NETAŞ Server

UniKits

User Guide

Version: V01.24.03.01

NETAŞ TELEKOMÜNİKASYON 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

LEGAL INFORMATION

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

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

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	● BMC network configuration ● BMC configuration ● BIOS configuration ● RAID configuration ● Configuration check ● Command configuration ● Power control ● PXE-based batch configuration ● OS installation This function is an advanced function and requires a license.
Firmware upgrade	● General firmware upgrade Supported firmware: BMC, BIOS, EPLD, FRU, and VR. ● Standard card and hard disk firmware upgrade
Routine inspection	● Out-of-band inspection ● In-band inspection ● Asset collection
Troubleshooting	● Log collection ● Parts replacement ● Stress test ● UID setting

O&M Function	Sub-Function
	● Alarm clearing
Fault prediction	● This function is an advanced function and requires a license. → Hard disk fault prediction → Memory fault prediction → Optical module fault prediction

1.2 Compatibility

The following OSs 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

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.NETAŞ.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

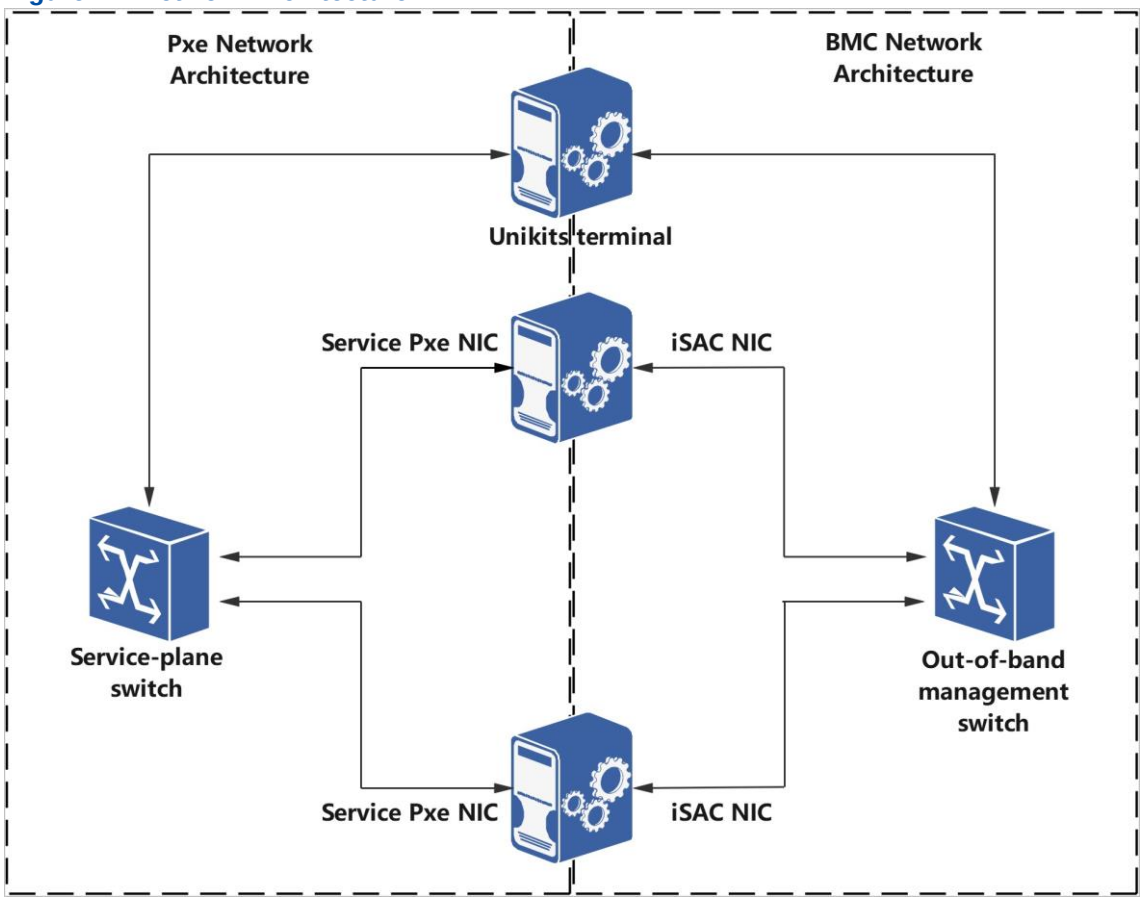
If the patch package is already installed, you can install the UniKits directly.

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

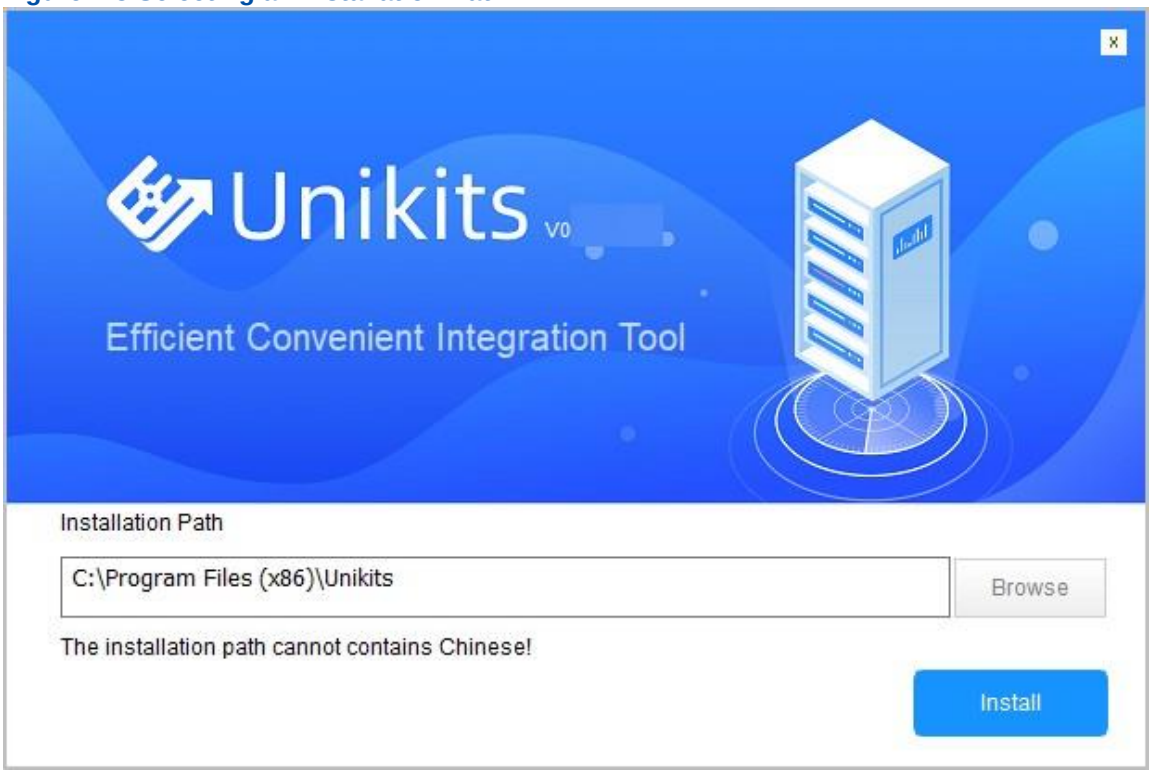
If the Firefox or Google browser is installed on the installation PC, the detection is passed.

Note

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 **Done**.
Start the UniKits	Click **Start**.

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, fin 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

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 

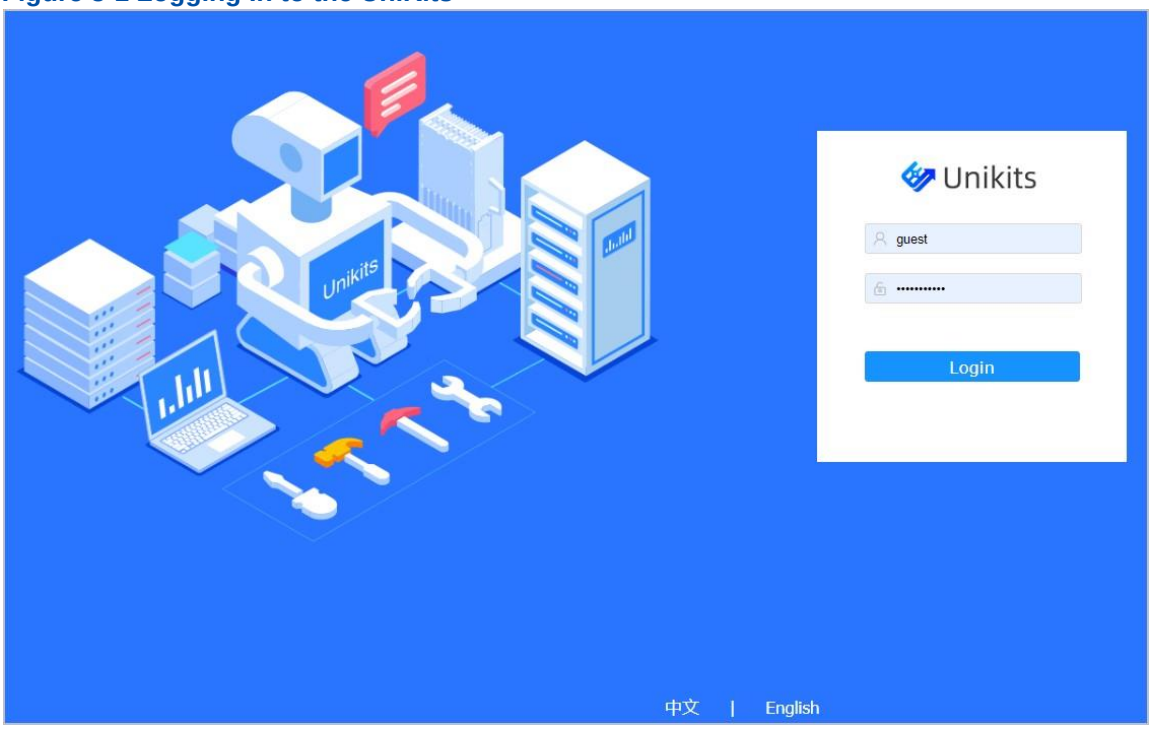
icon. The page for logging in to the UniKits is displayed, see Figure 3-1.

Note

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.

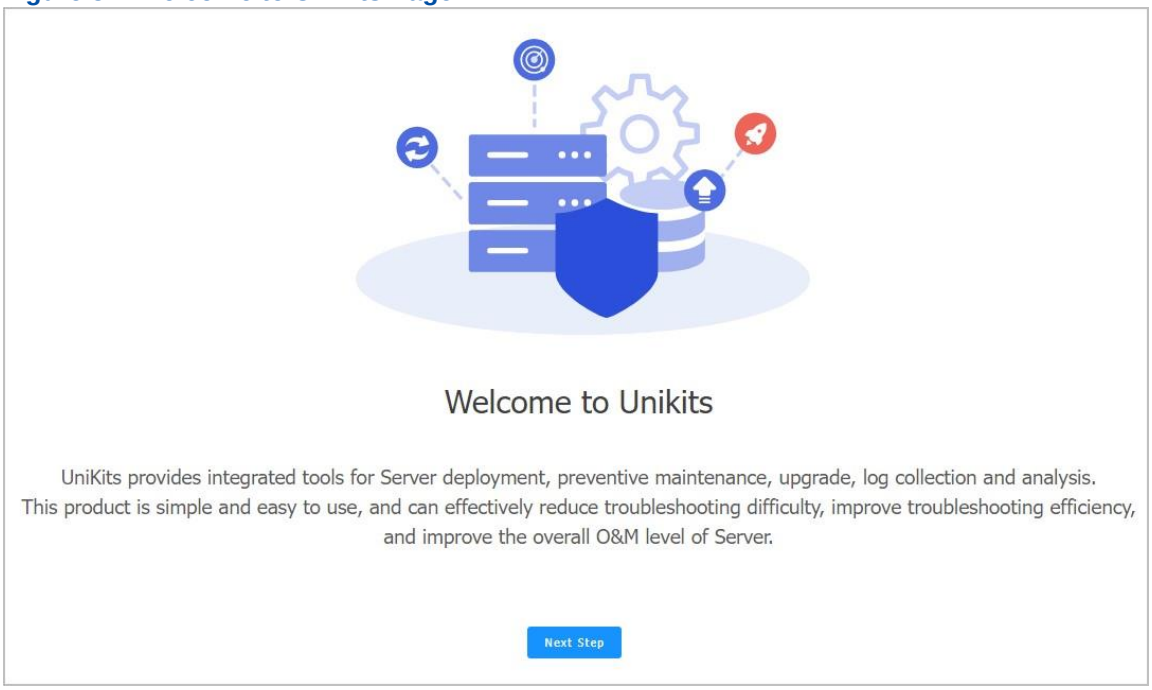
Note

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

- Username: guest
- Password: Superuser9!

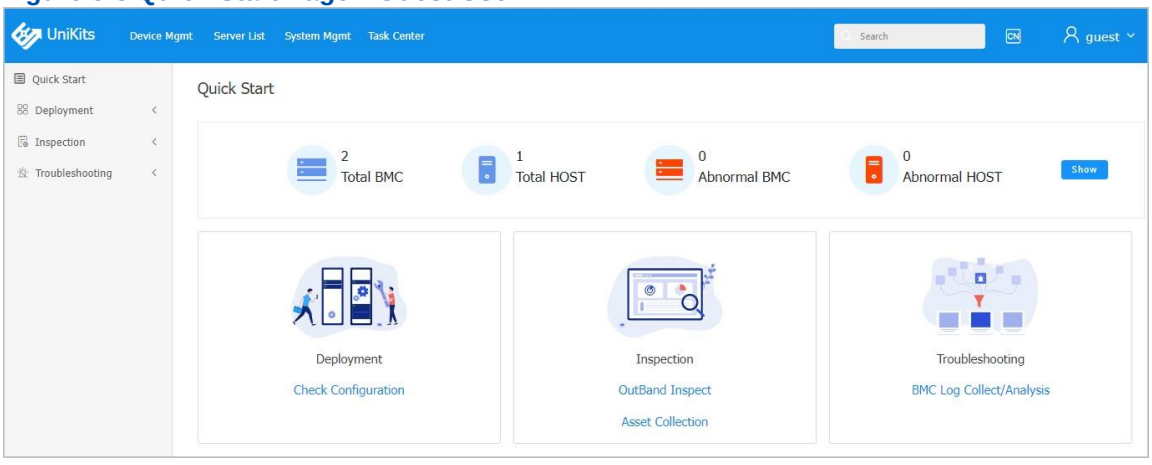
3. Click **Login**. The **Welcome to Unikits** page is displayed, see Figure 3-2.

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.

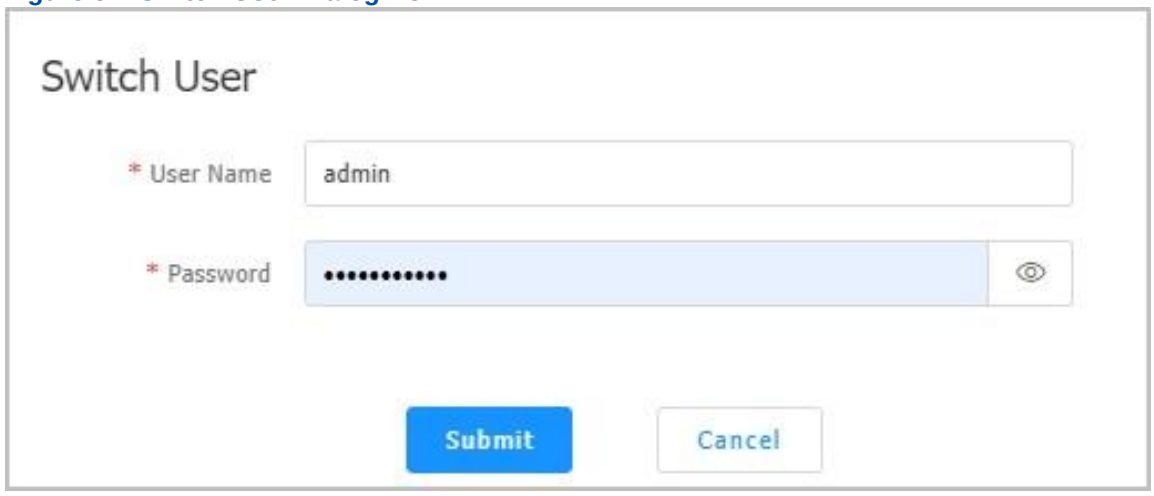
Figure 3-3 Quick Start Page—Guest User



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**.

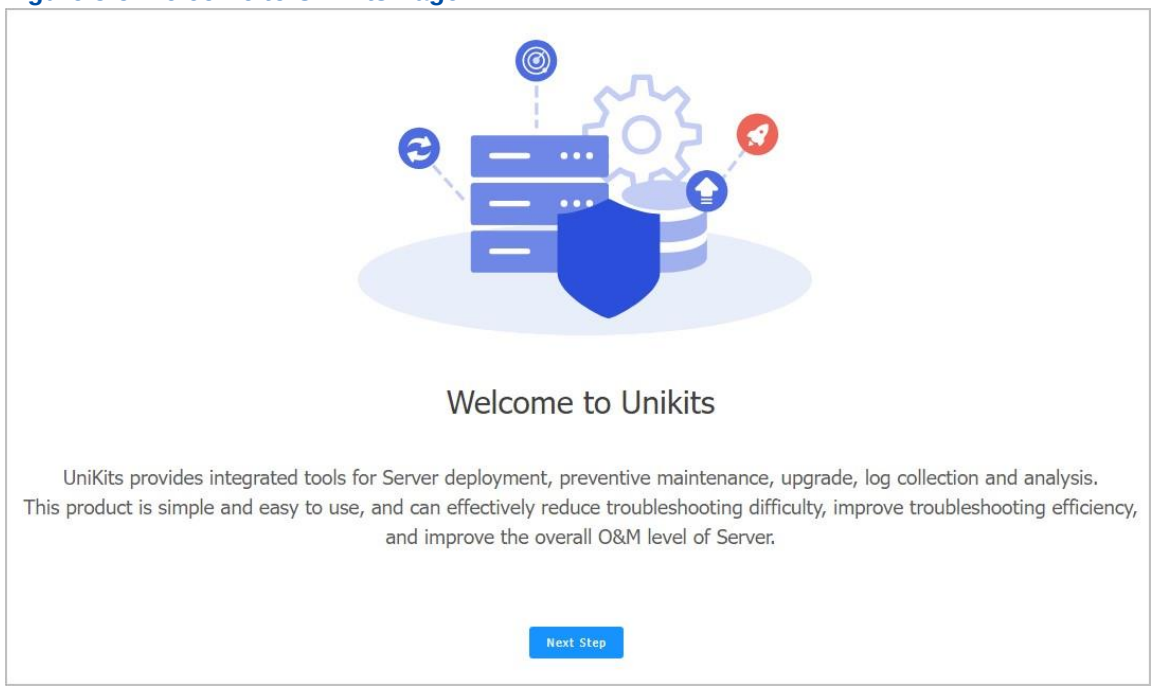
Note

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

- Username: admin
- Password: Superuser9!

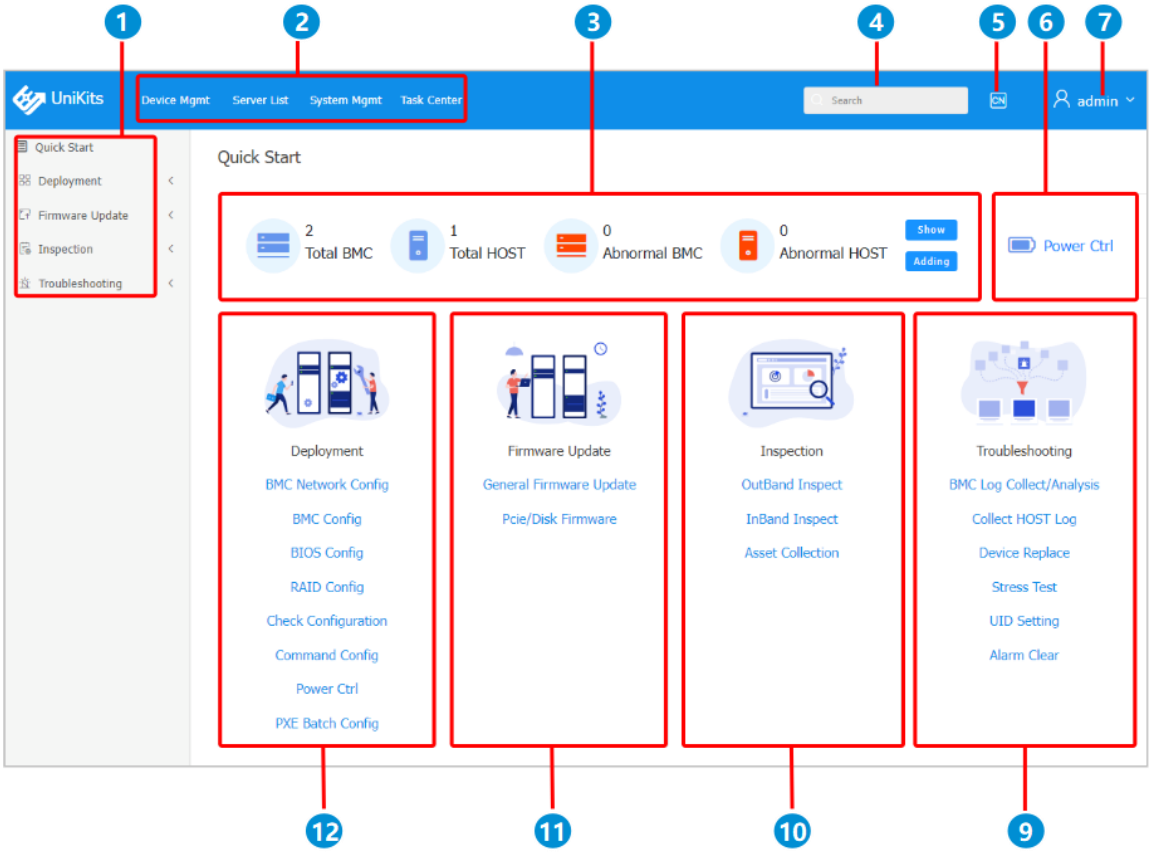
7. Click **Submit**. The **Welcome to UniKits** page is displayed, as shown in Figure 3-5.

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	Displays the overview of all the devices maintained through the UniKits. ● To view the details of all the devices, click **Show**. The **Server List** page is displayed, showing the device details. ● To add a device, click **Adding** and select the desired option from the shortcut menu. The options in the shortcut menu include: → **Adding BMC** For details, refer to "3.2 Adding a BMC". → **Add HOST** For details, refer to "3.3 Adding Hosts".
No.	**Name**	**Description**
4	Search box	Not supported.
5	Language button	Allows you to change the language.
6	Power control area	Allows you to control the power supply of device after you click **Power Ctrl** and enter the **Power Ctrl** page. For details, refer to "3.4.8 Controlling Power Supply".
7	Current user	Displays the currently logged-in user. ● To view the details of the currently logged-in user, hover the mouse cursor over this button. ● To change the password of the currently logged-in user, click **Modify Password** in the information box displayed after you hover the mouse cursor over this button. ● To switch to another user, click **Switch User** in the information box displayed after you hover the mouse cursor over this button. ● To log out the currently logged-in user, click **LogOut** in the information box displayed after you hover the mouse cursor over this button.
8	Troubleshooting area	Allows you to troubleshoot devices. For details, refer to "3.7 Troubleshooting".
9	Routine inspection area	Allows you to inspect devices. For details, refer to "3.6 Routine Inspection".
10	Firmware upgrade area	Allows you to upgrade firmware of devices. For details, refer to "3.5 Firmware Upgrade".
11	Deployment area	Allows you to deploy devices. For details, refer to "3.4 Commissioning and Deployment".

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".

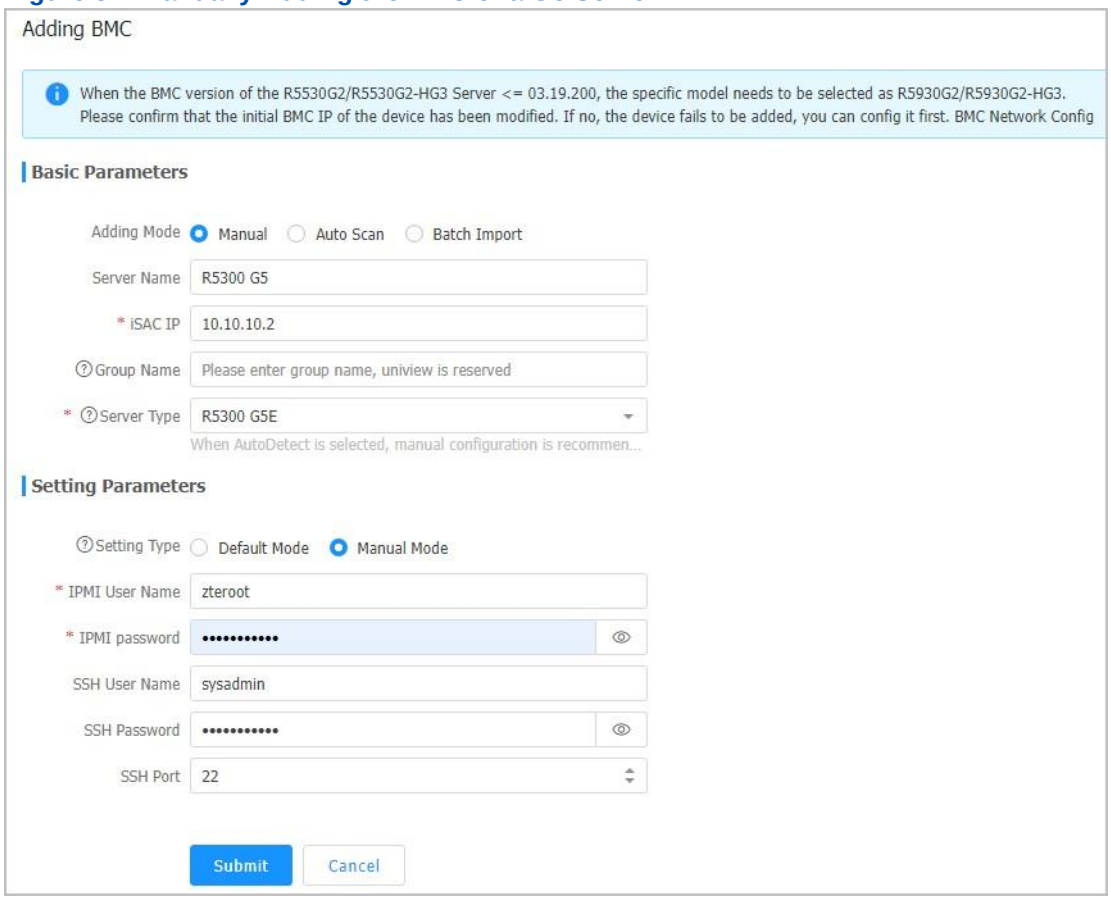
Steps

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



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

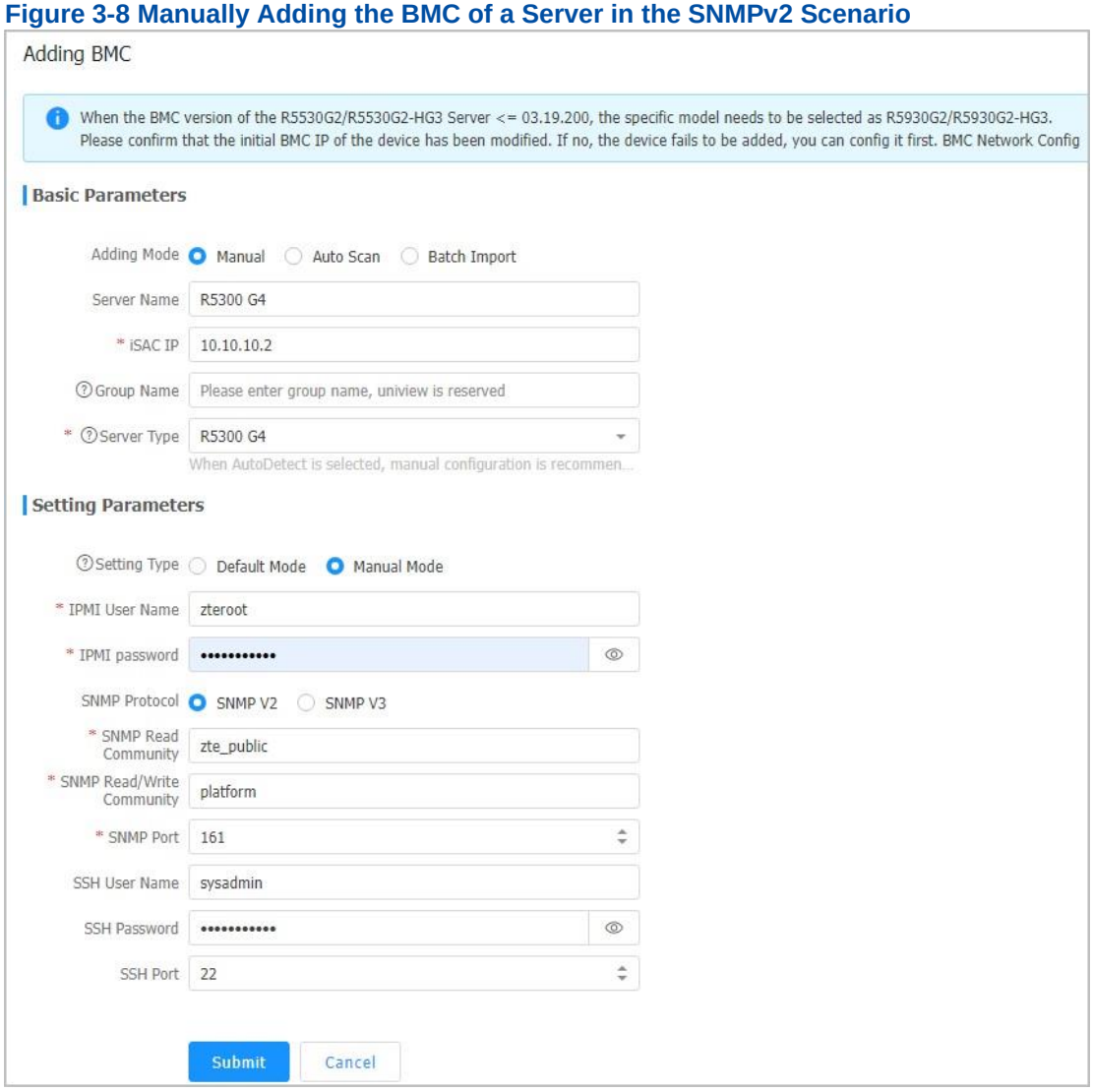
Table 3-2 Parameter Descriptions for Manually Adding the BMC of a G5 Server

Parameter	Description
Basic Parameters	
Adding Mode	Select **Manual**.
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. **uniview** is the reserved group name and you cannot use it.
Parameter	**Description**
Server Type	Select the server type. For an OEM server, select **AutoDetect**. If **Server Type** is set to **AutoDetect**, it is recommended that **Setting Type** be set to **Manual Mode**.
Setting Parameters	
Setting Type	Select a configuration mode. Options: → **Default Mode**: 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. → **Manual Mode**: 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 **User & Security > Local Users**. → For a server of other models, select **Settings > Group Management > Group Management Configuration**.
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: *sysadmin*.
SSH Password	Enter the password of the SSH user. The default password depends on the BMC version. → BMC V3: The default password is *superuser* for versions prior to V03.20.11.02, and that is *Superuser@123* for V03.20.11.02 and later. → BMC V4: The default password is *superuser* for versions prior to V04.23.01.02, and that is *Superuser@123* for V04.23.01.02 and later.
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



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
Basic Parameters	
Adding Mode	Select **Manual**.
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. **uniview** is the reserved group name and you cannot use it.
Server Type	Select the server type.

