server. The supported Linux OSs include:

- [RHEL](#) 7.0–7.9 and 8.0–8.5
- [CentOS](#) 8.0–8.5
- [SUSE](#) 15.2–15.4
- [CTYunOS](#)

The supported server models include:

- [NCS6722 N4 \(Gen 4\)](#)
- [NCS6722 N3](#)

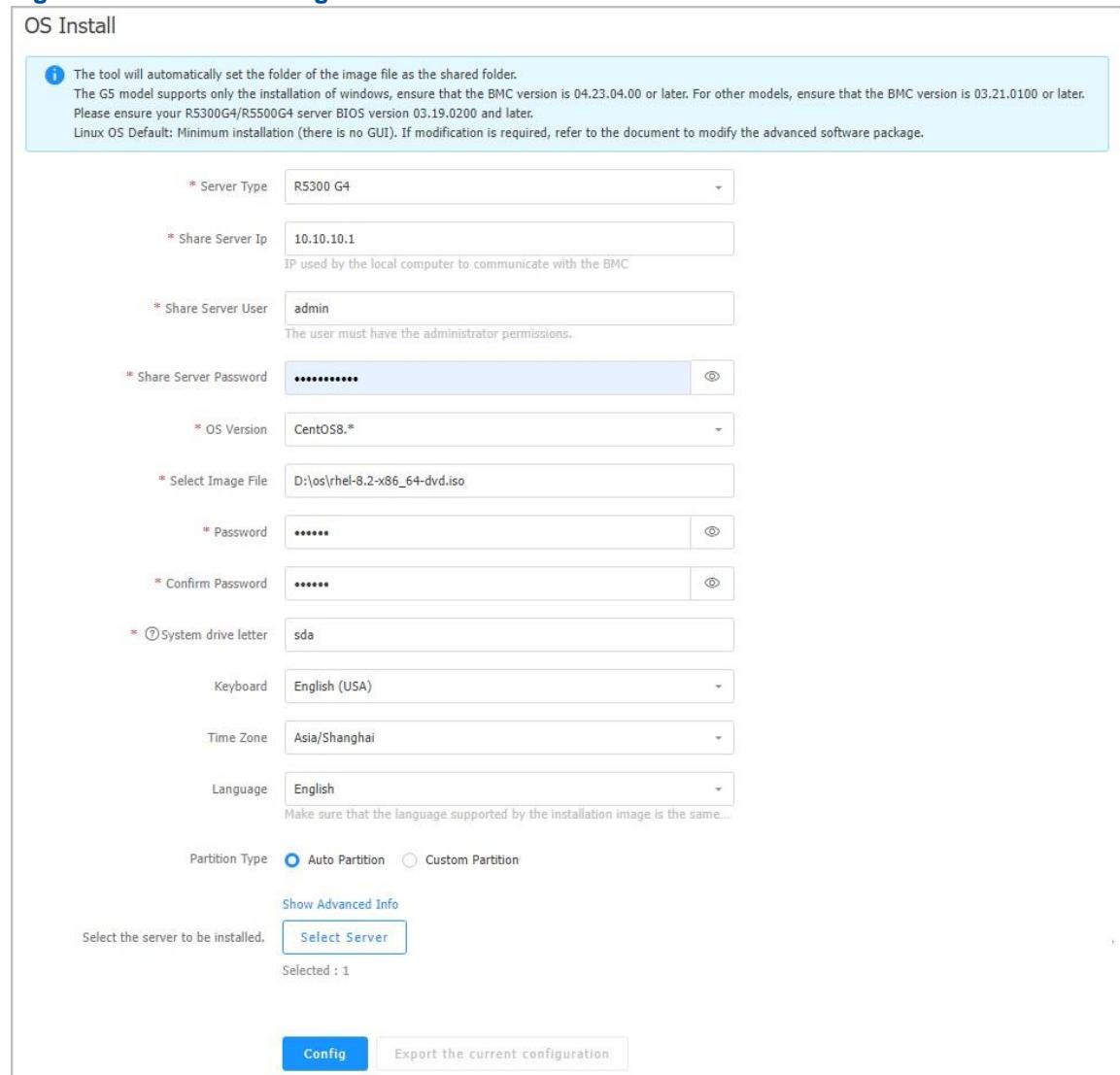
## Prerequisite

- The **SMB/CIFS** sharing function is already enabled on the **PC** (namely, the installation PC) where the UniKits is running. For details, refer to "[5 Reference: Enabling the SMB/CIFS File Sharing Function](#)".
- The ISO file of a Linux OS is already obtained and locally stored on the installation PC.

## Steps

1. Select **Device Mgmt > Deployment > OS Install**. The **OS Install** page is displayed, see [Figure 3-77](#).

**Figure 3-77 OS Install Page**



The screenshot shows the 'OS Install' configuration page. The fields are as follows:

- Server Type:** R5300 G4
- Share Server Ip:** 10.10.10.1 (IP used by the local computer to communicate with the BMC)
- Share Server User:** admin (The user must have the administrator permissions.)
- Share Server Password:** (Redacted)
- OS Version:** CentOS8.\*
- Select Image File:** D:\os\rhel-8.2-x86\_64-dvd.iso
- Password:** (Redacted)
- Confirm Password:** (Redacted)
- System drive letter:** sda
- Keyboard:** English (USA)
- Time Zone:** Asia/Shanghai
- Language:** English (Make sure that the language supported by the installation image is the same...)
- Partition Type:** Auto Partition (selected)
- Show Advanced Info:** (button)
- Select the server to be installed:** (button) Selected : 1
- Config:** (button)
- Export the current configuration:** (button)

2. Set the parameters. For a description of the parameters, refer to [Table 3-49](#).

**Table 3-49 Parameter Descriptions for Installing a Linux OS**

Parameter	Description
Server Type	Select the server model for which you want to install an OS.
Share Server Ip	Enter the IP address of the installation PC.
Share Server User	Enter the username (with administrator permissions) of the installation PC.
Share Server Password	Enter the password corresponding to the specified username.
OS Version	Select the desired OS version.
Select Image File	Enter the path where the OS ISO file is stored on the installation PC.
Password	Enter the password of the root user for logging in to the OS.
Confirm Password	Enter the password of the root user for logging in to the OS.
System drive letter	Enter the system drive letter. Default: <b>sda</b> .
Keyboard	Default: <b>English (USA)</b> .
Time Zone	Select the time zone of the server that the OS is to be installed on.
Language	Select the language of the OS to be installed. It must be the same as the language supported by the OS.
Partition Type	Select a partition type. If you select <b>Custom Partition</b> , click <b>Add Partition</b> to add a partition.
<b>Show Advanced Info</b>	
Kernel parameter	You do not need to set this parameter. If special parameters need to be passed to the kernel during system boot, set this parameter. For example, if you need to forbid the IDE to use the <b>DMA</b> interface, enter <code>ide=nodma</code> .
Installation Mode	Select the OS installation mode.
Module of the software package	This parameter is required when <b>OS Version</b> is set to <b>SUSE15.2-SUSE15.4</b> and <b>Installation Mode</b> is set to <b>Customized Installation</b> . Enter the module where the installation package is located.

Install Software Package	<p>This parameter is required when <b>Installation Mode</b> is set to <b>Customized Installation</b>.</p> <p>Enter the information about the software package that you want to install.</p>
Script After Installation	<ul style="list-style-type: none"> <li>For CentOS or RHEL, this parameter does not need to be set by default.</li> </ul>
<b>Parameter</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>For SUSE, enter the shell script that is automatically executed immediately after the installation is completed.</li> </ul>
Select the server to be installed	Click <b>Select Server</b> to select the servers for which you want to install the OS.

3. Click **Config**. A **Warning** dialog box is displayed.
4. Enter **yes** in the text box, and select **I have read it and know the influence**.
5. Click **Submit** to install the OS.



#### Note

The installation procedure is divided into the following two phases:

- a. Extract the OS ISO file on the installation PC, modify the related file, and compress it into a package.
- b. Deliver the package to the server to install the OS.

The installation duration varies with different OSs. It is estimated that the installation will take 30 to 60 minutes.

### 3.4.10.2 Installing a Windows OS

#### Abstract

Through the UniKits, you can install a Windows OS for a server. The supported Windows OSs include:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

The supported server models include:

- NCS6722 N4 (Gen 4)
- NCS6722 N3
- NCS6722 N4
- NCS6722A N3
- NCS6722A N4

- NCS6742 N4

## Prerequisite

- The [SMB/CIFS](#) sharing function is already enabled on the [PC](#) (namely, the installation PC) where the UniKits is running. For details, refer to "[5 Reference: Enabling the SMB/CIFS File Sharing Function](#)".
- The ISO file of a Windows OS is already obtained and locally stored on the installation PC.

## Steps

1. Select **Device Mgmt > Deployment > OS Install**. The **OS Install** page is displayed, see [Figure 3-78](#).

**Figure 3-78 OS Install Page**

## OS Install

**OS Install**

ⓘ The tool will automatically set the folder of the image file as the shared folder.  
The G5 model supports only the installation of windows, ensure that the BMC version is 04.23.04.00 or later. For other models, ensure that the BMC version is 03.21.0100 or later.  
Please ensure your R5300G4/R5500G4 server BIOS version 03.19.0200 and later.  
Linux OS Default: Minimum installation (there is no GUI). If modification is required, refer to the document to modify the advanced software package.

* Server Type	RS300 G4												
* Share Server Ip	10.10.10.1												
IP used by the local computer to communicate with the BMC													
* Share Server User	admin												
The user must have the administrator permissions.													
* Share Server Password	*****												
* OS Version													
Windows Server 2012r2/2016/2019/2022													
* Select Image File	D:\os\winserver-2016-dvd.iso												
* Password	*****												
* Confirm Password	*****												
* Installation Disk Number	0												
Keyboard	English (USA)												
Time and currency format	English (USA)												
Language	English												
Make sure that the language supported by the installation image is the same...													
* Boot Type	<input checked="" type="radio"/> UEFI <input type="radio"/> Legacy												
Make sure the boot mode of the same batch server is the same													
* Partition	<table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Format</th> <th>Capacity (GB)</th> <th>Label</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td>C</td> <td>P...</td> <td>N...</td> <td>100</td> <td>Windows</td> <td></td> </tr> </tbody> </table>	Name	Type	Format	Capacity (GB)	Label	Delete	C	P...	N...	100	Windows	
Name	Type	Format	Capacity (GB)	Label	Delete								
C	P...	N...	100	Windows									
 Add Partition													
* Installation Mode Index	2												
* Product Key	12345 12345 12345 12345 12345												
Select the server to be installed.	<b>Select Server</b>												
Selected : 1													
<input type="button" value="Config"/> <input type="button" value="Export the current configuration"/>													

2. Set the parameters. For a description of the parameters, refer to [Table 3-50](#).

**Table 3-50 Parameter Descriptions for Installing a Windows OS**

Parameter	Description
Server Type	Select the server model for which you want to install an OS.
Share Server Ip	Enter the IP address of the installation PC.

Parameter	Description
Share Server User	Enter the username (with administrator permissions) of the installation PC.
Share Server Password	Enter the password corresponding to the specified username.
OS Version	Select the desired OS version.
Select Image File	Enter the path where the OS ISO file is stored on the installation PC.
Password	Enter the password of the root user for logging in to the OS.
Confirm Password	Enter the password of the root user for logging in to the OS.
Installation Disk Number	Enter the serial number of the hard disk where the OS is to be installed. Only one serial number can be specified.
Keyboard	Default: <b>English (USA)</b> .
Time and currency format	Select the time and currency format.
Language	Select the language of the OS to be installed. It must be the same as the language supported by the OS.
Boot Type	Select the boot mode of the servers where the OS is to be installed. The boot modes of the servers with an OS installed in the same batch must be the same.
Partition	<p>The C drive with a size of 100 GB is created by default. It is not recommended that you modify parameters other than capacity. The servers where the OS is to be installed have at least the C drive. The UniKits uses it as the OS installation disk.</p> <p>If you need to add a partition, click <b>Add Partition</b>. The total partition size cannot exceed the maximum capacity of the hard disk. The partition size of the C drive used as the OS installation disk must be no less than 32 GB.</p>
Installation Mode Index	The installation mode index is used to customize an installation mode. The value of this parameter needs to be the same as that of <b>IMAGE INDEX</b> in the <i>sources\install.wim\[1].xml</i> file.
Product Key	Enter the product key.
Select the server to be installed	Click <b>Select Server</b> to select the servers for which you want to install the OS.

3. Click **Config**. A **Warning** dialog box is displayed.
4. Enter **yes** in the text box, and select **I have read it and know the influence**.
5. Click **Submit** to install the OS.

---

**Note**

The installation procedure is divided into the following two phases:

- a. Extract the OS ISO file on the installation PC, modify the related file, and compress it into a package.
- b. Deliver the package to the server to install the OS.

---

## 3.5 Firmware Upgrade

### 3.5.1 Upgrading General Firmware

**Abstract**

This procedure describes how to upgrade general firmware to update functions.

The following types of firmware can be upgraded:

- [BMC](#)
- [BIOS](#)
- [EPLD](#)
- [FRU](#)
- [VR](#)

---

**Notice**

The VR can be upgraded from one version to another a maximum of eight times. After that, the storage media inside the VR chip will be damaged, resulting in a function failure. Therefore, you must exercise caution when performing this operation.

---

- Third-party firmware

---

**Note**

The third-party firmware upgrade is supported only in the following three scenarios: → Expander firmware upgrade (of the third-party firmware) is supported only in the scenario where an NCS6722 N4 server is configured with the Expander on the BR2UM backplane and the BMC version is V03.13.0300 or later. → For NEO2 servers with BMC version V04.24.02.00 or later that are equipped with a DH board, the third-party firmware on the DH board can be upgraded. → The firmware of the GPU PCIe switch board can be upgraded on the R6900 G5.

---

- PSU



PSU firmware upgrade is supported on only G5 models.

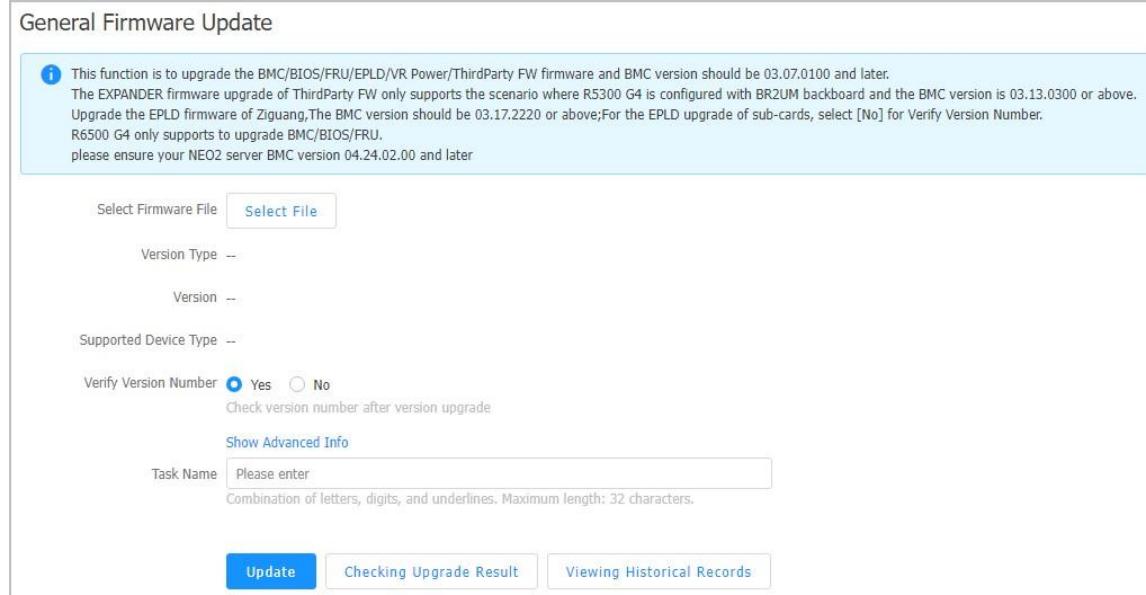
### Prerequisite

The firmware to be upgraded is already obtained.

### Steps

1. Select **Device Mgmt > Firmware Update > General Firmware Update**. The **General Firmware Update** page is displayed, see [Figure 3-79](#).

**Figure 3-79 General Firmware Update Page**



General Firmware Update

This function is to upgrade the BMC/BIOS/FRU/EPLD/VR Power/ThirdParty FW firmware and BMC version should be 03.07.0100 and later. The EXPANDER firmware upgrade of ThirdParty FW only supports the scenario where R5300 G4 is configured with BR2UM backboard and the BMC version is 03.13.0300 or above. Upgrade the EPLD firmware of Ziguang, The BMC version should be 03.17.2220 or above;For the EPLD upgrade of sub-cards, select [No] for Verify Version Number. R6500 G4 only supports to upgrade BMC/BIOS/FRU, please ensure your NEO2 server BMC version 04.24.02.00 and later

Select Firmware File

Version Type --

Version --

Supported Device Type --

Verify Version Number  Yes  No  
Check version number after version upgrade

Show Advanced Info

Task Name   
Combination of letters, digits, and underscores. Maximum length: 32 characters.

2. Click **Select File**, and select the desired firmware upgrade file. The file is selected, see [Figure 3-80](#).

### Figure 3-80 Firmware Upgrade File Selected

General Firmware Update

**ⓘ** This function is to upgrade the BMC/BIOS/FRU/EPLD/VR Power/ThirdParty FW firmware and BMC version should be 03.07.0100 and later. The EXPANDER firmware upgrade of ThirdParty FW only supports the scenario where R5300 G4 is configured with BR2UM backboard and the BMC version is 03.13.0300 or above. Upgrade the EPLD firmware of Ziguang, The BMC version should be 03.17.2220 or above; For the EPLD upgrade of sub-cards, select [No] for Verify Version Number. R6500 G4 only supports to upgrade BMC/BIOS/FRU. please ensure your NEO2 server BMC version 04.24.02.00 and later

Select Firmware File  R5X00G4X\_R53G4X\_BIOS\_X86\_64\_REL\_03\_07\_0300\_202304261440.ubf

Version Type --

Supported Device Type --

Verify Version Number  Yes  No  
Check version number after version upgrade

Show Advanced Info

Task Name   
Combination of letters, digits, and underlines. Maximum length: 32 characters.

3. Click **Upload**. The file is uploaded, see [Figure 3-81](#).

### Figure 3-81 Firmware Upgrade File Uploaded

General Firmware Update

**ⓘ** This function is to upgrade the BMC/BIOS/FRU/EPLD/VR Power/ThirdParty FW firmware and BMC version should be 03.07.0100 and later. The EXPANDER firmware upgrade of ThirdParty FW only supports the scenario where R5300 G4 is configured with BR2UM backboard and the BMC version is 03.13.0300 or above. Upgrade the EPLD firmware of Ziguang, The BMC version should be 03.17.2220 or above; For the EPLD upgrade of sub-cards, select [No] for Verify Version Number. R6500 G4 only supports to upgrade BMC/BIOS/FRU. please ensure your NEO2 server BMC version 04.24.02.00 and later

Select Firmware File  R5X00G4X\_R53G4X\_BIOS\_X86\_64\_REL\_03\_07\_0300\_202304261440.ubf Upload Success

Version Type BIOS

Version 03.07.0300

Supported Device Type R5500 G4X, R5300 G4X

Verify Version Number  Yes  No  
Check version number after version upgrade

Bios FW Update Policy  Default  Master/Slave  
Host power-off status: Active and standby boards are upgraded. Host power-on status:  
Only the standby BIOS are upgraded. You need to log in to the bmc page to validate the configuration.

Update Range  Selected : 2

Show Advanced Info

Task Name   
Combination of letters, digits, and underlines. Maximum length: 32 characters.



The upload result of the upgrade file, the version type, the version number, and the applicable server type are displayed.

---

4. Select whether to check the version number after the upgrade.
  - To check the version number, set **Verify Version Number** to **Yes**.
  - To not check the version number, set **Verify Version Number** to **No**.
5. (Optional) If the BIOS firmware is uploaded, set **Bios FW Update Policy**.
  - If the BIOS firmware is upgraded for a G2, G4, or G4X server model, refer to the BIOS upgrade policy in [Table 3-51](#).

**Table 3-51 BIOS Firmware Upgrade Policy for a G2, G4, or G4X Server Model**

Host Power-on Status	BIOS Upgrade Policy	
-	Default	Upgrade both the active BIOS and the standby BIOS.
Powered off	Upgrade both the active BIOS and the standby BIOS	Upgrade both the active BIOS and the standby BIOS.
Powered on	Upgrade the standby BIOS	a. Power off the host. b. Upgrade both the active BIOS and the standby BIOS. c. Power on the host.

- If the BIOS firmware is upgraded for a G5 server model, refer to the BIOS upgrade policy in [Table 3-52](#).

**Table 3-52 BIOS Firmware Upgrade Policy for a G5 Server Model**

Host Power-on Status	BIOS Upgrade Policy	
-	Default	Upgrade both the active BIOS and the standby BIOS.
Powered off	Upgrade both the active BIOS and the standby BIOS	Not supported.
Powered on	Upgrade the standby BIOS	Not supported.

6. Click **Select Server**, and select the server where firmware upgrade is required.
7. Click **Show Advanced Info**. The advanced information is displayed, see [Figure 3-82](#).

### Figure 3-82 Advanced Information Displayed

General Firmware Update

**Info** This function is to upgrade the BMC/BIOS/FRU/EPLD/VR Power/ThirdParty FW firmware and BMC version should be 03.07.0100 and later. The EXPANDER firmware upgrade of ThirdParty FW only supports the scenario where R5300 G4 is configured with BR2UM backboard and the BMC version is 03.13.0300 or above. Upgrade the EPLD firmware of Ziguang, The BMC version should be 03.17.2220 or above; For the EPLD upgrade of sub-cards, select [No] for Verify Version Number. R6500 G4 only supports to upgrade BMC/BIOS/FRU. please ensure your NEO2 server BMC version 04.24.02.00 and later

Select Firmware File  R5X00G4X\_R53G4X\_BIOS\_X86\_64\_REL\_03\_07\_0300\_202304261440.ubf Upload Success

Version Type BIOS

Version 03.07.0300

Supported Device Type R5500 G4X, R5300 G4X

Verify Version Number  Yes  No  
Check version number after version upgrade

Bios FW Update Policy  Default  Master/Slave  
Host power-off status: Active and standby boards are upgraded. Host power-on status:  
Only the standby BIOS are upgraded. You need to log in to the bmc page to validate the configuration.

Update Range  Selected : 2

[Hide Advanced Info](#)

② Maximum Threads  ② Maximum Retries  Task Name   
Combination of letters, digits, and underscores. Maximum length: 32 characters.

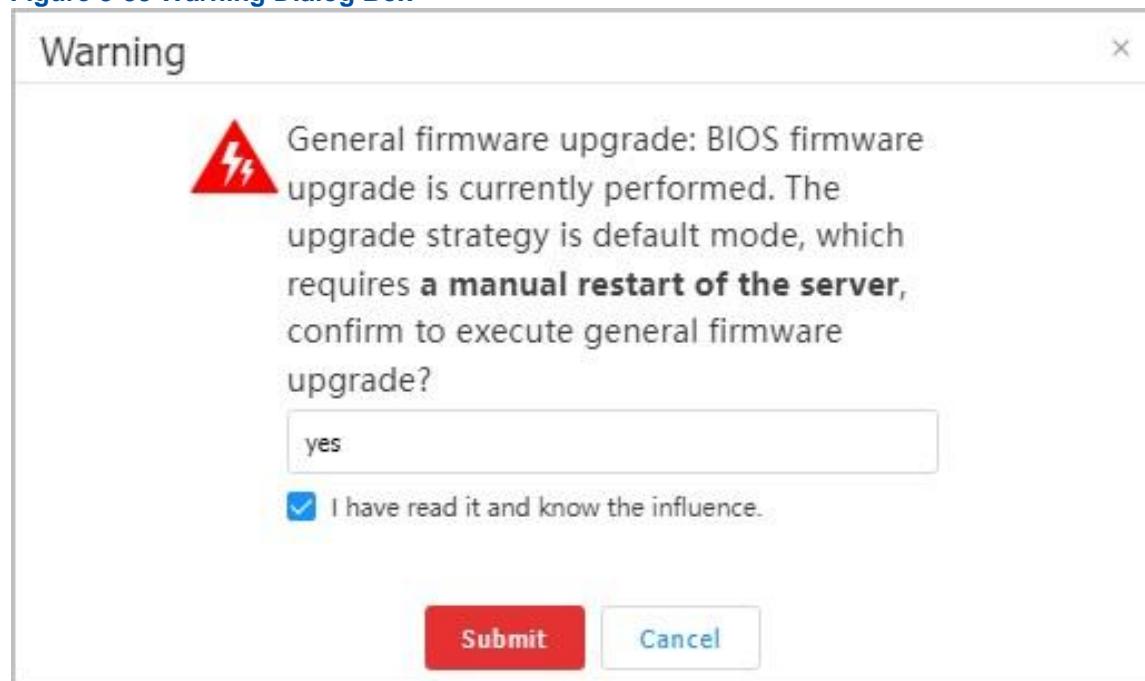
8. Configure upgrade parameters. For a description of the parameters, refer to [Table 3-53](#).

**Table 3-53 Upgrade Parameter Descriptions**

Parameter	Description
Maximum Threads	Enter the maximum number of servers where firmware upgrade is performed in parallel. Range: 1–60, default: 30.
Maximum Retries	Enter the maximum number of times that firmware upgrade of a single server can be retried upon an upgrade failure. Range: 0–10, default: 2. For a VR firmware upgrade, the value is 0 by default.
Task Name	Enter the name of the task which contains no more than 32 characters, including letters, digits, and underscores.

9. Click **Update**. The **Warning** dialog box is displayed, see [Figure 3-83](#).

Figure 3-83 Warning Dialog Box



10. Enter **yes** in the text box, and select **I have read it and know the influence**.

11. Click **Submit** to upgrade the firmware.



### Note

- During the upgrade, the progress bar is displayed on the page.
- After the upgrade is completed, the upgrade result is displayed on the page.

### Related Tasks

Perform the following operations as required on the upgrade result page.

To...	Do...
View the report	Click <b>View Report</b> to view the upgrade result of general firmware.
Reconfigure the parameters for upgrading general firmware	1. Click <b>Reconfiguration</b> . A message box is displayed. 2. Click <b>Submit</b> .
Export the report	Click <b>Export Report</b> to export the upgrade report of the general firmware.

## 3.5.2 Upgrading Standard Cards and Hard Disk Firmware

### Abstract

Standard cards refer to standard **PCIe** cards.

This procedure describes how to upgrade standard cards and hard disk firmware to update functions.

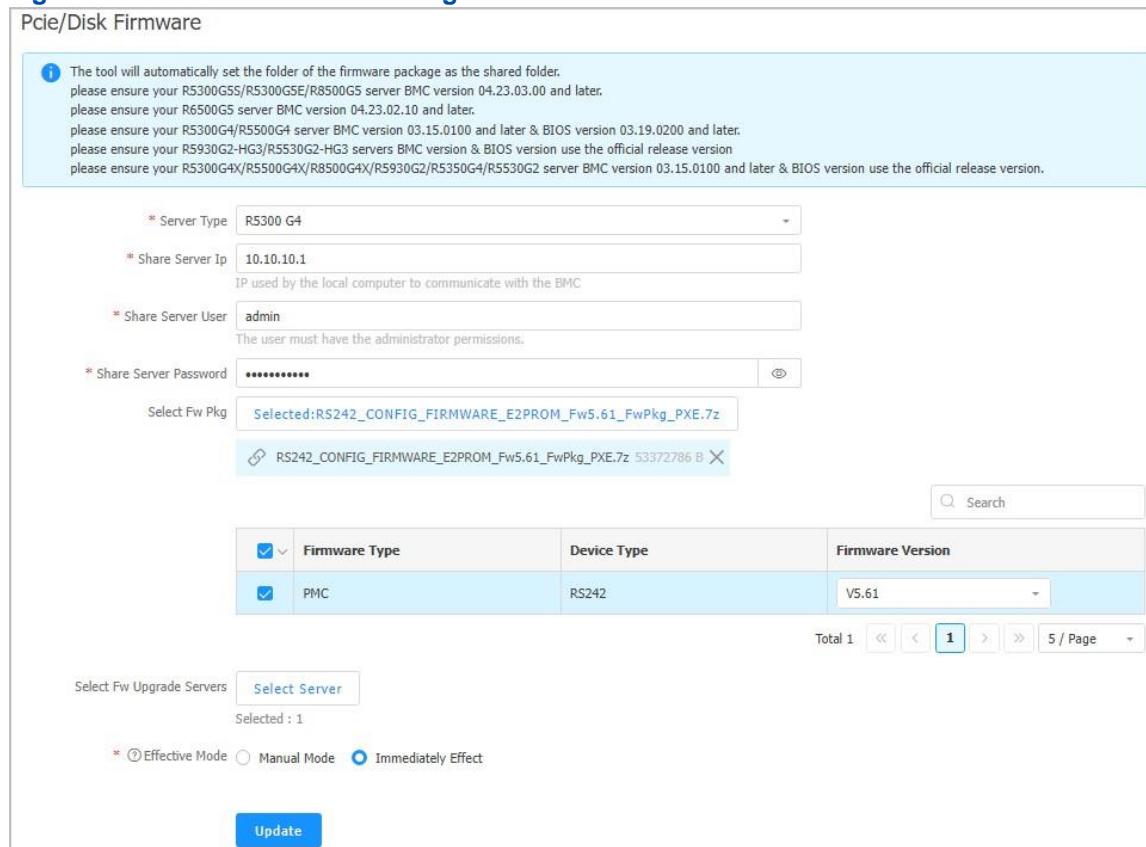
## Prerequisite

- If the **BMC** version of a server whose firmware needs to be upgraded is V3, the **SMB/CIFS** file sharing function needs to be enabled on the **PC** (namely, the installation PC) where the UniKits is running. For details, refer to "[5 Reference: Enabling the SMB/CIFS File Sharing Function](#)".
- The firmware to be upgraded is already obtained.

## Steps

1. Select **Device Mgmt > Firm Update > Pcie/Disk Firmware**. The **Pcie/Disk Firmware** page is displayed, see [Figure 3-84](#).

**Figure 3-84 Pcie/Disk Firmware Page**



The tool will automatically set the folder of the firmware package as the shared folder.  
please ensure your RS300G5/RS300G5E/R8500G5 server BMC version 04.23.03.00 and later.  
please ensure your R6500G5 server BMC version 04.23.02.10 and later.  
please ensure your RS300G4/R5500G4 server BMC version 03.15.0100 and later & BIOS version 03.19.0200 and later.  
please ensure your R5930G2-HG3/R5530G2-HG3 servers BMC version & BIOS version use the official release version  
please ensure your R5300G4X/R5500G4X/R8500G4X/R5930G2/R5350G4/R5530G2 server BMC version 03.15.0100 and later & BIOS version use the official release version.

\* Server Type: RS300 G4  
 \* Share Server Ip: 10.10.10.1  
 \* Share Server User: admin  
 \* Share Server Password:

Select Fw Pkg: Selected:RS242\_CONFIG\_FIRMWARE\_E2PROM\_Fw5.61\_FwPkg\_PXE.7z  
 RS242\_CONFIG\_FIRMWARE\_E2PROM\_Fw5.61\_FwPkg\_PXE.7z 53372786 B

	Firmware Type	Device Type	Firmware Version
<input checked="" type="checkbox"/>	PMC	RS242	V5.61

Total 1    1   5 / Page

Select Fw Upgrade Servers   
 Selected : 1

\*  Effective Mode  Manual Mode  Immediately Effect

2. Set the parameters. For a description of the parameters, refer to [Table 3-54](#).

**Table 3-54 Parameter Descriptions for Upgrading Standard Cards and Hard Disk Firmware**

Parameter	Description
Server Type	Select the server model for which you want to upgrade firmware.
Share Server Ip	Enter the IP address of the installation PC.

Parameter	Description
Share Server User	This parameter is required if the BMC version of the servers whose firmware needs to be upgraded is V3. Enter the username (with administrator permissions) of the installation PC.
Share Server Password	This parameter is required if the BMC version of the servers whose firmware needs to be upgraded is V3. Enter the password corresponding to the specified username.
Select Fw Pkg	Click <b>Select File</b> , and select the desired firmware file.
Select Fw Upgrade Servers	Click <b>Select Server</b> , and select the servers whose firmware needs to be upgraded.
Effective Mode	Select a validation mode. Options: <ul style="list-style-type: none"><li>● <b>Manual Mode:</b> After the configurations are completed, you must manually restart the related hosts to apply the configurations.</li><li>● <b>Immediately Effect:</b> After the configurations are completed, the related hosts are automatically restarted to apply the configurations.</li></ul>

3. Click **Update**. The **Warning** dialog box is displayed.
4. Enter **yes** in the text box, and select **I have read it and know the influence**.
5. Click **Submit** to upgrade the firmware.



#### Note

- During the upgrade, the progress bar is displayed on the page.
- After the upgrade is completed, the upgrade result is displayed on the page.

## 3.6 Routine Inspection

### 3.6.1 Performing Out-of-Band Inspection

#### Abstract

This procedure describes how to inspect a server through the **iSAC** network port to learn about the **O&M** status of the server.

#### Prerequisite

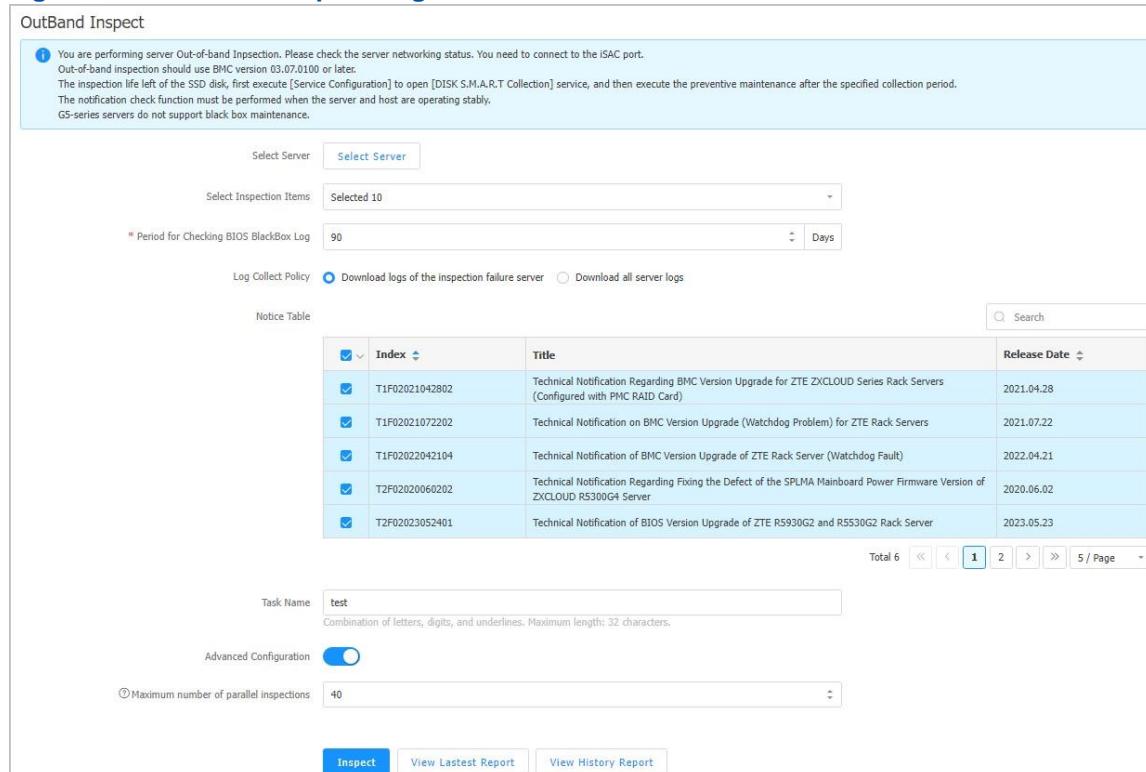
- The network status of the server is proper and the **iSAC** network port is connected.

- If you need to check the remaining service life of Intel SSDs, enable **DISK S.M.A.R.T.Collection**. For details, refer to "[3.4.2.12 Configuring Services](#)".

## Steps

1. Select **Device Mgmt > Inspection > OutBand Inspect**. The **OutBand Inspect** page is displayed, see [Figure 3-85](#).

**Figure 3-85 OutBand Inspect Page**



OutBand Inspect

You are performing server Out-of-band Inspection. Please check the server networking status. You need to connect to the iSAC port. Out-of-band inspection should use BMC version 03.07.0100 or later. The inspection life left of the SSD disk, first execute [Service Configuration] to open [DISK S.M.A.R.T Collection] service, and then execute the preventive maintenance after the specified collection period. The notification check function must be performed when the server and host are operating stably. GS-series servers do not support black box maintenance.

Select Server

Select Inspection Items

\* Period for Checking BIOS BlackBox Log

Log Collect Policy  Download logs of the inspection failure server  Download all server logs

Notice Table

<input checked="" type="checkbox"/> Index	Title	Release Date
<input checked="" type="checkbox"/> T1F02021042802	Technical Notification Regarding BMC Version Upgrade for ZTE ZXCLOUD Series Rack Servers (Configured with PMC RAID Card)	2021.04.28
<input checked="" type="checkbox"/> T1F02021072202	Technical Notification on BMC Version Upgrade (Watchdog Problem) for ZTE Rack Servers	2021.07.22
<input checked="" type="checkbox"/> T1F02022042104	Technical Notification of BMC Version Upgrade of ZTE Rack Server (Watchdog Fault)	2022.04.21
<input checked="" type="checkbox"/> T2F02020060202	Technical Notification Regarding Fixing the Defect of the SPLMA Mainboard Power Firmware Version of ZXCLOUD R5300G4 Server	2020.06.02
<input checked="" type="checkbox"/> T2F02023052401	Technical Notification of BIOS Version Upgrade of ZTE R5930G2 and R5530G2 Rack Server	2023.05.23

Total 6       5 / Page

Task Name  Combination of letters, digits, and underscores. Maximum length: 32 characters.

Advanced Configuration

Maximum number of parallel inspections

2. Set the parameters. For a description of the parameters, refer to [Table 3-55](#).

**Table 3-55 Parameter Descriptions for Out-of-Band Inspection**

Parameter	Description
Select Server	Click <b>Select Server</b> , and select the server that you want to inspect.

Select Inspection Items	<p>Select the desired inspection items.</p> <p>The inspection parameters displayed in the lower part of the page vary with the selected inspection items.</p> <ul style="list-style-type: none"> <li>• If <b>BIOS black box</b> is selected, you need to set <b>Period for Checking BIOS BlackBox Log</b>.</li> <li>• If <b>Asset Inspection</b> is selected, you can set <b>Disk Inspection Threshold</b>. The <b>Disk Inspection Threshold</b> switch can be enabled only after the corresponding license is imported.</li> <li>• If <b>Notice Check</b> is selected, you need to select notices in the <b>Notice Table</b> list to check whether the operations described in the notices are performed on the selected servers.</li> </ul>
<b>Parameter</b>	<b>Description</b>
Period for Checking BIOS BlackBox Log	<p>This parameter is displayed and required when <b>BIOS black box</b> is selected from the <b>Select Inspection Items</b> list.</p> <p>Enter the number of days within which BIOS failure logs to be checked were generated. For example, 90 indicates that the BIOS failure logs generated within the latest 90 days are to be checked.</p>
Log Collect Policy	<p>Select the log collection policy. Options:</p> <ul style="list-style-type: none"> <li>• <b>Download logs of the inspection failure server</b>: downloads log files from only the servers that fail the inspection.</li> <li>• <b>Download all server logs</b>: downloads log files from all the servers involved in the inspection.</li> </ul>
Notice Table	<p>This parameter is displayed and required when <b>Notice Check</b> is selected from the <b>Select Inspection Items</b> list.</p> <p>Select the desired notices from the list.</p>
Task Name	Enter the name of the inspection task.
Maximum number of parallel inspections	<p>Click the <b>Advanced Configuration</b> toggle button to enable this parameter.</p> <p>Set <b>Maximum number of parallel inspections</b>. Range: 30–60. Default: 40.</p> <p>It is recommended that you set this parameter in accordance with the number of CPU cores of a PC. If this parameter is set too high, the performance of the PC may be affected.</p>

3. Click **Inspect** to perform out-of-band inspection.



#### Note

- During the inspection, the progress bar is displayed on the page.
- After the inspection is completed, the inspection result is displayed on the page.

## Related Tasks

Perform the following operations as required on the inspection result page.

To...	Do...
View the detailed information	Click <b>Show Detail</b> . The detailed information about the out-of-band inspection is displayed.
Perform inspection again	<ol style="list-style-type: none"> <li>1. Click <b>Re-Inspection</b> to return to the <b>OutBand Inspect</b> page.</li> <li>2. Set the out-of-band inspection parameters again.</li> <li>3. Click <b>Inspect</b>.</li> </ol>
To...	Do...
View alarms	<ol style="list-style-type: none"> <li>1.  Click <b>Details</b> in the <b>Details</b> column. The alarm causes and handling suggestions of the corresponding alarm are displayed.</li> <li>2. (Optional) Click <b>OutBand Inspect . Detailed Inspection</b> in the upper left corner to return to the out-of-band inspection result page.</li> </ol>

## 3.6.2 Performing In-Band Inspection

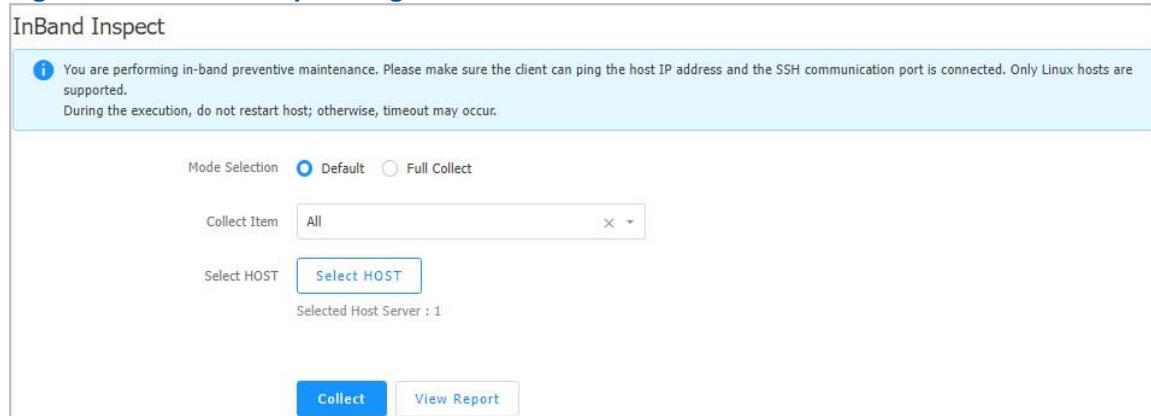
### Abstract

This procedure describes how to inspect a server through the service network port to learn about the **O&M** status of the server.

### Steps

1. Select **Device Mgmt > Inspection > InBand Inspect**. The **InBand Inspect** page is displayed, see [Figure 3-86](#).

**Figure 3-86 InBand Inspect Page**



2. Set the parameters. For a description of the parameters, refer to [Table 3-56](#).

**Table 3-56 Parameter Descriptions for Performing In-Band Inspection**

Parameter	Description
Mode Selection	Select the collection mode. Options: <ul style="list-style-type: none"> <li>● <b>Default:</b> collects the information of the specified modules. The collected information does not include large files and files that are time-consuming to be collected.</li> <li>● <b>Full Collect:</b> collects the information of the specified modules. The collected information includes large files and files that are time-consuming to be collected.</li> </ul>
Collect Item	Select the modules that you want to collect information from. There are a total of ten modules, all of which are selected by default.
Parameter	Description
Select HOST	Click <b>Select HOST</b> to select the host for which you want to perform inband inspection.

3. Click **Collect** to perform in-band inspection.

**Note**

- During the inspection, the progress bar is displayed on the page.
- After the inspection is completed, the inspection result is displayed on the page.

**Related Tasks**

Perform the following operations as required on the inspection result page.

To...	Do...
Recollect data	1. Re-select the server that you want to collect information from. 2. Click <b>Re-Collection</b> to return to the <b>InBand Inspect</b> page. 3. Set the in-band inspection parameters again. 4. Click <b>Collect</b> .
Export logs	1. Select the servers for which the collected logs need to be exported. 2. Click <b>Export Log</b> .
Perform a secondary collection	1. Select the server for a secondary collection. 2. Click <b>Second Collect</b> .

### 3.6.3 Collecting Asset Information

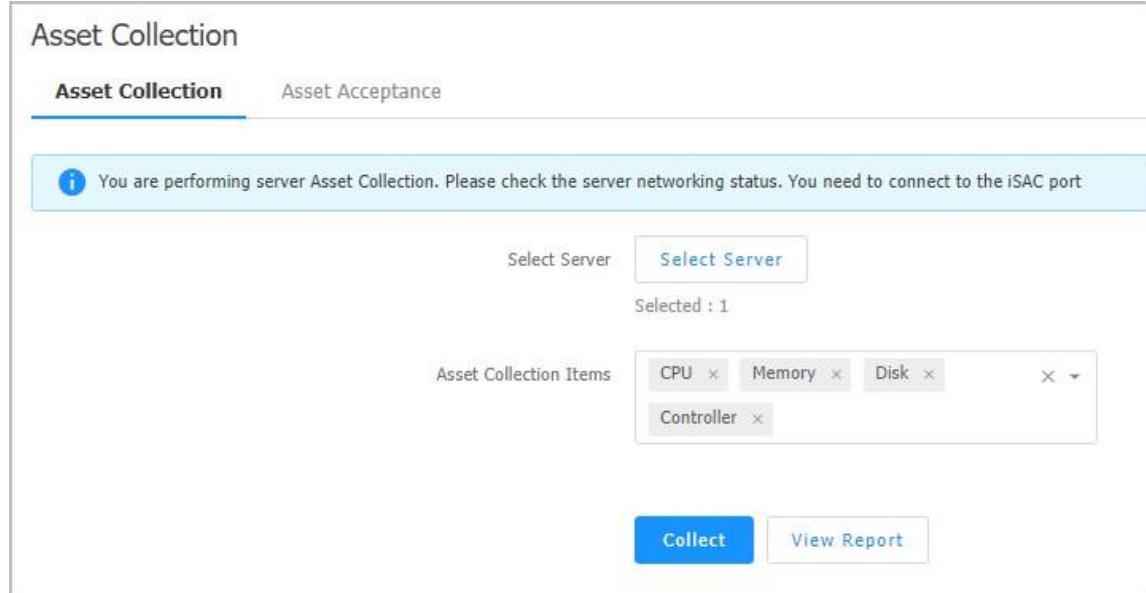
#### Abstract

This procedure describes how to collect asset information to learn more about each component of the server.

#### Steps

1. Select **Device Mgmt > Inspection > Asset Collection**. The **Asset Collection** page is displayed, see [Figure 3-87](#).

**Figure 3-87 Asset Collection Page**



2. Set the parameters. For a description of the parameters, refer to [Table 3-57](#).

**Table 3-57 Asset Collection Parameter Descriptions**

Parameter	Description
Select Server	Click <b>Select Server</b> , and select the server whose asset information is to be collected.
Asset Collection Items	Select the components whose asset information is to be collected. The G5 server model does not support fan information collection.

3. Click **Collect**. In the displayed message box, click **Submit** to collect asset information.



#### Note

- During the collection, the progress bar is displayed on the page.
- After the collection is completed, the inspection result is displayed on the page.

### 3.6.4 Asset Information Acceptance

In the UniKits, you can perform asset information acceptance for servers in batches.

You can perform asset information acceptance in the following ways:

- Performing asset information acceptance through a template server
  - For details, refer to "[3.6.4.1 Performing Asset Acceptance Through a Template Server](#)".
- Performing asset information acceptance through a configuration file
  - For details, refer to "[3.6.4.2 Performing Asset Acceptance Through a Check File](#)".