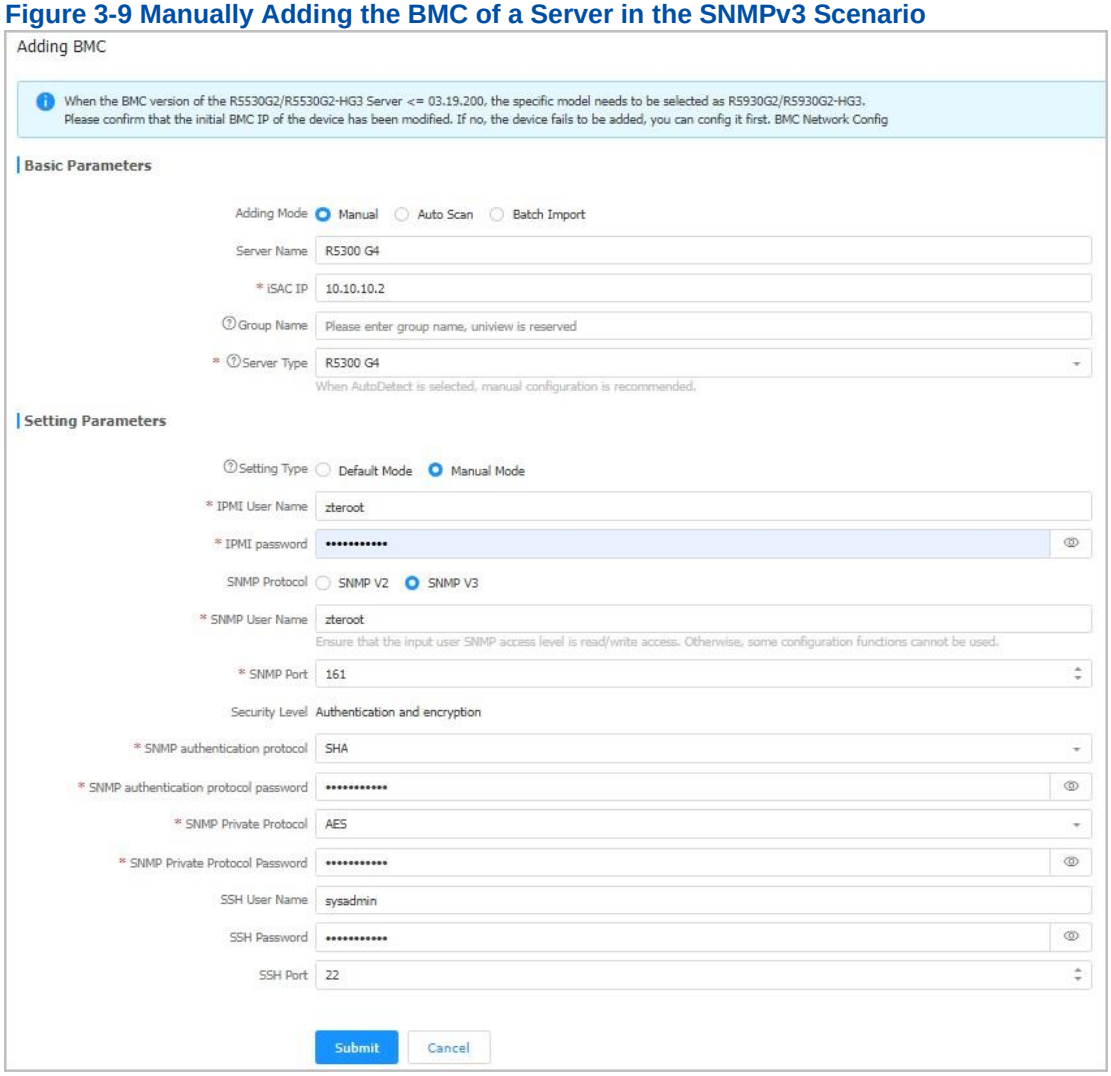
Parameter	Description
	For an OEM server, select **AutoDetect**. If **Server Type** is set to **AutoDetect**, it is recommended that **Setting Type** be set to **Manual Mode**.
Setting Parameters	
Setting Type	Select a configuration mode. Options: → **Default Mode**: The default configuration parameters of the server are used. It is recommended that this mode be used in the scenario where the parameters are not modified during commissioning. → **Manual Mode**: 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 **User & Security > Local Users**. → For a server of other models, select **Settings > Group Management > Group Management Configuration**.
IPMI password	Enter the password of the IPMI user.

SNMP Protocol	Select **SNMP V2**.
SNMP Read Community	Enter the SNMP read-only community of the server. Default: *NETAŞ_public*. For different server models, the methods for viewing the SNMP readonly community are different. → For a server of the G4X model, log in to the BMC of the server through SSH, and run the following command: **# cat /conf/snmp_users.conf** In the command output, the character string displayed next to **rocommunity** is the read-only community. → For a server of other models, log in to the Web portal of the BMC of the server, and select **Settings > SNMP Configurations > SNMP Community**.
SNMP Read/Write Community	Enter the SNMP read-write community of the server. Default: *platform*. For different server models, the methods for viewing the SNMP readwrite community are different.
Parameter	**Description**
	→ For a server of the G4X model, log in to the BMC of the server through SSH, and run the following command: **# cat /conf/snmp_users.conf** In the command output, the character string displayed next to **rwcommunity** is the read-write community. → For a server of other models, log in to the Web portal of the BMC of the server, and select **Settings > SNMP Configurations > SNMP Community**.
SNMP Port	Enter the SNMP port number of the server. You can log in to the Web portal of the BMC, and select **Settings > Services** to view the port number. Default: *161*.
SSH User Name	The UniKits communicates with the server through SSH. Enter the BMC administrator username. Default: *sysadmin*.
SSH Password	Enter the password of the SSH user. The default password depends on the BMC version. → BMC V3: The default password is *superuser* for versions prior to V03.20.11.02, and that is *Superuser@123* for V03.20.11.02 and later. → BMC V4: The default password is *superuser* for versions prior to V04.23.01.02, and that is *Superuser@123* for V04.23.01.02 and later.

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



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
Basic Parameters	
Adding Mode	Select **Manual**.
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. **uniview** is the reserved group name and you cannot use it.
Server Type	Select the server type. For an OEM server, select **AutoDetect**.

Parameter	**Description**
	If **Server Type** is set to **AutoDetect**, it is recommended that **Setting Type** be set to **Manual Mode**.
Setting Parameters	
Setting Type	Select a configuration mode. Options: → **Default Mode**: 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. → **Manual Mode**: 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 **User & Security > Local Users**. → For a server of other models, select **Settings > Group Management > Group Management Configuration**.
IPMI password	Enter the password of the IPMI user.
SNMP Protocol	Select **SNMP V3**.
SNMP User Name	Enter a username with the administrator permissions. You can log in to the Web portal of the BMC, and select **Settings > Group Management > Group Management Configuration** 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 **Settings > Services** to view the port number. Default: *161*.

Security Level	Default: **Authentication and encryption**, which does not need to be modified.
SNMP authentication protocol	Set the authentication protocol for SNMPv3. Options: MD5 and SHA . You can log in to the Web portal of the BMC, and select **Settings > Group Management > Group Management Configuration** 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.
Parameter	**Description**
SNMP Private Protocol	Set the privacy protocol for SNMPv3. Options: DES and AES. You can log in to the Web portal of the BMC, and select **Settings > Group Management > Group Management Configuration** 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: *sysadmin*.
SSH Password	Enter the password of the SSH user. The default password depends on the BMC version. → BMC V3: The default password is *superuser* for versions prior to V03.20.11.02, and that is *Superuser@123* for V03.20.11.02 and later. → BMC V4: The default password is *superuser* for versions prior to V04.23.01.02, and that is *Superuser@123* 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 **Abnormal BMC**. The **Viewing the Abnormal List** dialog box is displayed.
Modify the information about a BMC	1. Click **More** in the **Operation** column for the BMC, and select **Edit** from the shortcut menu. The **Update Server Info** dialog box is displayed. 2. Modify the information about the BMC.
To...	**Do...**
	3. Click **Submit**. Note: If any parameter other than **Server Name** and **Group Name** is modified, link diagnosis for the server is automatically triggered and the diagnosis result is updated accordingly on the page.
Refresh the information about a BMC	Click **More** in the **Operation** column for the BMC, and select **Refresh** from the shortcut menu.
Export BMC information	1. Select the desired BMCs. 2. Click **Export Server List**.
Delete BMCs	1. Select the desired BMCs. 2. Click **Remove Server**. Note: After a BMC is deleted, the deletion operation cannot be rolled back. If the BMC is needed, you can only add it again.

3.2.2 Adding BMCs Through Auto Scan

Abstract

This procedure describes how to add the BMCs 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.

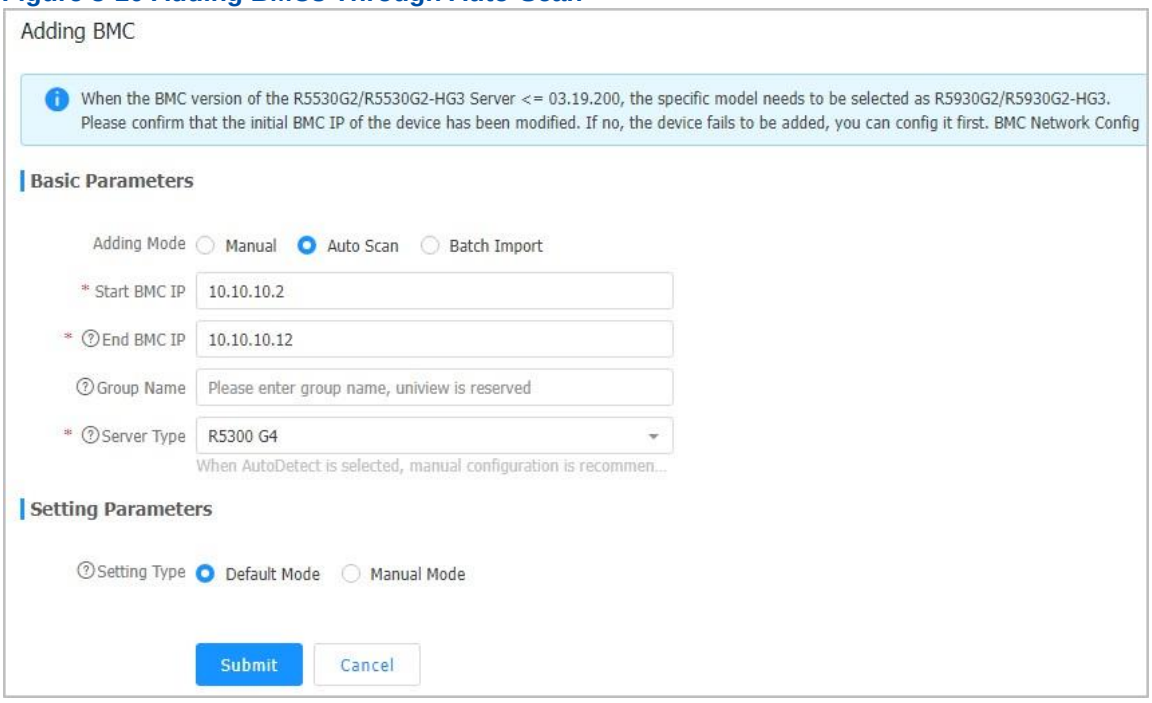
b. In the device overview area, click **Adding** and select **Adding BMC** from the shortcut menu.

- 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



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
Basic Parameters	
Adding Mode	Select **Auto Scan**.
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. **Start BMC IP** and **End BMC IP** must be in the same network segment, and **Start BMC IP** 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. **uniview** is the reserved group name and you cannot use it.
Server Type	Select the type of servers to be added. For an OEM server, select **AutoDetect**. If **Server Type** is set to **AutoDetect**, it is recommended that **Setting Type** be set to **Manual Mode**.

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.

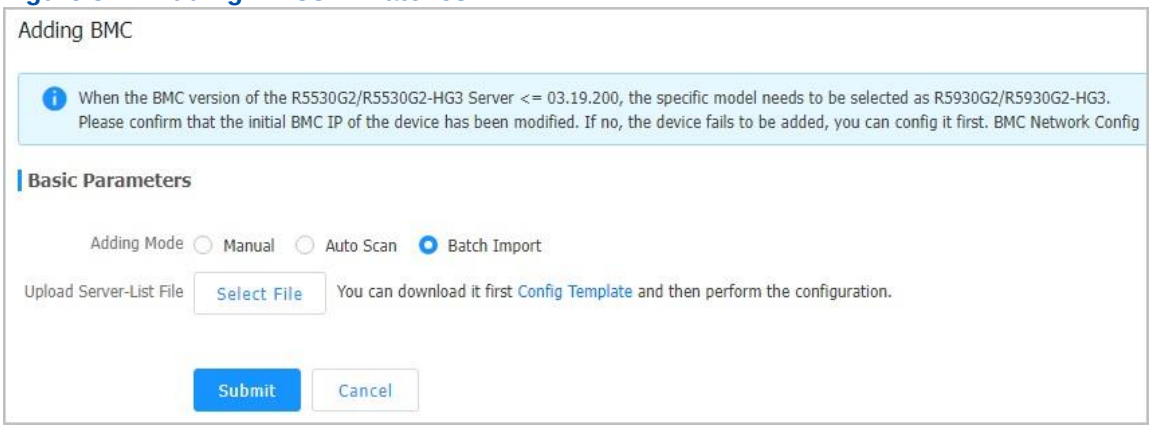
Prerequisite

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



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.

Note

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 IPv4 and IPv6.
Group	Group name.	It is recommended that you enter a rack number. **uniview** (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. ● For a server of the G5 model, view the server type on the **Homepage**. ● For a server of other models, view the server type on the **Overview** page.

ManageUser	IPMI username.	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 **User & Security > Local Users**. ● For a server of other models, select **Settings > Group Management > Group Management Configuration**. If it is left blank, the default value is used in accordance with the server model.
ManagePassword	IPMI password.	Enter the password of the IPMI user. If the password contains a symbol, add the escape character "\" before the symbol. If it is left blank, the default value is used in accordance with the server model.

Parameter	**Description**	**Setting**
SshUser	SSH username.	Enter the BMC administrator username. If it is left blank, the default value is used in accordance with the server model. Default: *sysadmin*.
SshPassword	SSH password.	Enter the password of the SSH user. If it is left blank, the default value is used in accordance with the server model. The default password depends on the BMC version. ● BMC V3: → For versions prior to V03.20.11.02, the default password is *superuser*. → For V03.20.11.02 and later, the default password is *Superuser@123*. ● BMC V4: → For versions prior to V04.23.01.02, the default password is *superuser*. → For V04.23.01.02 and later, the default password is *Superuser@123*.
SshPort	SSH port number.	Enter the SSH port number of a server. If it is left blank, the default value is used in accordance with the server model. Default: *22*.

SnmpVersion	SNMP protocol type.	Enter the SNMP version. Options: V2 and V3. If it is left blank, the default value (*V2*) 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 **Settings > Services** to view the port number. If it is left blank, the default value (*161*) is used.
SnmpReadCom-munity	SNMP read-only community.	It is valid for SNMPv2. Enter the SNMP read-only community of a server. For different server models, the methods for viewing the SNMP read-only community are different. ● For a server of the G4X model, log in to the BMC of the server through SSH, and run the following command: **# cat /conf/snmp_users.conf** In the command output, the character string displayed next to **rocommunity** is the read-only community. ● For a server of other models, log in to the Web portal of the BMC of the server, and select **Settings > SNMP Configurations > SNMP Community**. If it is left blank, the default value (*NETAŞ_public*) is used.

Parameter	Description	Setting
SnmpWriteCommunity	SNMP read-write community.	It is valid for SNMPv2. Enter the SNMP read-write community of the server. For different server models, the methods for viewing the SNMP read-write community are different. ● For a server of the G4X model, log in to the BMC of the server through SSH, and run the following command: **# cat /conf/snmp_users.conf** In the command output, the character string displayed next to **rwcommunity** is the read-write community. ● For a server of other models, log in to the Web portal of the BMC of the server, and select **Settings > SNMP Configurations > SNMP Community**. If it is left blank, the default value (*platform*) is used.
SnmpUser	SNMP username.	It is valid for SNMPv3 and required. Enter a username with the administrator permissions of the server. You can log in to the Web portal of the BMC, and select **Settings > Group Management > Group Management Configuration** to view the usernames.

SecurityLevel	Security level.	It is valid for SNMPv3 and required. Use the default value (*authPriv*).
AuthProtocol	Authentication protocol.	It is valid for SNMPv3 and required. Set the authentication protocol for SNMPv3. Options: MD5 and SHA. You can log in to the Web portal of the BMC, and select **Settings > Group Management > Group Management Configuration** 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: DES and AES . You can log in to the Web portal of the BMC, and select **Settings > Group Management > Group Management Configuration** 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.	This parameter is valid only when servers are imported in batches. Options: ● yes: indicates to check whether links are operating properly. ● no: indicates not to check whether links are operating properly. If it is set to **yes**, the link state is checked by default. If the link diagnosis fails, the involved BMC fails to be added.

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

Note

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.

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**.

3.3 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".

Note

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.

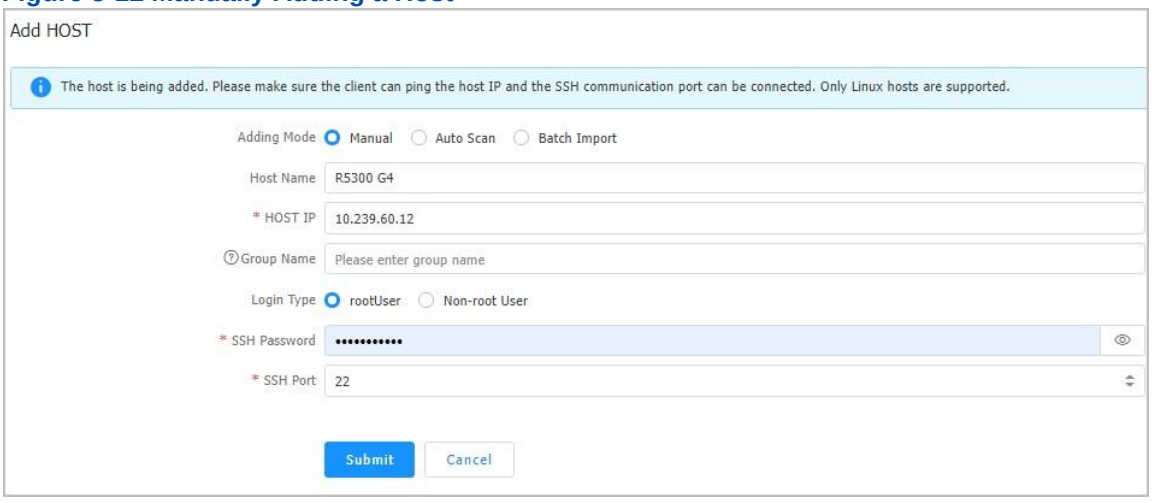
Prerequisite

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 **Manual**.
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. **uniview** is the reserved group name and you cannot use it.
Login Type		Select the way for logging in to the host. Options: ● **rootUser**: indicates to log in to the host as the *root* user. ● **Non-root User**: indicates to log in to the host as a non-root user.
rootUser	SSH Password	Enter the password to be used by the *root* 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 *root* 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 **Abnormal HOST**. The **Viewing the Abnormal List** dialog box is displayed.
Modify the information about a host	1. Click **More** in the **Operation** column for the host, and select **Edit** from the shortcut menu. The **Update Server Info** dialog box is displayed. 2. Modify the host information. 3. Click **Submit**. Note: If any parameter other than **Host Name** and **Group Name** is modified, link diagnosis for the host is automatically triggered and the diagnosis result is updated accordingly.

Refresh the information about a host	Click **More** in the **Operation** column for the host, and select **Refresh** from the shortcut menu.
Export host information	1. Select the hosts that you want to export. 2. Click **Export HOST List**.
Delete hosts	1. Select the hosts that you want to delete. 2. Click **Remove HOST**. Note: After a host is deleted, the deletion operation cannot be rolled back. If the host is needed, you can only add it again.

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.

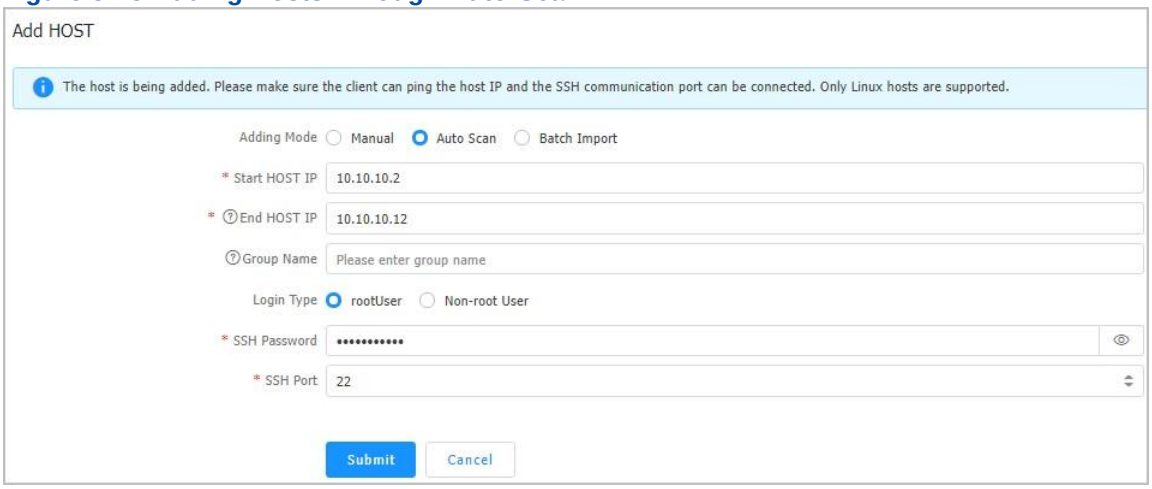
Prerequisite

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 **Auto Scan**.
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. **Start HOST IP** and **End HOST IP** must be in the same network segment, and **Start HOST IP** needs to be set first.
Group Name		Set a group name for the hosts. In this way, you can filter hosts by group name. **uniview** is the reserved group name and you cannot use it.
Login Type		Select the way for logging in to the hosts. Options: ● **rootUser**: indicates to log in to the hosts as the `root` user. ● **Non-root User**: indicates to log in to the hosts as a nonroot user.
rootUser	SSH Password	Enter the password to be used by the `root` 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 `root` 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

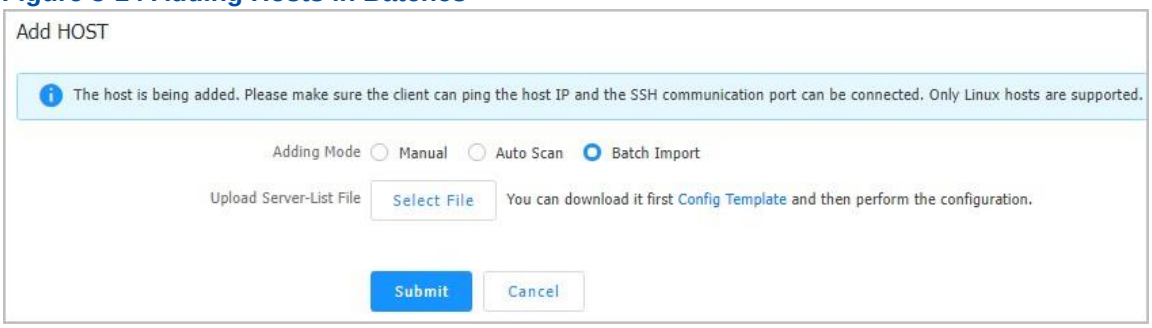
Abstract

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: IPv4 and IPv6.
SshUser	SSH username	It must be set to **root**. Otherwise, functions are affected.
SshPassword	SSH password	Enter the password to be used by the *root* 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. **uniview** (case insensitive) is the reserved group name and you cannot use it.
LinkDiag	Whether to diagnose links	It is valid only when hosts are imported in batches. Options: ● yes: indicates to check whether links are operating properly. ● no: indicates not to check whether links are operating properly. If it is set to **yes**, the link state is checked by default. If the link diagnosis fails, the involved host fails to be added.

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

Modify the default IP address of a single equipment	● The iSAC network ports of all servers to be configured must have the same factory default IP address, IPMI username and IPMI password. ● The installation PC must be directly connected to the iSAC network port of a server rather than being connected to the server through a switch or router. ● The installation PC is connected to only one server at a time. ● The installation PC can successfully ping the factory default IP address of a server.

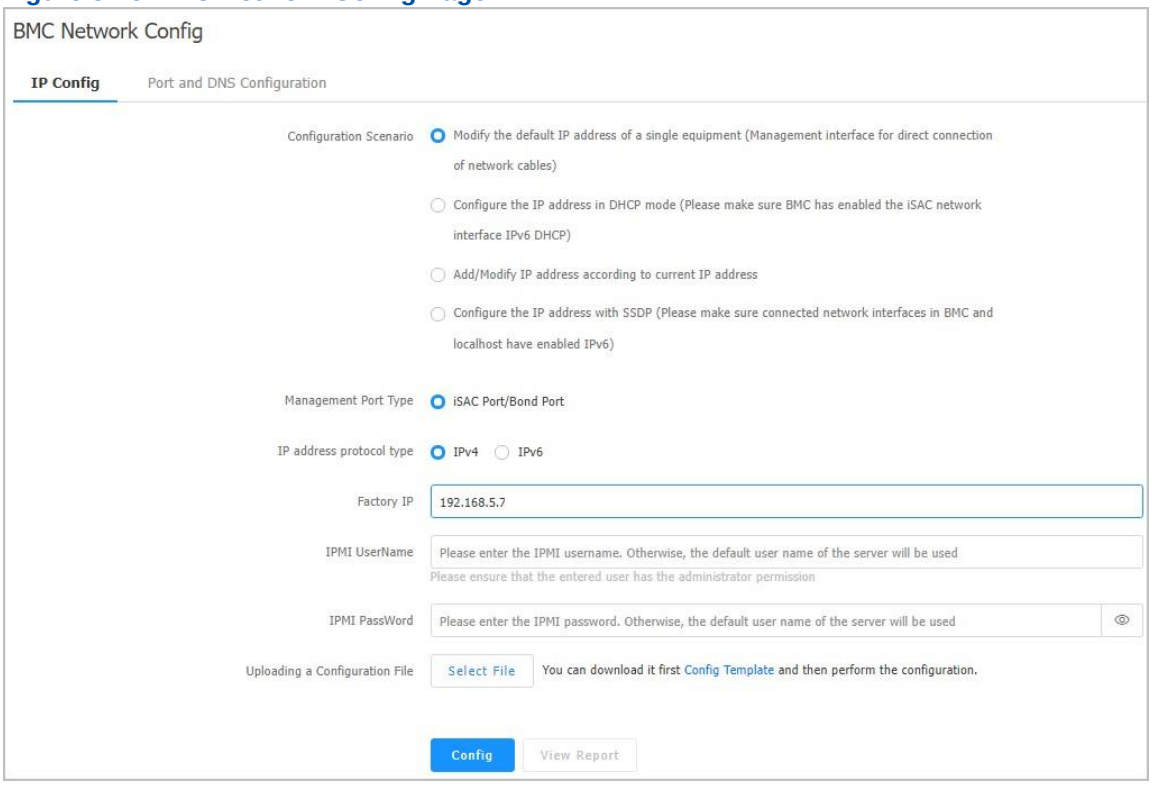
Scenario	Description
	● During configuration, network cables are plugged and unplugged manually. ● When the following message is displayed, you need to insert the network cable into the iSAC network port on another server to be configured and repeat the steps until all servers are configured. `Please insert the lan cable into the x server` ● 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.
Configure the IP address in DHCP mode	● All servers to be configured must have the same IPMI username and IPMI password. ● IPv6 DHCP is enabled on the iSAC network ports of all servers to be configured. ● 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. ● The shared network port cannot be in the same LAN as the iSAC network port. ● There is only one DHCPv6 server in the LAN. ● If no server needs to be allocated a temporary IPv6 address within 20 minutes, the configuration flow times out. ● If both IPv4 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. ● An IP address to be configured in the configuration file must be in the same network segment as that of the installation PC.

Add/Modify IP address according to current IP address	● The iSAC network ports of all servers to be configured and the network port of the installation PC are in the same LAN. ● 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. ● The username and password in the configuration file must be correct.
Configure the IP address with SSDP	● Applicable to G5 series servers with BMC version V04.23.01.02 or later. ● Applicable to G4 series servers with BMC version V03.20.02.00 or later. ● IPv6 is enabled on network ports for connection between the installation PC and a BMC. ● 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. ● In the configuration file, the serial number of each server must be valid.
Scenario	**Description**
	● 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. ● 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. ● The G4 series servers only support the configuration of IP addresses in SSDP mode when the BMC network interface is in normal mode.