#### 3.6.4.1 Performing Asset Acceptance Through a Template Server

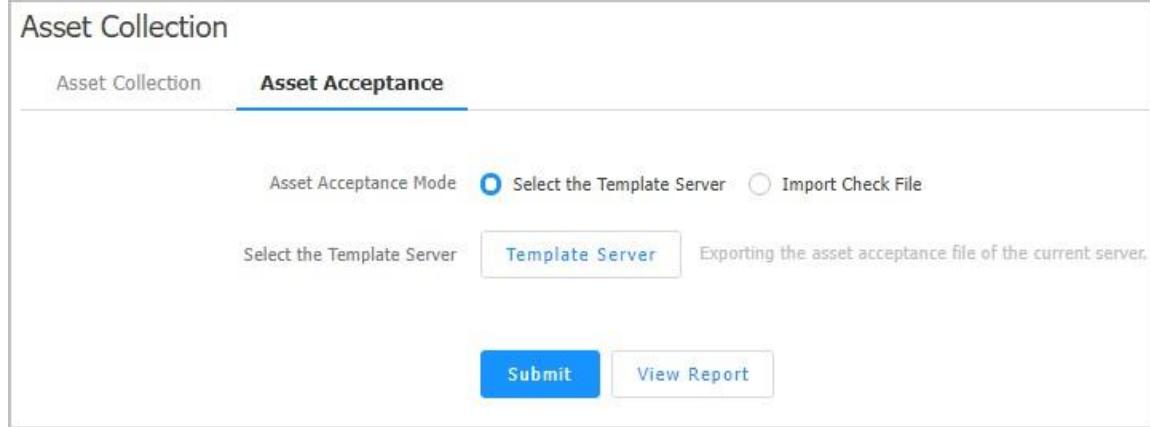
##### Abstract

A server is used as the template server to check whether the asset information on the target server of the same model matches that on the template server.

##### Steps

1. Select **Device Mgmt > Inspection > Asset Collection**. The **Asset Collection** page is displayed.
2. Click **Asset Acceptance**. The **Asset Acceptance** tab is displayed, see [Figure 3-88](#).

**Figure 3-88 Asset Acceptance Tab**



The screenshot shows the 'Asset Collection' page with the 'Asset Acceptance' tab selected. At the top, there are two radio buttons for 'Asset Acceptance Mode': 'Select the Template Server' (which is selected) and 'Import Check File'. Below these buttons is a button labeled 'Template Server'. At the bottom of the page are two buttons: 'Submit' and 'View Report'.

3. Set **Asset Acceptance Mode** to **Select the Template Server**.
4. Click **Template Server**, and select a template server in the displayed dialog box.
5. Click **Export**. The asset acceptance parameters of the template server are exported, see [Figure 3-89](#) and [Figure 3-90](#).

**Figure 3-89 Viewing Asset Acceptance Parameters—1**

Asset Collection

Asset Collection		Asset Acceptance															
Asset Acceptance Mode <input checked="" type="radio"/> Select the Template Server <input type="radio"/> Import Check File Select the Template Server <a href="#">Template Server</a> Exporting the asset acceptance file of the current server.																	
IP/ProductModel 10.239.226.145/R5300 G4																	
Version	<input checked="" type="checkbox"/> <table border="1"> <thead> <tr> <th>BMC Version</th> <th>BIOS Version</th> </tr> </thead> <tbody> <tr> <td>03.20.0200</td> <td>N/A</td> </tr> </tbody> </table>			BMC Version	BIOS Version	03.20.0200	N/A										
BMC Version	BIOS Version																
03.20.0200	N/A																
CPU	<input checked="" type="checkbox"/> <table border="1"> <thead> <tr> <th>Manufacture</th> <th>Model</th> <th>Count</th> </tr> </thead> </table>			Manufacture	Model	Count											
Manufacture	Model	Count															
Memory	<input checked="" type="checkbox"/> <table border="1"> <thead> <tr> <th>Manufacture</th> <th>Type</th> <th>Frequency(MHz)</th> <th>Capacity(GB)</th> <th>Count</th> </tr> </thead> </table>			Manufacture	Type	Frequency(MHz)	Capacity(GB)	Count									
Manufacture	Type	Frequency(MHz)	Capacity(GB)	Count													
Physical Disk	<input checked="" type="checkbox"/> <table border="1"> <thead> <tr> <th>Manufacture</th> <th>Media Type</th> <th>Capacity(GB)</th> <th>Count</th> </tr> </thead> </table>			Manufacture	Media Type	Capacity(GB)	Count										
Manufacture	Media Type	Capacity(GB)	Count														
Nic	<input checked="" type="checkbox"/> <table border="1"> <thead> <tr> <th>CardManufacture</th> <th>CardName</th> <th>InterfaceModel</th> <th>ChipManufacture</th> <th>ChipModel</th> <th>Firmware Version</th> <th>Count</th> </tr> </thead> <tbody> <tr> <td>ZTE</td> <td>SXGFA</td> <td>2*10GE+2*GE</td> <td>Intel</td> <td>X722</td> <td>4.3</td> <td>1</td> </tr> </tbody> </table>			CardManufacture	CardName	InterfaceModel	ChipManufacture	ChipModel	Firmware Version	Count	ZTE	SXGFA	2*10GE+2*GE	Intel	X722	4.3	1
CardManufacture	CardName	InterfaceModel	ChipManufacture	ChipModel	Firmware Version	Count											
ZTE	SXGFA	2*10GE+2*GE	Intel	X722	4.3	1											

**Figure 3-90 Viewing Asset Acceptance Parameters—2**

Nic	<input checked="" type="checkbox"/> <table border="1"> <thead> <tr> <th>CardManufacture</th> <th>CardName</th> <th>InterfaceModel</th> <th>ChipManufacture</th> <th>ChipModel</th> <th>Firmware Version</th> <th>Count</th> </tr> </thead> <tbody> <tr> <td>ZTE</td> <td>SXGFA</td> <td>2*10GE+2*GE</td> <td>Intel</td> <td>X722</td> <td>4.3</td> <td>1</td> </tr> </tbody> </table>							CardManufacture	CardName	InterfaceModel	ChipManufacture	ChipModel	Firmware Version	Count	ZTE	SXGFA	2*10GE+2*GE	Intel	X722	4.3	1
CardManufacture	CardName	InterfaceModel	ChipManufacture	ChipModel	Firmware Version	Count															
ZTE	SXGFA	2*10GE+2*GE	Intel	X722	4.3	1															
FC	<input checked="" type="checkbox"/> <table border="1"> <thead> <tr> <th>CardManufacture</th> <th>CardName</th> <th>InterfaceModel</th> <th>ChipManufacture</th> <th>ChipModel</th> <th>Firmware Version</th> <th>Count</th> </tr> </thead> </table>							CardManufacture	CardName	InterfaceModel	ChipManufacture	ChipModel	Firmware Version	Count							
CardManufacture	CardName	InterfaceModel	ChipManufacture	ChipModel	Firmware Version	Count															
Controller	<input checked="" type="checkbox"/> <table border="1"> <thead> <tr> <th>Manufacture</th> <th>Name</th> <th>ChipModel</th> <th>Firmware Version</th> <th>Count</th> </tr> </thead> </table>							Manufacture	Name	ChipModel	Firmware Version	Count									
Manufacture	Name	ChipModel	Firmware Version	Count																	
Power	<input checked="" type="checkbox"/> <table border="1"> <thead> <tr> <th>Manufacture</th> <th>Model</th> <th>MaxPower(W)</th> <th>Count</th> </tr> </thead> <tbody> <tr> <td>Great Wall</td> <td>CRPS800B</td> <td>800</td> <td>2</td> </tr> </tbody> </table>							Manufacture	Model	MaxPower(W)	Count	Great Wall	CRPS800B	800	2						
Manufacture	Model	MaxPower(W)	Count																		
Great Wall	CRPS800B	800	2																		
Fan	<input checked="" type="checkbox"/> <table border="1"> <thead> <tr> <th>Count</th> </tr> </thead> <tbody> <tr> <td>6</td> </tr> </tbody> </table>							Count	6												
Count																					
6																					
Select Server		<a href="#">Select Server</a>																			
		<a href="#">Submit</a> <a href="#">View Report</a>																			



After the asset acceptance parameters are exported, the **Exporting the asset acceptance file of the current server** button is activated.

6. (Optional) To export the asset acceptance parameters of the template server to a file, click **Exporting the asset acceptance file of the current server**.
7. Enable or disable asset acceptance items.
8. Click **Select Server**. The servers of the same model as the template server are listed in the displayed dialog box.
9. Select the desired servers.
10. Click **Submit** to return to the **Asset Acceptance** tab.
11. Click **Submit** to perform the asset acceptance operation.



#### Note

- During asset acceptance, the progress bar is displayed on the page.
- After asset acceptance is completed, the inspection result is displayed on the page.

#### Related Tasks

Perform the following operations as required on the acceptance result page.

To...	Do...
View the detailed information	Click <b>View Details</b> . The detailed asset acceptance information is displayed.
Perform asset acceptance again	1. Click <b>ReAcceptance</b> . The <b>ReAcceptance</b> dialog box is displayed. 2. Click <b>Submit</b> .
Export a statistical report	Click <b>Export Statistic Report</b> . The acceptance report is exported and saved to a local *.csv file.

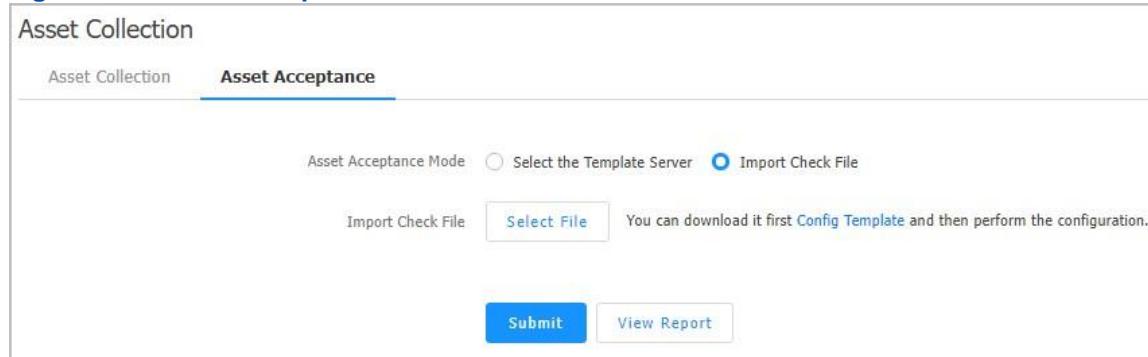
#### 3.6.4.2 Performing Asset Acceptance Through a Check File

##### Abstract

A server is used as the template server to check whether the asset information on the target server of the same model matches that on the template server.

##### Steps

1. Select **Device Mgmt > Inspection > Asset Collection**. The **Asset Collection** page is displayed.
2. Click **Asset Acceptance**. The **Asset Acceptance** tab is displayed, see [Figure 3-91](#).

**Figure 3-91 Asset Acceptance Tab**


3. Set **Asset Acceptance Mode** to **Import Check File**.
4. (Optional) If there is no check file, click **Config Template** to download and fill in the template.
5. Click **Select File**, and select the desired check file.



After a check file is imported, all the asset acceptance items in the file are displayed.

6. Enable or disable asset acceptance items.
7. Click **Select Server**. The servers of the same model as the template server are listed in the displayed dialog box.
8. Select the desired servers.
9. Click **Submit** to return to the **Asset Acceptance** tab.
10. Click **Submit** to perform the asset acceptance operation.



- During asset acceptance, the progress bar is displayed on the page.
- After asset acceptance is completed, the inspection result is displayed on the page.

## Related Tasks

Perform the following operations as required on the acceptance result page.

To...	Do...
View the detailed information	Click <b>View Details</b> . The detailed asset acceptance information is displayed.
Perform asset acceptance again	<ol style="list-style-type: none"> <li>1. Click <b>ReAcceptance</b>. The <b>ReAcceptance</b> dialog box is displayed.</li> <li>2. Click <b>Submit</b>.</li> </ol>

To...	Do...
Export a statistical report	Click <b>Export Statistic Report</b> . The acceptance report is exported and saved to a local *.csv file.

## 3.7 Troubleshooting

### 3.7.1 Collecting and Analyzing BMC Logs Online

#### Abstract

In the UniKits, you can collect the **BMC** logs of the server in batches in online mode, and analyze the collected logs for troubleshooting.

#### Prerequisite

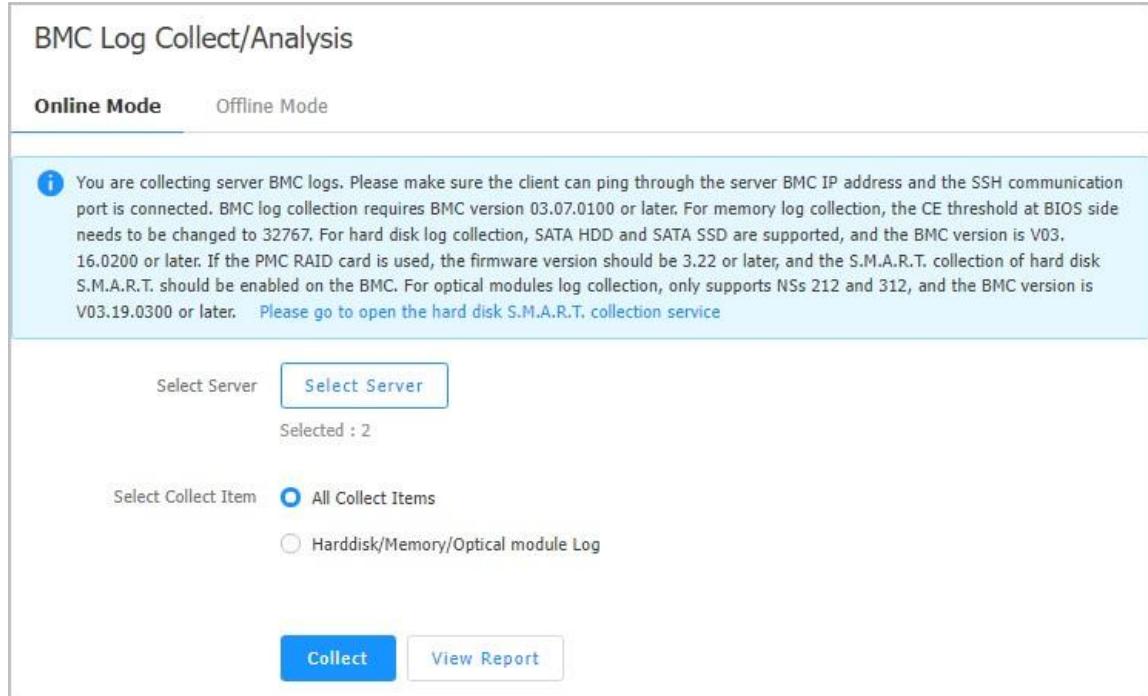
If you need to collect hard disk logs, enable the **DISK S.M.A.R.T.Collection** service. For details, refer to "[3.4.2.12 Configuring Services](#)".

#### Steps

##### Collecting Logs

1. Select **Device Mgmt > Troubleshooting > BMC Log Collect/Analysis**. The **BMC Log Collect/Analysis** page is displayed.
2. Click **Online Mode**. The **Online Mode** tab is displayed, see [Figure 3-92](#).

**Figure 3-92 Online Mode Tab**



**BMC Log Collect/Analysis**

**Online Mode**      Offline Mode

**Info:** You are collecting server BMC logs. Please make sure the client can ping through the server BMC IP address and the SSH communication port is connected. BMC log collection requires BMC version 03.07.0100 or later. For memory log collection, the CE threshold at BIOS side needs to be changed to 32767. For hard disk log collection, SATA HDD and SATA SSD are supported, and the BMC version is V03.16.0200 or later. If the PMC RAID card is used, the firmware version should be 3.22 or later, and the S.M.A.R.T. collection of hard disk S.M.A.R.T. should be enabled on the BMC. For optical modules log collection, only supports NSs 212 and 312, and the BMC version is V03.19.0300 or later. Please go to open the hard disk S.M.A.R.T. collection service

Select Server:       Selected : 2

Select Collect Item:  All Collect Items       Harddisk/Memory/Optical module Log

3. Click **Select Server**, and select the servers whose BMC logs are to be collected.

4. Select collection items. Options:

- **All Collect Items**: collects all BMC logs.
- **Harddisk/Memory/Optical module Log**: only collects the logs of hard disks, memory, and optical modules.

5. Click **Collect** to collect BMC logs.



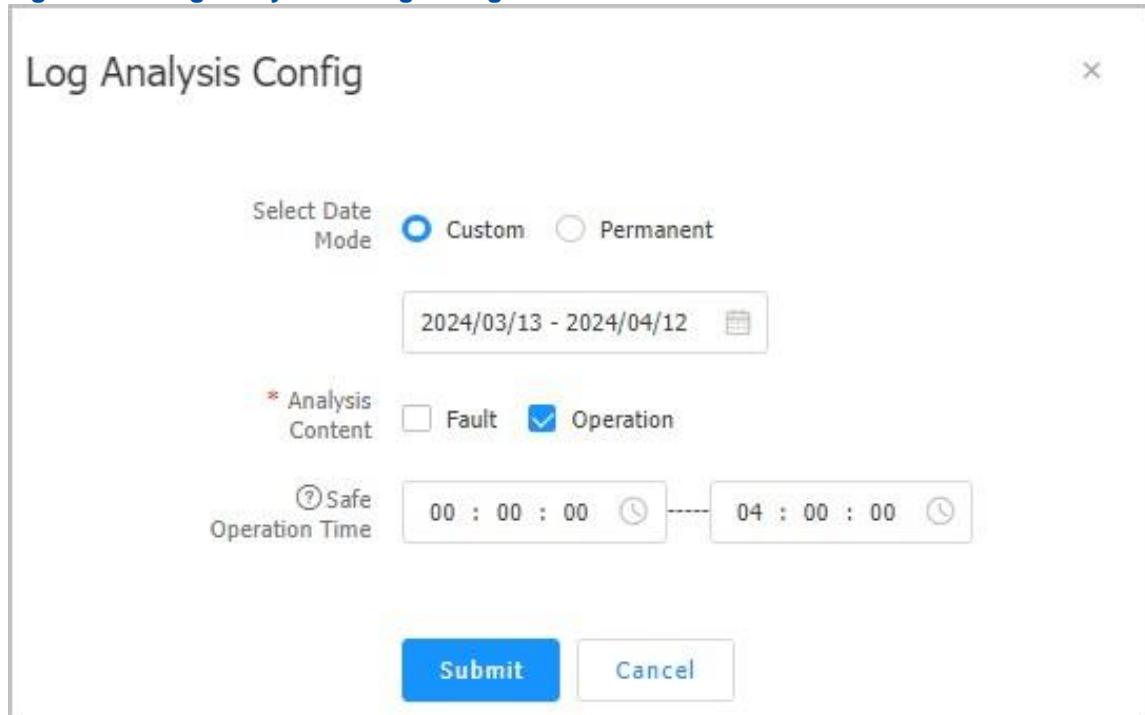
**Note**

- During the collection, the progress bar is displayed on the page.
- After the collection is completed, the collection result is displayed on the page.

### Analyzing Logs

6. On the collect result page, select the server for which you want to analyze logs, click **Start Log Analysis**. The **Log Analysis Config** dialog box is displayed, see [Figure 3-93](#).

[Figure 3-93 Log Analysis Config Dialog Box](#)



7. Set the parameters. For a description of the parameters, refer to [Table 3-58](#).

[Table 3-58 Parameter Descriptions for Log Analysis in Online Mode](#)

Parameter	Description
Select Date Mode	Select a time period within which the logs to be analyzed were generated. Options:

Parameter	Description
	<ul style="list-style-type: none"> <li>● <b>Custom:</b> Logs generated within the specified time period are analyzed. You need to select the start date and end date.</li> <li>● <b>Permanent:</b> Logs generated at any time are analyzed.</li> </ul>
Analysis Content	<p>Select the objects for log analysis. Options:</p> <ul style="list-style-type: none"> <li>● <b>Fault:</b> analyzes fault logs.</li> <li>● <b>Operation:</b> analyzes the logs about the operations such as power-on and power-off that are not performed within the allowed operation time.</li> </ul> <p>After <b>Operation</b> is selected, you also need to set <b>Safe Operation Time</b>.</p>
Safe Operation Time	<p>This parameter is required when <b>Analysis Content</b> is set to <b>Operation</b>.</p> <p>Select the allowed operation period. Default: 00:00:00–04:00:00.</p>

8. Click **Submit** to analyze logs.



#### Note

After the analysis is completed, the analysis result is displayed on the page.

### Related Tasks

Perform the following operations as required on the collection result page.

To...	Do...
Recollect logs	<ol style="list-style-type: none"> <li>1. Click <b>Re-Collection</b> to return to the <b>BMC Log Collect/Analysis</b> page.</li> <li>2. Set the collection parameters again.</li> <li>3. Click <b>Collect</b>.</li> </ol>
Export logs	<ol style="list-style-type: none"> <li>1. Select the servers for which the collected logs need to be exported.</li> <li>2. Click <b>Export Log</b>.</li> </ol>
Perform a secondary collection	<ol style="list-style-type: none"> <li>1. Select the server for which you want to collect logs for the second time.</li> <li>2. Click <b>Second Collect</b>.</li> </ol>

### 3.7.2 Analyzing BMC Logs Offline

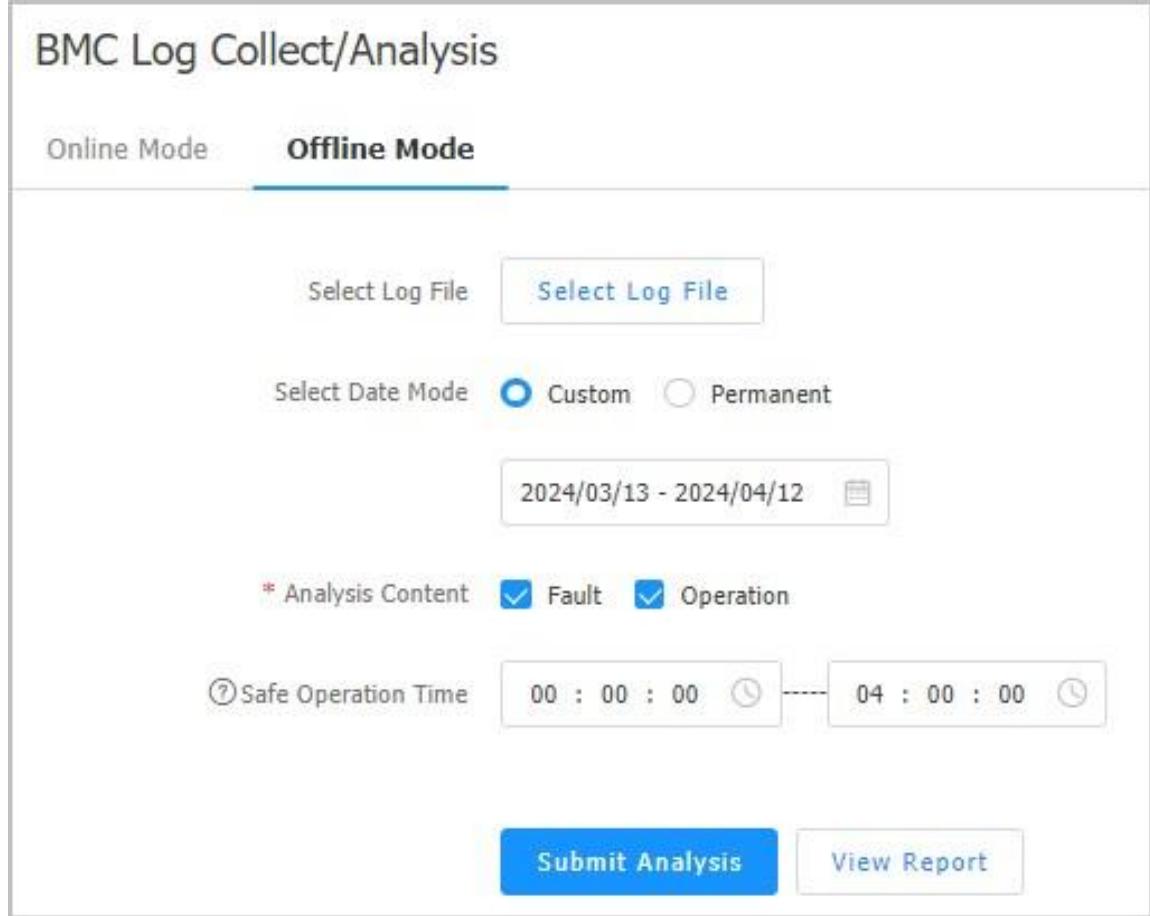
#### Abstract

In the UniKits, you can analyze the **BMC** logs of a server in offline mode to locate and handle faults.