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



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: ● **Modify the default IP address of a single equipment** ● **Configure the IP address in DHCP mode**

Parameter		Description
		● **Add/Modify IP address according to current IP address** ● **Configure the IP address with SSDP**
Modify the default IP address of a single equipment	Management Port Type	Select **iSAC Port/Bond Port**.
	IP address protocol type	Select the BMC IP version. Options: ● **IPv4** ● **IPv6**
	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 (**NETAŞroot**) of the server is used.
	IPMI Password	Enter the IPMI password of the server. If it is left blank, the default password (**superuser9!**) of the server is used.
	Uploading a Configuration File	If there is no configuration file, click **Config Template** to download and fill in the configuration template. For how to fill in the configuration template, refer to Table 3-12. The name of the configuration template downloaded to your local PC is *ImportIPConfiguration.xls*. Click **Select File**, and select the edited configuration file.
Configure the IP address in DHCP mode	Management Port Type	Select **iSAC Port/Bond Port**.
	IP address protocol type	Select the BMC IP version. Options: ● **IPv4** ● **IPv6** 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 (**NETAŞroot**) of the server is used.
	IPMI Password	Enter the IPMI password of the server. If it is left blank, the default password (**superuser9!**) of the server is used.
Parameter		**Description**
	Uploading a Configuration File	If there is no configuration file, click **Config Template** to download and fill in the configuration template. For how to fill in the configuration template, refer to Table 3-12. The name of the configuration template downloaded to your local PC is *ImportIPConfiguration.xls*. Click **Select File**, and select the edited configuration file.
Add/Modify IP address according	Management Port Type	Select **iSAC Port/Bond Port**.

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

Table 3-12 Configuration Template Descriptions

Scenario	Description
Modify the default IP address of a single equipment	● When configuring an IPv4 address, you need to set the following parameters: Serial Number, IPv4 Address, IPv4 Mask, and IPv4 Gateway. ● When configuring an IPv6 address, you need to set the following parameters: Serial Number, IPv6 Address, IPv6 Prefix, and IPv6 Gateway. ● No blank line is allowed between adjacent lines. ● The serial number or IPv4/IPv6 address must be unique. ● In the same line, the IPv4/IPv6 address and the gateway must be in the same network segment.
Configure the IP address in DHCP mode	● When configuring an IPv4 address, you need to set the following parameters: Serial Number, IPv4 Address, IPv4 Mask, and IPv4 Gateway. ● When configuring an IPv6 address, you need to set the following parameters: Serial Number, IPv6 Address, IPv6 Prefix, and IPv6 Gateway. ● No blank line is allowed between adjacent lines. ● The serial number or IPv4/IPv6 address must be unique.
Scenario	**Description**
	● In the same line, the IPv4/IPv6 address and the gateway must be in the same network segment.

Add/Modify IP address according to current IP address	• When configuring an IPv4 address, you need to set the following parameters: Current IP, UserName, Password, IPv4 Address, IPv4 Mask, and IPv4 Gateway. • When configuring an IPv6 address, you need to set the following parameters: Current IP, UserName, Password, IPv6 Address, IPv6 Prefix, and IPv6 Gateway. • No blank line is allowed between adjacent lines. • The current IP address or the IPv4/IPv6 address must be unique. • In the same line, the IPv4/IPv6 address and the gateway must be in the same network segment.
Configure the IP address with SSDP	• When configuring an IPv4 address, you need to set the following parameters: Serial Number, UserName, Password, IPv4 Address, IPv4 Mask, and IPv4 Gateway. • When configuring an IPv6 address, you need to set the following parameters: Serial Number, UserName, Password, IPv6 Address, IPv6 Prefix, and IPv6 Gateway. • No blank line is allowed between adjacent lines. • The serial number or IPv4/IPv6 address must be unique. • In the same line, the IPv4/IPv6 address and the gateway must be in the same network segment. • Both IPv4 and IPv6 addresses can be configured.

3. Click **Config**. A confirmation message box is displayed.
4. 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:

1. Select **Settings > Network & Internet > Change adapter options**. The **Network Connections** window is displayed.
2. 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

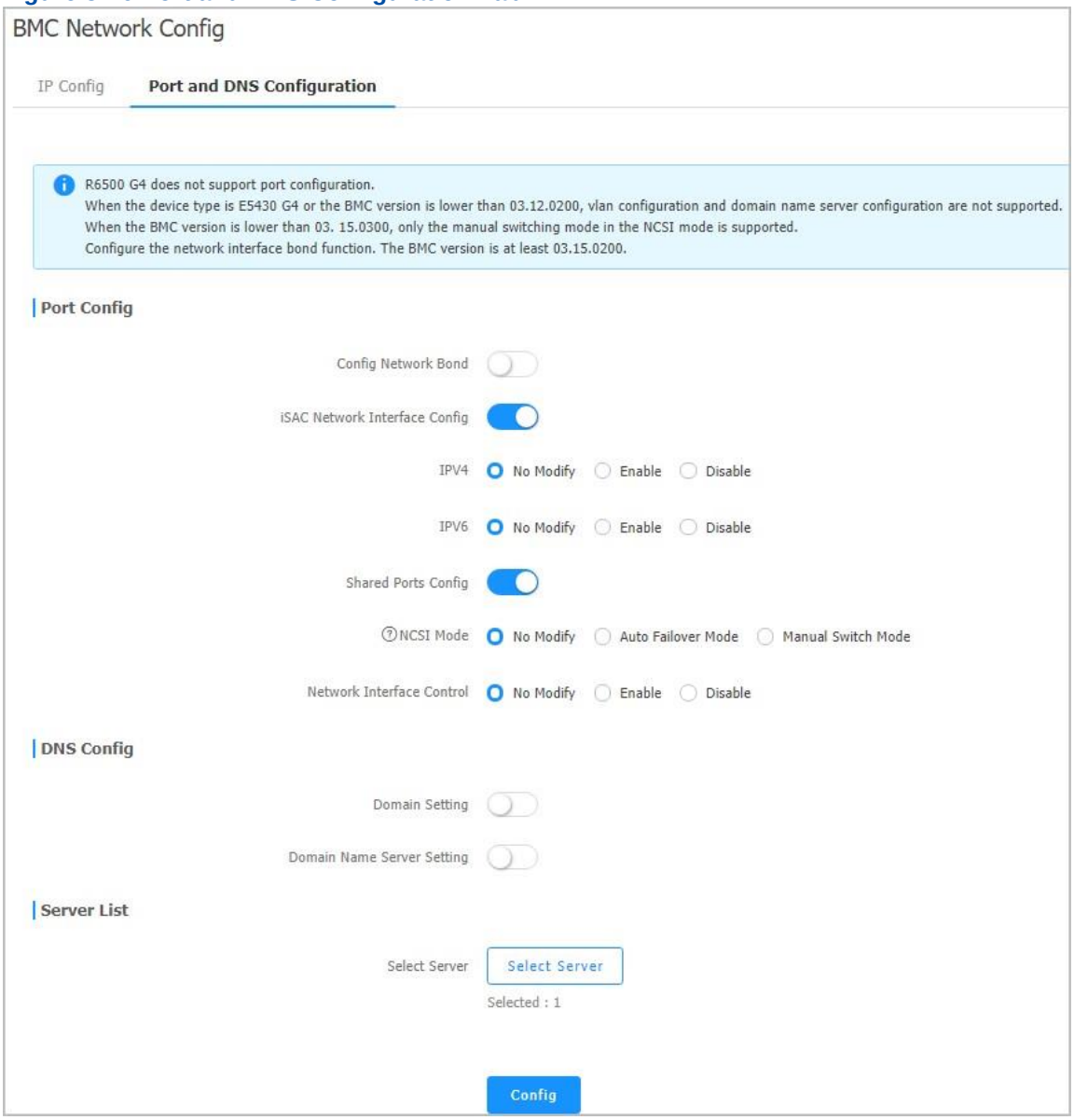
Abstract

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 **Config Network Bond** switch.
iSAC Network Interface Config	If you need to configure the iSAC network port parameters, turn on the **iSAC Network Interface Config** switch, and select whether to enable IPv4/IPv6 on the iSAC network port. ● **No Modify**: indicates not to modify the original server configuration. ● **Enable**: indicates to enable IPv4/IPv6 on the iSAC network port. ● **Disable**: indicates to disable IPv4/IPv6 on the iSAC network port.

Parameter	Description
	You cannot disable IPv4 and IPv6 at the same time.
Shared Ports Config	If you need to configure the shared network port parameters, turn on the **Shared Ports Config** switch and set the following parameters: ● **NCSI Mode**: **No Modify** indicates not to modify the original server configuration. **Auto Failover Mode** indicates to automatically switch to a shared network port when the iSAC network port fails. In this case, you need to set **Channel Index**, which indicates that the shared network port of the server is provided preferentially. **Manual Switch Mode** indicates to manually switch to a shared network port when the iSAC network port fails. In this case, you need to set **Channel Index**. ● **Channel Index**: enter a channel ID, range: 0–3. ● **Network Interface Control**: select whether to enable network control. After network port control is enabled, the shared network port is allocated to the VLAN of the BMC. ● **VLAN**: select whether to enable VLAN. If this parameter is set to **Enable**, you need to configure a VLAN ID. ● **VLAN ID**: enter a VLAN ID, range: 1–4094. Note: If there is no requirement for enabling VLAN and configuring a VLAN ID on site, it is recommended that you select **No Modify**.

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

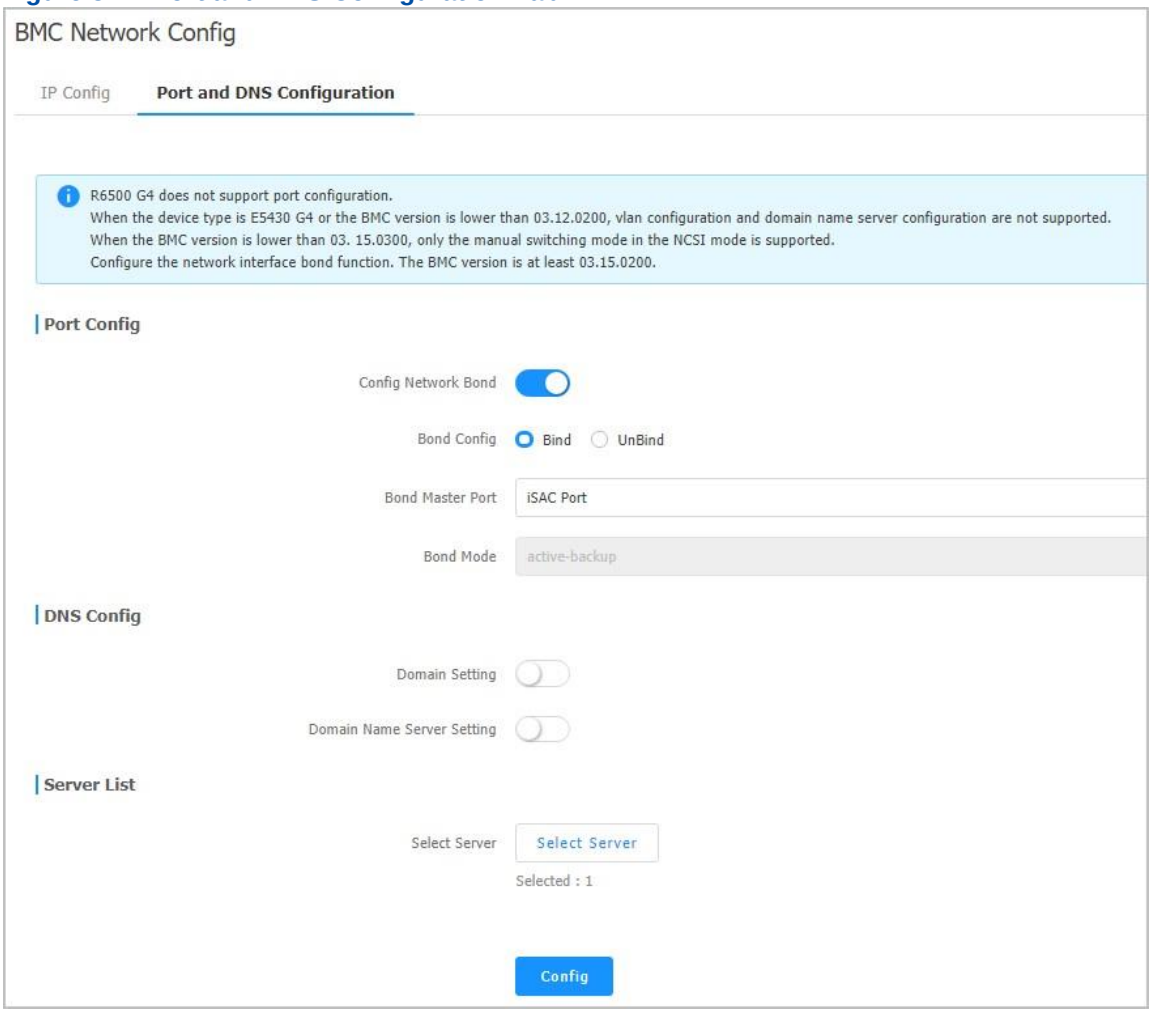
Abstract

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 **Config Network Bond** 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

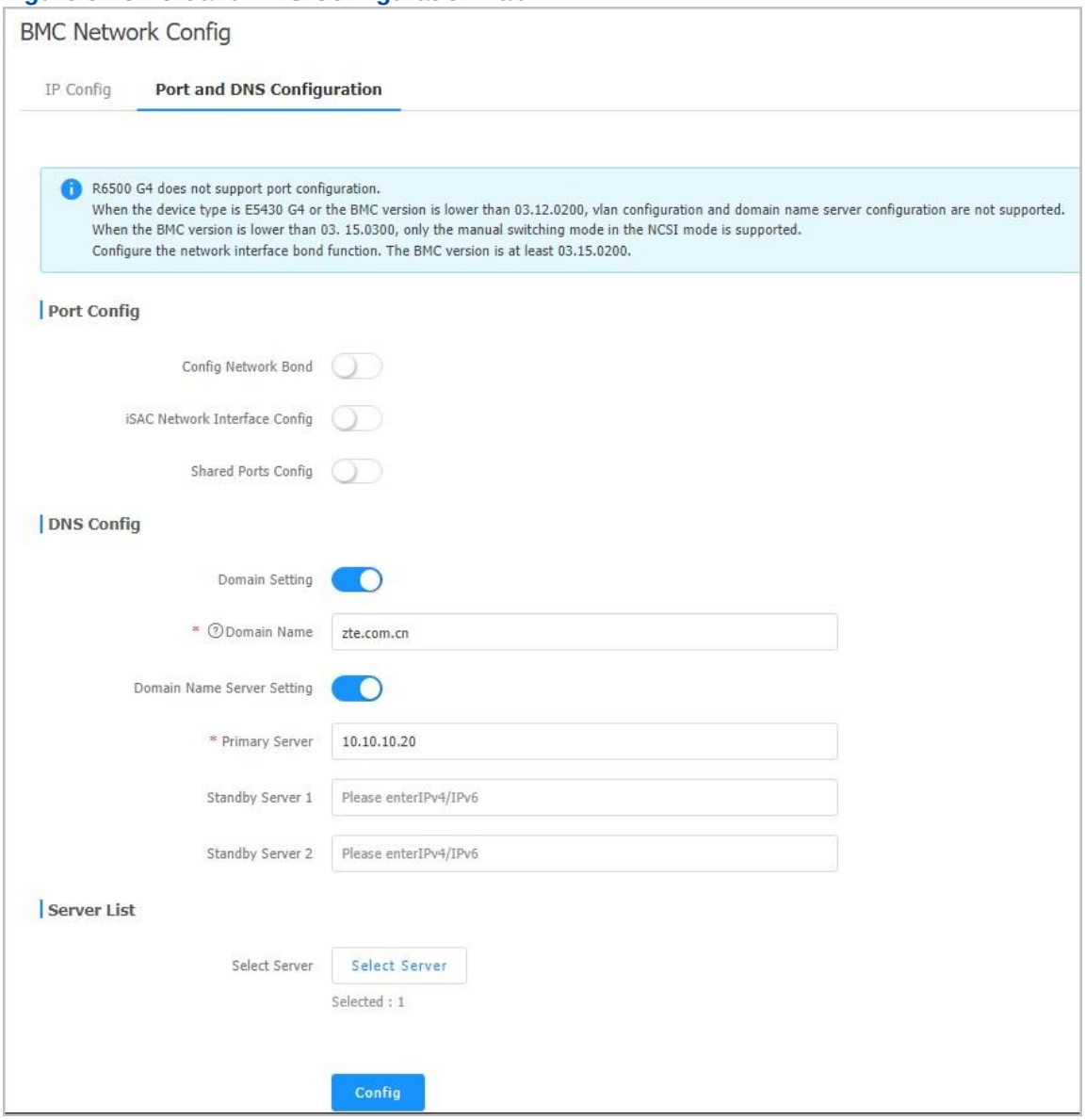
Abstract

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



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 **Domain Setting** switch.
Domain Name	Enter the domain name, which consists of digits, uppercase and lowercase letters, hyphens (–), and dots (.). A domain name cannot start or end with a hyphen. The length of a domain name cannot exceed 63 characters per label, and the length of a FQDN cannot exceed 255 characters.
Domain Name Server Setting	Select whether to set DNS servers. ● If you need to set DNS servers, turn on the **Domain Name Server Setting** switch, and set **Primary Server**, **Standby Server 1**, and **Standby Server 2** . The **Primary Server** parameter is required, while others are optional. The values of **Primary Server**, **Standby Server 1**, and **Standby Server 2** must be different. ● If you do not need to set DNS servers, turn off the **Domain Name Server Setting** switch.

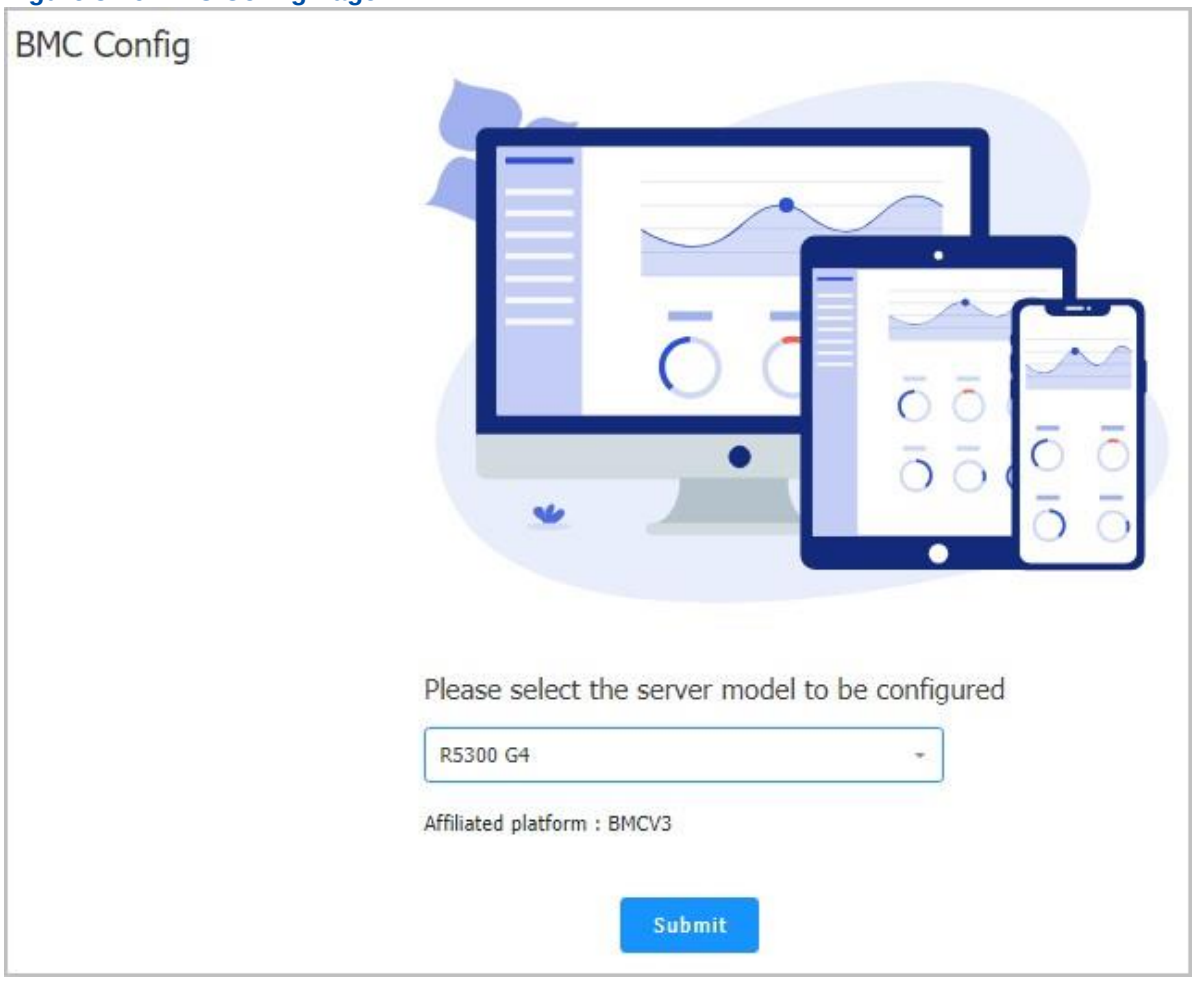
4. In the **Server List** area, click **Select Server**, and select the server that you want to configure.
5. Click **Config**.

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

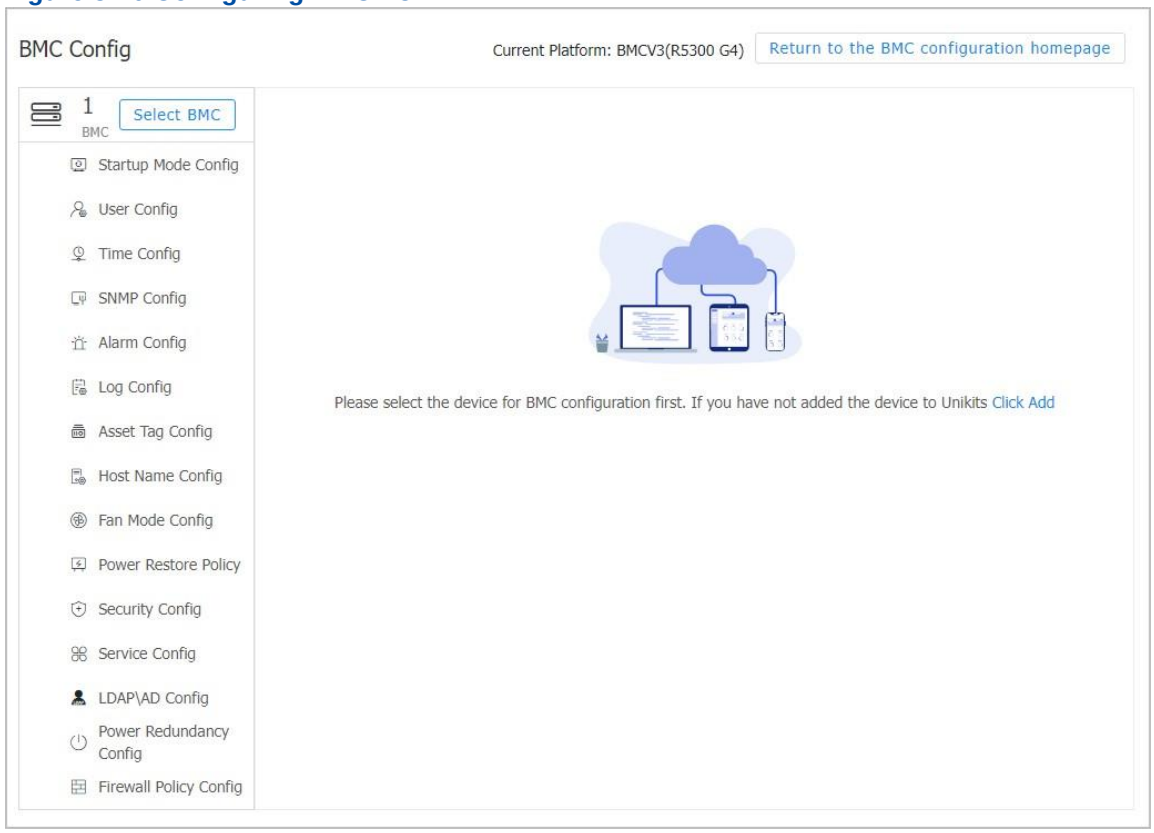
Abstract

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

Steps

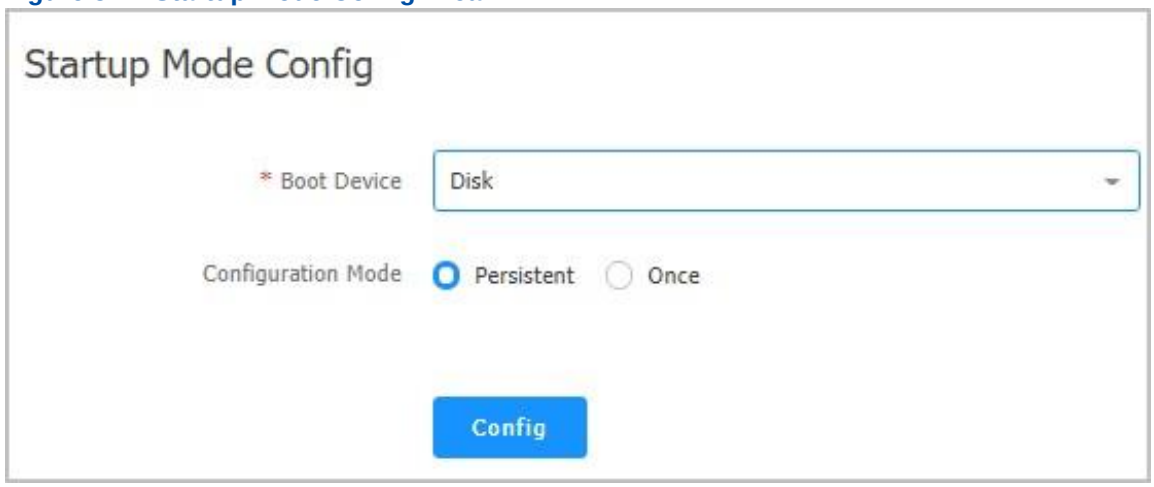
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page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

Figure 3-20 Configuring BMC V3



4. Click **Select BMC**, and select the BMC for which you want to configure boot options.
5. 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



6. 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: ● **No Override**: The first boot device is not set. The default boot mode set in BIOS is used, which is not controlled by the BMC. ● **Network**: The OS is forcibly started through a network. ● **Disk**: The OS is forcibly started through a hard disk. ● **USB**: The OS is forcibly booted through a USB flash drive. ● **CD Rom**: The OS is forcibly booted through a CD/DVD-ROM drive. ● **BIOS**: After the server is booted, the BIOS menu is displayed.
Configuration Mode	Select whether the reconfigured server boot option is applied to the current restart only. ● **Once**: only effective for the current restart. ● **Persistent**: permanently effective.

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

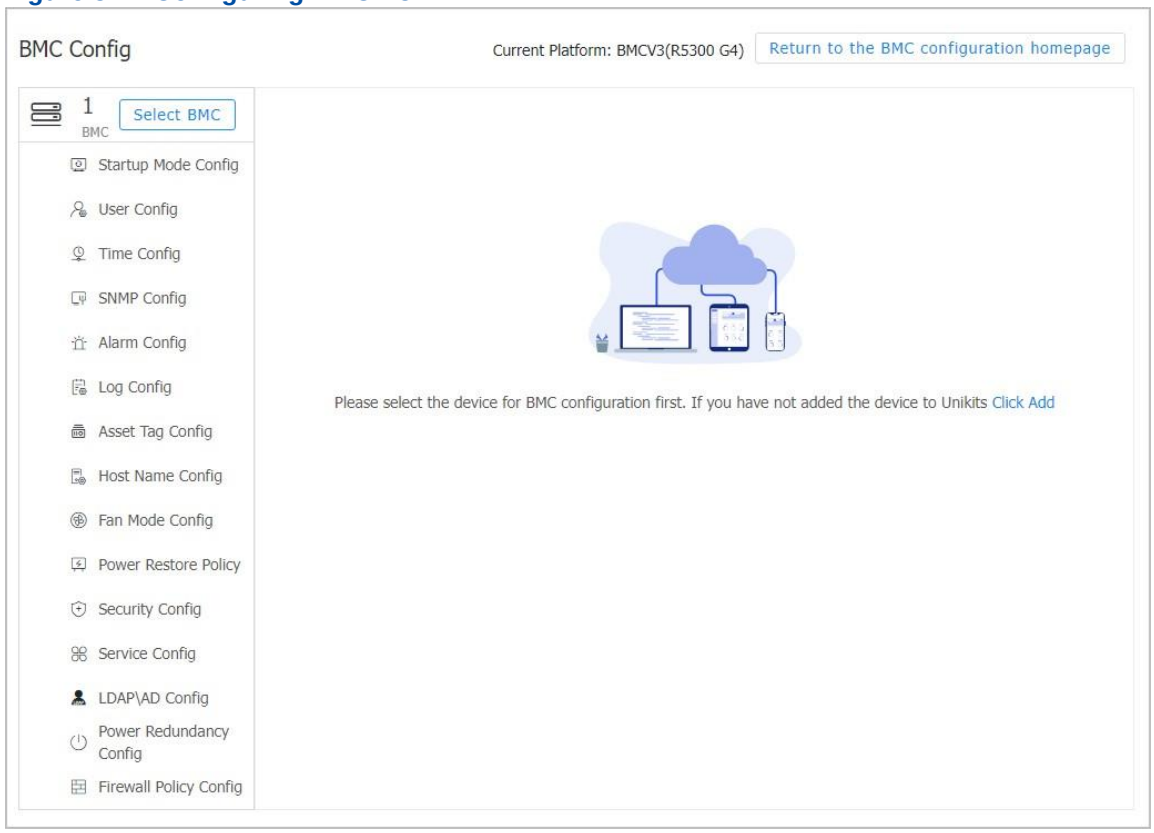
Abstract

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

Steps

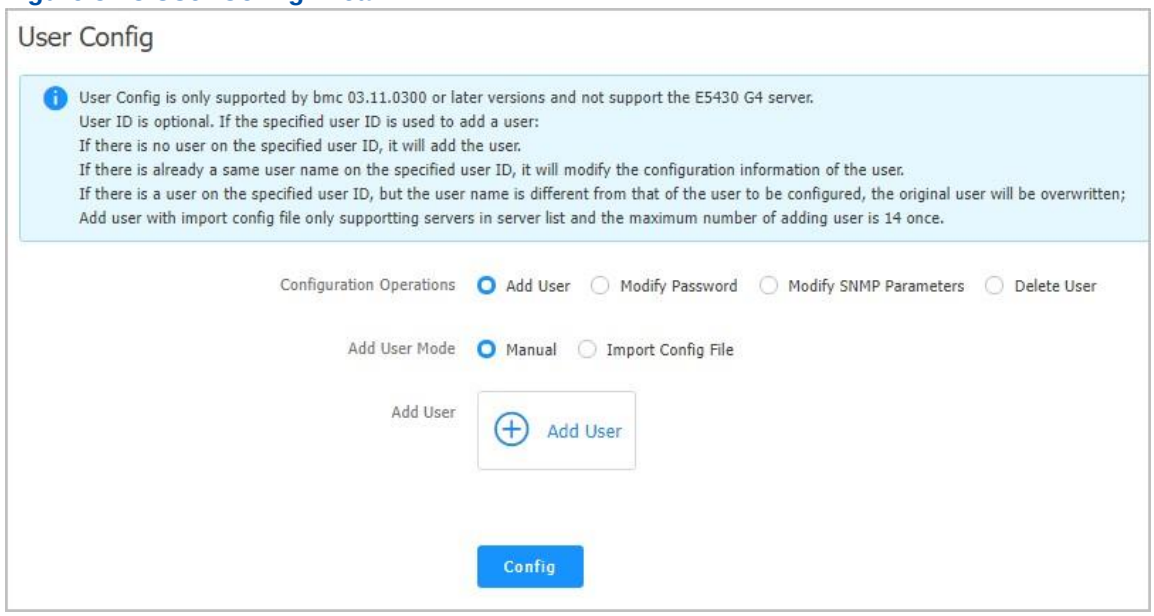
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page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

Figure 3-22 Configuring BMC V3



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



6. Perform the following operations as required.

To...	Do...
Manually add a user	a. Set **Configuration Operations** to **Add User**. b. Set **Add User Mode** to **Manual**. c. Click **Add User**. The **Add User** dialog box is displayed. d. Set the parameters. e. Click **Submit**. f. Click **Config** to deliver the configurations.
Add users in batches	a. Set **Configuration Operations** to **Add User**. b. Set **Add User Mode** to **Import Config File**. c. Click **Select File**, and select a configuration file. d. Click **Config** to deliver the configurations.
Manually modify a password	a. Set **Configuration Operations** to **Modify Password**. b. Set **Modify Type** to **Manual Modify**. c. Enter the username for which you want to modify the password. d. Select the password size. e. Enter a new password. f. Click **Config** to deliver the configurations.
Modify passwords in batches	a. Set **Configuration Operations** to **Modify Password**. b. Set **Modify Type** to **Import Config File**. c. Click **Select File**, and select a configuration file. d. Click **Config** to deliver the configurations.
Modify SNMP parameters	a. Set **Configuration Operations** to **Modify SNMP Parameters**. b. Enter the username for which you want to modify SNMP parameters. This user must have the administrator permissions. c. Modify the SNMP parameters. d. Click **Config** to deliver the configurations.
Delete a user	a. Set **Configuration Operations** to **Delete User**. b. Enter the username that you want to delete. c. Click **Config** to deliver the configurations.

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

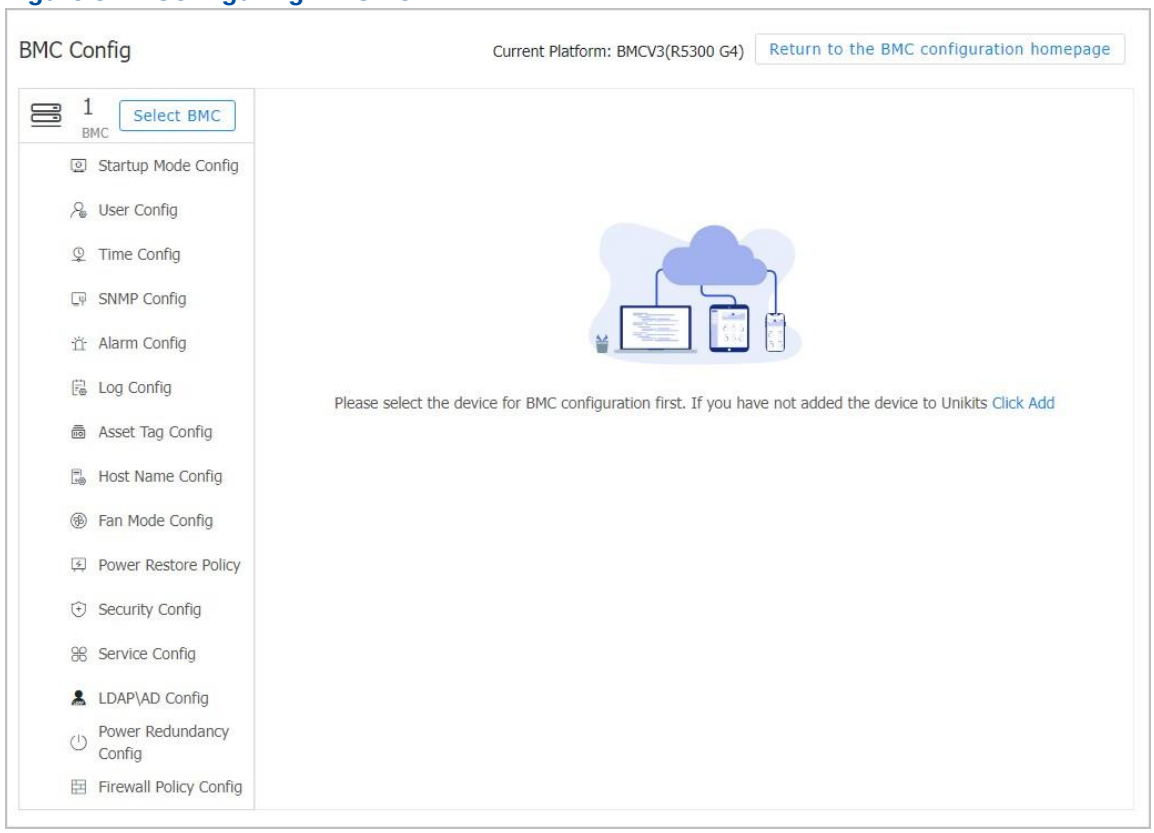
Abstract

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

Steps

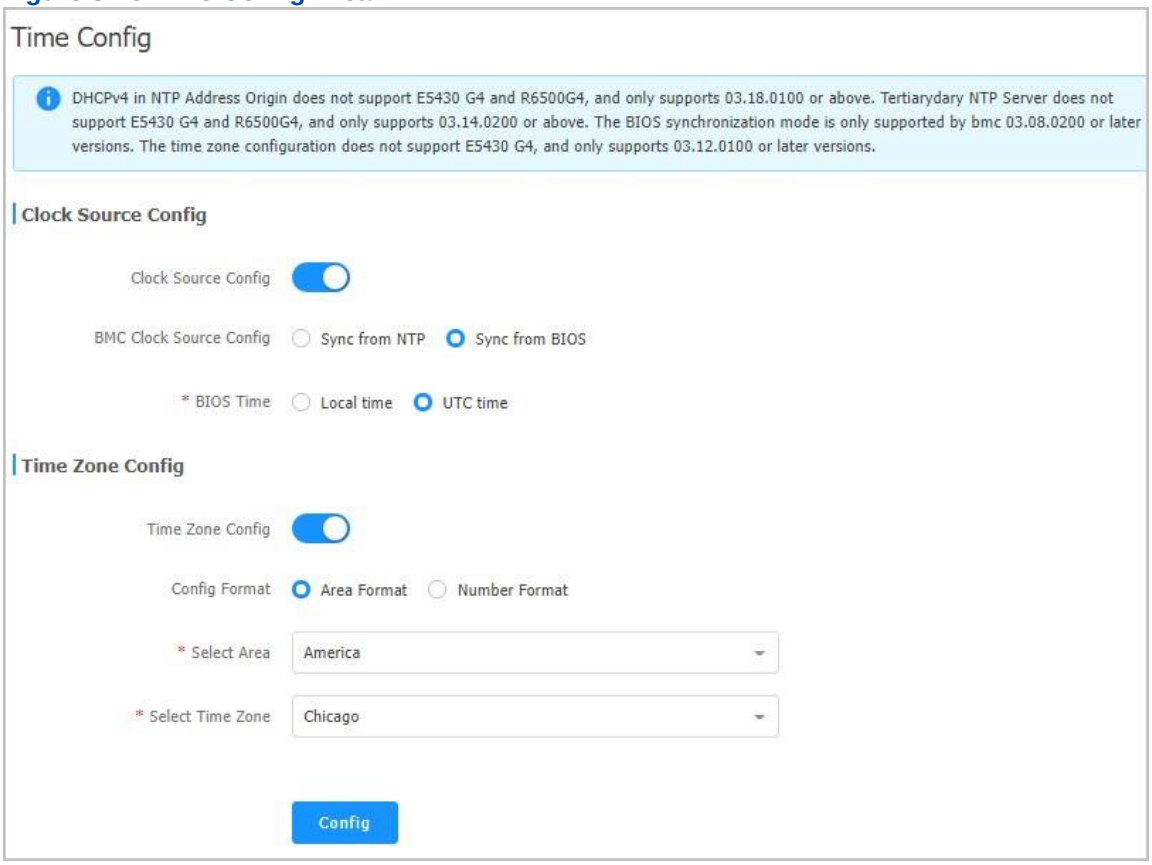
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page 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



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	a. Turn on the **Clock Source Config** switch. b. Set **BMC Clock Source Config** to **Sync from NTP**. c. Set **NTP Address Origin** to **Static**. d. Configure the following parameters: ● **Primary NTP Server**: Enter the IP address or FQDN of NTP server 1, with the length not exceeding 127 characters. Required. ● **Secondary NTP Server**: Enter the IP address or FQDN of NTP server 2, with the length not exceeding 127 characters. Optional. ● **Tertiarydary NTP Server**: Enter the IP address or FQDN of NTP server 3, with the length not exceeding 127 characters. Optional. ● **Sync Period**: Enter the time synchronization period in seconds, range: 60–65535.
Synchronize time from an NTP server over DHCP	a. Turn on the **Clock Source Config** switch. b. Set **BMC Clock Source Config** to **Sync from NTP**. c. Set **NTP Address Origin** to **DHCPv4**.
To...	**Do...**

Synchronize time from the BIOS	a. Turn on the **Clock Source Config** switch. b. Set **BMC Clock Source Config** to **Sync from BIOS**. c. Set **BIOS Time**. ● If the server runs the Linux OS, select **UTC time**. ● If the server runs the Windows OS, select **Local time**. UTC 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.

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 **Tertiarydary NTP Server** in turn.

7. 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 **Time Zone Config** switch.
Config Format		Select a time zone format. Options: ● **Area Format** ● **Number Format**
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.

8. 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

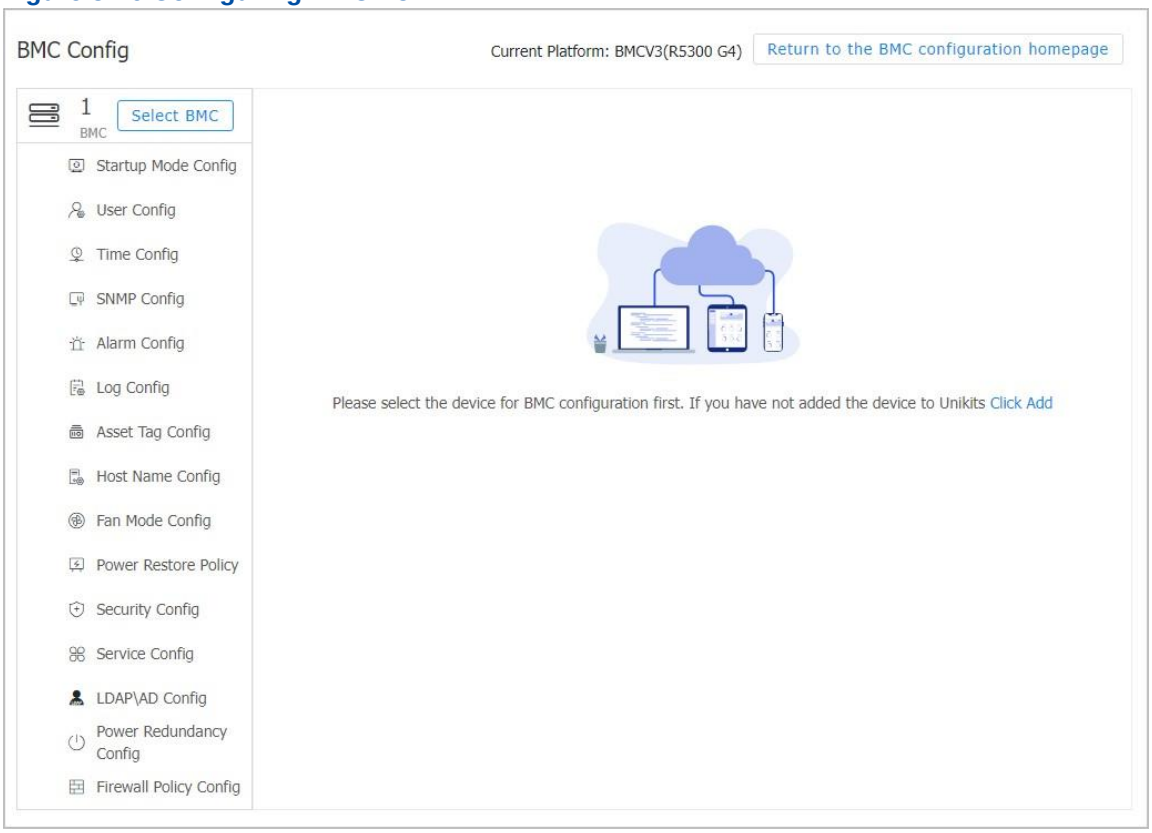
Abstract

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

Steps

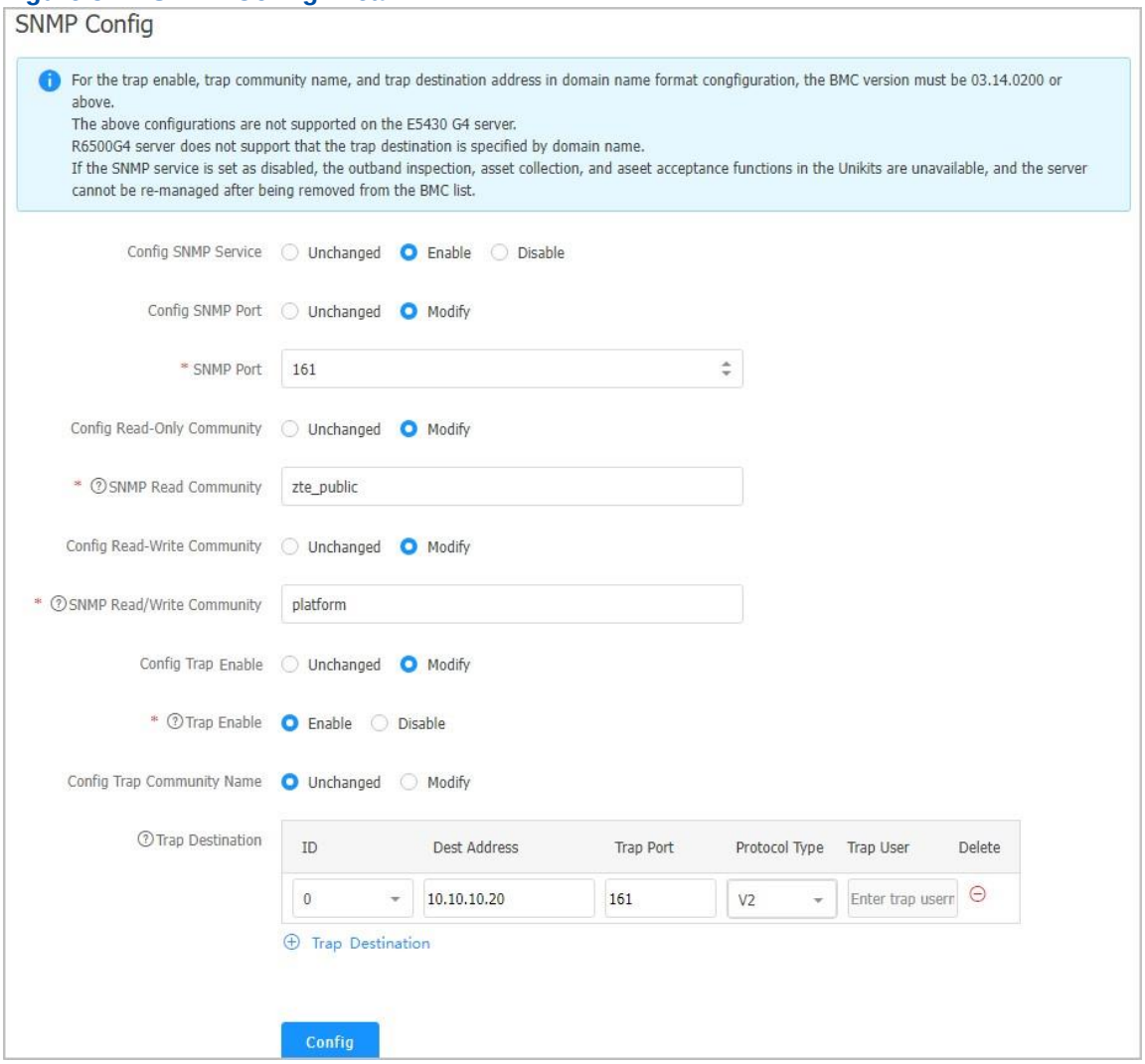
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page 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



6. Set the parameters. For a description of the parameters, refer to Table 3-18.

Table 3-18 SNMP Parameter Descriptions

Parameter	Description
Config SNMP Service	• To keep the original SNMP service configuration of the server, select **Unchanged**. • To enable the SNMP service, select **Enable**. • To disable the SNMP service, select **Disable**. 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.
Config SNMP Port	• To keep the original SNMP port of the server, select **Unchanged**. • To modify the SNMP port of the server, select **Modify** and set **SNMP Port**.

Config Read-Only Community	● To keep the original read-only community of the server, select **Unchanged**.
Parameter	**Description**
	● To modify the read-only community of the server, select **Modify** and set **SNMP Read Community**.
Config Read-Write Community	● To keep the original read-write community of the server, select **Unchanged**. ● To modify the read-write community of the server, select **Modify** and set **SNMP Read/Write Community**.
Config Trap Enable	● To keep the original trap enabling status of the server, select **Disable**. ● To modify the trap enabling status of the server, select **Modify** and set **Trap Enable**.
Config Trap Community Name	● To keep the original trap community name of the server, select **Unchanged**. ● To modify the trap community name of the server, select **Modify** and set **Trap Community Name**.
Trap Destination	Configure trap destinations. A maximum of 15 trap destinations can be configured. Click  to add another trap destination. ● **ID**: range: 0–14. ● **Dest Address**: SNMP destination IP address. ● **Trap Port**: range: 1–65535. ● **Protocol Type**: SNMP version, including V1, V2, and V3. ● **Trap User**: valid and required when **Protocol Type** is set to **V3**. You must enter an existing SNMP trap username with administrator permissions.

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

Note

- 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

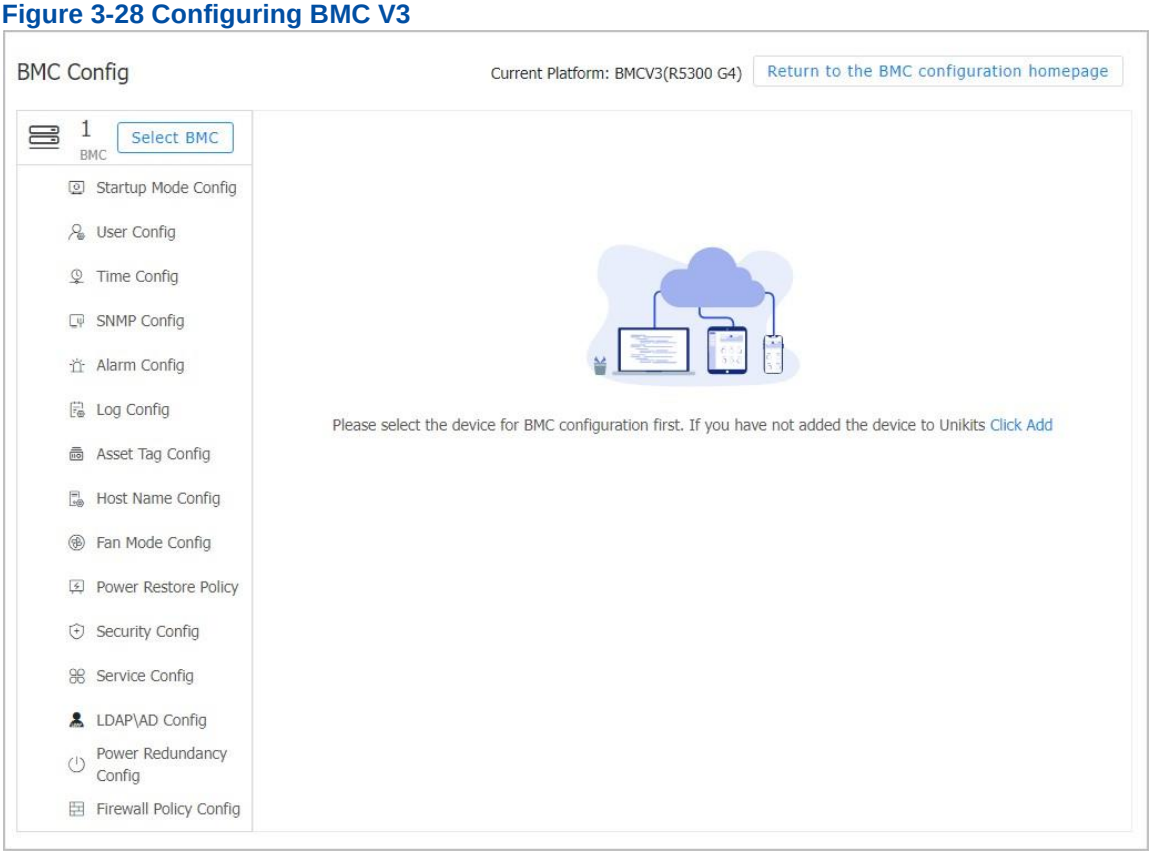
Alarm parameters include alarm source parameters and pre-alarm parameters.

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

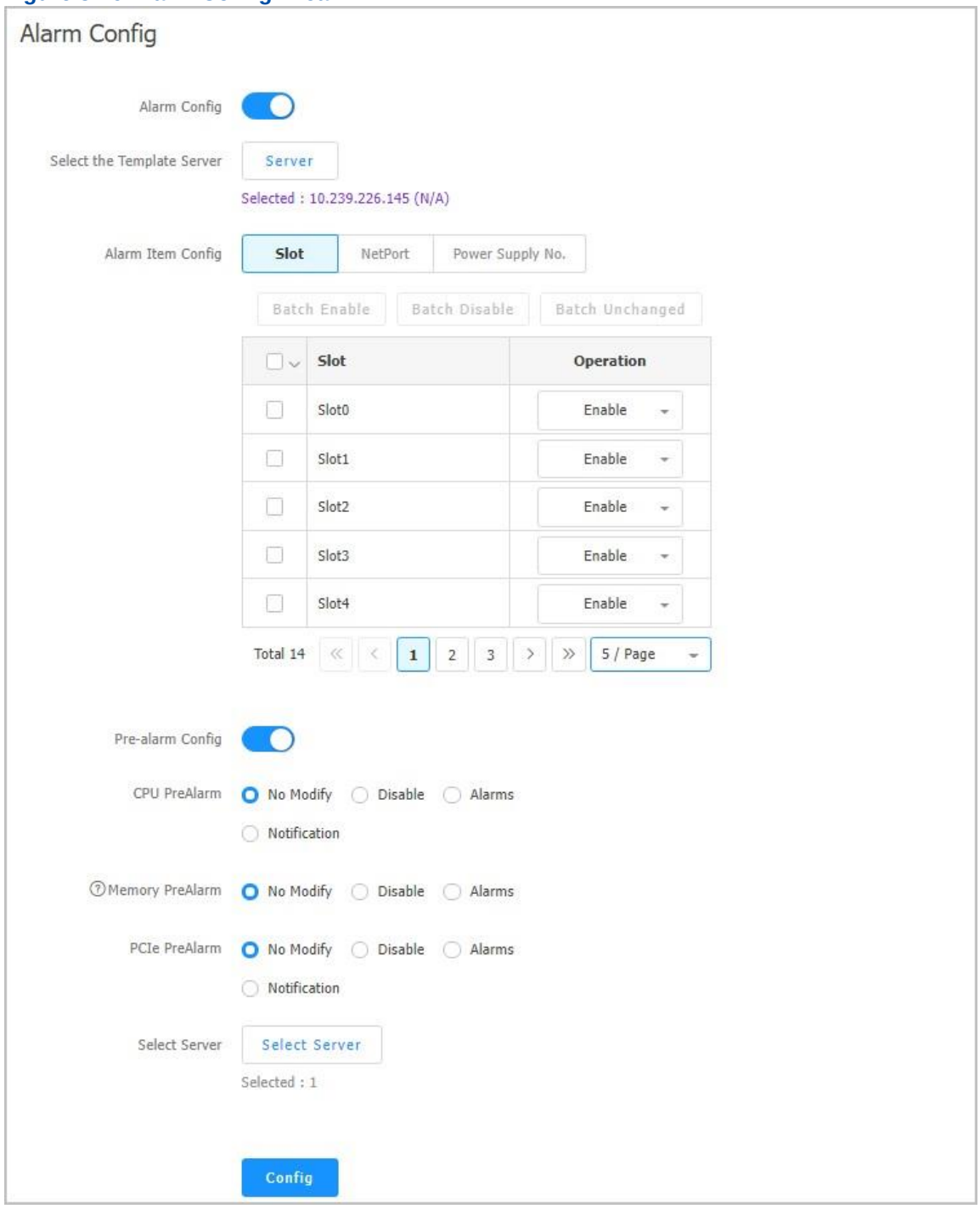
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page 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



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	• To configure an alarm source, turn on the **Alarm Config** switch. • To not configure an alarm source, turn off the **Alarm Config** switch.

Parameter	Description
Select the Template Server	Click **Server**, and select a server. The **Slot**, **NetPort**, and **Power Supply No.** of the server are obtained and used as the template to configure alarm sources.
Alarm Item Config	In the **Operation** column, click **Enable**, **Disable**, and **Unchanged** for the desired alarm source to configure whether to report alarms. ● **Enable**: indicates to report alarms. ● **Disable**: indicates not to report alarms. ● **No Modify**: indicates not to modify the original server configurations. If you select multiple alarm sources, click **Batch Enable**, **Batch Disable**, or **Batch Unchanged** to set whether to report alarms.
Pre-alarm Config	● To configure the pre-alarm function, turn on the **Pre-alarm Config** switch. ● To not configure the pre-alarm function, turn off the **Pre-alarm Config** switch.
CPU PreAlarm	Select whether to configure the CPU pre-alarm function. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Disable**: indicates to disable the CPU pre-alarm function. ● **Alarms**: indicates to send an alarm if the CPU usage reaches the threshold. ● **Notification**: indicates to send a notification if the CPU usage reaches the threshold. If **Alarms** or **Notification** is selected, set **Pre-alarm Threshold** (range: 1–100).
Memory PreAlarm	Select whether to configure the memory pre-alarm function. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Disable**: indicates to disable the memory pre-alarm function. ● **Alarms**: indicates to send an alarm if the memory usage reaches the threshold. If **Alarms** is selected, set **Alarm Type**. Options: ● **Accumulate Policy**: If the number of alarms reaches **CE Accumulate Alarm Threshold** within **CE Accumulate Alarm Window**, an alarm indicating memory alarm accumulation is raised. ● **Accumulate&Storm Policy**: indicates to use both the alarm accumulation policy and alarm storm policy. → If the number of alarms reaches **CE Accumulate Alarm Threshold** within **CE Accumulate Alarm Window**, an alarm indicating memory alarm accumulation is raised. → If the number of alarms reaches **CE Storm Alarm Time Threshold** within **CE Storm Alarm Time Window**, an alarm indicating too many memory alarms generated within a short time is raised. **CE Storm Alarm Time Window** is less than **CE Accumulate Alarm Window**, and **CE Storm Alarm Time Threshold** is less than **CE Accumulate Alarm Threshold**.