## Steps

1. Select **Device Mgmt > Troubleshooting > BMC Log Collect/Analysis**. The **BMC Log Collect/Analysis** page is displayed.
2. Click **Offline Mode**. The **Offline Mode** tab is displayed, see [Figure 3-94](#).

**Figure 3-94 Offline Mode Tab**



The screenshot shows the 'BMC Log Collect/Analysis' page with the 'Offline Mode' tab selected. Key elements include:

- Log Selection:** 'Select Log File' button.
- Date Selection:** 'Select Date Mode' dropdown with 'Custom' selected, showing a date range from '2024/03/13' to '2024/04/12'.
- Analysis Content:** Checkboxes for 'Fault' (checked) and 'Operation' (checked).
- Safe Operation Time:** A time range from '00 : 00 : 00' to '04 : 00 : 00' with a clock icon.
- Buttons:** 'Submit Analysis' (blue) and 'View Report'.

3. Set the parameters. For a description of the parameters, refer to [Table 3-59](#).

**Table 3-59 Parameter Descriptions for Log Analysis in Offline Mode**

Parameter	Description
Select Log File	Click <b>Select Log File</b> to select the log file that you want to analyze. Log files can be exported in the following ways: <ul style="list-style-type: none"> <li>UniKits</li> <li>Web portal of the BMC</li> </ul>
Select Date Mode	Select a time period within which the logs to be analyzed were generated. Options: <ul style="list-style-type: none"> <li><b>Custom:</b> Logs generated within the specified time period are analyzed. You need to select the start date and end date.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>● <b>Permanent:</b> Logs generated at any time are analyzed.</li> </ul>
Analysis Content	Select the objects for log analysis. Options: <ul style="list-style-type: none"> <li>● <b>Fault:</b> analyzes fault logs.</li> <li>● <b>Operation:</b> analyzes the logs about the operations such as power-on and power-off that are not performed within the allowed operation time.</li> </ul> After <b>Operation</b> is selected, you also need to set <b>Safe Operation Time</b> .
Safe Operation Time	This parameter is required when <b>Analysis Content</b> is set to <b>Operation</b> . Select the allowed operation period. Default: 00:00:00–04:00:00.

4. Click **Submit Analysis** to analyze the logs.



#### Note

After the analysis is completed, the analysis result is displayed on the page.

### 3.7.3 Collecting Host Logs

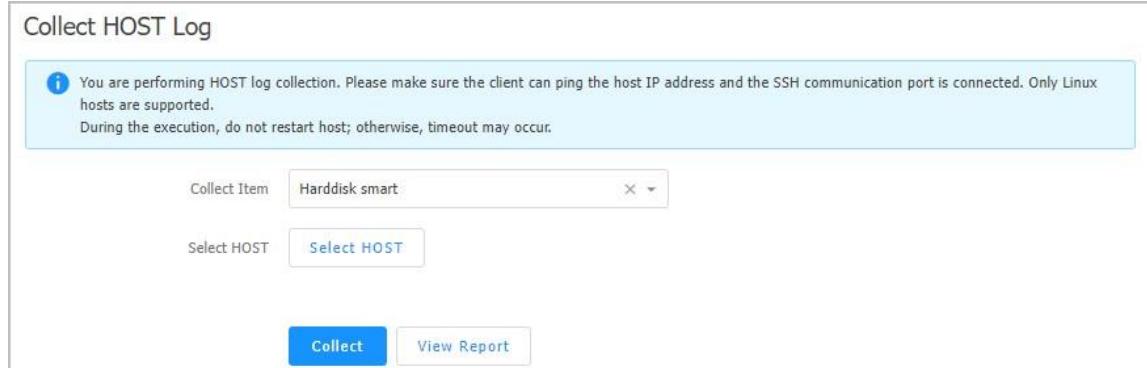
#### Abstract

In the UniKits, you can collect host logs of servers in batches to locate and handle faults.

#### Steps

1. Select **Device Mgmt > Troubleshooting > Collect HOST Log**. The **Collect HOST Log** page is displayed, see [Figure 3-95](#).

**Figure 3-95 Collect HOST Log Page**



2. From the **Collect Item** list, select the module whose logs are to be collected.
3. Click **Select HOST**, and select the servers whose host logs are to be collected.
4. Click **Collect** to collect host logs.

**Note**

- During the collection, the progress bar is displayed on the page.
- After the collection is completed, the collection result is displayed on the page.

**Related Tasks**

Perform the following operations as required on the collection result page.

To...	Do...
Recollect logs	<ol style="list-style-type: none"><li>1. Click <b>Re-Collection</b> to return to the <b>Collect HOST Log</b> page.</li><li>2. Set the collection parameters again.</li><li>3. Click <b>Collect</b>.</li></ol>
Export logs	<ol style="list-style-type: none"><li>1. Select the servers for which the collected logs need to be exported.</li><li>2. Click <b>Export Log</b>.</li></ol>
Perform a secondary collection	<ol style="list-style-type: none"><li>1. Select the servers for which you want to perform a secondary collection.</li><li>2. Click <b>Second Collect</b>.</li></ol>

### 3.7.4 Programming a UUID and Serial Number

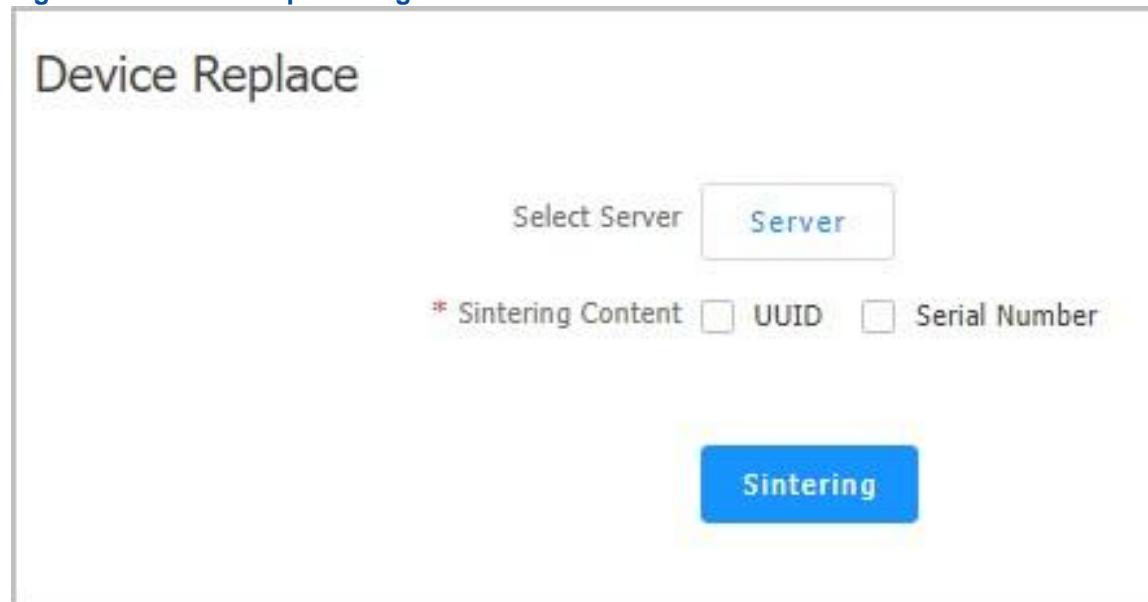
**Abstract**

After replacing a mainboard, you need to program the **UUID** and serial number of the original main board to the new mainboard.

**Steps**

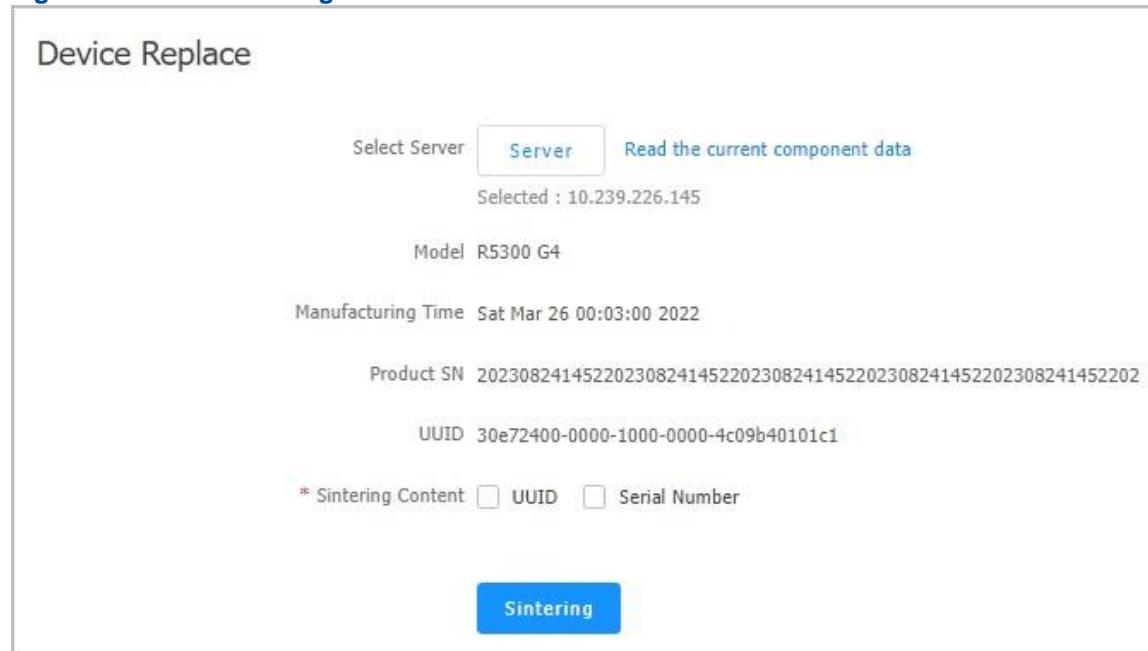
1. Select **Device Mgmt > Troubleshooting > Device Replace**. The **Device Replace** page is displayed, see [Figure 3-96](#).

Figure 3-96 Device Replace Page



2. Click **Server**. The **Select Server** dialog box is displayed.
3. Select the server where the mainboard has been replaced.
4. Click **Get Config**. The configurations of the server are obtained, see [Figure 3-97](#).

Figure 3-97 Server Configurations Obtained



5. Select the contents to be programmed, and enter the corresponding values, see [Figure 3-98](#)
  - **UUID**: 32-digit hexadecimal number. The 12 digits in the middle are fixed to 0000-1000-0000.
  - **Serial Number**: serial number of the product. Maximum length: 63 digits.

### Figure 3-98 Programming a UUID and Serial Number

## Device Replace

Select Server  Read the current component data

Selected : 10.239.226.145

Model R5300 G4

Manufacturing Time Sat Mar 26 00:03:00 2022

Product SN 202308241452202308241452202308241452202308241452202308241452202

UUID 30e72400-0000-1000-0000-4c09b40101c1

\* Sintering Content  UUID  Serial Number

\*  Enter the UUID 30e72400-0000-1000-0000-4c09b40101c1

## 6. Click **Sintering**.



• **Note**

- If the values before and after programming are the same, a confirmation dialog box is displayed.
- After the programming is completed, a message is displayed, indicating that the programming is successful.

### 3.7.5 Conducting a Stress Test

## Abstract

This procedure describes how to perform stress tests on the memory, [CPU](#), and [GPU](#) of a server to learn about the stress resistance of the server.

### Stress tests include:

- General stress tests: perform stress tests on memories and CPUs of all servers.
- Customized stress tests: perform stress tests on GPU performance of servers that use Biren's GPUs.

## Prerequisite

If the [BMC](#) version of a server whose firmware needs to be upgraded is V3, the [SMB/CIFS](#) file sharing function needs to be enabled on the [PC](#) (namely, the installation PC) where the UniKits is running. For details, refer to "[5 Reference: Enabling the SMB/CIFS File Sharing Function](#)".

## Steps

1. Select **Device Mgmt > Troubleshooting > Stress Test**. The **Stress Test** page is displayed, see [Figure 3-99](#) and [Figure 3-100](#).

**Figure 3-99 Stress Test Page—General Stress Test**

**Stress Test**

Only R5300G4,R5300G4X,R5500G4,R5500G4X,R8500G4X,R5930G2,R5930G2-HG3,R5300G5,R5350G5,R5200G5,R6500G5,R6900G5,R5530G2,R5530G2-HG3 servers are currently supported.  
 Please ensure your R5300G5, R5350G5, R5200G5, R6900G5 server BMC version 04.23.03.00 and later.  
 Please ensure your R6500G5 server BMC version 04.23.02.10 and later.  
 Please ensure your R5300G4, R5500G4 server BMC version 03.15.0100 and later & BIOS version 03.19.0200 and later.  
 please ensure your R5300G4X,R5930G2,R5930G2-HG3,R5500G4X,R8500G4X,R5530G2,R5530G2-HG3 server BMC version 03.15.0100 and later & BIOS version use the official release version.

* Server Type	<input type="text" value="R5300 G4X"/>
* Share Server Ip	<input type="text" value="10.10.10.2"/> IP used by the local computer to communicate with the BMC
* Share Server User	<input type="text" value="admin"/> The user must have the administrator permissions.
* Share Server Password	<input type="password" value="*****"/> <a href="#">@</a>
Stress test version type <input checked="" type="radio"/> General stress test version <input type="radio"/> OEM stress test version	
* TestContent	<input type="text" value="All"/>
* Time for memory stress Test	<input type="text" value="24"/> <a href="#">▼</a> <a href="#"> HOUR</a>
* Time for CPU Stress Test	<input type="text" value="24"/> <a href="#">▼</a> <a href="#"> HOUR</a>
* The CPU compression test adopts PTU mode	<input checked="" type="checkbox"/> PTU mode of CPU stress only support Intel CPU
* Stress percent	<input type="text" value="Search or select"/>
* Time for link stress Test	<input type="text" value="1"/> <a href="#">▼</a> <a href="#"> HOUR</a>
* Time for Disk Self Stress Test	<input type="text" value="24"/> <a href="#">▼</a> <a href="#"> HOUR</a>
* Time for disk write Test	<input type="text" value="24"/> <a href="#">▼</a> <a href="#"> HOUR</a>
* Group	<input type="text" value="1"/> The value contains a maximum of 10 alphanumeric characters
Select Server	<a href="#">Select Server</a>
<a href="#" style="background-color: #0072bc; color: white; padding: 5px 10px; border-radius: 5px;">Test</a> <a href="#" style="border: 1px solid #ccc; padding: 5px 10px; border-radius: 5px;">DeleteHistoryRecord</a> <a href="#" style="border: 1px solid #ccc; padding: 5px 10px; border-radius: 5px;">View Report</a>	

### Figure 3-100 Stress Test Page—Customized Stress Test

Stress Test

Only R5300G4,R5300G4X,R5500G4,R5500G4X,R8500G4X,R5930G2,R5930G2-HG3,R5300G5,R5350G5,R5200G5,R6900G5,R5530G2,R5530G2-HG3 servers are currently supported.  
Please ensure your R5300G5, R5350G5, R5200G5, R6900G5 server BMC version 04.23.03.00 and later.  
Please ensure your R6500G5 server BMC version 04.23.02.10 and later.  
Please ensure your R5300G4, R5500G4 server BMC version 03.15.0100 and later & BIOS version 03.19.0200 and later.  
please ensure your R5300G4X,R5930G2,R5930G2-HG3,R5300G5,R5500G4X,R8500G4X,R5530G2,R5530G2-HG3 server BMC version 03.15.0100 and later & BIOS version use the official release version.

* Server Type	R6900 G5
* Share Server Ip	10.10.10.2
IP used by the local computer to communicate with the BMC	
Stress test version type	<input type="radio"/> General stress test version <input checked="" type="radio"/> OEM stress test version
* TestContent	All
* Br Gpu stress test time	12
* ① Br GPU Stress test power level	default
* ② Br Gpu performance test time	12
* Group	1
The value contains a maximum of 10 alphanumeric characters	
Select Server	Select Server
<input type="button" value="Test"/> <input type="button" value="DeleteHistoryRecord"/> <input type="button" value="View Report"/>	

2. Set the parameters. For a description of the parameters, refer to [Table 3-60](#) and [Table 3-61](#).

**Table 3-60 Parameter Descriptions for General Stress Tests**

Parameter	Description
Server Type	Select the server model for which you want to conduct general stress tests.
Share Server Ip	Enter the IP address of the installation PC.
Share Server User	This parameter is required if the BMC version of the servers where stress tests are to be conducted is V3. Enter the username (with administrator permissions) of the installation PC.
Share Server Password	This parameter is required if the BMC version of the servers where stress tests are to be conducted is V3. Enter the password corresponding to the specified username.
Stress test version type	Select <b>General stress test version</b> .
TestContent	Select the desired test items. Options: <ul style="list-style-type: none"> <li>● <b>Memory stress Test</b></li> <li>● <b>CPU stress Test</b></li> <li>● <b>Link error code Test</b></li> <li>● <b>Hard disk self-check</b></li> <li>● <b>Hard disk write Test</b></li> </ul>

Time for memory stress Test	Enter the memory stress test duration. Range: 0.5–48 hours.
Time for CPU Stress Test	Enter the CPU stress test duration. Range: 0.5–48 hours.
Parameter	Description
The CPU compression test adopts PTU mode	Select whether to conduct a CPU stress test in <a href="#">PTU</a> mode. Only Intel CPUs support this mode. In PTU mode, a PTU tool is started to conduct a CPU stress test. If the PTU mode is not used, the default test mode is applicable to all types of CPUs, and the percentage of stress can be configured. The stress value is related to the stress test power.
Stress percent	Select the percentage of stress to be exerted on CPUs. Range: 10%–100%.
Time for link stress Test	Keep the default value. The duration of a bit error test for a link is one hour, which cannot be modified.
Time for Disk Self Stress Test	Enter the self-test duration of each hard disk. Range: 0.5–48 hours.
Time for disk write Test	Enter the disk write self-test duration. Range: 0.5–48 hours.
Group	Enter the batch number for the stress test. For multiple tests, each batch number must be unique, and the IP address of the server <a href="#">iSAC</a> management interface in each batch must be unique.
Select Server	Click <b>Select Server</b> , and select the servers for which you want to conduct stress tests.

**Table 3-61 Parameter Descriptions for Customized Stress Tests**

Parameter	Description
<b>Server Type</b>	Select the server model for which you want to conduct customized stress tests.
<b>Share Server Ip</b>	Enter the <a href="#">IP</a> address of the installation PC.
<b>Stress test version type</b>	Select <b>Oem stress test version</b> .
<b>TestContent</b>	Select the desired test items. Options: <ul style="list-style-type: none"> <li>● <b>BR GPU Stress Test</b></li> <li>● <b>BR GPU Performance Test</b></li> </ul>
<b>Br Gpu stress test time</b>	Enter the GPU stress test duration. Range: 0.5–48 hours.

<b>BR GPU Stress test power level</b>	Select a desired power consumption level. Options: <ul style="list-style-type: none"> <li>● <b>default</b></li> <li>● <b>50</b></li> <li>● <b>60</b></li> <li>● <b>70</b></li> <li>● <b>80</b></li> <li>● <b>90</b></li> <li>● <b>100</b></li> </ul>
<b>Parameter</b>	<b>Description</b>
	<p>The default option is <b>default</b>, indicating that consumption levels from <b>50</b> to <b>100</b> are set in sequence. When conducting a stress test, the test time of each power consumption level is: <b>Br GPU stress test time</b> <math>\div</math> 6.</p> <p>The purpose of setting the power consumption level is to ensure that the upper power limit of the GPU during the stress test is: GPU sub-card power <math>\times</math> the current power consumption level. For example, if the following error message is displayed when the test item is <b>board power</b>, it only indicates that the power exceeds the upper limit during the test. The displayed error message is irrelevant to the hardware.</p> <p>max should less than xxx</p>
<b>Br Gpu performance test time</b>	Enter the GPU performance test duration. Range: 0.5–48 hours.
<b>Group</b>	Enter the batch number for the stress test. For multiple tests, each batch number must be unique, and the IP address of the server <b>iSAC</b> management interface in each batch must be unique.
<b>Select Server</b>	Click <b>Select Server</b> , and select a server for which you want to conduct a stress test.

3. Click **Test**. A **Warning** dialog box is displayed.
4. Enter **yes** in the text box, and select **I have read it and know the influence**.
5. Click **Submit** to start the stress test task.



#### Note

- During the stress test, the progress bar is displayed on the page.
- After the stress test is completed, the stress test result is displayed on the page.

#### Related Tasks

Perform the following operations as required on the stress test result page.

To...	Do...
View the test results	Click <b>View Report</b> to view the progress and result of the previous or current stress test.
Reconduct a stress test	Click <b>ReTesting</b> to conduct the stress test again.
View the progress of a batch of tests	Click <b>Show Detail</b> in the <b>Operation</b> column for the desired batch.
View the progress of multiple batches of tests.	<ol style="list-style-type: none"> <li>1. Select the desired batches.</li> <li>2. Click <b>CheckProgress</b>.</li> </ol>
Export a stress test report	<ol style="list-style-type: none"> <li>1. Select the batch of tests for which the report needs to be exported.</li> <li>2. Click <b>Export Report</b>.</li> </ol>
<b>To...</b>	<b>Do...</b>

### 3.7.6 Setting a UID Indicator State

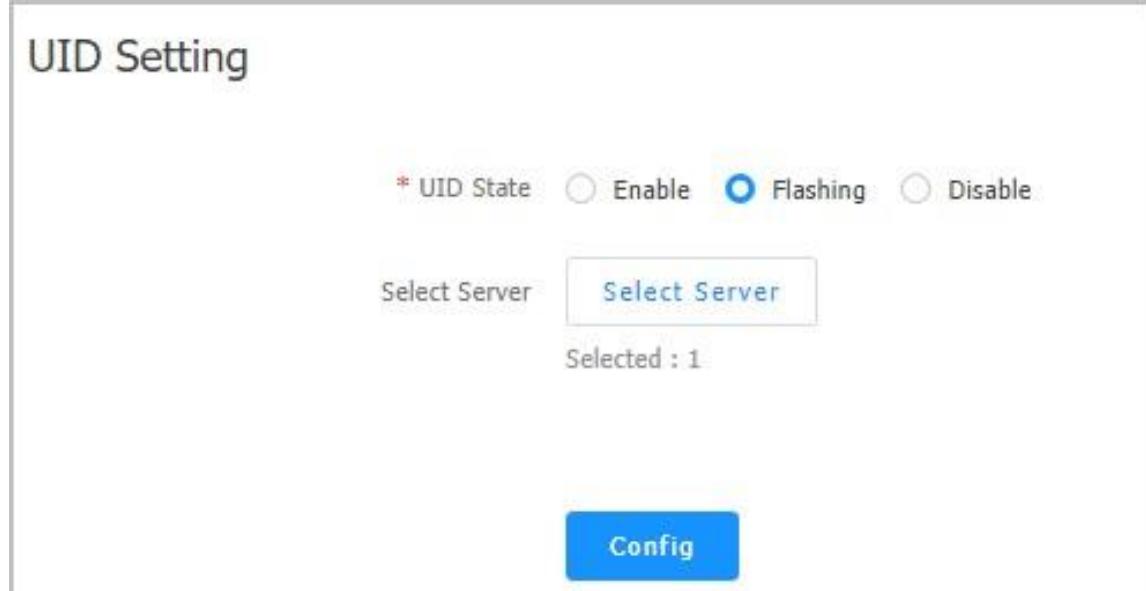
#### Abstract

The **UID** indicator states of a server help to identify the server.

#### Steps

1. Select **Device Mgmt > Troubleshooting > UID Setting**. The **UID Setting** page is displayed, as shown in [Figure 3-101](#).

[Figure 3-101 UID Setting Page](#)



The screenshot shows the 'UID Setting' page. At the top, it displays the title 'UID Setting'. Below the title, there is a label 'UID State' followed by three radio buttons: 'Enable' (unchecked), 'Flashing' (checked), and 'Disable' (unchecked). Below the radio buttons is a 'Select Server' label with a dropdown menu. The dropdown menu is open, showing the text 'Select Server' and 'Selected : 1'. At the bottom of the page is a large blue button labeled 'Config'.

2. Set the parameters. For a description of the parameters, refer to [Table 3-62](#).

**Table 3-62 UID Indicator Parameter Descriptions**

Parameter	Description
UID State	Select a UID indicator state. Options: <ul style="list-style-type: none"><li>● <b>Enable:</b> The UID indicator is turned on.</li><li>● <b>Flashing:</b> The UID indicator is flashing.</li><li>● <b>Disable:</b> The UID indicator is turned off.</li></ul>
Select Server	Click <b>Select Server</b> to select the servers for which you want to set the UID indicator state.

3. Click **Config** to deliver the configurations.

**Note**

- During UID indicator state configuration, the progress bar is displayed on the page.
- After UID indicator state configuration is completed, the configuration result is displayed on the page.

### 3.7.7 Clearing Historical BMC Alarms

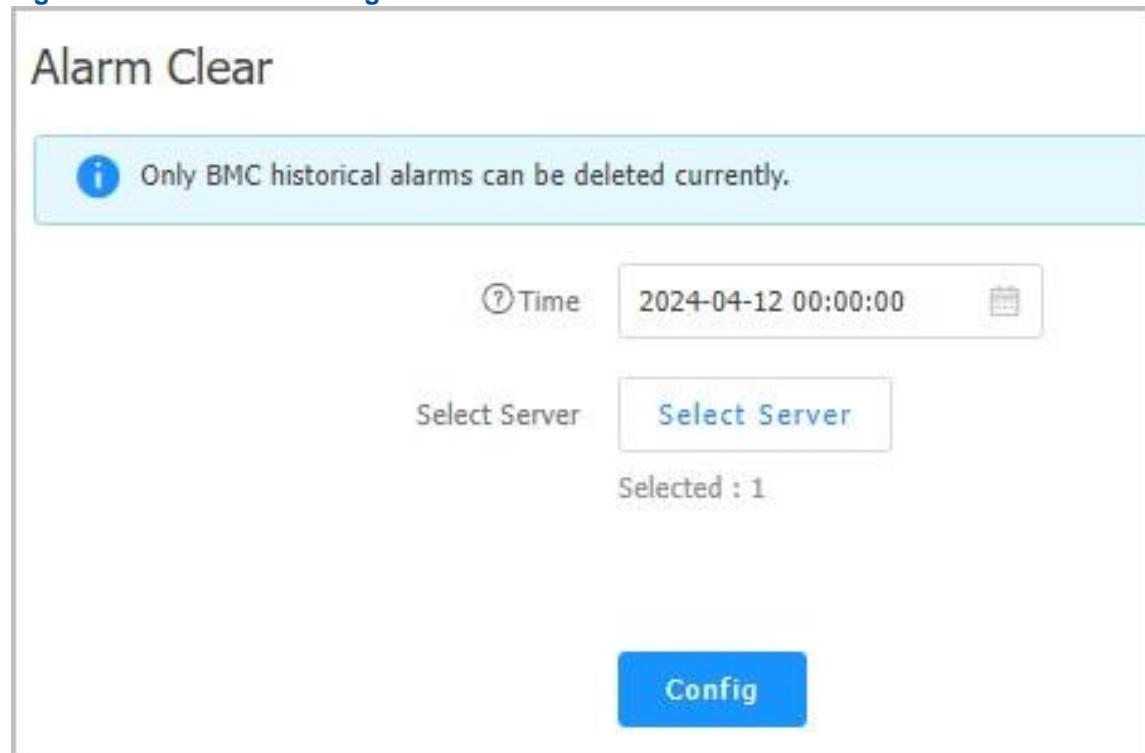
#### Abstract

This procedure describes how to clear the historical alarms of the **BMC** of a server to release the storage space.

#### Steps

1. Select **Device Mgmt > Troubleshooting > Alarm Clear**. The **Alarm Clear** page is displayed, as shown in [Figure 3-102](#).

Figure 3-102 Alarm Clear Page



2. Set the parameters. For a description of the parameters, refer to [Table 3-63](#).

**Table 3-63 Parameter Descriptions for Clearing Historical BMC Alarms**

Parameter	Description
Time	Click  and set a deadline.
Parameter	Description
	For example, if <b>Time</b> is set to <b>2024-04-12 00:00:00</b> , the alarms raised before 00:00:00 on April 12, 2024 are cleared.
Select Server	Click <b>Select Server</b> to select the servers whose historical BMC alarms need to be cleared.

3. Click **Config** to deliver the configurations.

**Note**

- During alarm clearing, the progress bar is displayed on the page.
- After alarms are cleared, the corresponding result is displayed on the page.

## 3.8 Fault Prediction

Fault prediction is an advanced function and requires a license. For how to import a license file, refer to "[3.9.4 Importing a License](#)".

### 3.8.1 Predicting a Hard Disk Fault

#### Abstract

This procedure describes how to collect and predict hard disk data to predict hard disk faults.

#### Steps

1. Select **Device Mgmt > Faultprediction > Hard Disk Failure Prediction**. The **Hard Disk Failure Prediction** page is displayed, see [Figure 3-103](#).

**Figure 3-103 Hard Disk Failure Prediction Page**



2. Set the parameters. For a description of the parameters, refer to [Table 3-64](#).

**Table 3-64 Parameter Descriptions for Hard Disk Fault Prediction**

Parameter	Description
Select Data Source	Select <b>Inspect Data</b> .
Select Server	Click <b>Select Server</b> , and select the server for which you want to predict hard disk faults.

3. Click **Collect** to deliver the collection command.



After the collection is completed, the collection results are displayed automatically.

4. Click **Start Forecasting**.



After the prediction is completed, the **Forecast Results** button is displayed next to the **Start Forecasting** button.

---

5. Click **Forecast Results** to view the prediction results.

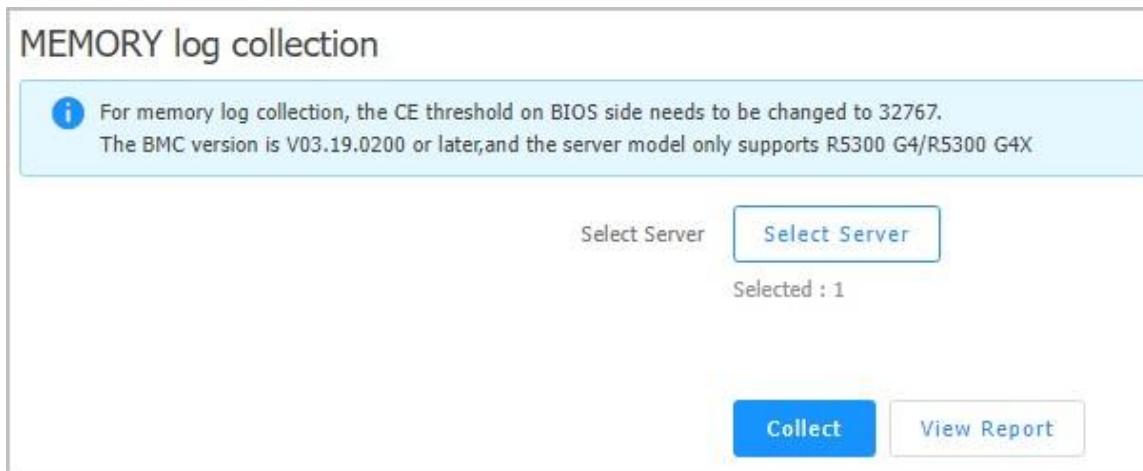
### 3.8.2 Predicting Memory Faults

#### Abstract

This procedure describes how to collect and predict memory data to predict memory faults.

#### Steps

1. Select **Device Mgmt > Troubleshooting > MEMORY log collection**. The **MEMORY log collection** page is displayed, see [Figure 3-104. Figure 3-104 MEMORY Log Collection Page](#)



MEMORY log collection

**Note** For memory log collection, the CE threshold on BIOS side needs to be changed to 32767. The BMC version is V03.19.0200 or later, and the server model only supports R5300 G4/R5300 G4X

Select Server **Select Server**  
Selected : 1

**Collect** **View Report**

2. Click **Select Server**, and select the server for which you want to predict memory faults.
3. Click **Collect** to deliver the collection command.



After the collection is completed, the collection results are displayed automatically.

4. Click **Start Forecasting**.



After the prediction is completed, the **Forecast Results** button is displayed next to the **Start Forecasting** button.

5. Click **Forecast Results** to view the prediction results.

### 3.8.3 Predicting Optical Module Faults

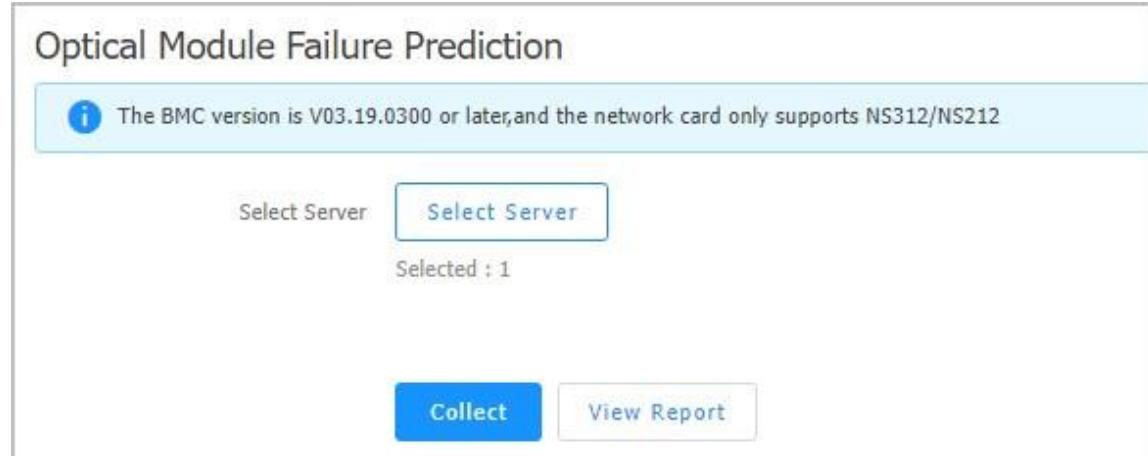
#### Abstract

This procedure describes how to collect and predict optical module data to predict optical module faults.

#### Steps

1. Select **Device Mgmt > Troubleshooting > Optical Module Failure Prediction**. The **Optical Module Failure Prediction** page is displayed, see [Figure 3-105](#).

[Figure 3-105 Optical Module Failure Prediction Page](#)



2. Click **Select Server**, and select the server for which you want to predict optical module faults.
3. Click **Collect** to deliver the collection command.



After the collection is completed, the collection results are displayed automatically.

4. Click **Start Forecasting**.



After the prediction is completed, the **Forecast Results** button is displayed next to the **Start Forecasting** button.

5. Click **Forecast Results** to view the prediction results.

## 3.9 System Management

### 3.9.1 Adding a Local User

#### Abstract

Local users refer to users of the UniKits itself. This procedure describes how to add a local user. In the UniKits, the local user can configure and manage the servers maintained. A maximum of 16 local users can be added.



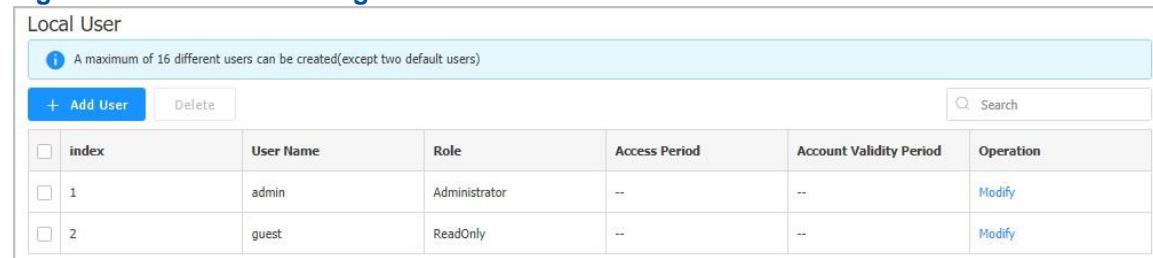
#### Notice

The **admin** and **guest** users cannot be deleted from the local users.

#### Steps

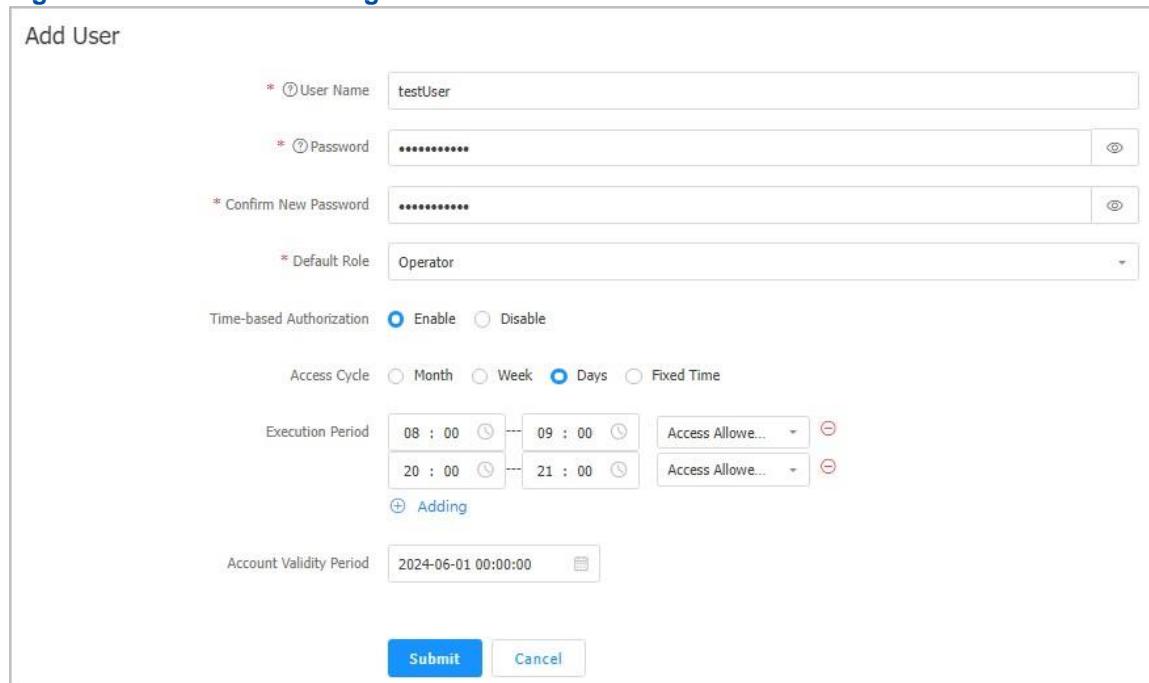
1. Select **System Mgmt > User Mgmt > Local User**. The **Local User** page is displayed, see [Figure 3-106](#).

**Figure 3-106 Local User Page**



Local User						
<small> ⓘ A maximum of 16 different users can be created(except two default users)</small>						
<small>+ Add User</small>		<small>Delete</small>		<small>Search</small>		
index	User Name	Role	Access Period	Account Validity Period	Operation	
1	admin	Administrator	--	--	Modify	
2	guest	ReadOnly	--	--	Modify	

2. Click **Add User**. The **Add User** dialog box is displayed, see [Figure 3-107](#).

**Figure 3-107 Add User Dialog Box**


The screenshot shows the 'Add User' dialog box. It includes fields for User Name (testUser), Password, Confirm New Password, Default Role (Operator), Time-based Authorization (Enable), Access Cycle (Days), Execution Period (08:00-09:00 and 20:00-21:00), Account Validity Period (2024-06-01 00:00:00), and buttons for Submit and Cancel.

3. Set the parameters. For a description of the parameters, refer to [Table 3-65](#).

**Table 3-65 Parameter Descriptions for Adding a Local User**

Parameter	Description
User Name	Enter the username of the local user. The requirements for the username are as follows: <ul style="list-style-type: none"> <li>• A string of 4–16 digits and letters</li> <li>• Case sensitive</li> <li>• Allowed special characters: -, _, and @.</li> </ul>
Password	Enter the password of the local user. The requirements for the password are as follows: <ul style="list-style-type: none"> <li>• The password cannot be the same as the username.</li> <li>• The length is 8–20 characters.</li> <li>• The password must contain four types of characters (uppercase letters, lowercase letters, digits, and symbols).</li> <li>• The password must not contain spaces or tabs.</li> </ul>
Confirm Password	Enter the password again.
Default Role	Select the role of the local user. Options: <ul style="list-style-type: none"> <li>• <b>Administrator</b>: indicates that the local user has permissions on all functions.</li> <li>• <b>Operator</b>: indicates that the local user has permissions on collection inspection and configuration delivery (except the configurations related to user management and <a href="#">LDAP</a>), and the local user has no permission on</li> </ul>

Parameter	Description
	<p>user management (including adding or deleting a user, and modifying user permissions and password).</p> <ul style="list-style-type: none"> <li>● <b>ReadOnly</b>: indicates that the local user has permissions on configuration check, out-of-band inspection, asset collection, BMC log collection/analysis, and host log collection only.</li> </ul>
Time-based Authorization	<p>Select whether to enable the time-based authorization function. Options:</p> <ul style="list-style-type: none"> <li>● <b>Enable</b>: indicates to enable the time-based authorization function. After the function is enabled, <b>Access Cycle</b> and <b>Execution Period</b> should be configured to specify the permissions of the newly added user within a fixed period.</li> <li>● <b>Disable</b>: indicates to disable the time-based authorization function.</li> </ul>
Account Validity Period	Click  to set the account validity period.

4. Click **Submit**.

### Related Tasks

Perform the following operations as required.

To...	Do...
Modify a local user	<ol style="list-style-type: none"> <li>1. Click <b>Modify</b> in the <b>Operation</b> column for the local user. The <b>Change User</b> dialog box is displayed.</li> <li>2. Modify the parameters for the local user.</li> <li>3. Click <b>Submit</b>.</li> </ol>
Delete a local user	<ol style="list-style-type: none"> <li>1. Click <b>Delete</b> in the <b>Operation</b> column for the local user. The <b>Delete Local User</b> dialog box is displayed.</li> <li>2. Click <b>Submit</b>.</li> </ol>
Delete local users in batches	<ol style="list-style-type: none"> <li>1. Select the local users that you want to delete.</li> <li>2. Click <b>Delete</b>.</li> </ol>

## 3.9.2 Adding a Domain User

### Abstract

Domain users are not the users of the UniKits itself. The detailed information about domain users is stored on an [LDAP](#) server.

This procedure describes how to configure authentication parameters for a domain user so that the domain user can be authenticated through an LDAP server.

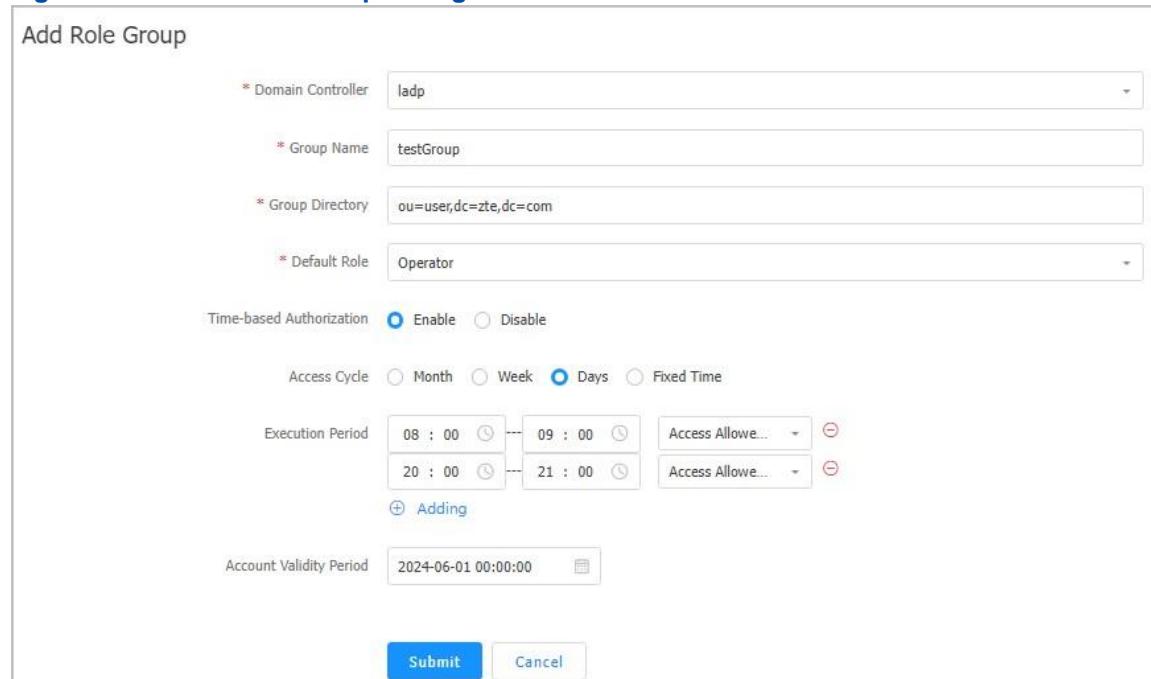
### Prerequisite

An LDAP server is already added. For details, refer to "[3.9.3 Adding an LDAP Server](#)".

## Steps

1. Select **System Mgmt > User Mgmt > Domain User**. The **Domain User** page is displayed.
2. Click **Add Role Group**. The **Add Role Group** dialog box is displayed, see [Figure 3-108](#).

**Figure 3-108 Add Role Group Dialog Box**



The screenshot shows the 'Add Role Group' dialog box. It contains the following fields:

- \* Domain Controller: ladp
- \* Group Name: testGroup
- \* Group Directory: ou=user,dc=zte,dc=com
- \* Default Role: Operator
- Time-based Authorization:  Enable  Disable
- Access Cycle:  Month  Week  Days  Fixed Time
- Execution Period: 08 : 00 - 09 : 00 (Access Allow...), 20 : 00 - 21 : 00 (Access Allow...), with a 'Adding' button below.
- Account Validity Period: 2024-06-01 00:00:00

At the bottom are 'Submit' and 'Cancel' buttons.

3. Set the role group parameters. For a description of the parameters, refer to [Table 3-66](#).

**Table 3-66 Role Group Parameter Descriptions**

Parameter	Description
Domain controller	Select the domain controller that the domain user belongs to.
Group Name	Enter the name of the new role group.
Group Directory	Enter the directory where the new role group is located.

Default Role	Select the role of the new role group. Options: <ul style="list-style-type: none"><li>● <b>Administrator</b>: indicates that the domain user has permissions on all functions.</li><li>● <b>Operator</b>: indicates that the domain user has permissions on collection inspection and configuration delivery (except the configurations related to user management and LDAP), and the domain user has no permission on user management (including adding or deleting a user, and modifying user permissions and password).</li><li>● <b>ReadOnly</b>: indicates that the domain user only has permissions on collection inspection.</li></ul>
Time-based Authorization	Select whether to enable the time-based authorization function. Options:
<b>Parameter</b>	<b>Description</b>
	<ul style="list-style-type: none"><li>● <b>Enable</b>: indicates to enable the time-based authorization function. After the function is enabled, <b>Access Cycle</b> and <b>Execution Period</b> should be configured to specify the permissions of the newly added user within a fixed period.</li><li>● <b>Disable</b>: indicates to disable the time-based authorization function.</li></ul>
Account Validity Period	Click  to set the account validity period.

4. Click **Submit**.

### Related Tasks

Perform the following operations as required.

To...	Do...
Modify a domain user	1. Click <b>Modify</b> in the <b>Operation</b> column for the domain user. The <b>Change User</b> dialog box is displayed. 2. Modify the parameters for the domain user. 3. Click <b>Submit</b> .
Delete a domain user	1. Click <b>Delete</b> in the <b>Operation</b> column for the domain user. The <b>Delete Domain User</b> dialog box is displayed. 2. Click <b>Submit</b> .
Delete domain users in batches	1. Select the domain users that you want to delete. 2. Click <b>Delete</b> .