PCIe PreAlarm	Select whether to configure the PCIe pre-alarm function. Options: ● **No Modify**: indicates not to modify the original server configurations.
Parameter	**Description**
	● **Disable**: indicates to disable the PCIe pre-alarm function. ● **Alarms**: indicates to send an alarm if the PCIe usage reaches the threshold. ● **Notification**: indicates to send a notification if the PCIe usage reaches the threshold. If **Alarms** or **Notification** is selected, set **Pre-alarm Threshold** (range: 1–100).
Select Server	Click **Select Server** 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

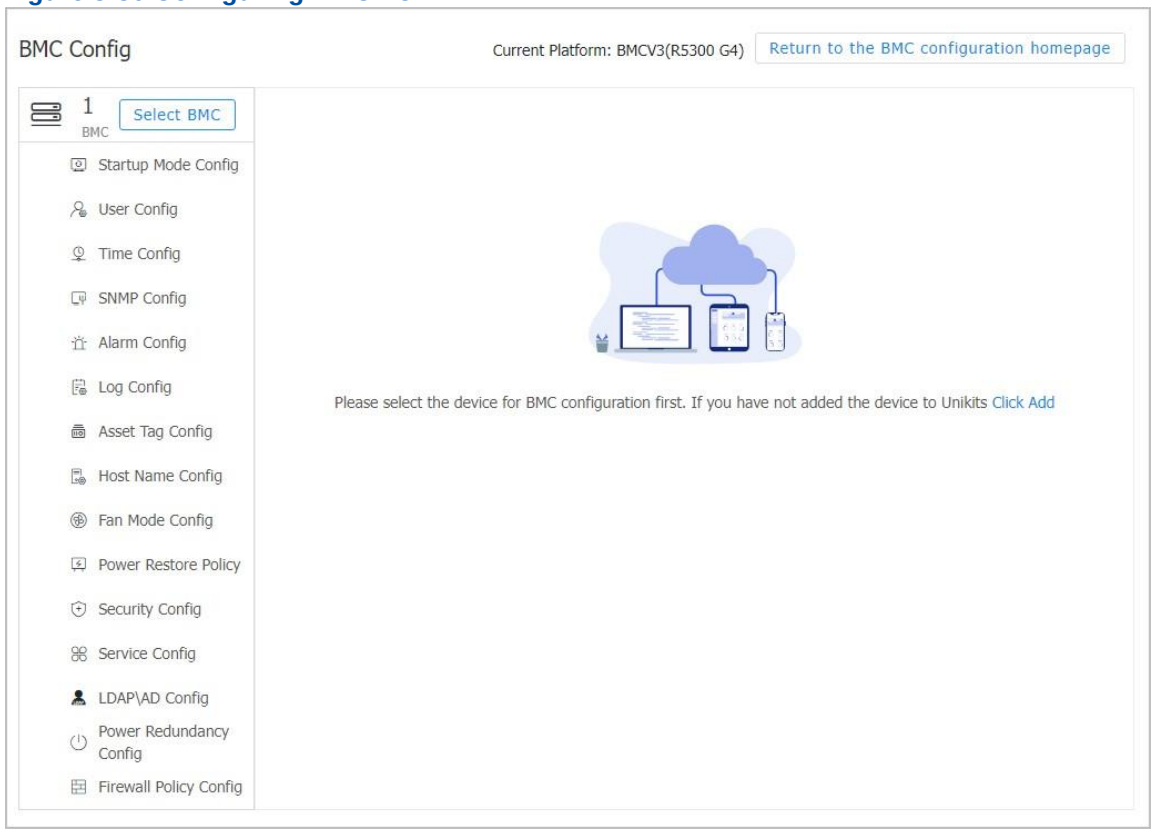
Abstract

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

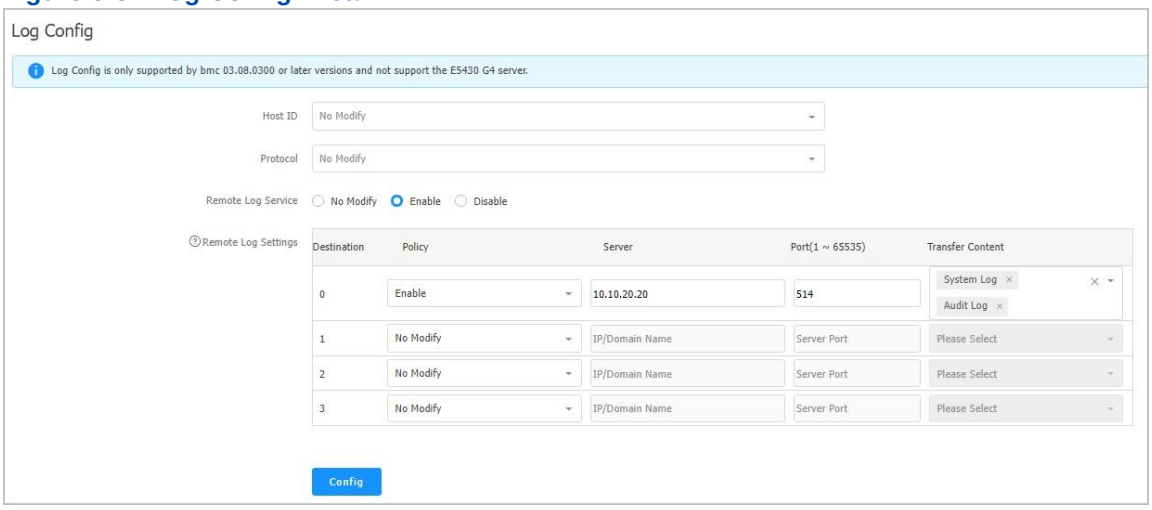
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page 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



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: ● **No Modify**: indicates not to modify the original configurations. ● **Board serial number**: indicates to use the board serial number. ● **Asset label**: indicates to use the asset tag. ● **Host Name**: indicates to use the host name.
Protocol	Select the log transmission protocol. Options: ● **No Modify**: indicates not to modify the original configurations. ● **UDP**: indicates to use UDP. ● **TCP**: indicates to use TCP.
Remote Log Service	Set the parameters of the log server that logs are to be synchronized with: ● **Policy**: select whether to enable the configuration policy. Options include **No Modify**, **Enable**, and **Disable**. If the configuration policy is disabled, the corresponding configurations on the selected BMC are cleared. ● **Server**: enter the IP address of the log server. ● **Port**: enter the port number of the log server. Range: 1–65535. ● **Transfer Content**: select at least one type of logs to be transmitted, including system logs, operation logs, and audit logs. Note: Only two remote log servers can be configured.

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

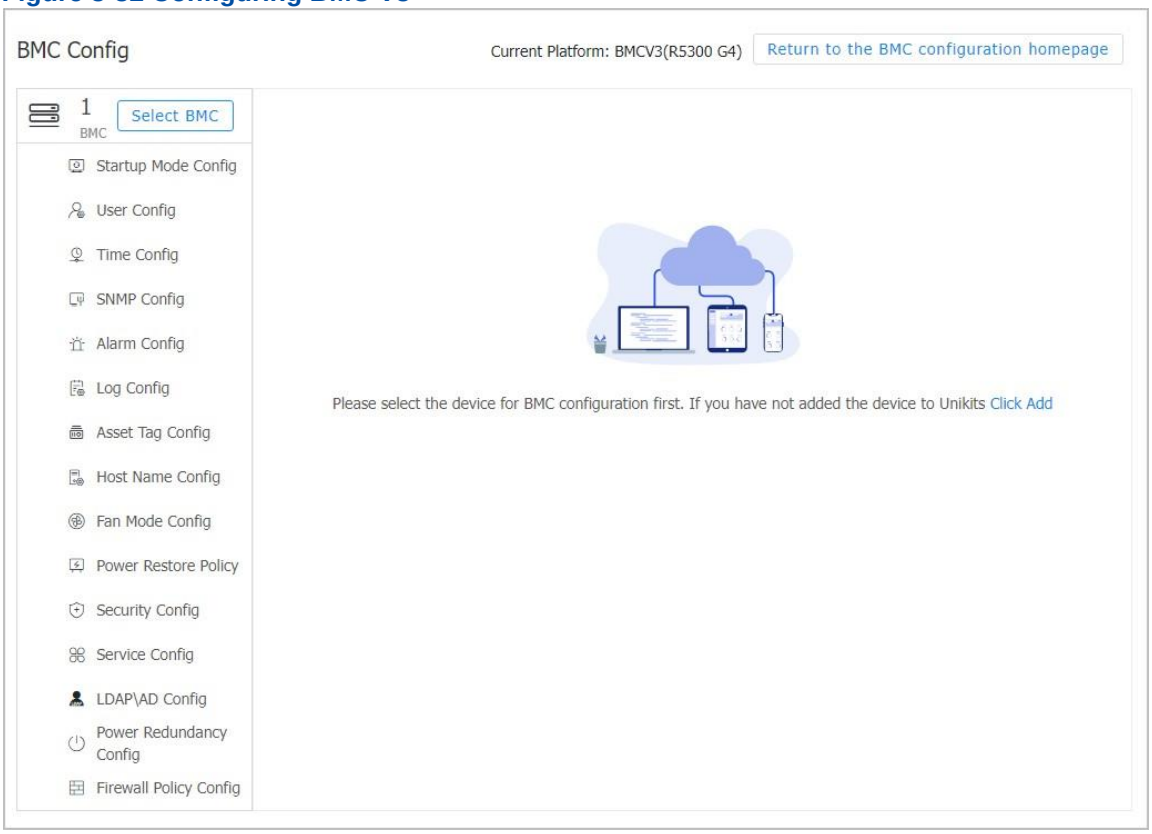
This procedure describes how to modify the asset tags of servers when they need to be updated in batches.

Steps

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

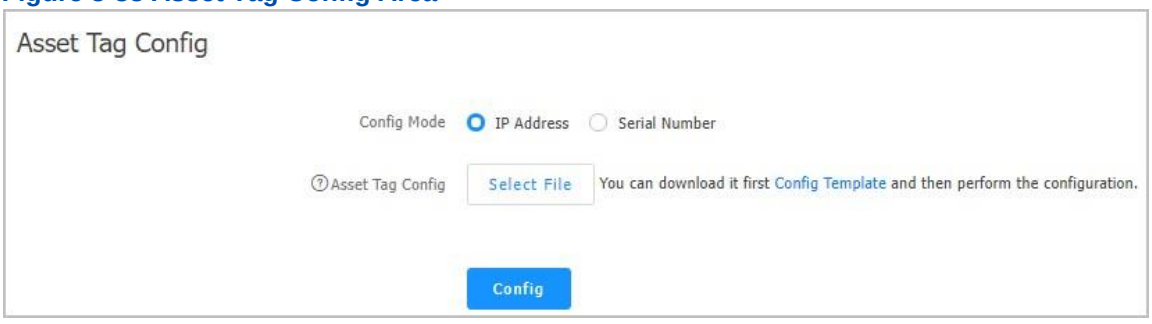
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in Figure 3-32.

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	• To match servers based on BMC IP addresses and then configure asset tags, select **IP Address**. In this mode, you do not need to select a BMC. • To match servers based on serial numbers and then configure asset tags, select **Serial Number**. In this mode, you need to select a BMC.
Asset Tag Config	a. (Optional) If there is no asset tag configuration file, click **Config Template** to download and fill in the configuration template. • If **Config Mode** is set to **IP Address**, the name of the configuration template downloaded to your local PC is *ImportAssetTag.csv*. • If **Config Mode** is set to **Serial Number**, the name of the configuration template downloaded to your local PC is *ImportAssetTagWithSN.csv*. b. 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.

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

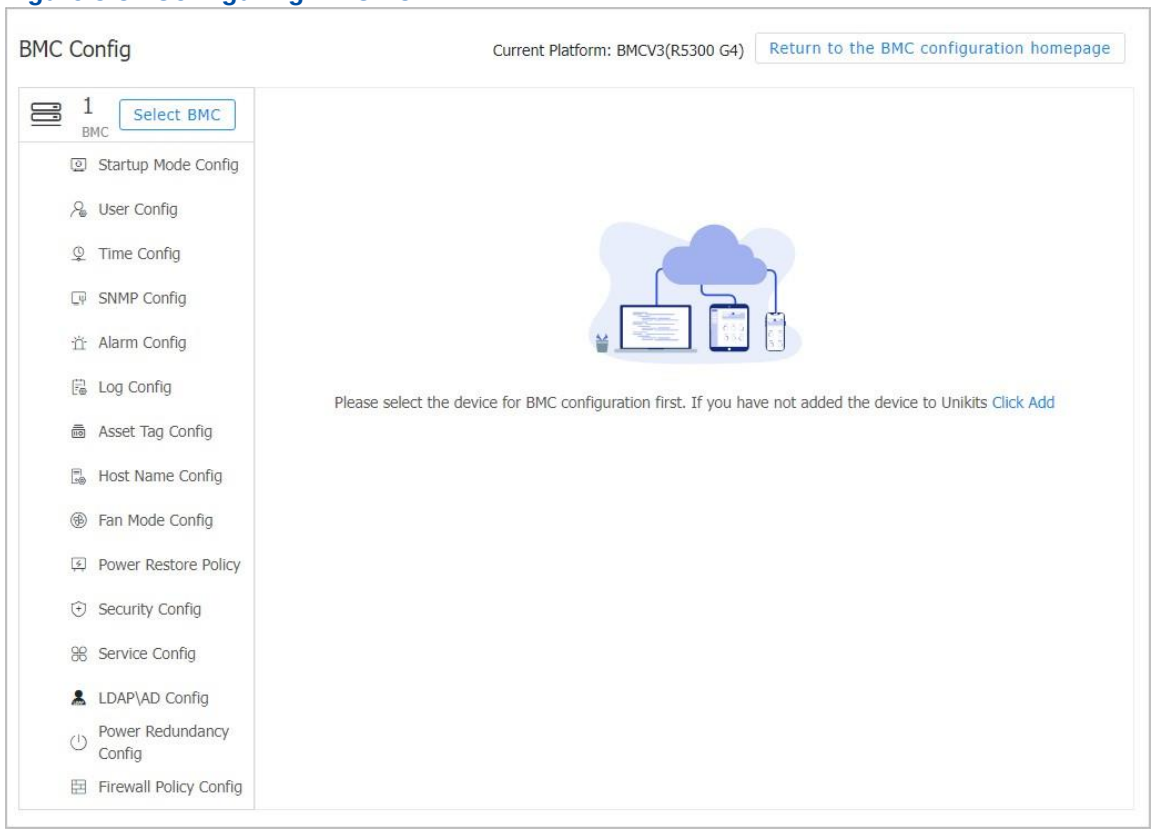
Abstract

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

Steps

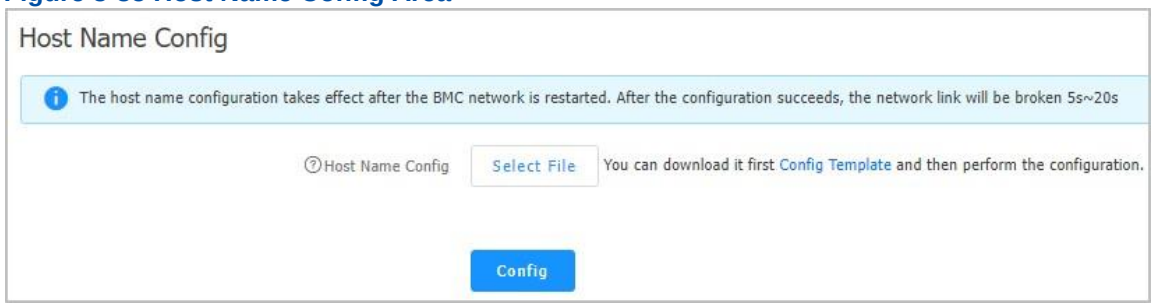
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page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

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.

Note

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

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

Note

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.

Note

- 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

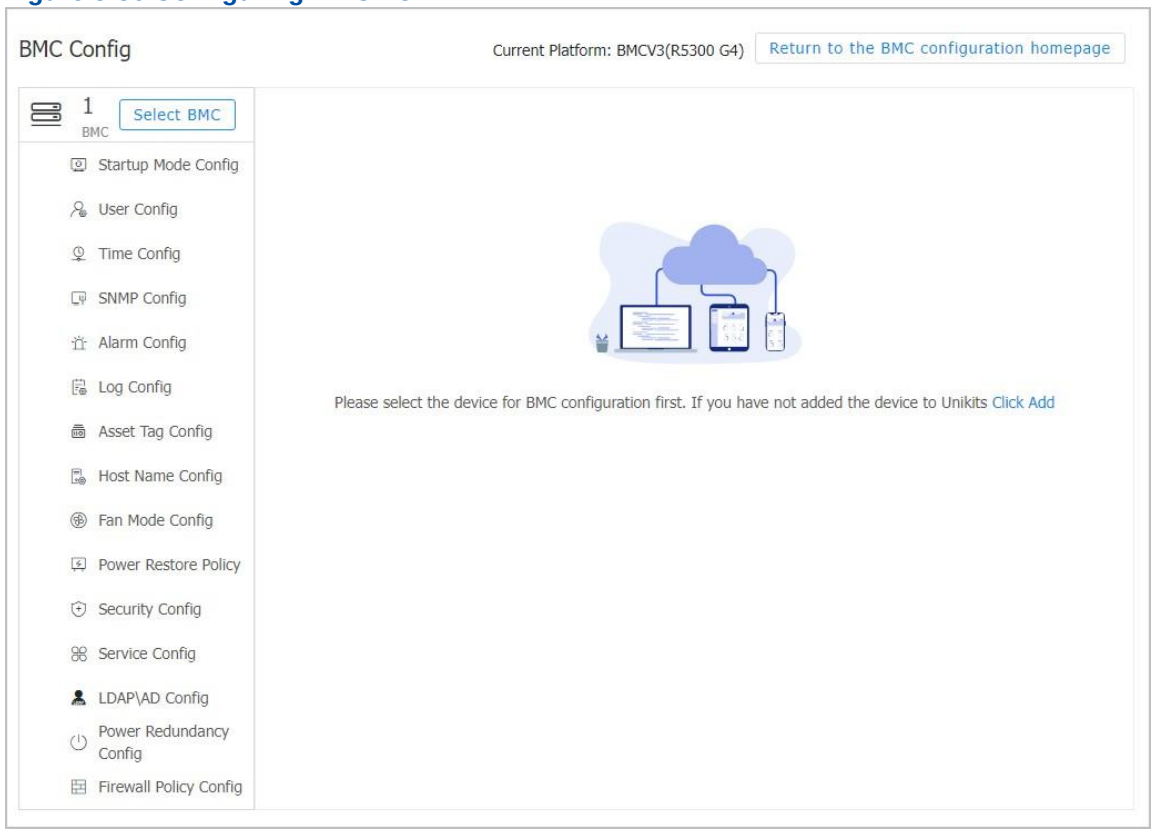
Abstract

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

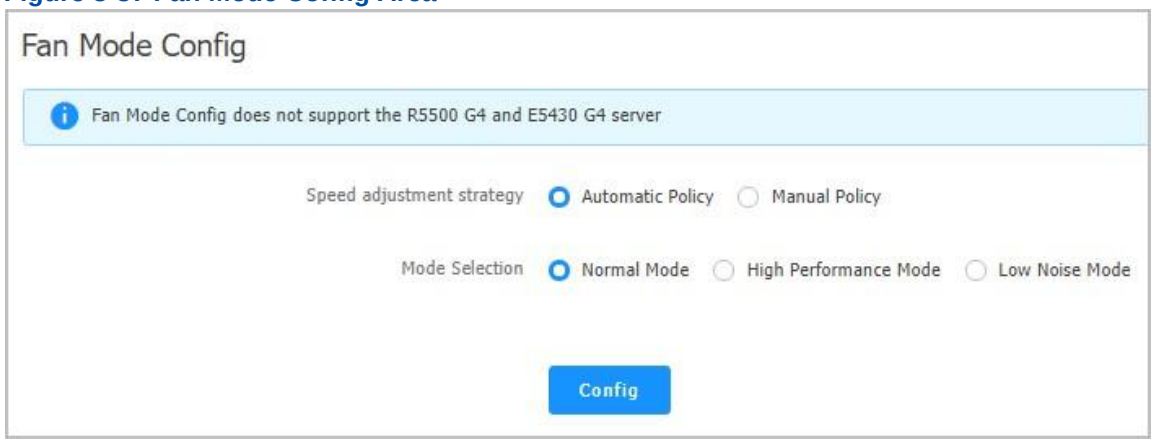
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page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

Figure 3-36 Configuring BMC V3



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



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: ● **Automatic Policy** ● **Manual Policy**
Mode Selection	This parameter is required when **Speed adjustment strategy** is set to **Automatic Policy**. Select an automatic speed regulation mode. Options: ● **Normal Mode**: selected when there is clearance above the top surface of the server and the server is insensitive to noise. ● **High Performance Mode**: selected when servers are stacked together and there is no clearance between them. ● **Low Noise Mode**: selected when servers are placed in an office or other areas that are sensitive to noise.
Speed Percentage	This parameter is required when **Speed adjustment strategy** is set to **Manual Policy**. 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.

Note

- 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

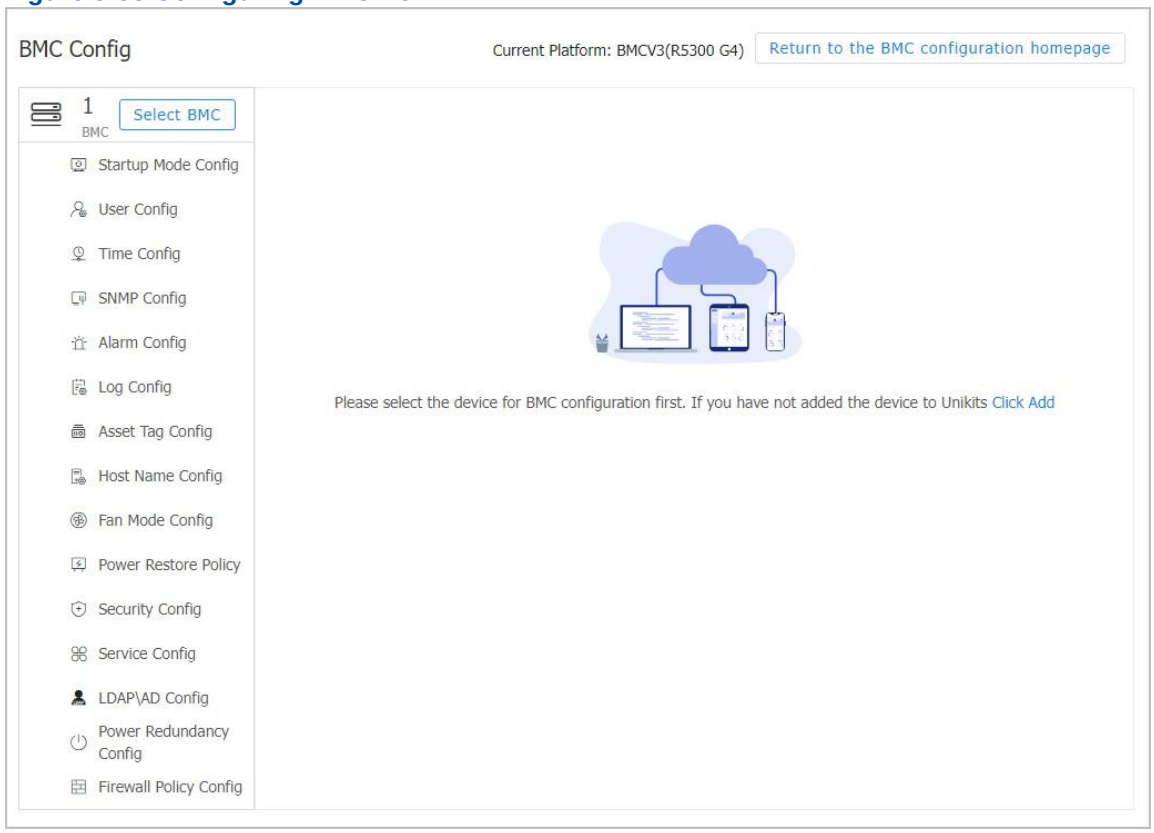
Abstract

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

Steps

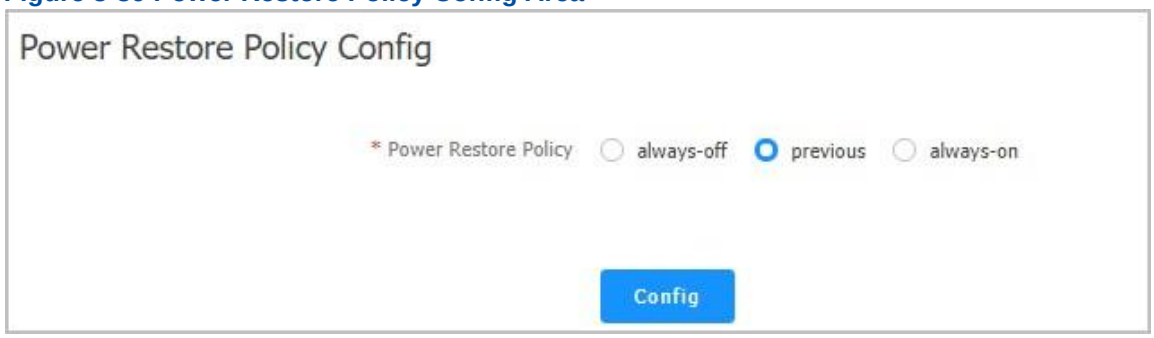
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page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

Figure 3-38 Configuring BMC V3



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



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

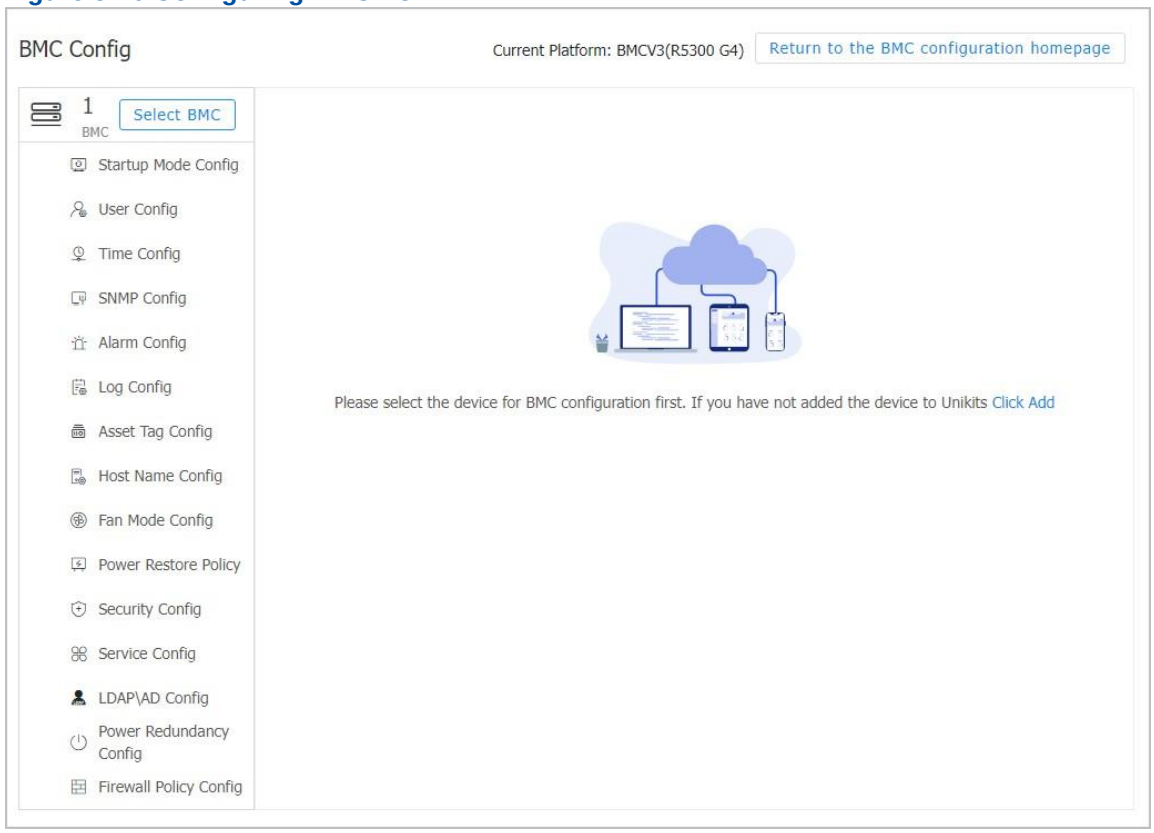
Abstract

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

Steps

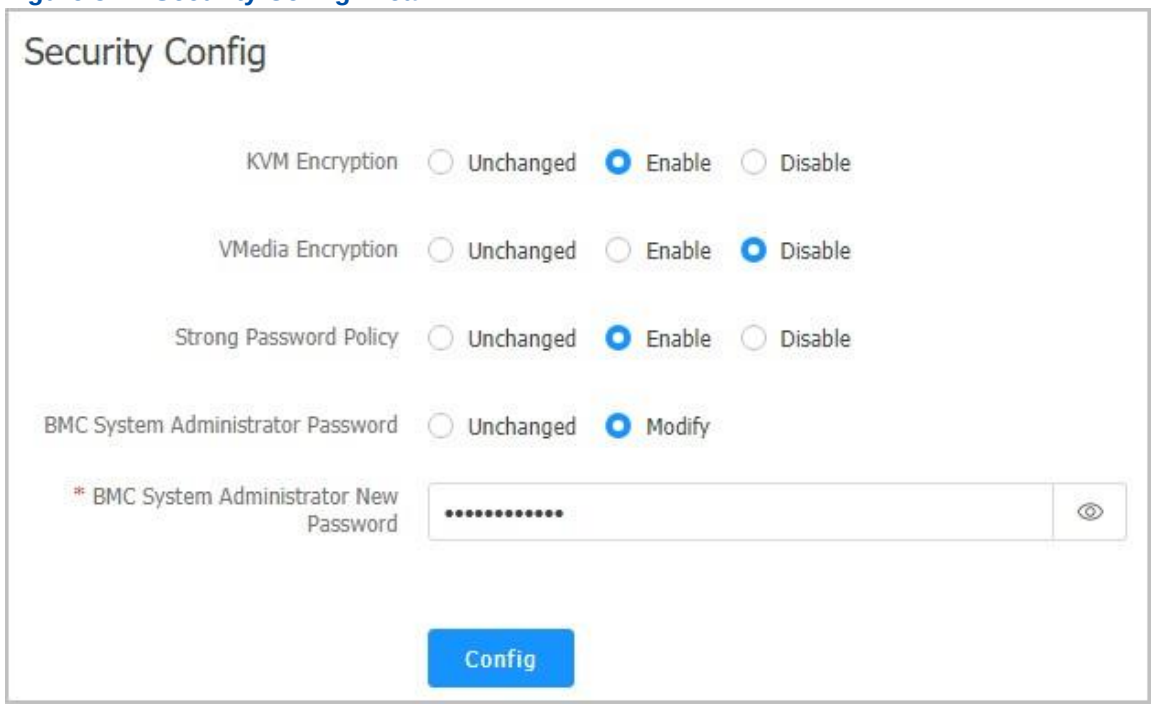
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page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

Figure 3-40 Configuring BMC V3



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



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 **KVM Encryption** is set to **Enable**, 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 **VMedia Encryption** is set to **Enable**, files remotely uploaded to the server through the KVM are encrypted.
Strong Password Policy	Select whether to enable the strong password policy. Options: ● **Unchanged**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the strong password policy. ● **Disable**: indicates to disable the strong password policy.
BMC System Administrator Password	Password for logging in to the server through SSH. Select whether to modify the original BMC system administrator password of the server. Options: ● **Unchanged**: indicates not to modify the original server configurations. ● **Modify**: indicates to modify the original password. Enter the new password in the **BMC System Administrator New Password** text box.