### 3.9.3 Adding an LDAP Server

#### Abstract

This procedure describes how to add an **LDAP** server. After the LDAP server is added, it can authenticate domain users who are logging in to the UniKits.

## Steps

1. Select **System Mgmt > System Setting > LDAP Setting**. The **LDAP Setting** page is displayed, see [Figure 3-109](#).

**Figure 3-109 LDAP Setting Page**

LDAP Setting								
 The LDAP configuration is compatible with both Linux OpenLDAP and Window AD								
<input type="button" value="+ Add LDAP"/> <input type="button" value="Delete"/>		<input type="text" value="Search"/>						
Domain Controller	LDAP Type	LDAP Server Addr	LDAP Server Port	Administrator DN	User Root Directory(dn)	Role	Link Status	Operation
ldap	ldaps	10.228.34.67	389	cn=ldapadm,dc=zte,dc=com	ou=user,dc=zte,dc=com	Administrator	abnormal	<a href="#">Modify</a> <a href="#">Delete</a>

2. Click **Add LDAP**. The **Add LDAP Configuration** dialog box is displayed, see [Figure 3-110](#).

**Figure 3-110 Add LDAP Configuration Dialog Box**

### Add LDAP Configuration

LDAP Type  LDAP  LDAPS

\*  Domain Controller

\* LDAP Server Addr

\* LDAP Server Port

\* Administrator DN

\* Administrator Password

\* User Root Directory(dn)

\*  Login Attribute

\*  Default Role

Connect Test

3. Set the parameters. For a description of the parameters, refer to [Table 3-67](#).

**Table 3-67 LDAP Configuration Parameter Descriptions**

Parameter	Description
LDAP Type	Select an LDAP version. Options: <ul style="list-style-type: none"><li>● <b>LDAP</b>: indicates that communications are not encrypted.</li><li>● <b>LDAPS</b>: indicates that communications are encrypted.</li></ul>
Domain Controller	Enter the name of the domain controller. The name contains 4–64 characters, including digits, letters, and underscores. The name cannot start with a digit.
Parameter	Description
LDAP Server Addr	Enter the <a href="#">IP</a> address of the LDAP server. Both the <a href="#">IPv4</a> address and domain name are supported.
LDAP Server Port	Enter the port number of the LDAP server. For example: <ul style="list-style-type: none"><li>● LDAP port number: 389</li><li>● LDAPS port number: 636</li></ul>
Administrator <a href="#">DN</a>	Enter the DN with the administrator permissions on the LDAP server. For example, <code>cn=ldapadm,dc=NETAS,dc=com</code> . DNs are unique and used for distinguishing between users. A DN has three attributes: <a href="#">CN</a> , <a href="#">DC</a> , and <a href="#">OU</a> .
Administrator Password	Enter the password of the administrator of the LDAP server.
User Root Directory(dn)	Enter the root directory where the user information is stored. For example, <code>ou=user,dc=NETAS,dc=com</code> .
Login Attribute	Select a user login attribute. Options: <ul style="list-style-type: none"><li>● <b>cn</b>: The common name of a user is used for login.</li><li>● <b>uid</b>: The user ID of a user is used for login.</li><li>● <b>mail</b>: The email address of a user is used for login.</li></ul>
Default Role	Select the default role. If a role group is already configured for a domain user, the default role is overwritten.
Connect Test	Check whether the LDAP server can be connected to properly. Click <b>Test</b> to test the connectivity.

4. Click **Submit**.

## Related Tasks

Perform the following operations as required.

To...	Do...
View the LDAP configuration details	Click the controller name in the <b>Domain Controller</b> column. The LDAP configuration details are displayed.
Modify the information about an LDAP server	<ol style="list-style-type: none"> <li>1. Click <b>Modify</b> in the <b>Operation</b> column for the LDAP server. The <b>Update LDAP Configuration</b> dialog box is displayed.</li> <li>2. Modify the LDAP configurations.</li> <li>3. Click <b>Submit</b>.</li> </ol>
Delete an LDAP server	Click <b>Delete</b> in the <b>Operation</b> column for the LDAP server.
Delete LDAP servers in batches	<ol style="list-style-type: none"> <li>1. Select the LDAP servers that you want to delete.</li> <li>2. Click <b>Delete</b>.</li> </ol>

## 3.9.4 Importing a License

### Abstract

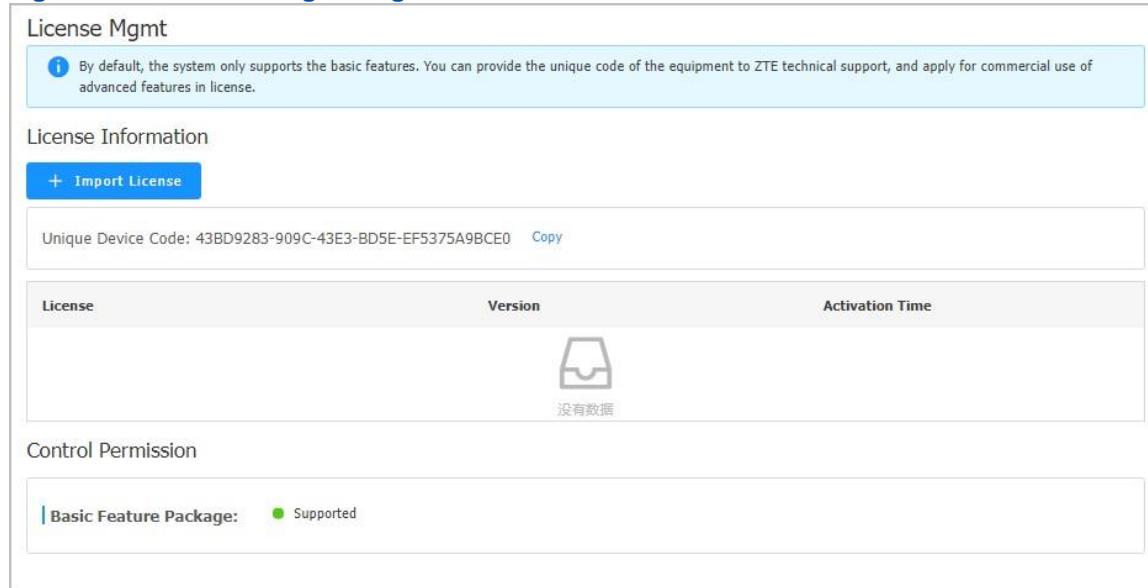
After the UniKits is installed, only basic functions are supported by default. To use an advanced function (for example, fault prediction, **OS** installation, and configuration migration), you need to import the corresponding commercial license.

### Prerequisite

You have provided **Unique Device Code** for NETAŞ technical support and applied for a license.

### Steps

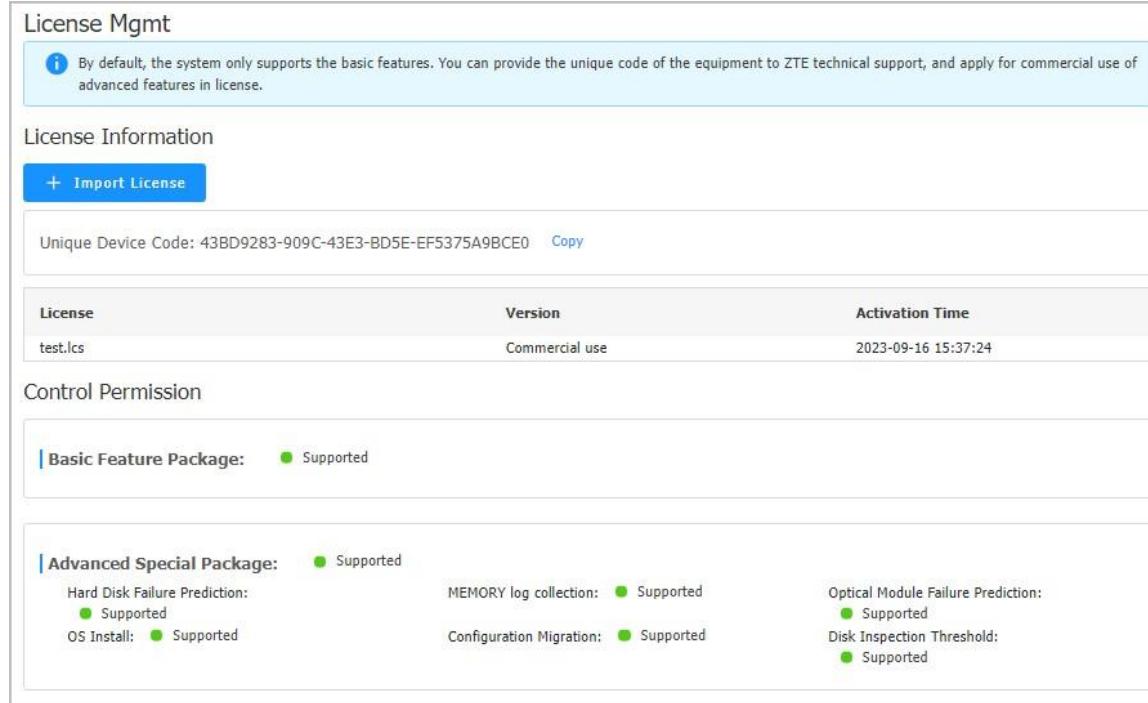
1. Select **System Mgmt > License Mgmt**. The **License Mgmt** page is displayed, see [Figure 3-111](#).

**Figure 3-111 License Mgmt Page**


The screenshot shows the 'License Mgmt' page. At the top, a note says: 'By default, the system only supports the basic features. You can provide the unique code of the equipment to ZTE technical support, and apply for commercial use of advanced features in license.' Below this is a 'License Information' section with a 'Import License' button. A table lists a single license entry: 'Unique Device Code: 43BD9283-909C-43E3-BD5E-EF5375A9BCE0' with a 'Copy' link. The table has columns for 'License', 'Version', and 'Activation Time'. The 'License' row shows a small icon and the text '没有数据'. In the 'Control Permission' section, it says 'Basic Feature Package: Supported'.

2. Click **Import License** to import the desired license.

After a license is imported, the **License Mgmt** page shows the advanced functions supported by the license, see [Figure 3-112](#).

**Figure 3-112 License Imported**


The screenshot shows the 'License Mgmt' page after a license has been imported. The note at the top remains the same. The 'License Information' section shows the imported license: 'Unique Device Code: 43BD9283-909C-43E3-BD5E-EF5375A9BCE0' with a 'Copy' link. The table now shows a single row: 'test.lics' (License), 'Commercial use' (Version), and '2023-09-16 15:37:24' (Activation Time). In the 'Control Permission' section, it says 'Basic Feature Package: Supported'. Below this, under 'Advanced Special Package:', there are three columns of features: 'Hard Disk Failure Prediction: Supported', 'MEMORY log collection: Supported', 'Optical Module Failure Prediction: Supported'; 'OS Install: Supported', 'Configuration Migration: Supported', 'Disk Inspection Threshold: Supported'.

### 3.9.5 Querying Management Logs

#### Abstract

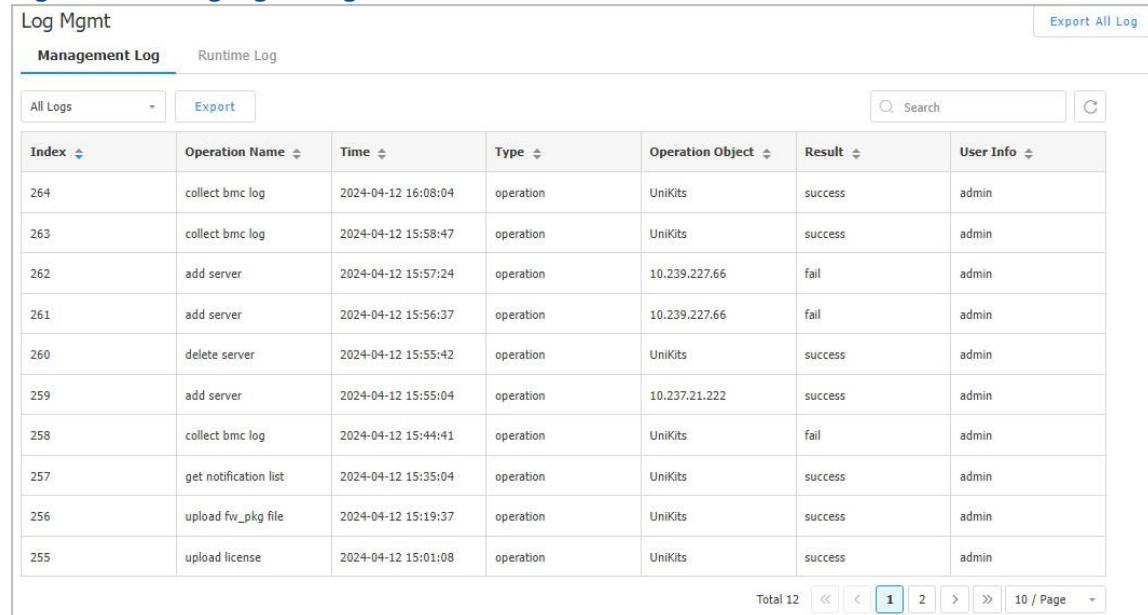
Management logs record your operations in the UniKits, including operation logs and login logs.

Management logs of the last 30 days are saved.

## Steps

1. Select **System Mgmt > Log Mgmt**. The **Log Mgmt** page is displayed, see [Figure 3-113](#).

**Figure 3-113 Log Mgmt Page**



Index	Operation Name	Time	Type	Operation Object	Result	User Info
264	collect bmc log	2024-04-12 16:08:04	operation	UniKits	success	admin
263	collect bmc log	2024-04-12 15:58:47	operation	UniKits	success	admin
262	add server	2024-04-12 15:57:24	operation	10.239.227.66	fail	admin
261	add server	2024-04-12 15:56:37	operation	10.239.227.66	fail	admin
260	delete server	2024-04-12 15:55:42	operation	UniKits	success	admin
259	add server	2024-04-12 15:55:04	operation	10.237.21.222	success	admin
258	collect bmc log	2024-04-12 15:44:41	operation	UniKits	fail	admin
257	get notification list	2024-04-12 15:35:04	operation	UniKits	success	admin
256	upload fw_pkg file	2024-04-12 15:19:37	operation	UniKits	success	admin
255	upload license	2024-04-12 15:01:08	operation	UniKits	success	admin

2. Click **Management Log**. The **Management Log** tab is displayed.



By default, all management logs of the last 30 days are displayed on the page.

3. From the drop-down list, select the type of management logs that you want to query, including operation logs and login logs.

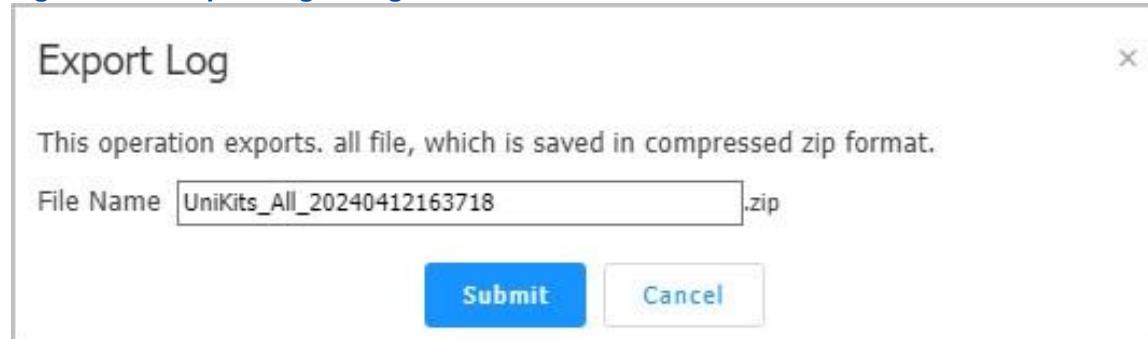


After a type of management logs is selected, the logs of this type within the latest 30 days are automatically displayed.

## Related Tasks

To export logs, perform the following operations:

1. Click **Export**. The **Export Log** dialog box is displayed, see [Figure 3-114](#).

**Figure 3-114 Export Log Dialog Box**

2. (Optional) Enter the filename in the **File Name** text box.
3. Click **Submit**.

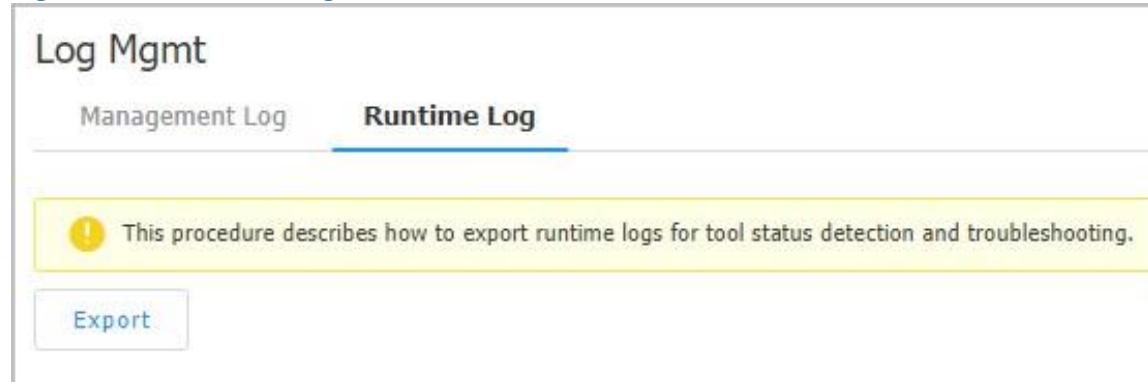
### 3.9.6 Exporting Operational Logs

#### Abstract

Operational logs record operational information about the UniKits to detect the operational status of the UniKits and troubleshoot faults.

#### Steps

1. Select **System Mgmt > Log Mgmt**. The **Log Mgmt** page is displayed.
2. Click **Runtime Log**. The **Runtime Log** tab is displayed, see [Figure 3-115](#).

**Figure 3-115 Runtime Log Tab**

3. Click **Export**.

### 3.9.7 Viewing Version Information

#### Abstract

This procedure describes how to view the detailed version information about the UniKits.

## Steps

1. Select **System Mgmt > About**. The **About** page is displayed, see [Figure 3-116](#).

[Figure 3-116 About Page](#)



2. View the version number of the tool.

## 3.10 Task Center Management

### 3.10.1 Creating a Task Schedule

#### Abstract

This procedure describes how to create a task schedule so that the task can be executed at a scheduled time.

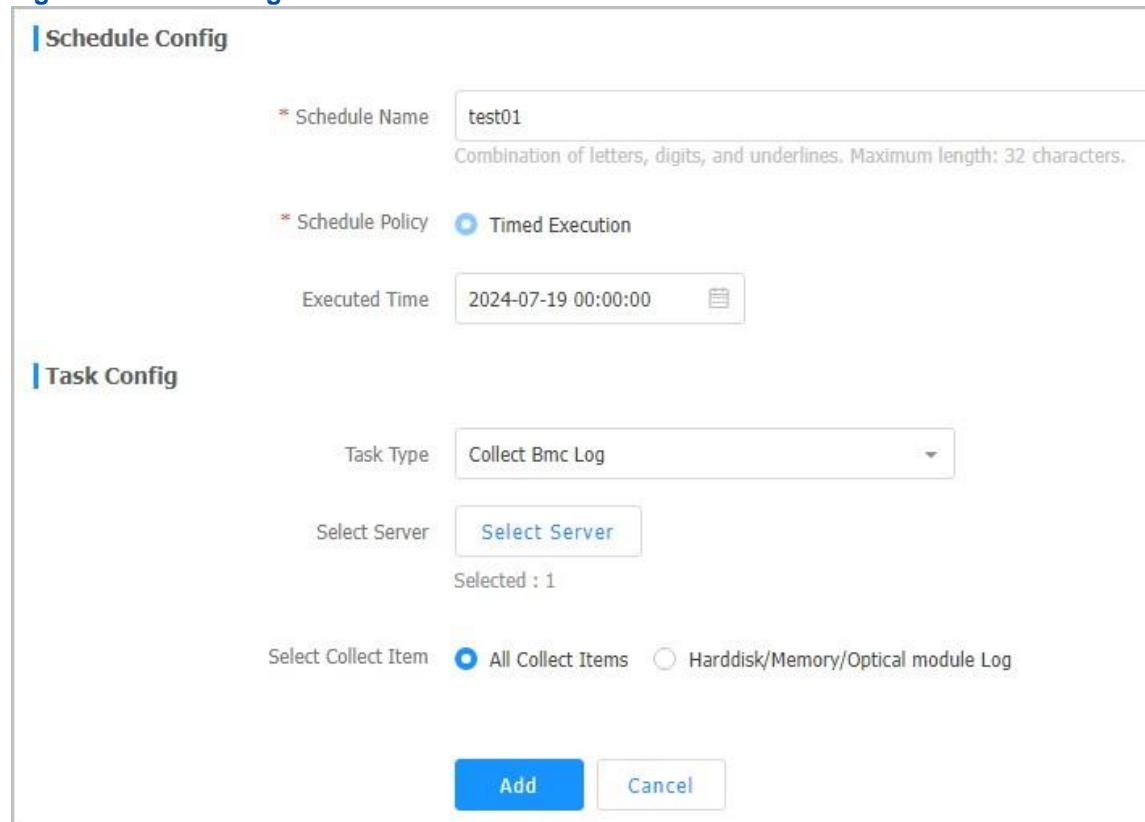
#### Steps

1. Select **Task Center > Task Schedule**. The **Task Schedule** page is displayed, as shown in [Figure 3-117](#).

[Figure 3-117 Task Schedule Page](#)

Task Schedule								
		New Schedule		Delete		Search		
No.	Schedule Name	Task Type	Execute Policy	Schedule Status	Creator	Creation Time	Operation	
1	test	Collect Bmc Log	date 2024-07-18 14:00:00	finished	admin	2024-07-18 11:57:09	Show Detail	
Total 1 << < 1 > >> 10 / Page								

2. Click **New Schedule**. The dialog box for creating a task schedule is displayed, as shown in [Figure 3-118](#).

**Figure 3-118 Creating a Task Schedule**


**Schedule Config**

\* Schedule Name: test01  
Combination of letters, digits, and underscores. Maximum length: 32 characters.

\* Schedule Policy:  Timed Execution

Executed Time: 2024-07-19 00:00:00

**Task Config**

Task Type: Collect Bmc Log

Select Server:  Selected : 1

Select Collect Item:  All Collect Items  Harddisk/Memory/Optical module Log

3. Set the parameters. For a description of the parameters, refer to [Table 3-68](#).

**Table 3-68 Parameter Descriptions for Creating a Task Schedule**

Parameter	Description
<b>Schedule Config</b>	
<b>Schedule Name</b>	Name of the schedule. It consists of letters, digits, and underscores. A maximum of 32 characters are supported.
<b>Schedule Policy</b>	By default, <b>Timed Execution</b> is selected.
<b>Executed Time</b>	Click <input type="button" value=""/> to set the start time of the task.
<b>Task Config</b>	
<b>Task Type</b>	By default, <b>Collect Bmc Log</b> is selected.
<b>Select Server</b>	Click <b>Select Server</b> , and select a server on which the scheduled task will be executed.

<b>Select Collect Item</b>	Select the item to be collected.
----------------------------	----------------------------------

4. Click **Add**.

### Related Tasks

On the **Task Schedule** page, perform the following operations as required.

To...	Do...
View the detailed information	<ol style="list-style-type: none"> <li>Click <b>Show Detail</b> in the <b>Operation</b> column to view the schedule details.</li> <li>Check the schedule details and task execution result.</li> </ol>
Delete task schedules	<ol style="list-style-type: none"> <li>Select the task schedules to be deleted.</li> <li>Click <b>Delete</b>.</li> </ol>

## 3.10.2 Viewing Task Execution Records

### Abstract

The page for viewing task execution results records operational information of out-of-band inspections, general firmware upgrades, and log collection tasks through the **BMC**.