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

Note

- 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

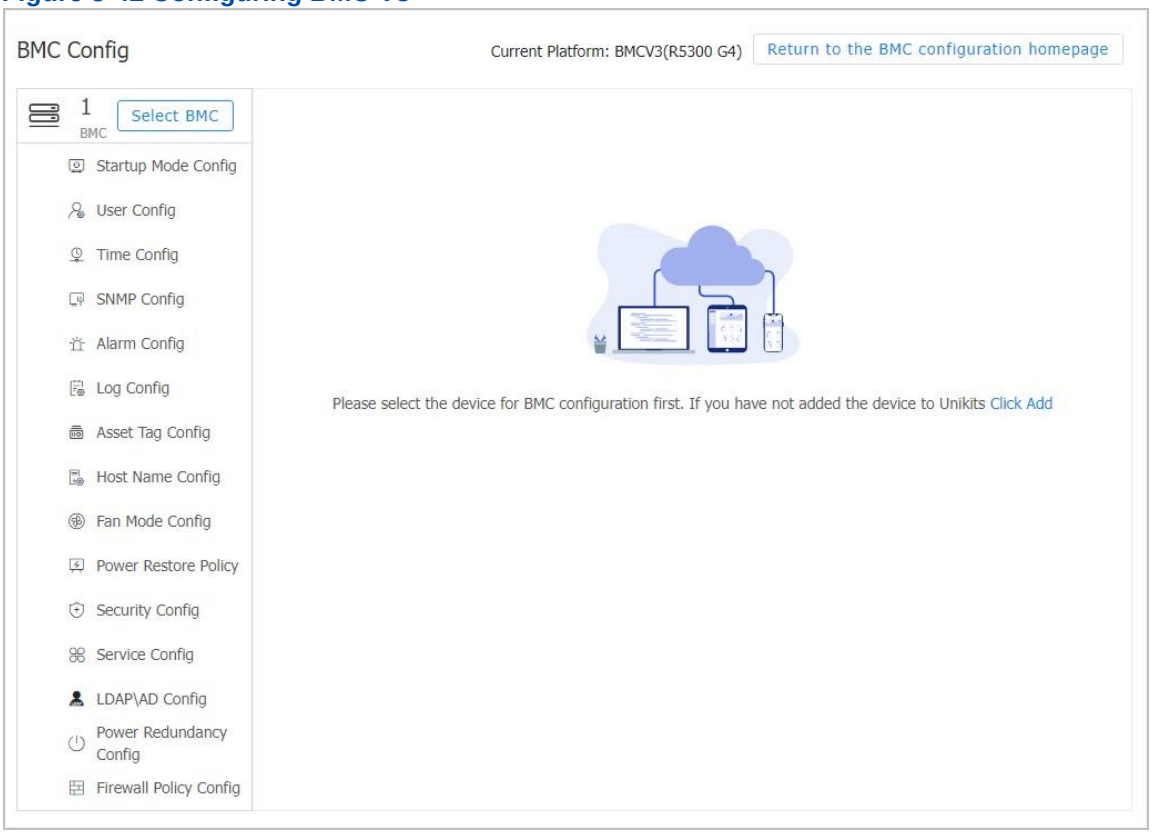
This procedure describes how to configure the status, secure port, non-secure port, and timeout for each service of a BMC.

Steps

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

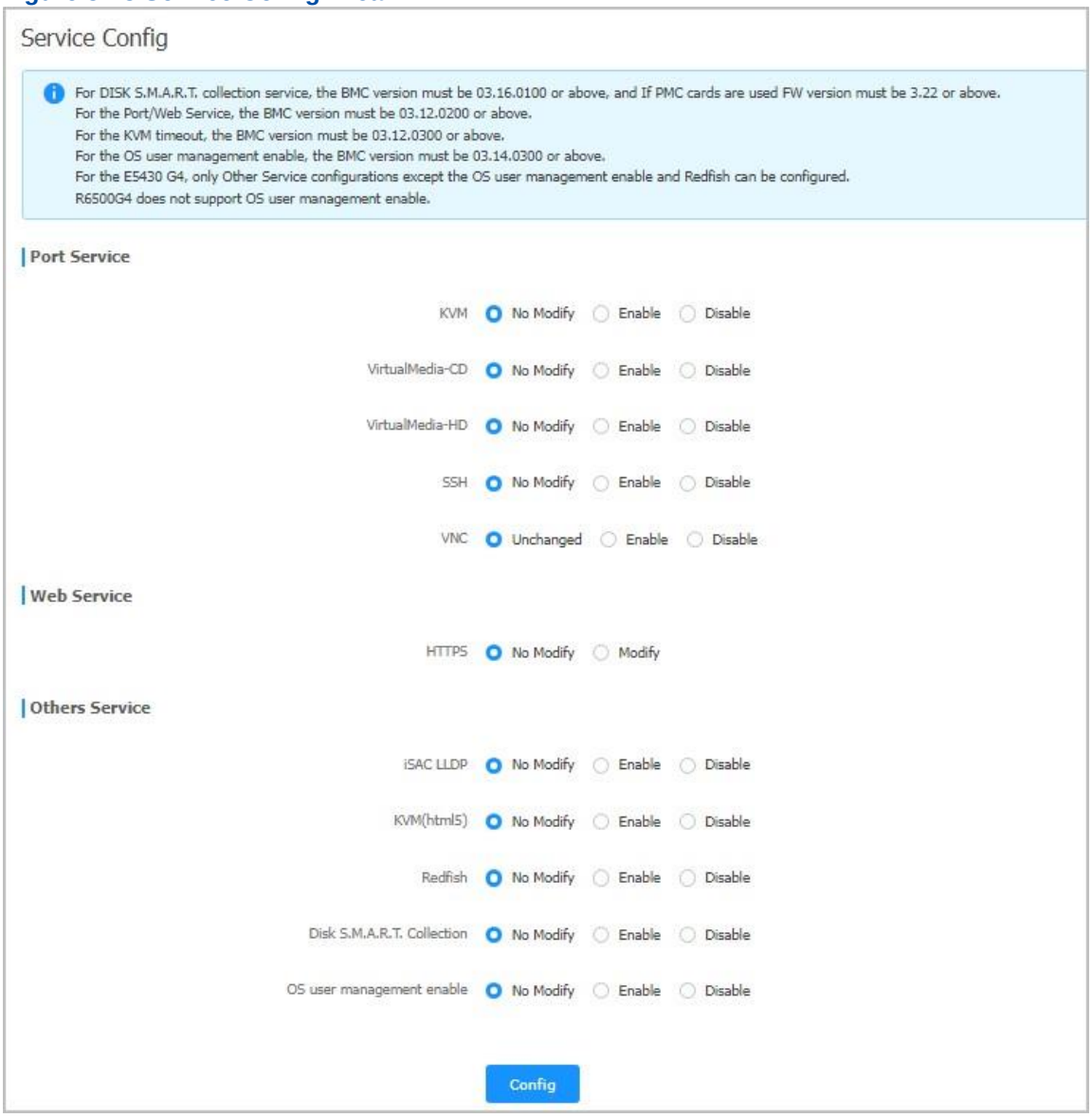
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page for configuring BMC V3 is displayed, as shown in Figure 3-42.

Figure 3-42 Configuring BMC V3



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



6. Set the parameters. For a description of the parameters, refer to Table 3-24.

Table 3-24 Service Parameter Descriptions

Parameter	Description
Port Service	
KVM	Select the KVM service configuration mode. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the KVM service.

Parameter	Description

	● **Disable**: indicates to disable the KVM service. After enabling the KVM service, you need to configure the following parameters: ● **KVM Port**: security port (default: 7582) in KVM encryption mode and non-security port (default: 7578) in KVM non-encryption mode. Port number range: 1–65535. ● **KVM TimeOut**: KVM service timeout period, range: 5–30 minutes.
VirtualMedia-CD	Select the VirtualMedia-CD service mode. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the VirtualMedia-CD service. ● **Disable**: indicates to disable the VirtualMedia-CD service. After enabling the VirtualMedia-CD service, you need to configure the following parameter: **VirtualMedia-CD Port**: security port (default: 5124) in VMedia encryption mode and non-security port (default: 5120) in VMedia non-encryption mode. Port number range: 1–65535.
VirtualMedia-HD	Select the VirtualMedia-HD service mode. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the VirtualMedia-HD service. ● **Disable**: indicates to disable the VirtualMedia-HD service. After enabling the VirtualMedia-HD service, you need to configure the following parameter: **VirtualMedia-HD Port**: security port (default: 5127) in VMedia encryption mode and non-security port (default: 5123) in VMedia non-encryption mode. Port number range: 1–65535.
SSH	Select the SSH service configuration mode. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the SSH service. ● **Disable**: indicates to disable the SSH service. After enabling the SSH service, you need to configure the following parameter: **SSH Port**: default: 22. Port number range: 1–65535.
VNC	Select the VNC service configuration mode. Options: ● **Unchanged**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the VNC service. ● **Disable**: indicates to disable the VNC service. After enabling the VNC service, you need to configure the following parameters: ● **VNC Nonsecure Port**: Enter a non-secure port number. Default: 5900, range: 1–65535.

Parameter	Description
	● **VNC Secure Port**: Enter a secure port number. Default: 5901, range: 1–65535. ● **VNC Service Password**: Select **Modify** and enter the new VNC password.
Web Service	
HTTPS	Select the HTTPS service configuration mode. Options: ● **No Modify**: indicates not to modify the original port number. ● **Modify**: indicates not to modify the original port number. After **Modify** is selected, the following parameter needs to be set: **HTTPS Port**: security port (default: 443). Port number range: 1–65535.
Others Service	
iSAC LLDP	Select the iSAC LLDP service configuration mode. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the iSAC LLDP service. ● **Disable**: indicates to disable the iSAC LLDP service.
KVM(html5)	Select the KVM(html5) service configuration mode. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the KVM(html5) service. ● **Disable**: indicates to disable the KVM(html5) service.
Redfish	Select the Redfish service configuration mode. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the Redfish service. ● **Disable**: indicates to disable the Redfish service.
DISK S.M.A.R.T. Collection	Select the DISK S.M.A.R.T. Collection service configuration mode. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the DISK S.M.A.R.T. Collection service. ● **Disable**: indicates to disable the DISK S.M.A.R.T. Collection service. The collection period ranges from 1 through 360 days.
OS user management enable	Select the configuration mode of the user management service. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Enable**: indicates to the enable the user management service in the BIOS/OS. That is, BMC users can be configured in the BIOS/OS. ● **Disable**: indicates to the disable the user management service in the BIOS/OS. That is, BMC users cannot be configured in the BIOS/OS.

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.

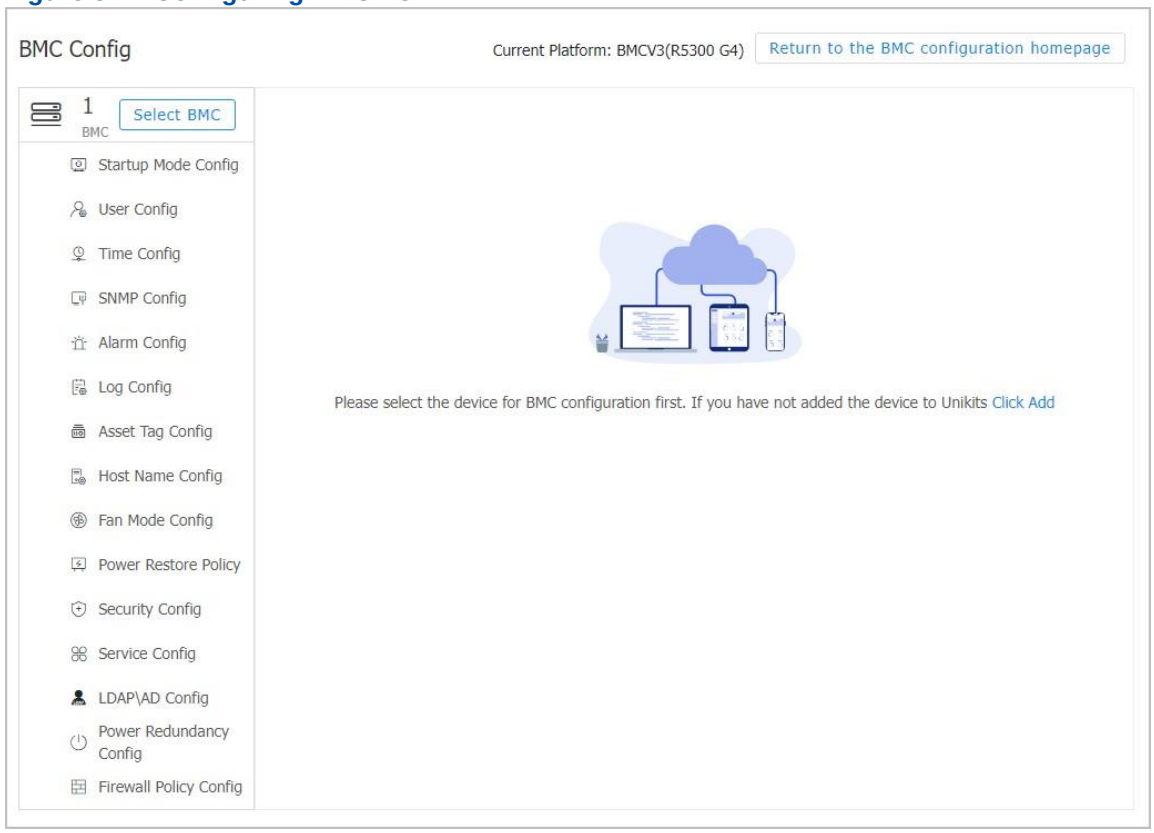
Note

External users refer to non-BMC users.

Steps

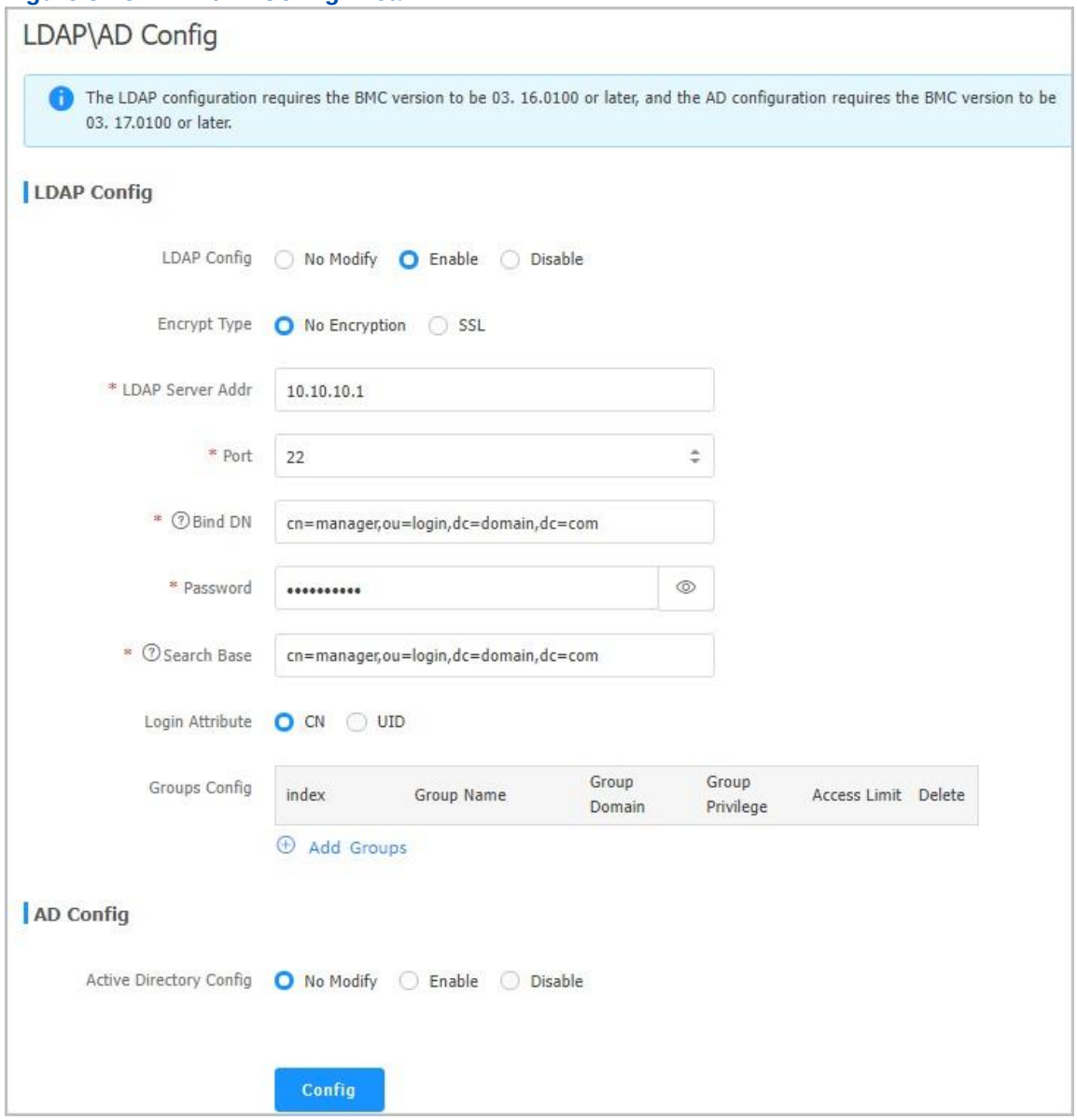
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page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

Figure 3-44 Configuring BMC V3



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



6. Set the parameters. For a description of the parameters, refer to Table 3-25.

Table 3-25 LDAP/AD Parameter Descriptions

Parameter	Description
LDAP Config	
LDAP Config	Select the LDAP configuration mode. Options: ● **No Modify**: indicates not to modify the original server configuration.

Parameter	Description

	• **Enable**: indicates to enable LDAP authentication. • **Disable**: indicates to disable LDAP authentication. After **LDAP Config** is set to **Enable**, LDAP parameters are activated.
Encrypt Type	Select the encryption type. Options: • **No Encryption**: indicates that no encryption is used. • **SSL**: indicates that SSL encryption is used.
LDAP Server Addr	Enter the IP address of the LDAP server in IPv4 or IPv6 format.
Port	Enter the port number. Range: 1–65535. Default: 389. If **Encrypt Type** is set to **SSL**, 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, *cn=manager,ou=login,dc=domain,dc=com*.
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, *ou=login,dc=domain,dc=com*.
Login Attribute	Select the attribute used by the LDAP server to identify users.
Groups Config	Click **Add Groups** to add a group and set the corresponding parameters.
AD Config	
Active Directory Config	Select the AD configuration mode. Options: • **No Modify**: indicates not to modify the original server configurations. • **Enable**: indicates to enable AD authentication. • **Disable**: indicates to disable AD authentication. After **Active Directory Config** is set to **Enable**, AD parameters are activated.
Encrypt Type	Select the encryption type. Options: • **No Encryption**: indicates that no encryption is used. • **SSL**: indicates that SSL encryption is used.

User Name	Enter the username for logging in to the AD server. ● The username is a string of 1–64 characters consisting of letters and digits. ● The username must start with an alphabetic character. ● Letters are case-sensitive. ● Special characters are not allowed.
Parameter	**Description**
	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, *MyDomain.com*.
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 **Add Groups** 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.

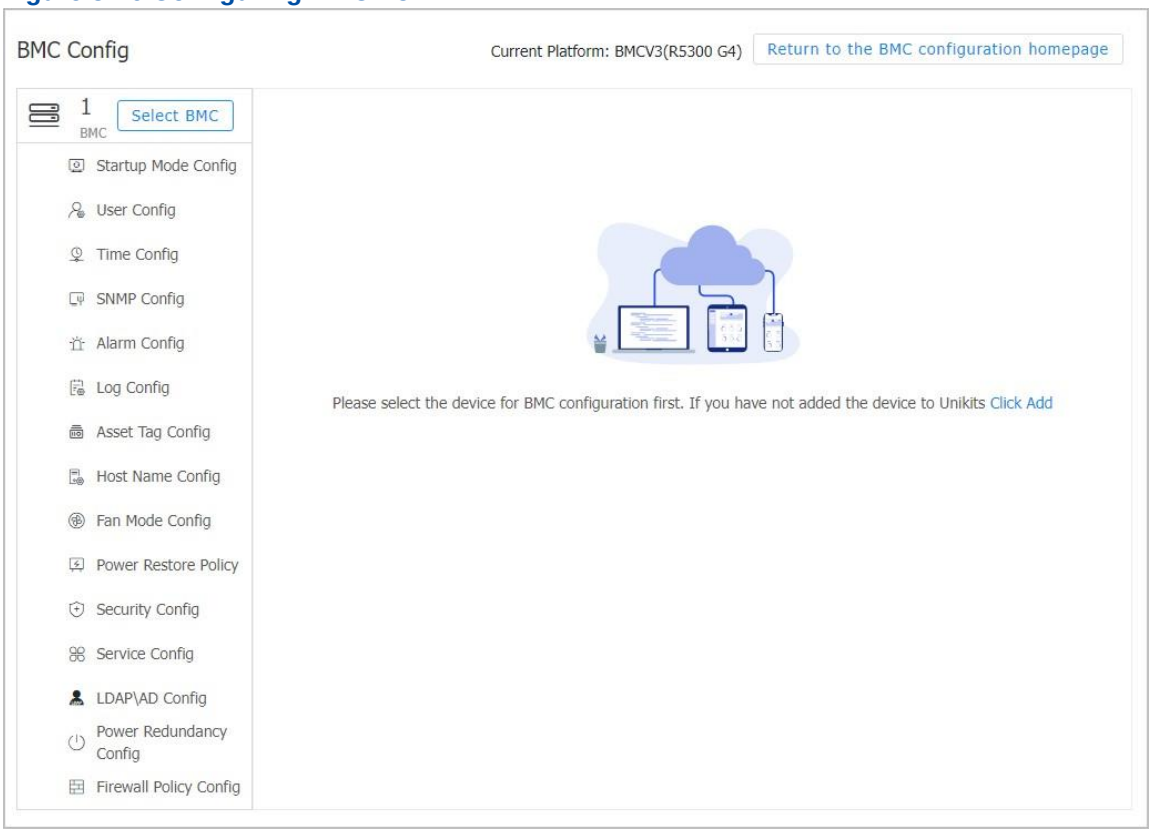
Prerequisite

The license is already imported. For how to import a license, refer to "3.9.4 Importing a License".

Steps

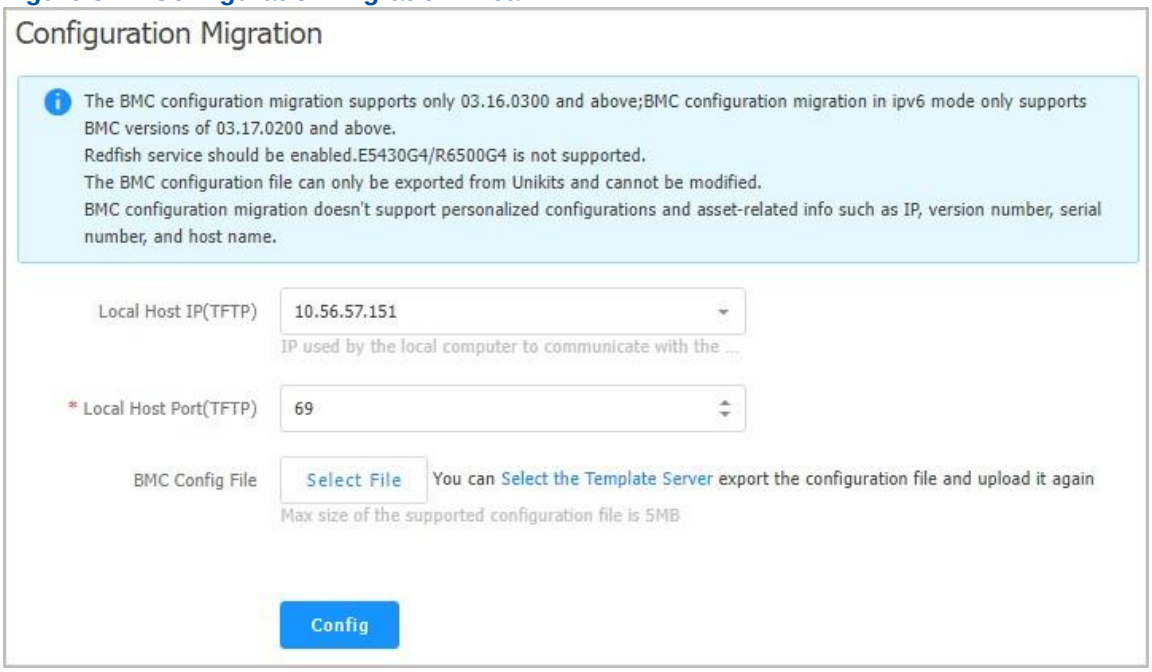
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page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

Figure 3-46 Configuring BMC V3



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



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	• If there is a local configuration file, click **Select File**, and select the configuration file. • If there is no local configuration file, click **Select the Template Server**, and select the corresponding template server to use the configuration file exported from the template server.

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:

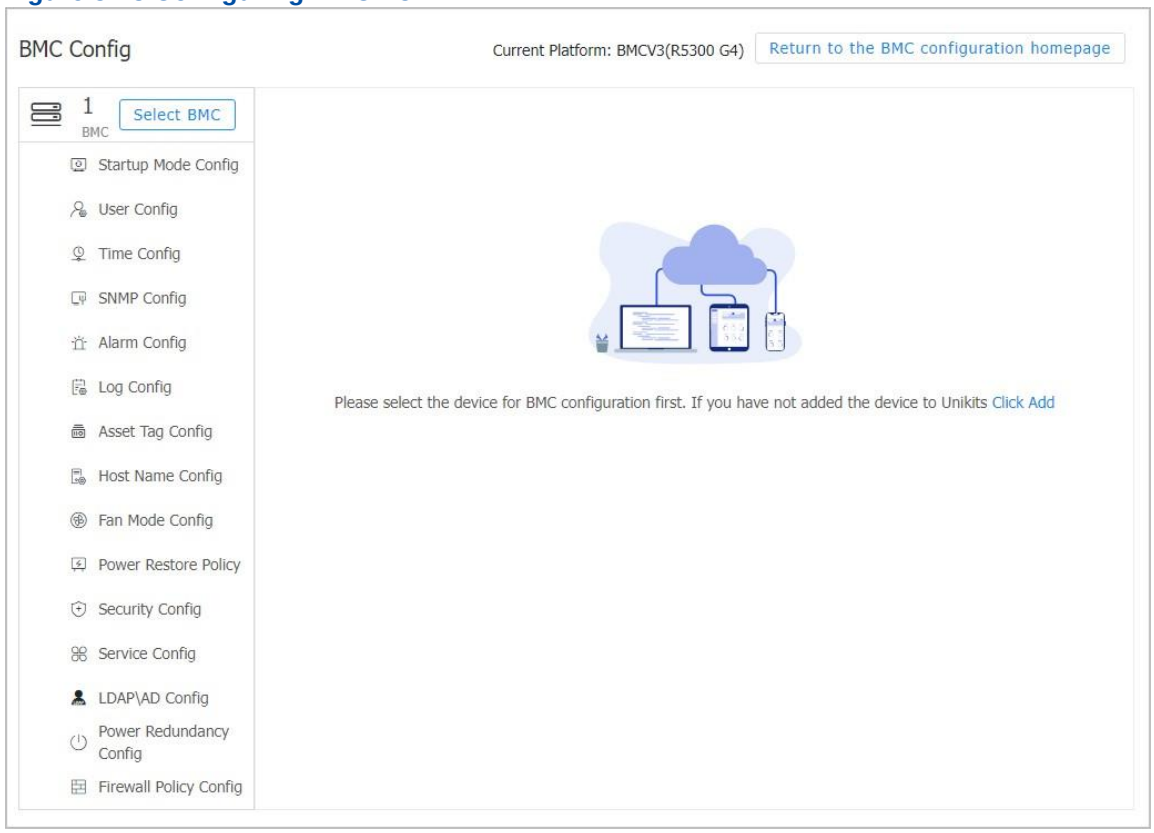
- **Sharing**: The power modules supply power in load-balancing mode.
- **Failover**: The power modules supply power in active/standby mode.

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

Steps

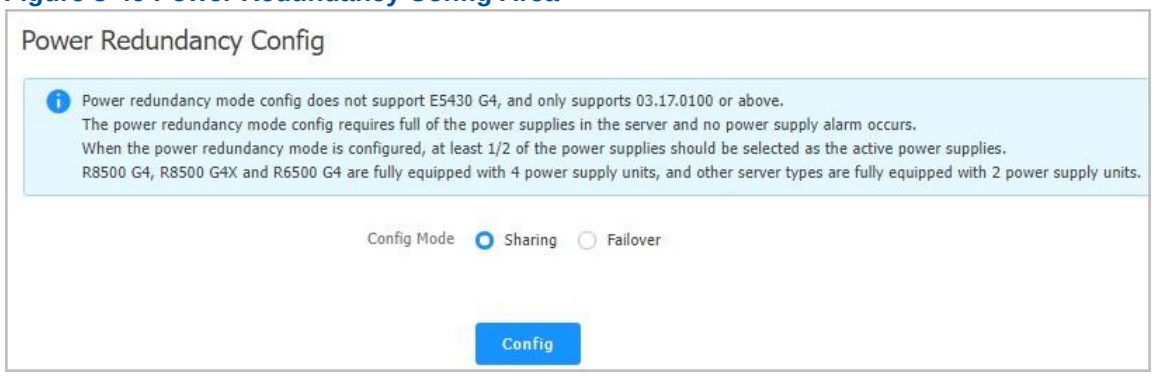
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content corresponding to BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The page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

Figure 3-48 Configuring BMC V3



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



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.

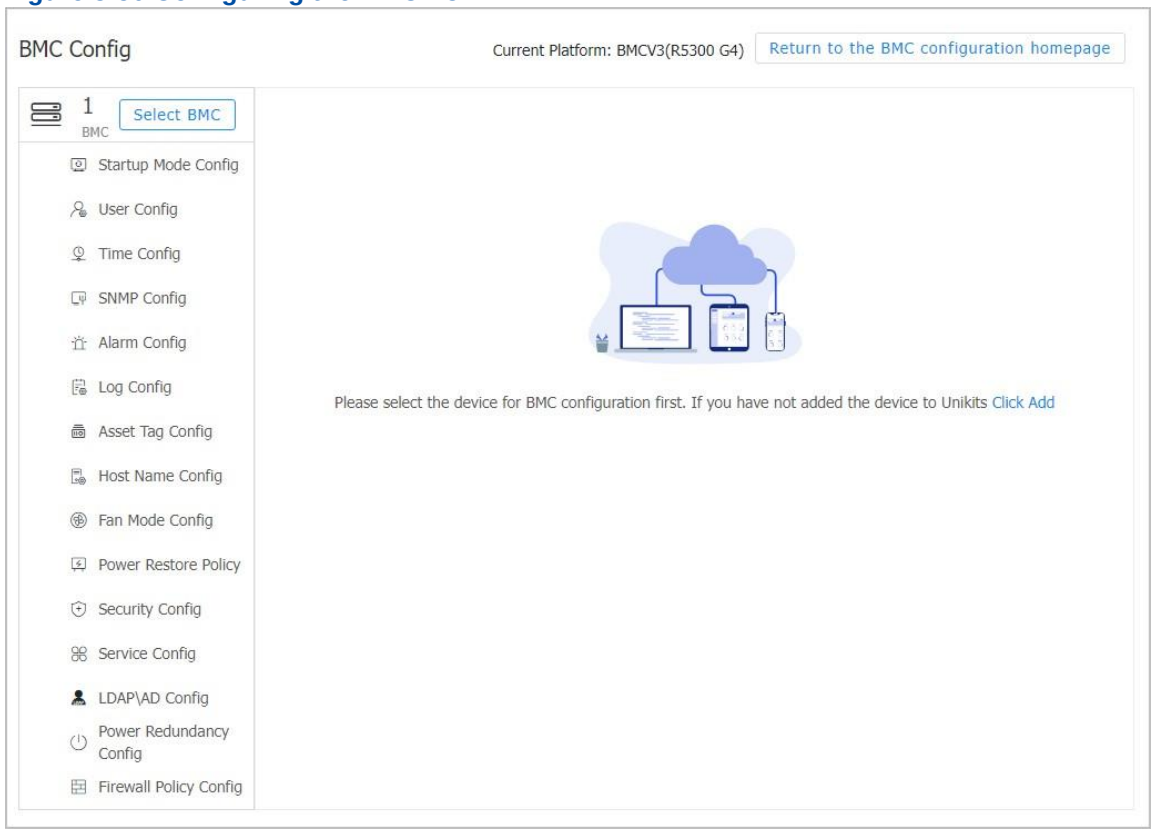
- The devices in a blacklist are forbidden to access the BMC.
- Only the devices in a whitelist are allowed to access the BMC.
  When adding a whitelist, you must first add the IP address of your local PC (acting as a client PC) to the whitelist to ensure that your local PC can access the Web portal of the BMC.

This procedure describes how to configure firewall parameters.

Steps

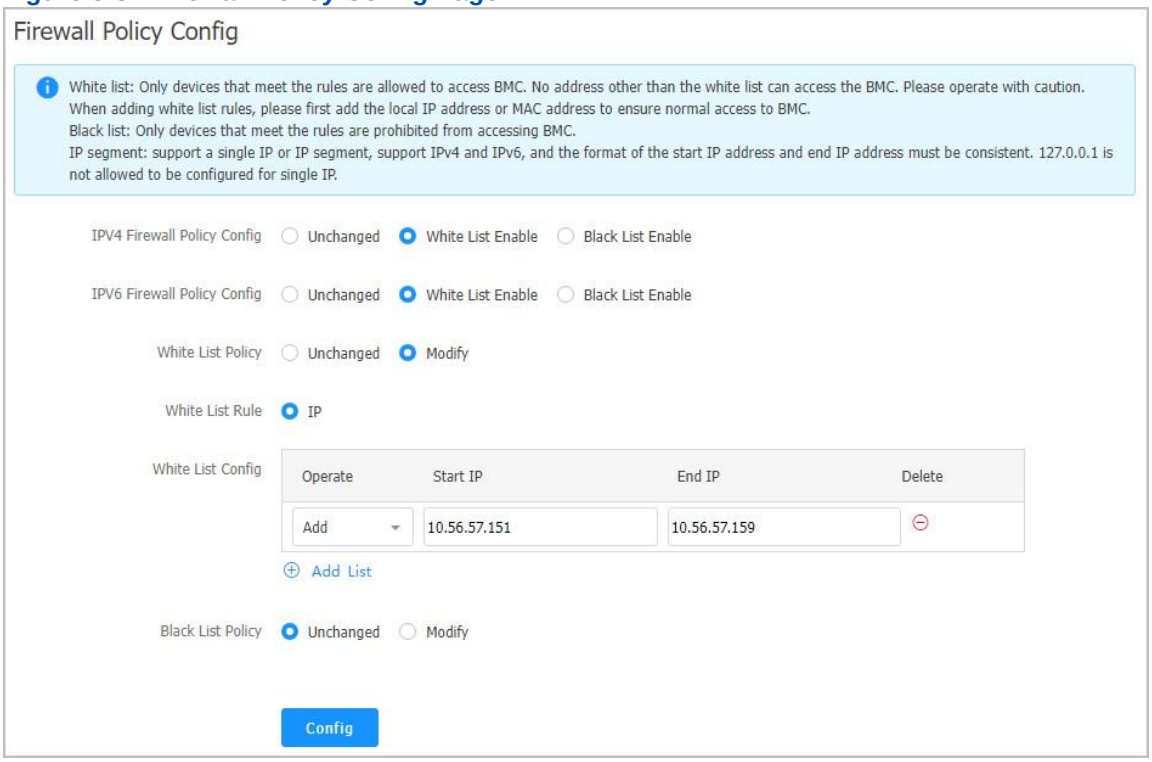
1. Select **Device Mgmt > Deployment > BMC Config**. The **BMC Config** page is displayed.
2. From the **Please select the server model to be configured** list, select the desired server model. The content of the corresponding BMC V3 is automatically displayed on the UniKits.
3. Click **Submit**. The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

Figure 3-50 Configuring the BMC V3



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



6. Set the parameters. For a description of the parameters, refer to Table 3-27.

Table 3-27 Firewall Parameter Descriptions

Parameter	Description
IPv4 Firewall Policy Config	Select the IPv4 firewall policy. Options: ● **Unchanged**: indicates not to modify the original server configurations. ● **White List Enable**: indicates that only the devices in a whitelist are allowed to access the Web portal of the BMC. ● **Black List Enable**: indicates that the devices in a blacklist are not allowed to access the Web portal of the BMC.
IPv6 Firewall Policy Config	Select the IPv6 firewall policy. Options: ● **Unchanged**: indicates not to modify the original server configurations. ● **White List Enable**: indicates that only the devices in a whitelist are allowed to access the Web portal of the BMC. ● **Black List Enable**: indicates that only the devices in a blacklist are not allowed to access the Web portal of the BMC.
White List Policy	Select whether to modify the whitelist. Options: ● **Unchanged**: indicates not to modify the original server whitelist. ● **Modify**: indicates to modify the original whitelist of the server, and adds or deletes IP address segments in **White List Config**.

Black List Policy	Select whether to modify the blacklist. Options: ● **Unchanged**: indicates not to modify the original server blacklist.
Parameter	**Description**
	● **Modify**: indicates to modify the original blacklist of the server, and adds or deletes IP address segments in **Black List Config**.

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

Note

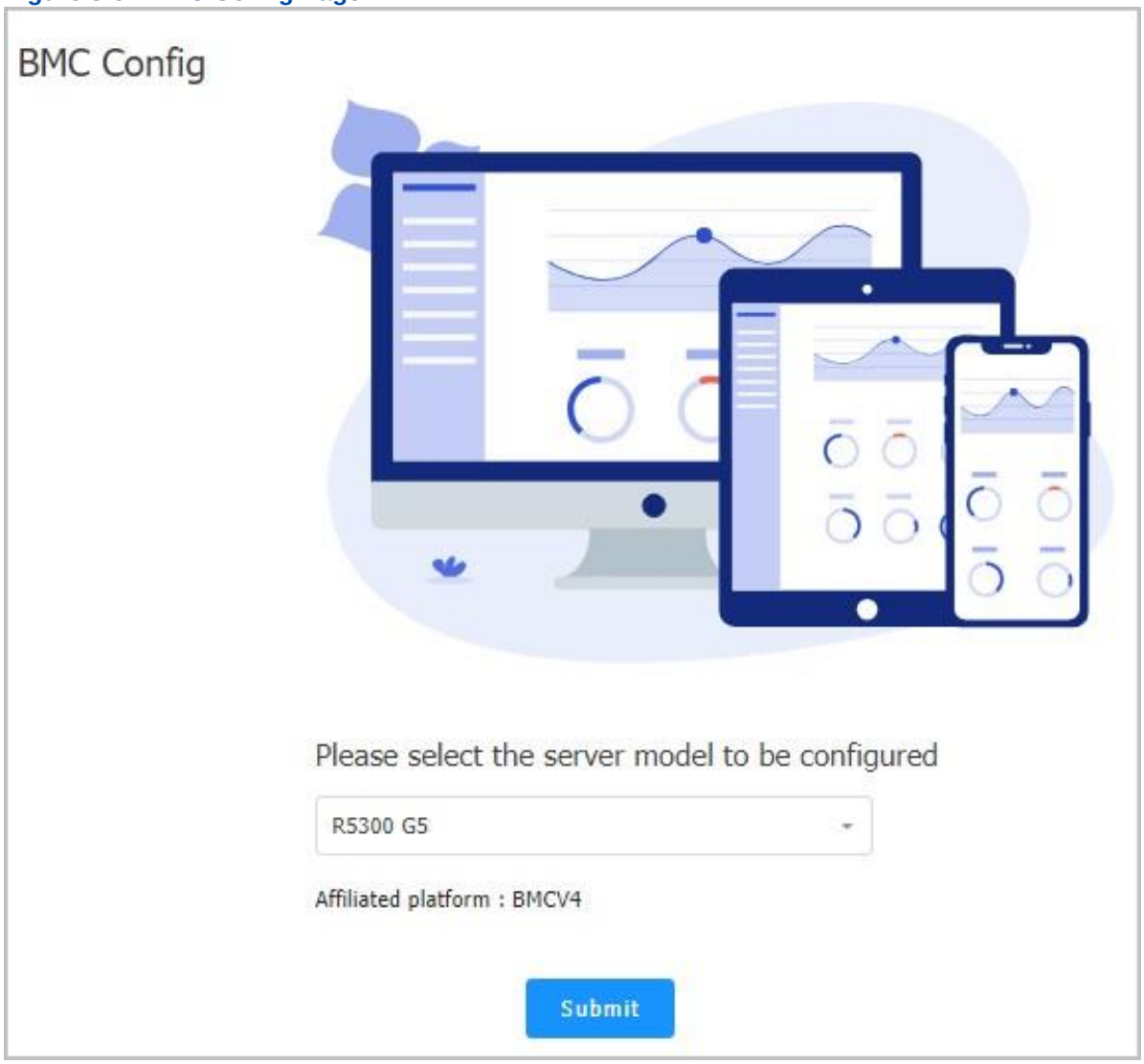
- During firewall parameter configuration, the progress bar is displayed on the page.
- After firewall parameter configuration is completed, the configuration result is displayed on the page.

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

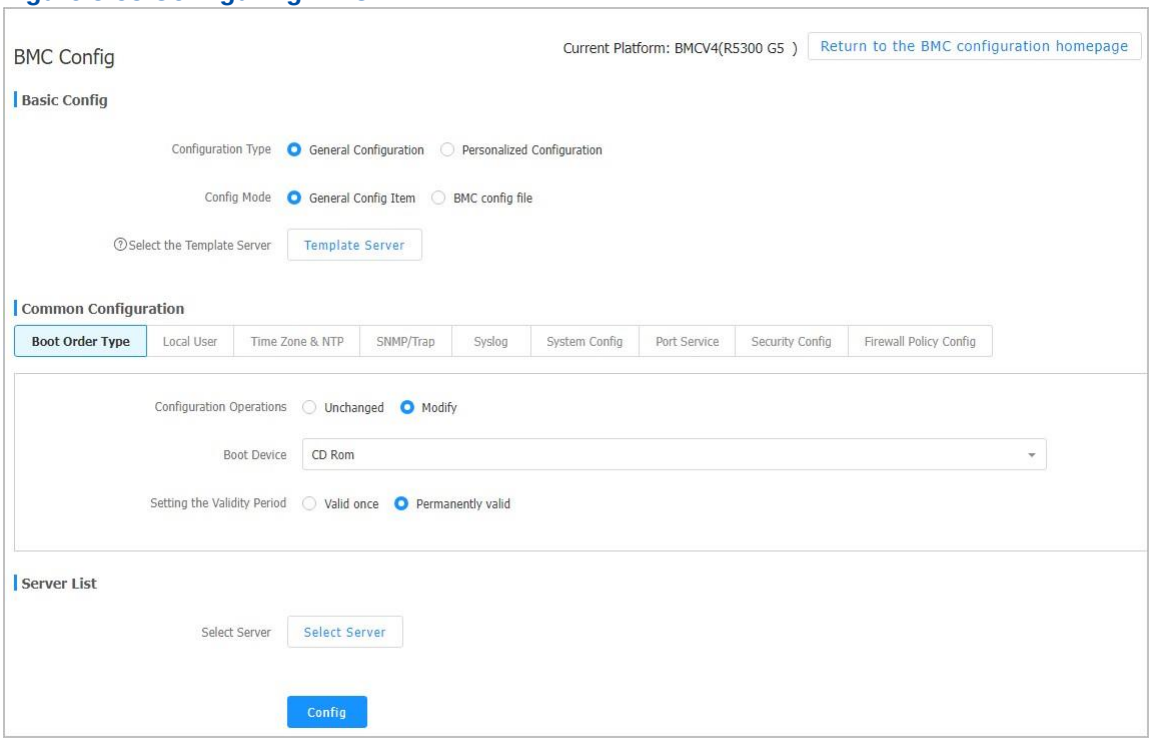
Abstract

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



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 **General Configuration**.
Config Mode	Select a configuration mode. Options: ● **General Config Item** → To import the configurations from a template server, click **Template Server**, 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 **Common Configuration** area, and can be modified. → To not import the configurations from a template server, do not select this option. ● **BMC config file** → To import the configurations in a BMC configuration file, click **Select File**, 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 **Common Configuration** area, and can be modified. → To not import a BMC configuration file, do not select this option.

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

6. 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.

3.4.3.2 Configuring a User

Abstract

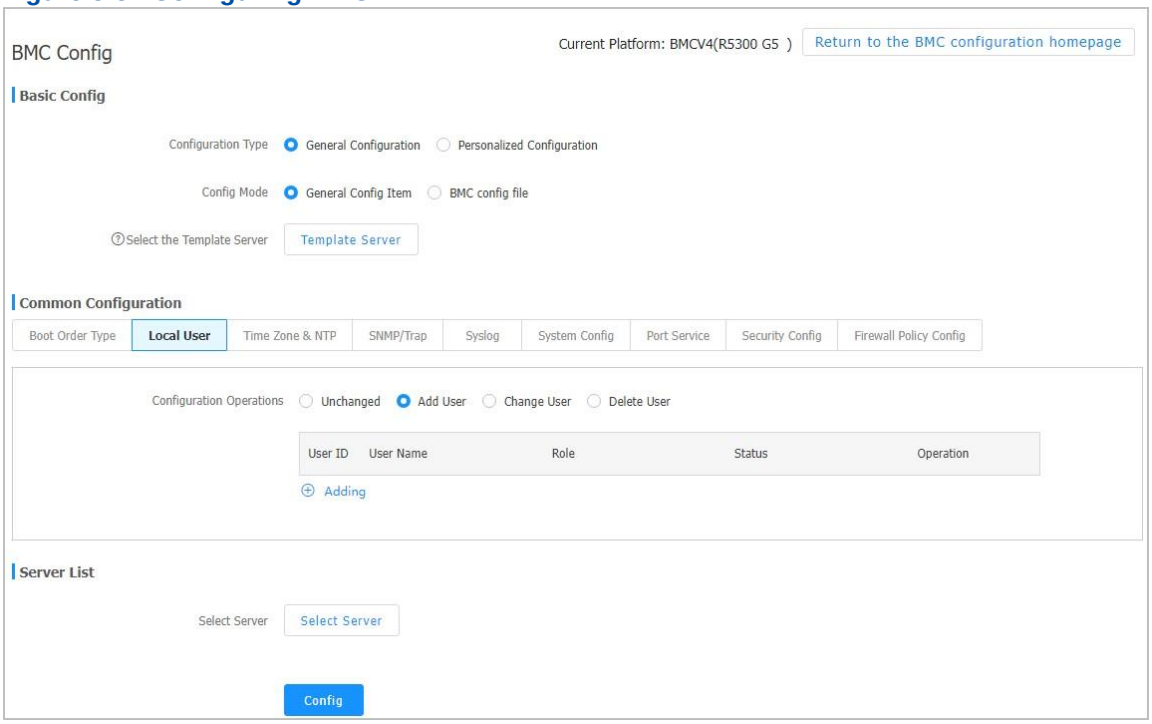
This procedure describes how to configure a BMC user for BMC configuration and management.

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



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 **General Configuration**.
Config Mode	User configuration does not support import or export. Therefore, this parameter does not need to be configured.
Configuration Operations	Select whether to add, modify, or delete a BMC user. ● To not modify the original user configurations, select **Unchanged**. ● To add a BMC user, select **Add User**. After **Add User** is selected, the **Adding** button is activated. Click **Adding**, and set the user parameters in the displayed dialog box. ● To modify a BMC user, select **Change User**. After **Change User** is selected, the **Select User** button is activated. Click **Select User**, and modify the user parameters in the displayed dialog box. ● To delete a BMC user, select **Delete User**. After **Delete User** is selected, the **Adding** button is activated. Click **Adding**, and enter the BMC username that you want to delete.

Select Server	Click **Select Server**, 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

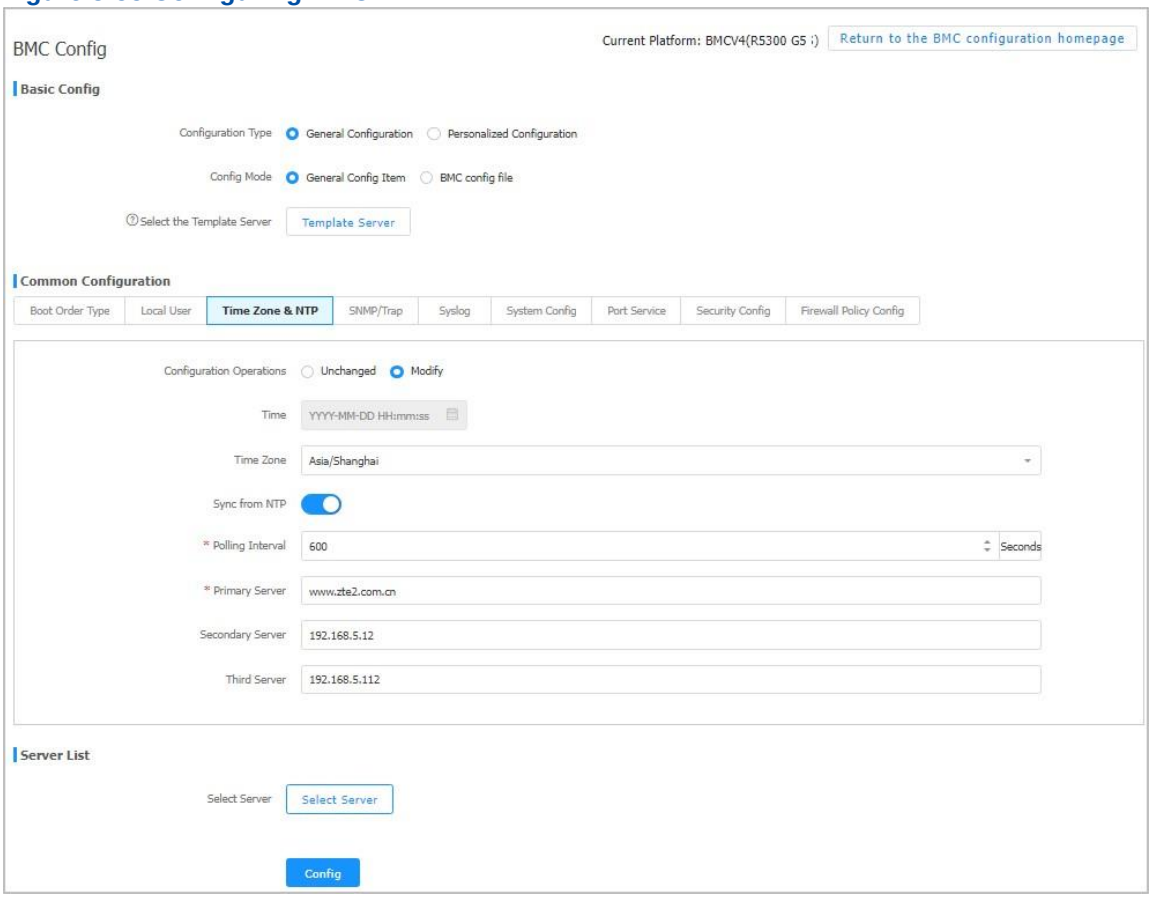
Abstract

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



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 **General Configuration**.

Config Mode	Select a configuration mode. Options: ● **General Config Item** → To import the configurations from a template server, click **Template Server**, 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 **Common Configuration** area, and can be modified. → To not import the configurations from a template server, do not select this option. ● **BMC config file** → To import the configurations in a BMC configuration file, click **Select File**, 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 **Common Configuration** area, and can be modified. → To not import a BMC configuration file, do not select this option.
Configuration Operations	Select whether to modify the original server configurations. ● **Unchanged**: indicates not to modify the original server configurations. ● **Modify**: indicates to modify the original server configurations. After selecting **Modify**, you also need to set the following parameters: ● **Time** ● **Time Zone** ● **Sync from NTP** ● **Polling Interval** ● **Primary Server** ● **Secondary Server** ● **Third Server**
Time	● This parameter can be set when **Sync from NTP** is disabled. Click and then set the time. ● This parameter cannot be set when **Sync from NTP** is enabled.
Time Zone	Select a time zone identified by location.
Sync from NTP	● To synchronize time with an NTP server, enable **Sync from NTP**. After **Sync from NTP** is enabled, the following parameters are activated: → **Polling Interval** → **Primary Server** → **Secondary Server**
Parameter	**Description**
	→ **Third Server** ● To not synchronize time with an NTP server, disable **Sync from NTP**.
Polling Interval	Enter the time synchronization interval in seconds, range: 60–65535.

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

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

Note

- 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

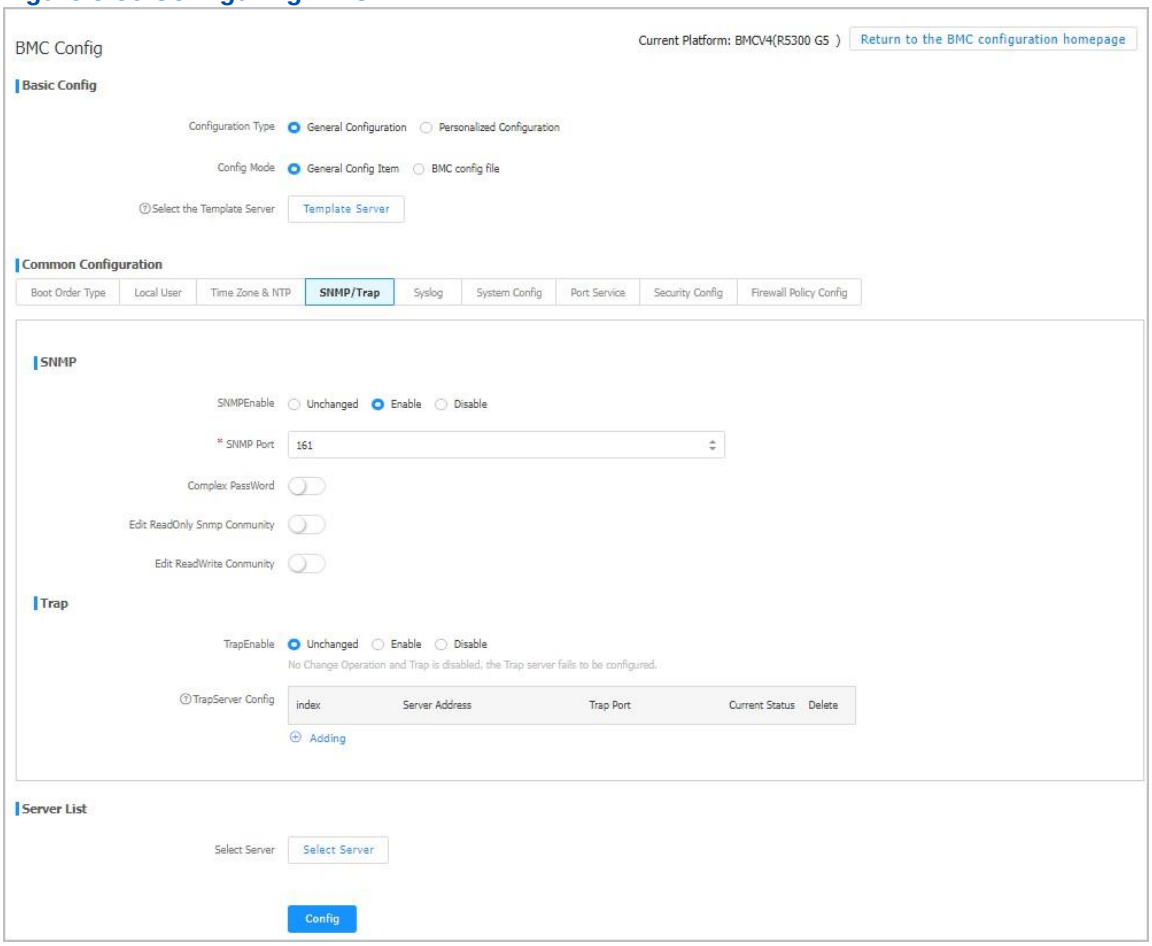
Abstract

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



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 **General Configuration**.

Configuration Mode	Select a configuration mode. Options: ● **General Config Item** → To import the configurations from a template server, click **Template Server**, 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 **Common Configuration** area, and can be modified. → To not import the configurations from a template server, do not select this option. ● **BMC config file** → To import the configurations in a BMC configuration file, click **Select File**, 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 **Common Configuration** area, and can be modified.

Parameter	**Description**
	→ To not import a BMC configuration file, do not select this option. SNMP community names cannot be imported or exported.
SNMPEnable	Select whether to enable the SNMP function. Options: ● **Unchanged**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the SNMP function. ● **Disable**: indicates to disable the SNMP function. After enabling the SNMP function, you also need to set the following parameters: ● **SNMP Port** ● **Complex PassWord** ● **Edit ReadOnly Snmp Community** ● **Edit ReadWrite Community**
SNMP Port	Enter the non-secure port number of the SNMP service. Range: 1–65535, default: 161.
Complex PassWord	● To use a strong password, enable **Complex PassWord**. After this function is enabled, the read-only community name and read-write community name must comply with the password strength rules. ● To not use a strong password, disable **Complex PassWord**.
Edit ReadOnly Snmp Community	● To edit the read-only community name, enable **Edit ReadOnly Snmp Community** and then enter the read-only community name (default: roAdmin9!). ● To not edit the read-only community name, disable **Edit ReadOnly Snmp Community**.

Edit ReadWrite Community	• To edit the read-write community name, enable **Edit ReadWrite Community** and then enter the read-write community name (default: rwAdmin9!). • To not edit the read-write community name, disable **Edit ReadWrite Community**.
TrapEnable	Select whether to enable the trap function. Options: • **Unchanged**: indicates not to modify the original server configurations. • **Enable**: indicates to enable the trap function. • **Disable**: indicates to disable the trap function. After enabling the trap function, you also need to set the following parameters: • **Trap Version** • **Select V3 User** • **Community** • **Confirm Community** • **TrapHost ID** • **TrapAlarm Severity** • **TrapServer Config**
Trap Version	Select the SNMP version for traps. Options: **V1**, **V2C**, and **V3**.
Parameter	**Description**
Select V3 User	This parameter is required when **Trap Version** is set to **V3**. Select an SNMPv3 user as the alarm sender.
Community	This parameter is required when**Trap Version** is set to **V1** or **V2C**. Enter the trap community name.
Confirm Community	This parameter is required when **Trap Version** is set to **V1** or **V2C**. Enter the trap community name, which must be the same as that in **Community**.
TrapHost ID	Select the identifier of the host that reports alarms.
TrapAlarm Severity	Select the level of events to be reported. For example, if **TrapAlarm Severity** is set to **Critical**, only critical alarms are reported.
TrapServer Config	Click **Adding** to add trap servers. A maximum of four trap servers can be added. After adding a trap server, you need to set the following parameters: • **index**: Select the sequence of the trap server. Range: 1–4. • **Server Address**: Enter the address of the server that receives alarms. An IPv4 address, IPv6 address, or domain name is supported. • **Trap Port**: Enter the port number of the server that receives alarms. Range: 1–65535. • **Current Status**: Select whether to enable the current server to receive alarms.

Select Server	Click **Select Server**, and select the servers to be configured in the displayed dialog box.