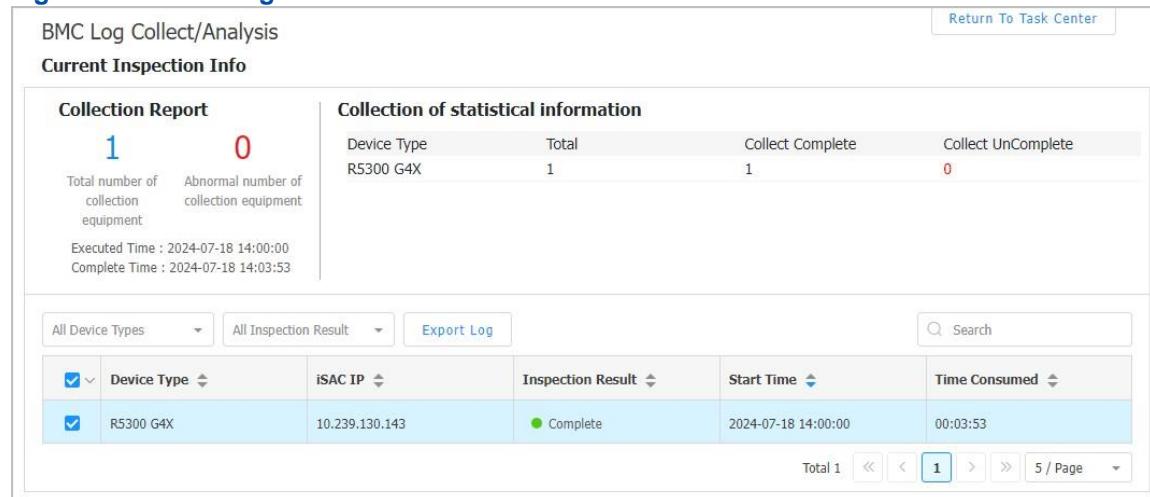
### Steps

1. Select **Task Center > Task List**. The **Task List** page is displayed, as shown in [Figure 3-119](#).

**Figure 3-119 Task List Page**

Task List										
		Delete		Search						
No.	Task Name	Task Type	Start Time	Time Consumed	Status	Execute Type	Schedule Name	Detail	Operation	
1	test	OutBand Inspect	2024-07-18 14:33:36	00:01:14	finished	Instant Task	--	Passed: 0, Need Attention: 0, Not Passed: 1, Uncompleted: 0	Show Detail	
2	test_1	Collect Bmc Log	2024-07-18 14:00:00	00:03:53	success	Scheduler Task	test	--	Show Detail	

2. Click **Show Detail** in the **Operation** column to view the detailed task execution information, as shown in [Figure 3-120](#).

**Figure 3-120 Viewing the Task Execution Information**

The screenshot shows the 'BMC Log Collect/Analysis' interface under the 'Current Inspection Info' section. It displays a 'Collection Report' with 1 collection and 0 abnormal collection equipment. The report includes execution and completion times. A table shows the collection of statistical information for the R5300 G4X device, with 1 total item, 1 collect complete, and 0 collect incomplete. Below this is a search and filter interface for inspection results, showing one entry for the R5300 G4X device with an iSAC IP of 10.239.130.143, an inspection result of 'Complete', and a start time of 2024-07-18 14:00:00. The page navigation shows 1 page of 5.

Collection Report		Collection of statistical information			
1	0	Device Type	Total	Collect Complete	Collect UnComplete
Total number of collection equipment	Abnormal number of collection equipment	R5300 G4X	1	1	0
Executed Time : 2024-07-18 14:00:00	Complete Time : 2024-07-18 14:03:53				

All Device Types		All Inspection Result		Export Log	Search	
<input checked="" type="checkbox"/>	Device Type	iSAC IP	Inspection Result	Start Time	Time Consumed	
<input checked="" type="checkbox"/>	R5300 G4X	10.239.130.143	● Complete	2024-07-18 14:00:00	00:03:53	

Total 1 | << | < | 1 | > | >> | 5 / Page |

# Chapter 4

# Troubleshooting

---

## Table of Contents

Information Not Completely Displayed in the Installation Dialog Box.....	201
Front-End Page Improperly Displayed.....	202
IPMI Command Failure on a Server with an IPv6 Address.....	203
IPMI Link Error.....	204
ISO File Mounting Failure.....	206
Unable to Find Out the Administrator's DN and the LDAP Directory of the Logged-In User....	207
Configuration Migration Failure.....	209
UniKits Operation Failure in the Windows Server 2012 R2 OS.....	209
UniKits Operation Failure in the 64-Bit Windows 7 OS.....	210
Common OS Installation Problems.....	211
SNMP Link Check.....	212
Failure in the Standard Card Firmware Upgrade, In-Band RAID Configuration, or Out-of-Band Stress Test.....	214
Operation Suggestions for Common Errors.....	215

## 4.1 Information Not Completely Displayed in the Installation Dialog Box

### Symptom

During the installation of the tool, the content displayed in the dialog box is incomplete, see Figure 4-1.

Figure 4-1 Installation Dialog Box



### Probable Cause

The setting of the window display in the operating system is set to a small value.

### Steps

1. Perform the following operations as required.

If...	Then...
Windows 7 is used	<ol style="list-style-type: none"><li>a. Start the control panel of the operating system.</li><li>b. Click <b>Appearance and Personalization</b>. The <b>Appearance and Personalization</b> window is displayed.</li><li>c. Click <b>Display</b>. The <b>Display</b> window is displayed.</li><li>d. Select <b>Smaller (S)-100%(default)</b>.</li><li>e. Click <b>Apply</b>.</li></ol>
Windows 10 is used	<ol style="list-style-type: none"><li>a. Right-click the desktop and select <b>Display settings</b>. The <b>Display</b> window is displayed.</li><li>b. Select <b>100% (Recommended)</b> for <b>Change the size of text, apps, and other items</b>.</li></ol>

## 4.2 Front-End Page Improperly Displayed

### Symptom

Both Chinese and English characters are displayed on a front-end page.

### Probable Cause

The buffer of the browser is not cleared.

## Steps

1. Clear the cache of the browser.
2. Log in to the page again.

## 4.3 IPMI Command Failure on a Server with an IPv6 Address

### Symptom

During functional implementation, a server where an **IPv6** address is configured returns the "could not open socket" message.

### Probable Cause

- In the Win7 environment, the sequence priority of server **NICs** is not the highest.
- In the Win10 environment, the NICs of the server are hidden and disabled.

### Steps

- Adjust the **NIC** sequence in a Windows 7 environment.
  1. Open the control panel.
  2. Click **Network and Internet**. The **Network and Internet** window is displayed.
  3. Click **Network and Sharing Center**. The **Network and Sharing Center** window is displayed.



### Note

Verify that the NIC networks are identified and can be connected to the Internet.

- 4. Select **Change adapter settings** from the menu on the left. The **Network Connections** window is displayed.
- 5. Click **Organize**. Select **Layout > Menu bar**. The menu bar is displayed.
- 6. Select **Advanced > Advanced Settings**. The **Advanced Settings** dialog box is displayed.
- 7. Click the arrow on the right to move the NIC to the top (highest priority).
- 8. Click **OK**.
- Disable hidden NICs in a Windows 10 environment
  1. Open the control panel.
  2. Set **View by** to **Small icons**.
  3. Click **Device Manager**. The **Device Manager** window is displayed.
  4. Select **View>Show hidden devices**. Check the hidden NICs.
  5. Right-click the NIC to be disabled, and select **Disable**.

6. Click **OK**.

## 4.4 IPMI Link Error

### Symptom

When you add a device, the UniKits displays the following information:

```
IPMI error: The IPMI link check fails
```

### Probable Cause

- The username and password of the [IPMI](#) user are incorrect.
- Network link error.
- IPMI link error.

### Steps

#### [Checking the Username and Password of the IPMI User](#)

1. Check whether the username and password of the [IPMI](#) user are correct.
  - Yes → [Step 3](#).
  - No → [Step 2](#).
2. Modify the username and password of the IPMI user and then add the device again to see whether the fault is removed.
  - Yes → End.
  - No → [Step 3](#).

#### [Checking the Network Link](#)

3. Open the command line window.
4. Run the following command to enter the UniKits installation directory:  

```
# cd Unikits\Unikits\bin
```
5. Run the following command to check whether the network link is abnormal:  

```
# ipmitool -I lanplus -H ip address -U ipmi username -P ipmi
password mc info
```

If the following information is displayed, it indicates that the network link is abnormal.

```
Error: Unable to establish IPMI v2 / RMCP+ session
```

- Yes → [Step 12](#).
- No → [Step 6](#).

## Checking the IPMI Link

6. Log in to the faulty server or remotely connect to it through [SSH](#).
7. Run the following command to check whether the IPMI service is normal:

```
# ipmitool -I lanplus -H ip address -U ipmi username -P ipmi
password mc info
```

If the following information is displayed in the command execution result, it indicates that the IPMI service is proper:

```
? MobaXterm 12.1 ?
(SSH client, X-server and networking tools)

> SSH session to zteroot@10.228.34.75
? SSH compression : ✓
? SSH-browser : ✓
? X11-forwarding : ✘ (disabled or not supported by server)
? DISPLAY : 10.56.41.22:0.0

> For more info, ctrl+click on help or visit our website
```

```
- $ ls
- $ ll
sh: ll: not found
- $ ipmitool -I lanplus -H 127.0.0.1 -U [REDACTED] -P [REDACTED] mc info
Device ID : 10
Device Revision : 0
Firmware Revision : 3.13
IPMI Version : 2.0
Manufacturer ID : 3902
Manufacturer Name : Unknown (0xF3E)
Product ID : 12576 (0x3120)
Product Name : Unknown (0x3120)
Device Available : yes
Provides Device SDRs : yes
Additional Device Support :
  Sensor Device
  SDR Repository Device
  SEL Device
  FRU Inventory Device
  IPMB Event Receiver
  IPMB Event Generator
  Chassis Device
Aux Firmware Rev Info :
  0x64
  0x00
  0x00
  0x00
- $
```

- Yes → [Step 12](#).
- No → [Step 8](#).

8. Log in to the Web portal of the [BMC](#).
9. Select **Setting > Service**. The **Service** page is displayed.
10. Check whether the IPMI port in the configuration information is the same as the port actually configured on the server.

- Yes → [Step 12.](#)
- No → [Step 11.](#)

11. Modify the port information and then add the device again to see whether the fault is removed.

- Yes → End.
- No → [Step 12.](#)

12. Contact [NETAŞ](#) technical support.

## 4.5 ISO File Mounting Failure

### Symptom

When you upgrade a standard card/disk firmware, perform in-band [RAID](#) configuration, or conduct a stress test, the following error message is reported:

```
mount on image by redfish fail : the virtual_media_vmm_control process is abnormal.  
For details, please refer to the running log.
```

### Probable Cause

- The firewall and antivirus software are not disabled.
- The [SMB/CIFS](#) sharing function is not enabled and the ports (445 and 139) for the SMB/CIFS sharing function are not enabled.
- The username and password of the shared device are incorrectly configured.

### Steps

1. Check whether the firewall and antivirus software are disabled.
  - Yes → [Step 3.](#)
  - No → [Step 2.](#)
2. Disable the firewall and antivirus software, and check whether the fault is removed.
  - Yes → End.
  - No → [Step 3.](#)
3. Check whether the [SMB/CIFS](#) sharing function is enabled and the ports (445 and 139) for the SMB/CIFS sharing function are enabled.
  - Yes → [Step 5.](#)
  - No → [Step 4.](#)
4. Enable the [SMB/CIFS](#) sharing function and the ports (445 and 139) for the SMB/CIFS sharing function, and check whether the fault is removed.

For details, refer to "[5 Reference: Enabling the SMB/CIFS File Sharing Function](#)".

- Yes → End.
- No → [Step 5](#).

5. Check whether the username and password of the shared device are correctly configured. If the shared device is a domain-joined computer, the domain username and password are used.
  - Yes → [Step 7](#).
  - No → [Step 6](#).
6. Reconfigure the username and password of the shared device, and check whether the fault is removed.
  - Yes → End.
  - No → [Step 7](#).
7. Contact NETAS technical support.

## 4.6 Unable to Find Out the Administrator's DN and the LDAP Directory of the Logged-In User

### Problem

You cannot find out the administrator's [DN](#) and the [LDAP](#) directory of the logged-in user. An LDAP directory is similar to a file system directory, including [CN](#), [OU](#), and [DC](#). The format of the LDAP connection string is `ldap://servername/DN`. In the string, DN has three attributes, namely, [CN](#), [OU](#), and [DC](#).

In an LDAP directory, [CN](#), [OU](#), and [DC](#) are described as follows:

- [CN](#): Common Name
- [OU](#): Organizational Unit
- [DC](#): Domain Component

### Probable Cause

1. Log in to the LDAP server as the `root` user.
2. Run the following command to find out the administrator's DN and the LDAP directory of the logged-in user.

```
# ldapsearch -H ldap://IP:Port -x -b dc=NETAS, dc=com
```

In the above command, IP:Port indicates the [IP](#) address and port number of the LDAP server.

After the command is executed, the following output is displayed.

```

[root@ ~]# ldapsearch -H ldap://1.2.3.6:389 -x -b dc=zte,dc=com
# extended LDIF
#
# LDAPv3
# base <dc=zte,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# zte.com
dn: dc=zte,dc=com
dc: zte
objectClass: top
objectClass: domain

# ldapadm, zte.com
dn: cn=ldapadm,dc=zte,dc=com DN of the administrator
objectClass: organizationalRole
cn: ldapadm
description: LDAP Manager

# user, zte.com
dn: ou=user,dc=zte,dc=com
objectClass: organizationalUnit
ou: user

# testgroup, zte.com
dn: ou=testgroup,dc=zte,dc=com
objectClass: organizationalUnit
ou: testgroup

# ldapgrl, testgroup, zte.com
dn: cn=ldapgrl,ou=testgroup,dc=zte,dc=com
objectClass: groupOfNames
cn: ldapgrl
member: cn=LDAPUser1,ou=user,dc=zte,dc=com

# LDAPUser1, user, zte.com
dn: cn=LDAPUser1,ou=user,dc=zte,dc=com User directory
objectClass: uidObject
objectClass: top
objectClass: person
objectClass: inetOrgPerson
uid: test001
sn: LDAP
cn: LDAPUser1
mail: test@zte.com.cn
userPassword:: TERBUFVzZXIwMDE=

```

Login attributes of the user

## 4.7 Configuration Migration Failure

### Symptom

BMC configurations fail to be migrated.

### Probable Cause

- The IP address of the **TFTP** server and that of the BMC to be configured are not in the same network.
- The TFTP port is disabled in the network (firewall/switch).

### Steps

1. Check whether the IP address of the TFTP server and that of the BMC to be configured are in the same network.
  - Yes → [Step 3](#).
  - No → [Step 2](#).
2. Reconfigure the IP address of the TFTP server and that of the BMC to ensure that they are in the same network, and check whether the fault is removed.
  - Yes → End.
  - No → [Step 3](#).
3. Check whether the TFTP port is disabled.
  - Yes → [Step 4](#).
  - No → [Step 5](#).
4. Enable the TFTP port, and check whether the fault is removed.
  - Yes → End.
  - No → [Step 5](#).
5. Contact NETAŞ technical support.

## 4.8 UniKits Operation Failure in the Windows Server 2012 R2 OS

### Symptom

In the Windows Server 2012 R2 OS, when you double-click the UniKits, the **unikits\_python.exe-System Error** message box is displayed.

### Probable Cause

The Windows Server 2012 R2 OS requires a Python update.

### Steps

1. Install the *Windows 8.1 - KB2999226-x64.msu* patch package.  
The patch package is downloaded at <https://www.microsoft.com/en-us/download/details.aspx?id=49063>. If the link is unavailable, you can search for and download the patch package.

**Note**

If an error occurs when you install the *Windows 8.1 - KB2999226-x64.msu* patch package, install the *Windows 8.1-KB2919355- x64.msu* patch package first and then the *Windows 8.1KB2999226-x64.msu* patch package. The *Windows 8.1-KB2919355- x64.msu* patch package is downloaded at <https://www.microsoft.com/en-us/download/details.aspx?id=42335>. If the link is unavailable, you can search for and download the patch package.

2. Uninstall the UniKits.
3. Reinstall the UniKits.

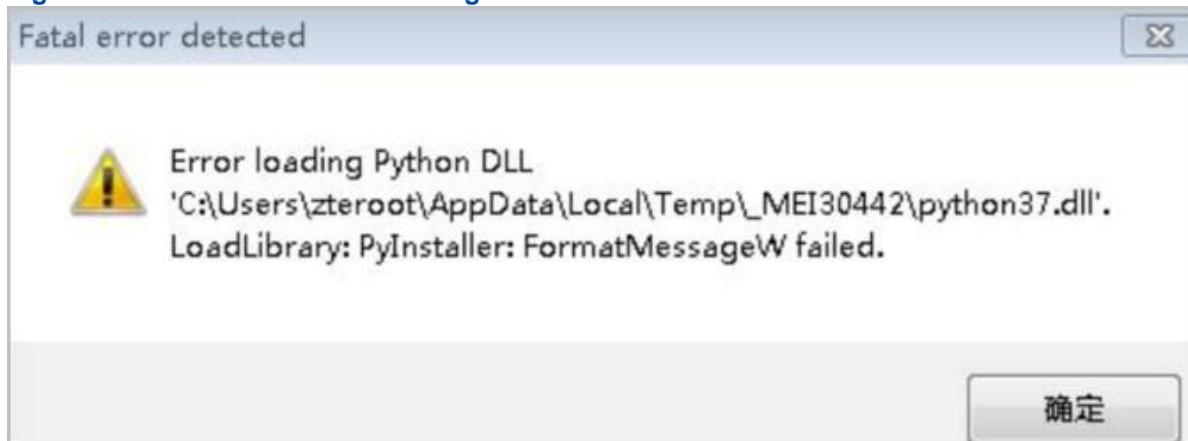
## 4.9 UniKits Operation Failure in the 64-Bit Windows 7 OS

**Symptom**

In the 64-bit Windows 7 OS, when you double-click the UniKits, an error dialog box is displayed, as shown in [Figure 4-2](#) and [Figure 4-3](#).

[Figure 4-2 Fatal error detected Dialog Box—1](#)



**Figure 4-3 Fatal error detected Dialog Box—2**

### Probable Cause

The 64-bit Windows 7 OS requires patch package installation.

### Steps

1. Install the *Windows 6.1 - KB2999226-x64.msu* patch package.

The patch package is downloaded at <https://www.microsoft.com/zh-cn/download/details.aspx?id=49062&751be11f-ede8-5a0c-058c-2ee190a24fa6=True>. If the link is unavailable, you can search for and download the patch package.

2. Uninstall the UniKits.
3. Reinstall the UniKits.

## 4.10 Common OS Installation Problems

### Symptom

After an **OS** is installed, the server is automatically restarted and the grub screen is displayed, see [Figure 4-4](#).

**Figure 4-4 Grub Screen**

```

SilkScreen | CurrentFrequency | MaxFrequency | Manufacturer | Size | PartNumber
-----+-----+-----+-----+-----+-----+-----+
DIMM1G1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM1H1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM1E1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM1F1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM1C1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM1D1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM1A1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM1B1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM2G1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM2H1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM2E1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM2F1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM2C1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM2D1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM2A1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
DIMM2B1 | 2666MHz | 2933MHz | Samsung | 32GB | M393A4K40CB2-CVF
Memory Slot (Total) : 32
Memory Slot (Unused) : 16
Memory Slot (Available) : 16

Minimal BASH-like line editing is supported. For the first word, TAB lists possible command completions. Anywhere
else TAB lists possible device or file completions.

grub>

```

**Steps**

1. Format the OS installation disk.
2. Reinstall the OS, and then check whether the fault is removed.
  - Yes → End.
  - No → [Step 3](#).
3. Contact NETAS technical support.

## 4.11 SNMP Link Check

**Problem**

This procedure describes how to check whether the [SNMP](#) link is proper on the installation [PC](#).

**Steps**

1. Verify that the SNMP service is enabled and SNMP parameters are correctly configured.
2. In the [CLI](#), enter the installation path of the UniKits, for example, *D:\Program Files (x86)\Unikits\Unikits\bin*.
3. Run the corresponding command as required to check whether the SNMP link is proper.
  - If SNMPv2c is used, run the following command.
 

```
.\snmpwalk.exe -v 2c -c <read-only community> <IP address>:161
1.3.6.1.4.1.3902.6053.19.1.3.2.1.1.4.
```

```
.\snmpwalk.exe -v 2c -c <read-write community> <IP address>:161
1.3.6.1.4.1.3902.6053.19.1.3.2.1.1.4.
```

If the command output is as shown in [Figure 4-5](#) and [Figure 4-6](#), the SNMP link is operating properly. Otherwise, the SNMP link is not operating properly.

**Figure 4-5 Normal SNMP Link Using the SNMPv2c Protocol—Example 1**

```
D:\workspace\UniKits_Feature\SAc-568952\UniKits\tools\version\windows\bin>.\snmpwalk.exe -v 2c -c zte_public 10.239.226.147:161 1.3.6.1.4.1.3902.6053.19.1.3.2.1.1.4.0
MIB search path: c:/user/share/snmp/mibs
Cannot find module (SNMPv2-MIB): At line 0 in (none)
Cannot find module (IF-MIB): At line 0 in (none)
Cannot find module (IP-MIB): At line 0 in (none)
Cannot find module (TCP-MIB): At line 0 in (none)
Cannot find module (UDP-MIB): At line 0 in (none)
Cannot find module (SNMP-VIEW-BASED-ACM-MIB): At line 0 in (none)
Cannot find module (SNMP-COMMUNITY-MIB): At line 0 in (none)
Cannot find module (DISMAN-EVENT-MIB): At line 0 in (none)
iso.3.6.1.4.1.3902.6053.19.1.3.2.1.1.4.0 = STRING: "R5300 G4"

Statistics:
RTT(min/avg/max):0.000000/0.000000/0.000000
RTT distribution:
 0-10ms   10-50ms   50-100ms  100-500ms  500-1000ms 1-2s      2-3s      >3s
 0          0          0          0          0          0          0          0
Total traversal time = 1.600000 seconds
```

**Figure 4-6 Normal SNMP Link Using the SNMPv2c Protocol—Example 2**

```
D:\workspace\F_Tool\支持69G5\UniKits\tools\version\windows\bin>.\snmpwalk.exe -v 2c -c platform 10.237.21.222:161 1.3.6.1.4.1.3902.6053.19.1.3.2.1.1.4.0
MIB search path: c:/user/share/snmp/mibs
Cannot find module (SNMPv2-MIB): At line 0 in (none)
Cannot find module (IF-MIB): At line 0 in (none)
Cannot find module (IP-MIB): At line 0 in (none)
Cannot find module (TCP-MIB): At line 0 in (none)
Cannot find module (UDP-MIB): At line 0 in (none)
Cannot find module (SNMP-VIEW-BASED-ACM-MIB): At line 0 in (none)
Cannot find module (SNMP-COMMUNITY-MIB): At line 0 in (none)
Cannot find module (DISMAN-EVENT-MIB): At line 0 in (none)
iso.3.6.1.4.1.3902.6053.19.1.3.2.1.1.4.0 = STRING: "R5300 G4"

Statistics:
RTT(min/avg/max):0.000000/0.000000/0.000000
RTT distribution:
 0-10ms   10-50ms   50-100ms  100-500ms  500-1000ms 1-2s      2-3s      >3s
 0          0          0          0          0          0          0          0
Total traversal time = 0.525000 seconds
```

- If SNMPv3 is used, run the following command.

```
.\snmpwalk.exe -v 3 -u NETA$root -a MD5 -A Superuser9! -l authPriv
-x DES -X Superuser9! <IP address>:161
1.3.6.1.4.1.3902.6053.19.1.3.2.1.1.4.0
```

If the command output is as shown in [Figure 4-7](#), the SNMP link is operating properly. Otherwise, the SNMP link is not operating properly.

**Figure 4-7 Example of Proper SNMP Link When SNMPv3 Is Used**

```
D:\Users\10281390\Download\bmc_tools\Windows>.\snmpwalk.exe -v 3 -u zteroot -a MD5 -A Superuser9! -l authPriv -x DES -X
Superuser9! 10.239.226.147:161 1.3.6.1.4.1.3902.6053.19.1.3.2.1.1.4.0
MIB search path: c:/user/share/snmp/mibs
Cannot find module (SNMPv2-MIB): At line 0 in (none)
Cannot find module (IF-MIB): At line 0 in (none)
Cannot find module (IP-MIB): At line 0 in (none)
Cannot find module (TCP-MIB): At line 0 in (none)
Cannot find module (UDP-MIB): At line 0 in (none)
Cannot find module (SNMP-VIEW-BASED-ACM-MIB): At line 0 in (none)
Cannot find module (SNMP-COMMUNITY-MIB): At line 0 in (none)
Cannot find module (DISMAN-EVENT-MIB): At line 0 in (none)
iso.3.6.1.4.1.3902.6053.19.1.3.2.1.1.4.0 = STRING: "R5300 G4"

Statistics:
RTT(min/avg/max):0.000000/0.000000/0.000000
RTT distribution:
 0-10ms   10-50ms   50-100ms  100-500ms  500-1000ms 1-2s      2-3s      >3s
 0          0          0          0          0          0          0          0
Total traversal time = 0.667000 seconds
```

**Note**

The above commands are used to check the device type and can also be used to verify whether the SNMP link is operating properly.

## 4.12 Failure in the Standard Card Firmware Upgrade, In-Band RAID Configuration, or Out-of-Band Stress Test

### Symptom

An error is reported during the standard card firmware upgrade, in-band **RAID** configuration, or out-of-band stress test. Two common symptoms are as follows:

- Symptom 1: When the standard card firmware upgrade, in-band RAID configuration, or out-of-band stress test is performed on the server whose **BMC** version is V3, the image file fails to be mounted, and the following error message is reported:

```
mount iso image by redfish fail: Redfish interface execution error (error code: 400)
```

- Symptom 2: Fails when the execution progress reaches 40%.

### Steps

#### Solutions for Symptom 1

1. On a PC where the UniKits is installed, enable the **SMB** or **CIFS** sharing function, and restart the PC to apply the configuration.  
For details, refer to [5 Reference: Enabling the SMB/CIFS File Sharing Function](#).
2. During the operation, set **Share Server User** to the local administrator account or domain administrator account, instead of the online Microsoft account.
3. On the PC where the UniKits is installed, disable the firewall and antivirus software.
4. Check the switch port to ensure that the **IPMI**, **SSH**, **SNMP**, and Redfish links between the PC (with the installed UniKits) and the target server are normal and the L3 network can be crossed.

For the default ports of the IPMI, SSH, SNMP, Redfish, SMB, and CIFS services, refer to [Table 4-1](#).

**Table 4-1 Default Port Descriptions**

Service Type	Default Port Number
IPMI	623
SSH	22

SSH (Host Connected)	2222
SNMP	161
<b>Service Type</b>	<b>Default Port Number</b>
BMC Web Interface (Redfish)	443
SMB	139
CIFS	445

5. If the operation still fails, add a local administrator and use the account to perform the operation.

### Solutions for Symptom 2

1. Perform the following operations as required.

To...	Do...
Upgrade the standard card firmware	Use the ISO image file from the firmware package to upgrade the firmware by mounting the file through <a href="#">KVM</a> .
Configure in-band RAID	Re-execute the operation.
Conduct an out-of-band stress test	Re-execute the operation.

## 4.13 Operation Suggestions for Common Errors

For operation suggestions for common errors in the UniKits, refer to [Table 4-2](#).

**Table 4-2 Operation Suggestions for Common Errors**

Error Type	Operation Suggestions
<a href="#">IPMI link error</a>	<ol style="list-style-type: none"> <li>1. Check whether the network connection is proper. For example, run the <code>ping</code> command to check connectivity.</li> <li>2. Check whether the username and password are correct.</li> <li>3. Check whether the IPMI link is proper. For details, refer to "<a href="#">4.4 IPMI Link Error</a>".</li> <li>4. (Optional) If the fault persists, contact NETAS technical support.</li> </ol>

SNMP link error	<ol style="list-style-type: none"> <li>1. Check whether the network connection is proper. For example, run the <b>ping</b> command to check connectivity.</li> <li>2. On the Web portal of the BMC of the server, check whether the SNMP service is enabled and whether the SNMP port number is correct.</li> <li>3. Check whether the SNMP link is proper. For details, refer to "<a href="#">4.11 SNMP Link Check</a>".</li> <li>4. Check whether the read-only community and read-write community are configured correctly. For how to view the read-only community and readwrite community, refer to <a href="#">3.2.1 Manually Adding a BMC</a>.</li> <li>5. (Optional) If the fault persists, contact NETAS technical support.</li> </ol>
-----------------	---

Error Type	Operation Suggestions
Internal SNMP error	<ol style="list-style-type: none"> <li>1. Check whether the SNMP link is proper. For details, refer to "<a href="#">4.11 SNMP Link Check</a>".</li> <li>2. (Optional) If the fault persists, contact NETAS technical support.</li> </ol>
HTTP network connection error	<ol style="list-style-type: none"> <li>1. Check whether the network connection is proper. For example, run the <b>ping</b> command to check connectivity.</li> <li>2. Try to log in to the Web portal of the BMC of the server.</li> <li>3. (Optional) If the fault persists, contact NETAS technical support.</li> </ol>
SSH link error	<ol style="list-style-type: none"> <li>1. Check whether the network connection is proper. For example, run the <b>ping</b> command to check connectivity.</li> <li>2. On the Web portal of the BMC of the server, check whether the SSH service is enabled and whether the SSH port number is correct.</li> <li>3. Try to log in to the BMC of the server through SSH.</li> <li>4. (Optional) If the fault persists, contact NETAS technical support.</li> </ol>
Redfish interface execution error	<p>In accordance with the operation type, select the corresponding handling method:</p> <ul style="list-style-type: none"> <li>● If the ISO file fails to be mounted during the following operations, refer to "<a href="#">4.5 ISO File Mounting Failure</a>". → Standard card or disk firmware upgrade → In-band RAID configuration → Stress test</li> <li>● If the BIOS configuration function fails to be implemented, check whether the BMC version of the configured server meets the BMC version requirements of the UniKits.       <ul style="list-style-type: none"> <li>→ If not, upgrade the BMC version of the server and then configure the BIOS.</li> <li>→ If yes, contact NETAS technical support.</li> </ul> </li> <li>● If other functions fail to be implemented, contact NETAS technical support.</li> </ul>

# Chapter 5

## Reference: Enabling the SMB/CIFS File Sharing Function

---

### Abstract

This procedure describes how to enable the **SMB/CIFS** file sharing function in the OS on the installation **PC**. In this way, the in-band functions can be implemented in the UniKits.

The operation of enabling the SMB/CIFS sharing function in the Windows 7 OS is different from that in the Windows 10 OS.

### Steps

- Enabling the SMB/CIFS File Sharing Function in the Windows 7 OS
  1. Select **Control Panel > Network and Internet > Network and Sharing Center**. The **Network and Sharing Center** window is displayed.
  2. Click **Change advanced sharing settings**. The **Change advanced sharing settings** window is displayed.
  3. Perform advanced sharing settings in accordance with the actual network configuration scenarios (home or work, public, and domain). If you are not sure about the network configuration scenarios, turn on **Network discovery**, **File and printer sharing**, and **Public folder sharing**.
  4. Click **Save changes**.
- Enabling the SMB/CIFS File Sharing Function in the Windows 10 OS
  1. Select **Start > Settings > Network and Internet > Network and Sharing Center**. The **Network and Sharing Center** window is displayed.
  2. Click **Change advanced sharing settings**. The **Change advanced sharing settings** window is displayed.

3. In accordance with the actual network configuration scenarios (Private, Guest or Public, Domain, and All networks), select **Turn on network discovery** and **Turn on file and printer sharing**.

**Note**

If you are not sure about the current network configuration, enable the sharing function in the above four scenarios.

4. Click **Save changes**.
5. Use either of the following ways to enable the SMB/CIFS file sharing function:  
→ Select **Control Panel > Programs > Programs and Features > Turn Windows features on or off**, and select the corresponding items, and click **OK**. → Run the following commands to enable the SMB/CIFS file sharing function.

```
dism /online /enable-feature /featurename:SMB1Protocol
dism /online /enable-feature /featurename:SMB1Protocol-Client
dism /online /enable-feature /featurename:SMB1Protocol-Server
```

6. Restart the system to apply the configuration.

# Figures

---

Figure 2-1 Network Architecture.....	4
Figure 2-2 Installing the UniKits.....	6
Figure 2-3 Selecting an Installation Path.....	7
Figure 3-1 Logging In to the UniKits.....	10
Figure 3-2 Welcome to Unikits Page.....	11
Figure 3-3 Quick Start Page—Guest User.....	11
Figure 3-4 Switch User Dialog Box.....	12
Figure 3-5 Welcome to UniKits Page.....	12
Figure 3-6 Quick Start Page—Administrator.....	13
Figure 3-7 Manually Adding the BMC of a G5 Server.....	16
Figure 3-8 Manually Adding the BMC of a Server in the SNMPv2 Scenario.....	18
Figure 3-9 Manually Adding the BMC of a Server in the SNMPv3 Scenario.....	21
Figure 3-10 Adding BMCs Through Auto-Scan.....	25
Figure 3-11 Adding BMCs in Batches.....	26
Figure 3-12 Manually Adding a Host.....	32
Figure 3-13 Adding Hosts Through Auto-Scan.....	34
Figure 3-14 Adding Hosts in Batches.....	35
Figure 3-15 BMC Network Config Page.....	39
Figure 3-16 Port and DNS Configuration Tab.....	44
Figure 3-17 Port and DNS Configuration Tab.....	46
Figure 3-18 Port and DNS Configuration Tab.....	47

Figure 3-19 BMC Config Page.....	49
Figure 3-20 Configuring BMC V3.....	50
Figure 3-21 Startup Mode Config Area.....	50
Figure 3-22 Configuring BMC V3.....	52
Figure 3-23 User Config Area.....	52
Figure 3-24 Configuring BMC V3.....	54
Figure 3-25 Time Config Area.....	55
Figure 3-26 Configuring BMC V3.....	57
Figure 3-27 SNMP Config Area.....	58
Figure 3-28 Configuring BMC V3.....	60
Figure 3-29 Alarm Config Area.....	61
Figure 3-30 Configuring BMC V3.....	64
Figure 3-31 Log Config Area.....	64
Figure 3-32 Configuring BMC V3.....	66
Figure 3-33 Asset Tag Config Area.....	66
Figure 3-34 Configuring BMC V3.....	68
Figure 3-35 Host Name Config Area.....	68
Figure 3-36 Configuring BMC V3.....	70
Figure 3-37 Fan Mode Config Area.....	70
Figure 3-38 Configuring BMC V3.....	72
Figure 3-39 Power Restore Policy Config Area.....	72
Figure 3-40 Configuring BMC V3.....	74
Figure 3-41 Security Config Area.....	75

Figure 3-42 Configuring BMC V3.....	76
Figure 3-43 Service Config Area.....	77
Figure 3-44 Configuring BMC V3.....	80
Figure 3-45 LDAP\AD Config Area.....	81
Figure 3-46 Configuring BMC V3.....	84
Figure 3-47 Configuration Migration Area.....	85
Figure 3-48 Configuring BMC V3.....	86
Figure 3-49 Power Redundancy Config Area.....	87
Figure 3-50 Configuring the BMC V3.....	88
Figure 3-51 Firewall Policy Config Page.....	89
Figure 3-52 BMC Config Page.....	91
Figure 3-53 Configuring BMC V4.....	92
Figure 3-54 Configuring BMC V4.....	94
Figure 3-55 Configuring BMC V4.....	95
Figure 3-56 Configuring BMC V4.....	98
Figure 3-57 Configuring BMC V4.....	101
Figure 3-58 Configuring BMC V4.....	103
Figure 3-59 Configuring BMC V4.....	106
Figure 3-60 Configuring BMC V4.....	110
Figure 3-61 Configuring the BMC V4.....	112
Figure 3-62 Configuring BMC V4.....	114
Figure 3-63 Configuring BMC V4.....	115
Figure 3-64 BIOS Config Page—General Configuration Items.....	117
Figure 3-65 BIOS Config Page.....	122

Figure 3-66 BIOS Config Page.....	123
Figure 3-67 Outband Raid Config Tab—Manual Mode.....	125
Figure 3-68 Outband Raid Config—Import from Local.....	127
Figure 3-69 Inband Raid Config Tab.....	129
Figure 3-70 Check Configuration Page.....	132
Figure 3-71 Check Configuration Page.....	135
Figure 3-72 Check Configuration Page.....	138
Figure 3-73 Command Config Page.....	140
Figure 3-74 Power Ctrl Page.....	142
Figure 3-75 PXE Batch Config Page.....	144
Figure 3-76 Warning Dialog Box.....	145
Figure 3-77 OS Install Page.....	146
Figure 3-78 OS Install Page.....	150
Figure 3-79 General Firmware Update Page.....	153
Figure 3-80 Firmware Upgrade File Selected.....	154
Figure 3-81 Firmware Upgrade File Uploaded.....	154
Figure 3-82 Advanced Information Displayed.....	156
Figure 3-83 Warning Dialog Box.....	157
Figure 3-84 Pcie/Disk Firmware Page.....	158
Figure 3-85 OutBand Inspect Page.....	160
Figure 3-86 InBand Inspect Page.....	162
Figure 3-87 Asset Collection Page.....	164
Figure 3-88 Asset Acceptance Tab.....	165
Figure 3-89 Viewing Asset Acceptance Parameters—1.....	166

Figure 3-90 Viewing Asset Acceptance Parameters—2.....	166
Figure 3-91 Asset Acceptance Tab.....	168
Figure 3-92 Online Mode Tab.....	169
Figure 3-93 Log Analysis Config Dialog Box.....	170
Figure 3-94 Offline Mode Tab.....	172
Figure 3-95 Collect HOST Log Page.....	173
Figure 3-96 Device Replace Page.....	175
Figure 3-97 Server Configurations Obtained.....	175
Figure 3-98 Programming a UUID and Serial Number.....	176
Figure 3-99 Stress Test Page—General Stress Test.....	177
Figure 3-100 Stress Test Page—Customized Stress Test.....	178
Figure 3-101 UID Setting Page.....	181
Figure 3-102 Alarm Clear Page.....	182
Figure 3-103 Hard Disk Failure Prediction Page.....	183
Figure 3-104 MEMORY Log Collection Page.....	184
Figure 3-105 Optical Module Failure Prediction Page.....	185
Figure 3-106 Local User Page.....	186
Figure 3-107 Add User Dialog Box.....	187
Figure 3-108 Add Role Group Dialog Box.....	189
Figure 3-109 LDAP Setting Page.....	190
Figure 3-110 Add LDAP Configuration Dialog Box.....	191
Figure 3-111 License Mgmt Page.....	193
Figure 3-112 License Imported.....	194
Figure 3-113 Log Mgmt Page.....	195

Figure 3-114 Export Log Dialog Box.....	196
Figure 3-115 Runtime Log Tab.....	196
Figure 3-116 About Page.....	197
Figure 3-117 Task Schedule Page.....	197
Figure 3-118 Creating a Task Schedule.....	198
Figure 3-119 Task List Page.....	199
Figure 3-120 Viewing the Task Execution Information.....	200
Figure 4-1 Installation Dialog Box.....	202
Figure 4-2 Fatal error detected Dialog Box—1.....	210
Figure 4-3 Fatal error detected Dialog Box—2.....	211
Figure 4-4 Grub Screen.....	212
Figure 4-5 Normal SNMP Link Using the SNMPv2c Protocol—Example 1.....	213
Figure 4-6 Normal SNMP Link Using the SNMPv2c Protocol—Example 2.....	213
Figure 4-7 Example of Proper SNMP Link When SNMPv3 Is Used.....	213

## Tables

---

Table 1-1 O&M Function Descriptions.....	1
Table 2-1 Default Ports of Common Services.....	5
Table 3-1 Quick Start Page Descriptions.....	13
Table 3-2 Parameter Descriptions for Manually Adding the BMC of a G5 Server..	16
Table 3-3 Parameter Descriptions for Manually Adding the BMC of a Server in the SNMPv2 Scenario.....	18
Table 3-4 Parameter Descriptions for Manually Adding the BMC of a Server in the SNMPv3 Scenario.....	21
Table 3-5 Parameter Descriptions for Adding BMCs Through Auto-Scan.....	25

Table 3-6 Parameter Descriptions for the BMC Configuration Template.....	27
Table 3-7 Parameter Descriptions for Manually Adding a Host.....	32
Table 3-8 Parameter Descriptions for Adding Hosts Through Auto-Scan.....	34
Table 3-9 Parameter Descriptions for the Host Configuration Template.....	36
Table 3-10 Descriptions of BMC IP Configuration Scenarios.....	37
Table 3-11 IP Configuration Parameter Descriptions.....	39
Table 3-12 Configuration Template Descriptions.....	41
Table 3-13 Parameter Descriptions for Configuring a Network Port.....	44
Table 3-14 Parameter Descriptions for Network Port Bonding.....	46
Table 3-15 DNS Parameter Descriptions.....	48
Table 3-16 Boot Option Parameter Descriptions.....	51
Table 3-17 Time Zone Parameter Descriptions.....	56
Table 3-18 SNMP Parameter Descriptions.....	58
Table 3-19 Alarm Configuration Parameter Descriptions.....	61
Table 3-20 Log Parameter Descriptions.....	65
Table 3-21 Asset Tag Parameter Descriptions.....	67
Table 3-22 Parameter Descriptions for Heat Dissipation Mode.....	71
Table 3-23 Security Parameter Descriptions.....	75
Table 3-24 Service Parameter Descriptions.....	77
Table 3-25 LDAP/AD Parameter Descriptions.....	81
Table 3-26 Configuration Migration Parameter Descriptions.....	85
Table 3-27 Firewall Parameter Descriptions.....	89
Table 3-28 Boot Option Parameter Descriptions.....	92
Table 3-29 Local User Parameter Descriptions.....	94

Table 3-30 Time Zone & NTP Parameter Descriptions.....	96
Table 3-31 SNMP Parameter Descriptions.....	98
Table 3-32 Syslog Parameter Descriptions.....	101
Table 3-33 System Configuration Parameter Descriptions.....	103
Table 3-34 Port Service Parameter Descriptions.....	107
Table 3-35 Security Parameter Descriptions.....	110
Table 3-36 Firewall Parameter Descriptions.....	112
Table 3-37 Asset Tag Parameter Descriptions.....	114
Table 3-38 Host Name Parameter Descriptions.....	115
Table 3-39 BIOS Parameter Descriptions—General Configuration Items.....	117
Table 3-40 Parameter Descriptions for Selecting a Template Server.....	122
Table 3-41 Parameter Descriptions for Importing a BIOS Configuration File.....	124
Table 3-42 Parameter Descriptions for Manually Performing Out-of-Band RAID Configuration.....	125
Table 3-43 Parameter Descriptions for Importing a Local Configuration File.....	127
Table 3-44 Parameter Descriptions for Performing In-band RAID Configuration.	129
Table 3-45 Parameter Descriptions for Configuration Check Through a Template Server.....	132
Table 3-46 Parameter Descriptions for Performing a Configuration Check Based on a Check File.....	135
Table 3-47 Parameter Descriptions for Performing a Configuration Check Based on a Customized File.....	138
Table 3-48 Command Parameter Descriptions.....	140
Table 3-49 Parameter Descriptions for Installing a Linux OS.....	147
Table 3-50 Parameter Descriptions for Installing a Windows OS.....	150
Table 3-51 BIOS Firmware Upgrade Policy for a G2, G4, or G4X Server Model.	155

Table 3-52 BIOS Firmware Upgrade Policy for a G5 Server Model.....	155
Table 3-53 Upgrade Parameter Descriptions.....	156
Table 3-54 Parameter Descriptions for Upgrading Standard Cards and Hard Disk Firmware.....	158
Table 3-55 Parameter Descriptions for Out-of-Band Inspection.....	160
Table 3-56 Parameter Descriptions for Performing In-Band Inspection.....	162
Table 3-57 Asset Collection Parameter Descriptions.....	164
Table 3-58 Parameter Descriptions for Log Analysis in Online Mode.....	170
Table 3-59 Parameter Descriptions for Log Analysis in Offline Mode.....	172
Table 3-60 Parameter Descriptions for General Stress Tests.....	178
Table 3-61 Parameter Descriptions for Customized Stress Tests.....	179
Table 3-62 UID Indicator Parameter Descriptions.....	181
Table 3-63 Parameter Descriptions for Clearing Historical BMC Alarms.....	182
Table 3-64 Parameter Descriptions for Hard Disk Fault Prediction.....	184
Table 3-65 Parameter Descriptions for Adding a Local User.....	187
Table 3-66 Role Group Parameter Descriptions.....	189
Table 3-67 LDAP Configuration Parameter Descriptions.....	191
Table 3-68 Parameter Descriptions for Creating a Task Schedule.....	198
Table 4-1 Default Port Descriptions.....	214
Table 4-2 Operation Suggestions for Common Errors.....	215

# Glossary

---

## **AD**

- Active Directory

## **AES**

- Advanced Encryption Standard

## **BIOS**

- Basic Input/Output System

## **BMC**

- Baseboard Management Controller

## **CD**

- Compact Disk

## **CIFS**

- Common Internet File System

## **CLI**

- Command Line Interface

## **CN**

- Common Name

## **CPU**

- Central Processing Unit

## **CentOS**

- Community Enterprise Operating System

## **DC**

- Domain Controller

## **DES**

- Data Encryption Standard

**DMA**

- Direct Memory Access

**DN**

- Distinguished Name

**DN**

- Directory Name

**DNS**

- Domain Name Server

**EPLD**

- Erasable Programmable Logic Device

**FQDN**

- Fully Qualified Domain Name

**FRU**

- Field Replaceable Unit

**GPU**

- Graphics Processing Unit

**HD**

- Hard disk

**HTTP**

- Hypertext Transfer Protocol

**HTTPS**

- Hypertext Transfer Protocol Secure

**IP**

- Internet Protocol

**IPMI**

- Intelligent Platform Management Interface

- Internet Protocol Version 4

**IPv6**

- Internet Protocol Version 6

**KVM**

- Keyboard, Video and Mouse

**KVM**

- Kernel-based Virtual Machine

**LAN**

- Local Area Network

**LDAP**

- Lightweight Directory Access Protocol

**LLDP**

- Link Layer Discovery Protocol

**MD5**

- Message Digest 5 Algorithm

**MEC**

- Mobile Edge Computing

**NCSI**

- Network Controller Sideband Interface

**NIC**

- Network Interface Card

**NMS**

- Network Management System

**NTP**

- Network Time Protocol

**NUMA**

- Non-Uniform Memory Access Architecture

**O&M**

- Operation & Maintenance

## **OEM**

- Original Equipment Manufacturer

## **OS**

- Operating System

## **OU**

- organizational unit

## **PC**

- Personal Computer

## **PCIe**

- Peripheral Component Interconnect Express

## **PSU**

- Power Supply Unit

## **PTU**

- Power/Thermal Utility

## **PXE**

- Preboot eXecution Environment

## **RAID**

- Redundant Array of Independent Disks

## **RHEL**

- Red Hat Enterprise Linux

## **SHA**

- Secure Hash Algorithm

## **SMB**

- Server Message Block

## **SNMP**

- Simple Network Management Protocol

**SR-IOV**

- Single-Root I/O Virtualization

**SSD**

- Solid State Drive

**SSDP**

- Simple Service Discovery Protocol

**SSH**

- Secure Shell

**SSL**

- Secure Sockets Layer

**TFTP**

- Trivial File Transfer Protocol

**UDP**

- User Datagram Protocol

**UEFI**

- Unified Extensible Firmware Interface

**UID**

- Unit Identification Light

**USB**

- Universal Serial Bus

**UTC**

- Universal Time Coordinated

**UUID**

- Universal Unique Identifier

**VMX**

- Virtual Machine Extension

**VNC**

- Virtual Network Console

## **VR**

- Voltage Regulator

## **ZTE**

- Zhongxing Telecommunications Equipment

## **iSAC**

- Integrated Server Administrator Controller