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

Note

- 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

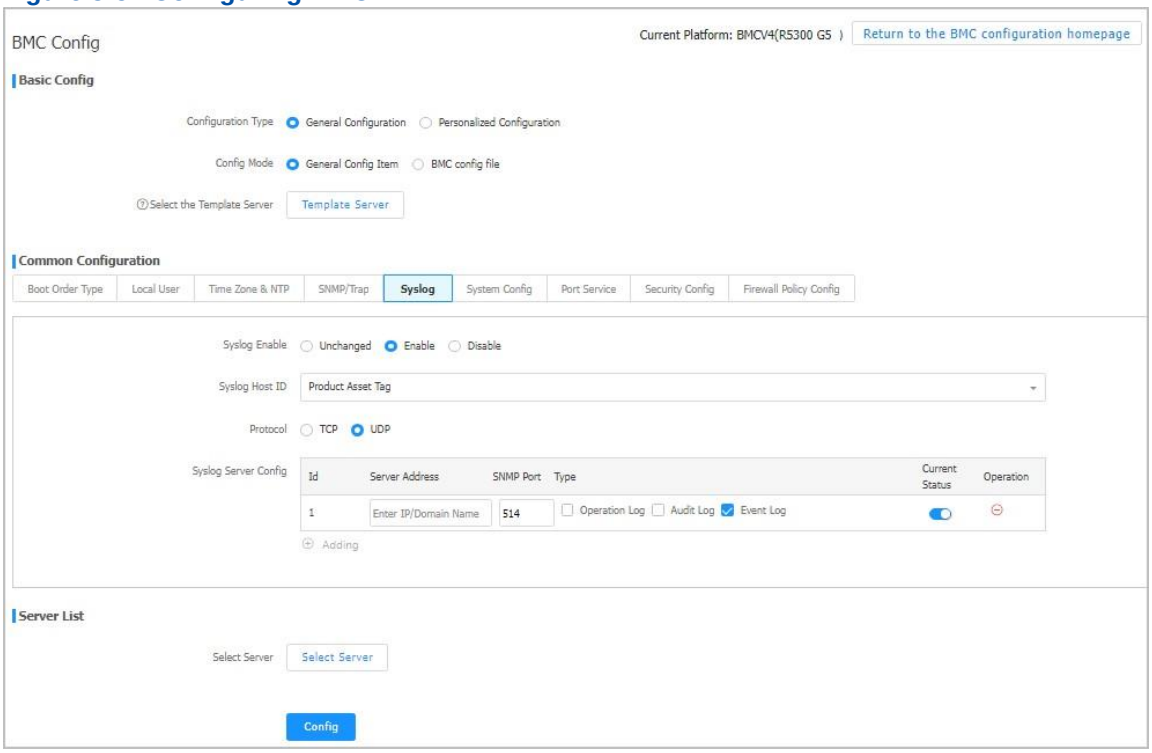
Abstract

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



4. In the **Common Configuration** area, click **Syslog** to switch to the **Syslog** tab.
5. 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 **General Configuration**.
Config Mode	Select a configuration mode. Options: ● **General Config Item** → To import the configurations from a template server, click **Template Server**, 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 **Common Configuration** area, and can be modified. → To not import the configurations from a template server, do not select this option. ● **BMC config file** → To import the configurations in a BMC configuration file, click **Select File**, 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 **Common Configuration** area, and can be modified.
Parameter	**Description**
	→ To not import a BMC configuration file, do not select this option.

Syslog Enable	Select whether to enable the syslog function. ● **Unchanged**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the syslog function. ● **Disable**: indicates to disable the syslog function. After **Enable** is selected, the following parameters also need to be set: ● **Syslog Host ID** ● **Protocol** ● **Syslog Server Config**
Syslog Host ID	Select how to identify the host in a log file. Options: ● **Host Name**: identified by host name. ● **Product Asset Tag**: identified by asset tag. ● **Board serial number**: identified by board SN.
Protocol	Select the log transmission protocol. Options: ● **UDP** ● **TCP**
Syslog Server Config	Set the parameters related to the syslog server. ● **Server Address**: enter the IP address of the syslog server. ● **SNMP Port**: enter the port number of the syslog server. Range: 1–65535. ● **Type**: 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.
Select Server	Click **Select Server**, and select the servers to be configured in the displayed dialog box.

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

Note

- 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

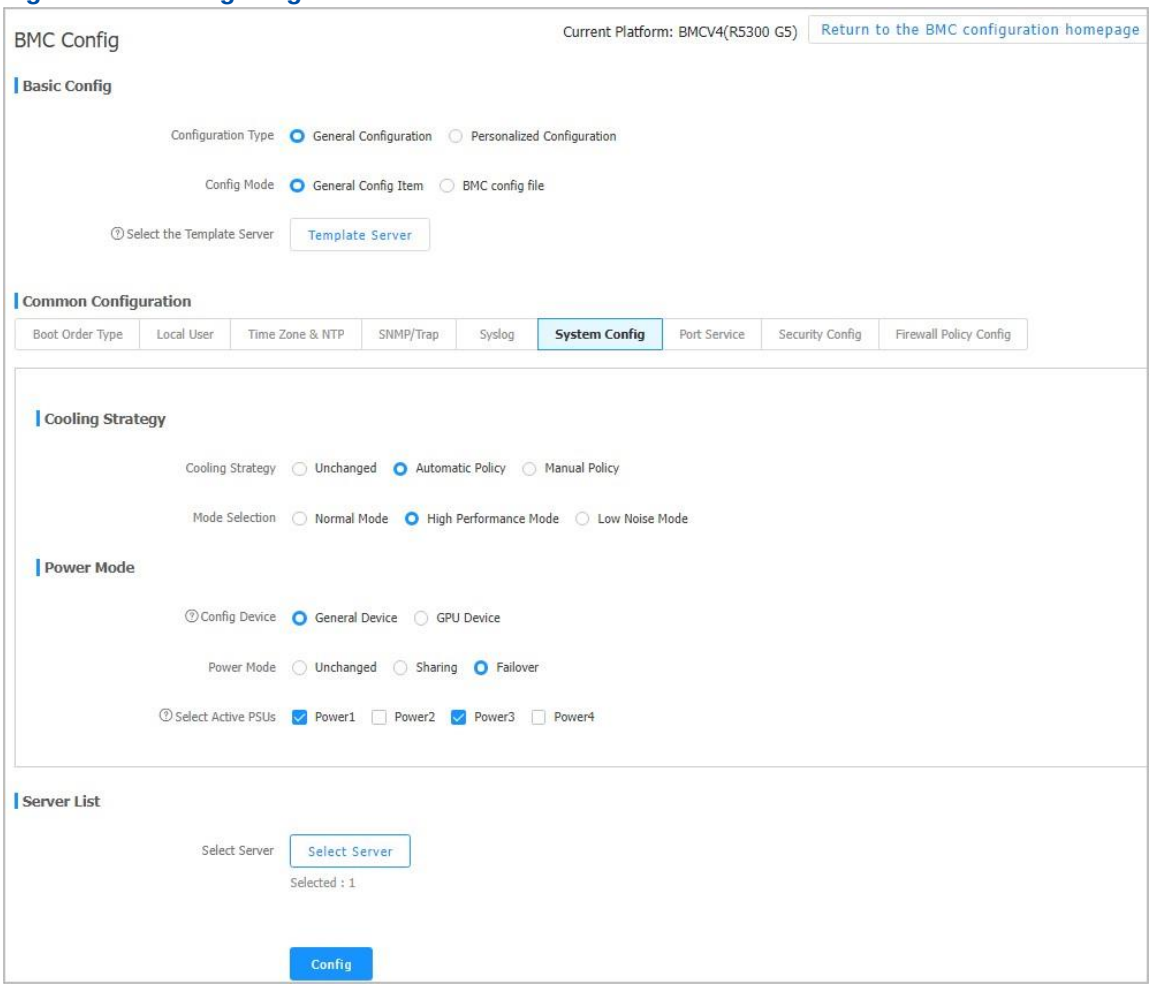
System parameters include the cooling policy and power mode.

- 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



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 **General Configuration**.
Config Mode	Select a configuration mode. Options: ● **General Config Item**

Parameter	Description
	→ To import the configurations from a template server, click **Template Server**, 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 **Common Configuration** area, and can be modified. → To not import the configurations from a template server, do not select this option. ● **BMC config file** → To import the configurations in a BMC configuration file, click **Select File**, 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 **Common Configuration** area, and can be modified. → To not import a BMC configuration file, do not select this option.
Cooling Strategy	Select a cooling policy. Options: ● **Unchanged**: indicates not to modify the original server configurations. ● **Automatic Policy**: indicates to automatically regulate the rotational speed of fan units. After selecting **Automatic Policy**, you also need to set **Mode Selection**. ● **Manual Policy**: indicates to manually regulate the rotational speed of fan units. After selecting **Manual Policy**, you also need to set **Speed Percentage**.
Mode Selection	This parameter is required when **Cooling Strategy** is set to **Automatic Policy**. Select an automatic speed regulation mode. ● **Normal Mode**: selected when there is clearance above the top surface of a server and the server is insensitive to noise. ● **High Performance Mode**: selected when servers are stacked together and there is no clearance between them. ● **Low Noise Mode**: selected when servers are placed in an office or other areas that are sensitive to noise. **Low Noise Mode** is not available for the NCS6742G N4 servers.
Speed Percentage	This parameter is required when **Cooling Strategy** is set to **Manual Policy**. The speed ratio is the ratio of the current speed of a fan to the maximum speed of the fan. Enter a percentage, range: 10%–100%.
Config Device	Select a server model to be configured. Options: ● **General Device**: a model without GPU modules. ● **GPU Device**: a model configured with GPU modules.

Power Mode/Main-Board Power Mode	When **Config Device** is set to **General Device**, the **Power Mode** parameter is displayed. When **Config Device** is set to **GPU Device**, the **MainBoard Power Mode** parameter is displayed. Select a power mode. Options:
Parameter	**Description**
	• **Unchanged**: indicates not to modify the original server configurations. • **Sharing**: 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. • **Failover**: 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 **Failover** mode can be selected only when two or more power modules are present and operating properly. If **Power Mode** is set to **Failover**, you also need to set the **Select Active PSUs** parameter to select the active power modules.
Select Active PSUs	This parameter is required when **Power Mode** is set to **Failover**. Select the active power modules. For a dual-power-module server, you can select **Power1** and **Power2** only.
GPU Power Mode	This parameter is required when **Config Device** is set to **GPU Device**. Select the power mode of the GPU module. Options: • **Unchanged**: indicates not to modify the original server configurations. • **Sharing**: 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. • **Failover**: 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 **Failover** mode can be selected only when two or more power modules are present and operating properly. If **Power Mode** is set to **Failover**, you also need to set the **Select Active PSUs** parameter to select the active power modules.

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

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

Note

- 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

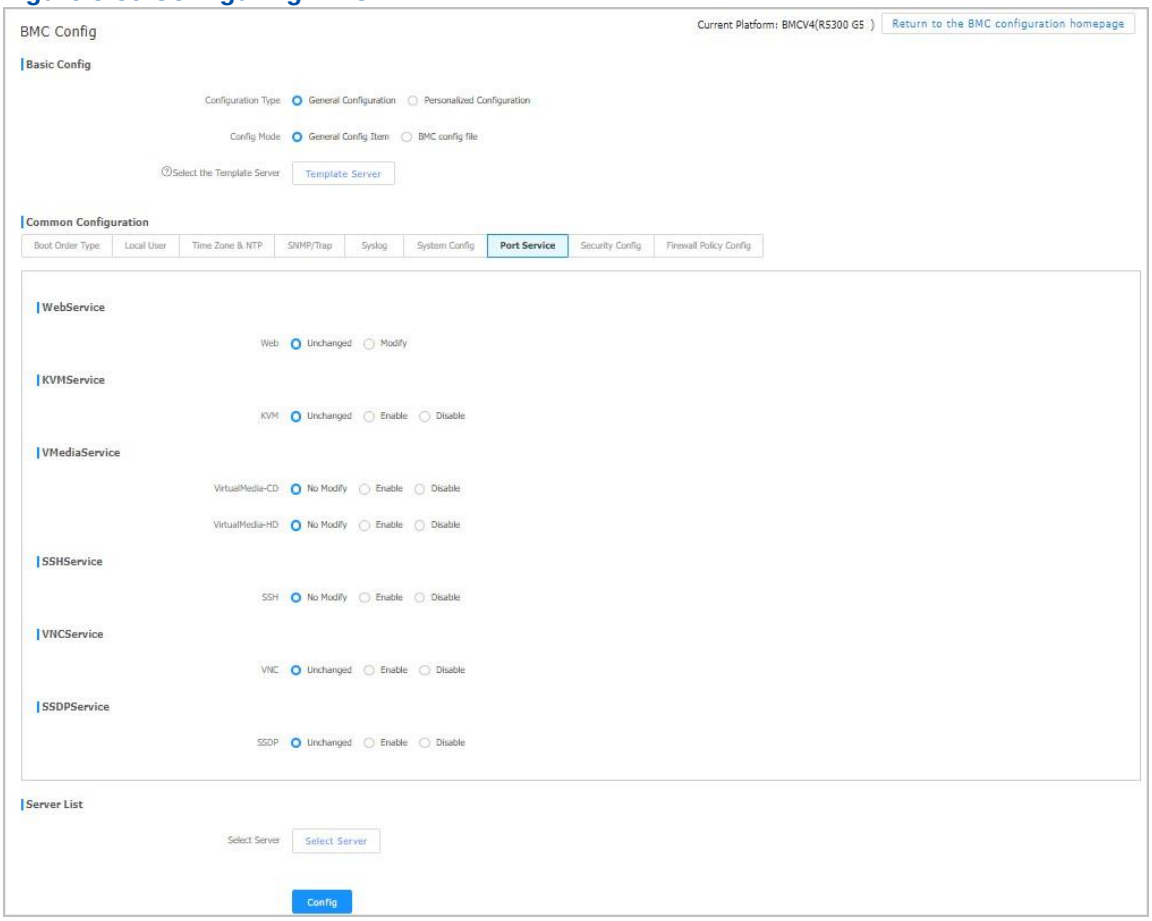
Abstract

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



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 **General Configuration**.

Config Mode	Select a configuration mode. Options: ● **General Config Item** → To import the configurations from a template server, click **Template Server**, 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 **Common Configuration** area, and can be modified. → To not import the configurations from a template server, do not select this option. ● **BMC config file** → To import the configurations in a BMC configuration file, click **Select File**, 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 **Common Configuration** area, and can be modified. → To not import a BMC configuration file, do not select this option.
Web	Select the HTTPS service configuration mode. Options: ● **Unchanged**: indicates not to modify the original server configurations. ● **Modify**: indicates to modify the original server configurations. After **Modify** is selected, the following parameters need to be set: ● **HTTPS Port**: Enter a secure port number. Default: 443. ● **HTTPS TimeOut**: Enter the timeout period. Range: 1–60, unit: minutes.
KVM	Select the KVM service configuration mode. Options: ● **Unchanged**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the KVM service. ● **Disable**: indicates to disable the KVM service. After enabling the KVM service, you need to configure the following parameters: ● **KVM Port**: 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. ● **KVM TimeOut**: Enter the timeout period. Range: 1–60, unit: minutes.
VirtualMedia-CD	Select the VirtualMedia-CD service configuration mode. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the VirtualMedia-CD service. ● **Disable**: indicates to disable the VirtualMedia-CD service. After enabling the VirtualMedia-CD service, you need to configure the following parameter:

Parameter	**Description**

	VirtualMedia-CD Port: 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.
VirtualMedia-HD	Select the VirtualMedia-HD service configuration mode. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the VirtualMedia-HD service. ● **Disable**: indicates to disable the VirtualMedia-HD service. After enabling the VirtualMedia-HD service, you need to configure the following parameter: **VirtualMedia-HD Port**: 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.
SSH	Select the SSH service configuration mode. Options: ● **No Modify**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the SSH service. ● **Disable**: indicates to disable the SSH service. After enabling the SSH service, you need to configure the following parameter: **SSH Port**: Enter a secure port number. Default: 22, range: 1–65535.
VNC	Select the VNC service configuration mode. Options: ● **Unchanged**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the VNC service. ● **Disable**: indicates to disable the VNC service. After enabling the VNC service, you need to configure the following parameters: ● **Nonsecure Port**: Enter a non-secure port number. Default: 5900, range: 1–65535. ● **Secure Port**: Enter a secure port number. Default: 5901, range: 1–65535. ● **VNC Service Password**: Select whether to change the original VNC service password. To change the password, select **Modify** and then enter a new password in the **VNC Service New Password** text box.
SSDP	Select the SSDP service configuration mode. Options: ● **Unchanged**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the SSDP service. ● **Disable**: indicates to disable the SSDP service. After enabling the SSDP service, you need to configure the following parameters: ● **SSDPPort**: Enter a port number. Default: 1900, range: 1–65535. ● **SSDP Notify**: Select whether to enable the SSDP multicast function. ● **SSDP Multicast Interval**: Enter the multicast interval. Range: 0–1800, unit: seconds. ● **SSDP IPv6 Scope**: Select the IPv6 multicast scope.

Parameter	Description
Select Server	Click **Select Server**, and select the servers to be configured in the displayed dialog box.

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

Note

- 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

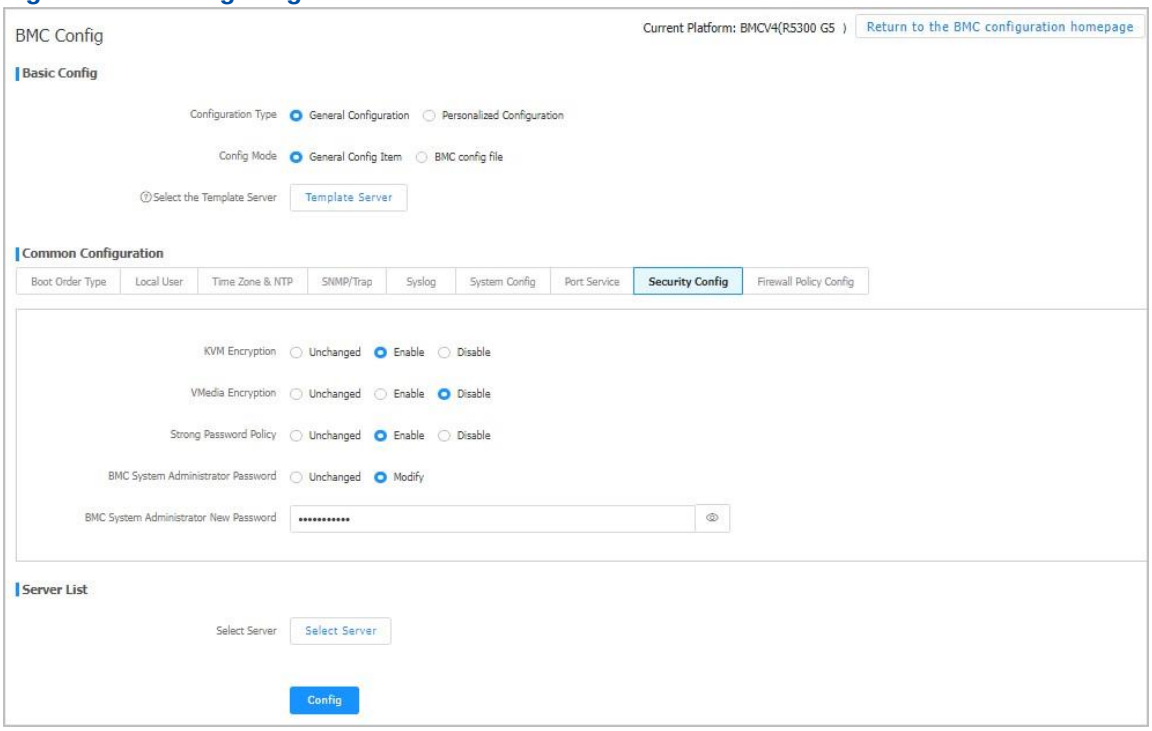
Abstract

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



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 **General Configuration**.
Config Mode	Select a configuration mode. Options: ● **General Config Item** → To import the configurations from a template server, click **Template Server**, 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 **Common Configuration** area, and can be modified. → To not import the configurations from a template server, do not select this option. ● **BMC config file** → To import the configurations in a BMC configuration file, click **Select File**, 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 **Common Configuration** area, and can be modified. → To not import a BMC configuration file, do not select this option.
KVM Encryption	Select whether to enable the KVM encryption function. Options: ● **Unchanged**: indicates not to modify the original server configurations.
Parameter	**Description**
	● **Enable**: indicates to enable the KVM encryption function. ● **Disable**: indicates to disable the KVM encryption function. 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: ● **Unchanged**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the VMedia encryption function. ● **Disable**: indicates to disable the VMedia encryption function. 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: ● **Unchanged**: indicates not to modify the original server configurations. ● **Enable**: indicates to enable the strong password policy. ● **Disable**: indicates to disable the strong password policy.
BMC System Administrator Password	Password for logging in to the server through SSH. Select whether to modify the original BMC system administrator password of the server. Options: ● **Unchanged**: indicates not to modify the original server configurations. ● **Modify**: indicates to modify the original password. Enter the new password in the **BMC System Administrator New Password** text box.
Select Server	Click **Select Server**, and select the servers to be configured in the displayed dialog box.

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

Note

- 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.

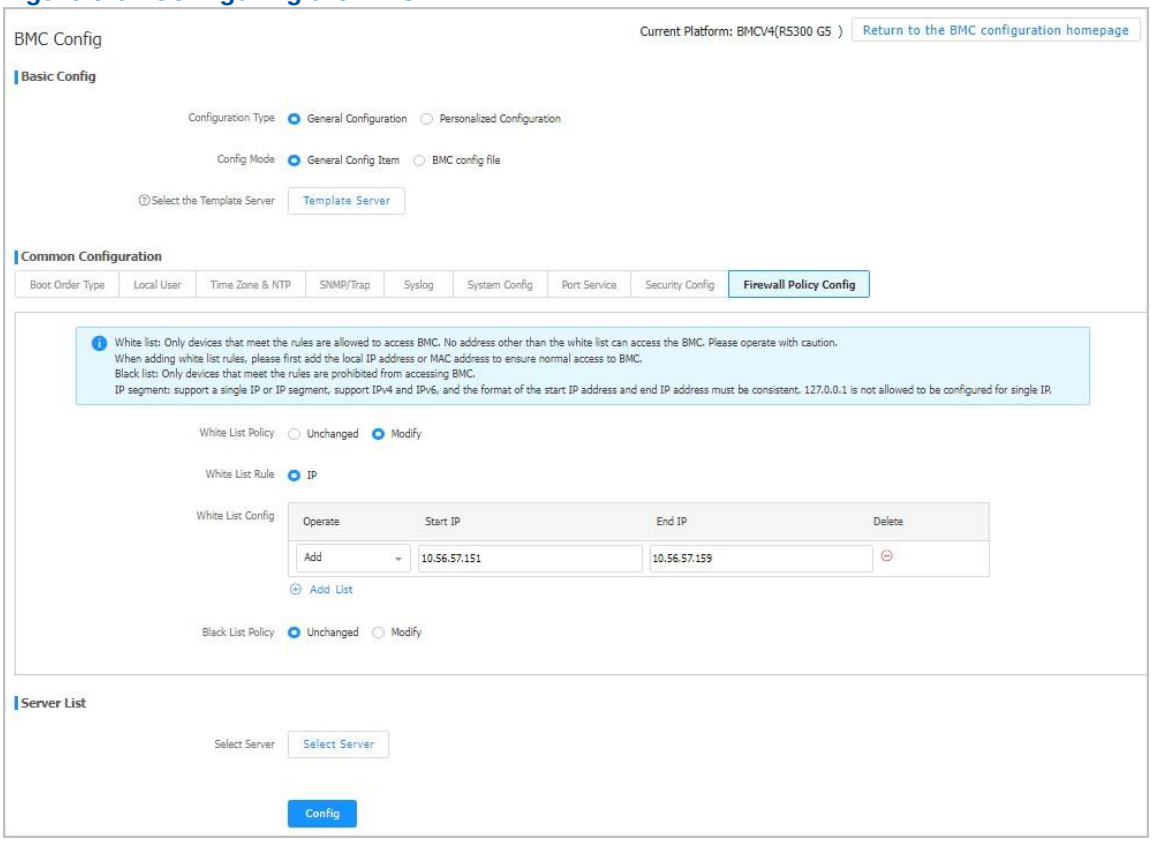
- The devices in a blacklist are forbidden to access the BMC.
- Only the devices in a whitelist are allowed to access the BMC.
  When adding a whitelist, you must first add the IP address of your local PC (acting as a client PC) to the whitelist to ensure that your local PC can access the Web portal 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



4. In the **Common Configuration** area, click **Firewall Policy Config** to switch to the **Firewall Policy Config** tab.
5. Set the parameters. For a description of the parameters, refer to Table 3-36.

Table 3-36 Firewall Parameter Descriptions

Parameter	Description
White List Policy	Select whether to modify the whitelist. Options: ● **Unchanged**: indicates not to modify the original server whitelist.
Parameter	**Description**
	● **Modify**: indicates to modify the original whitelist of the server, and adds or deletes IP address segments in **White List Config**.
Black List Policy	Select whether to modify the blacklist. Options: ● **Unchanged**: indicates not to modify the original server blacklist. ● **Modify**: indicates to modify the original blacklist of the server, and adds or deletes IP address segments in **Black List Config**.
Select Server	Click **Select Server**. In the displayed dialog box, select a server to be configured.

6. 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

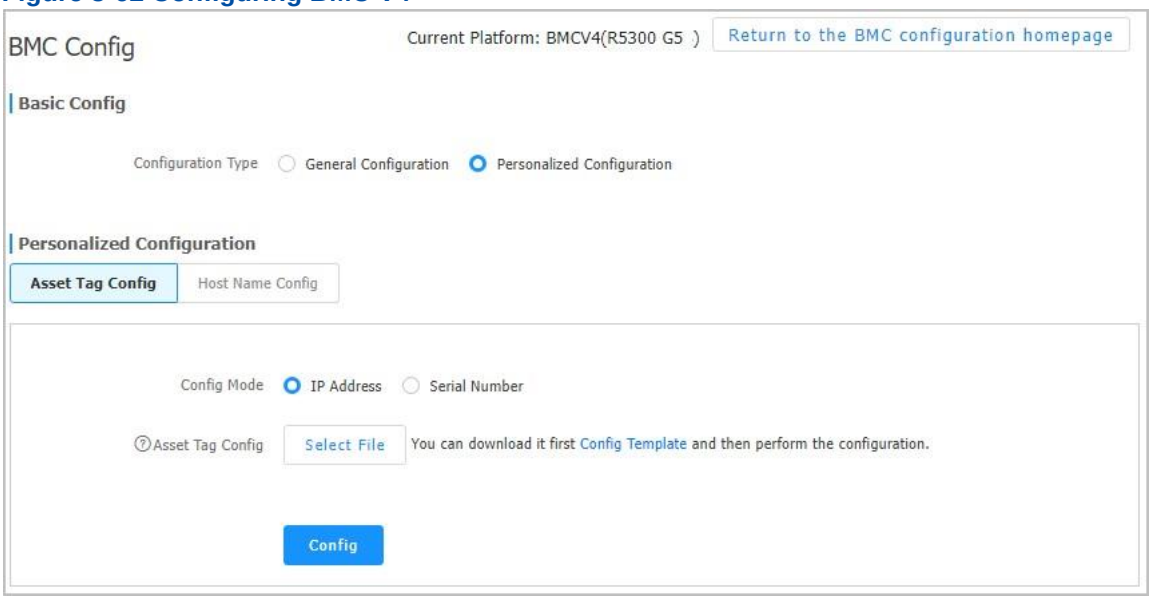
Abstract

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



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 **Personalized Configuration**.
Config Mode	• To match servers based on BMC IP addresses and then configure asset tags, select **IP Address**. In this mode, you do not need to select a BMC. • To match servers based on serial numbers and then configure asset tags, select **Serial Number**. In this mode, you need to select a BMC.
Asset Tag Config	a. (Optional) If there is no asset tag configuration file, click **Config Template** to download and fill in the configuration template. • If **Config Mode** is set to **IP Address**, the name of the configuration template downloaded to your local PC is *ImportAssetTag.csv*. • If **Config Mode** is set to **Serial Number**, the name of the configuration template downloaded to your local PC is *ImportAssetTagWithSN.csv*. b. Click **Select File**, and select the edited configuration file. The selected file is automatically verified. If it fails the verification, the error lines and causes are displayed.

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

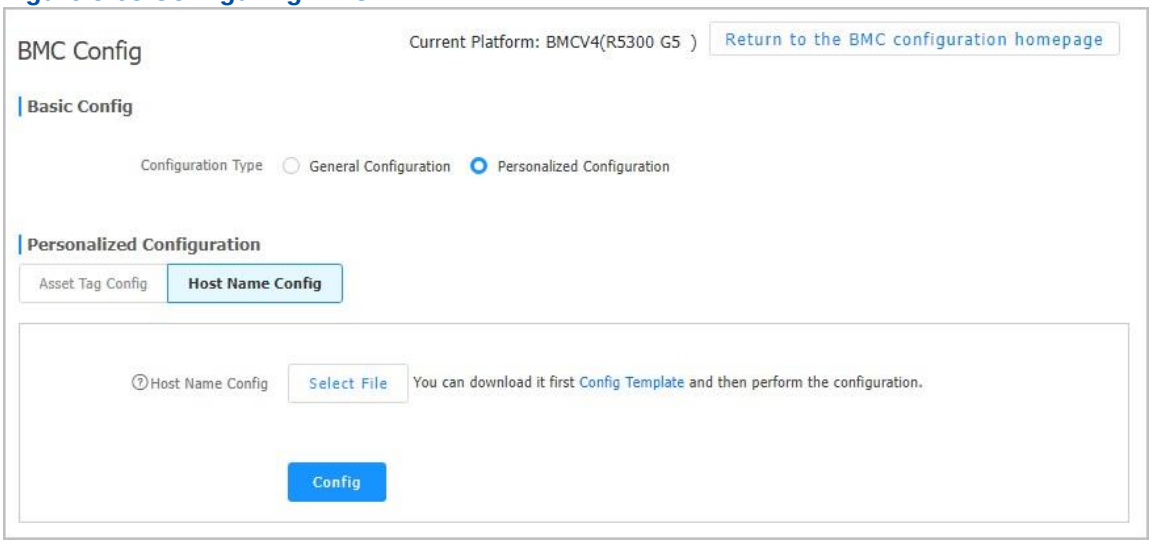
Abstract

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

Steps

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 3-63.

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 **Personalized Configuration**.
Host Name Config	a. (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*. b. Click **Select File**, and select the edited configuration file. The selected file is automatically verified. If it fails the verification, the error lines and causes are displayed.

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

Note

- 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

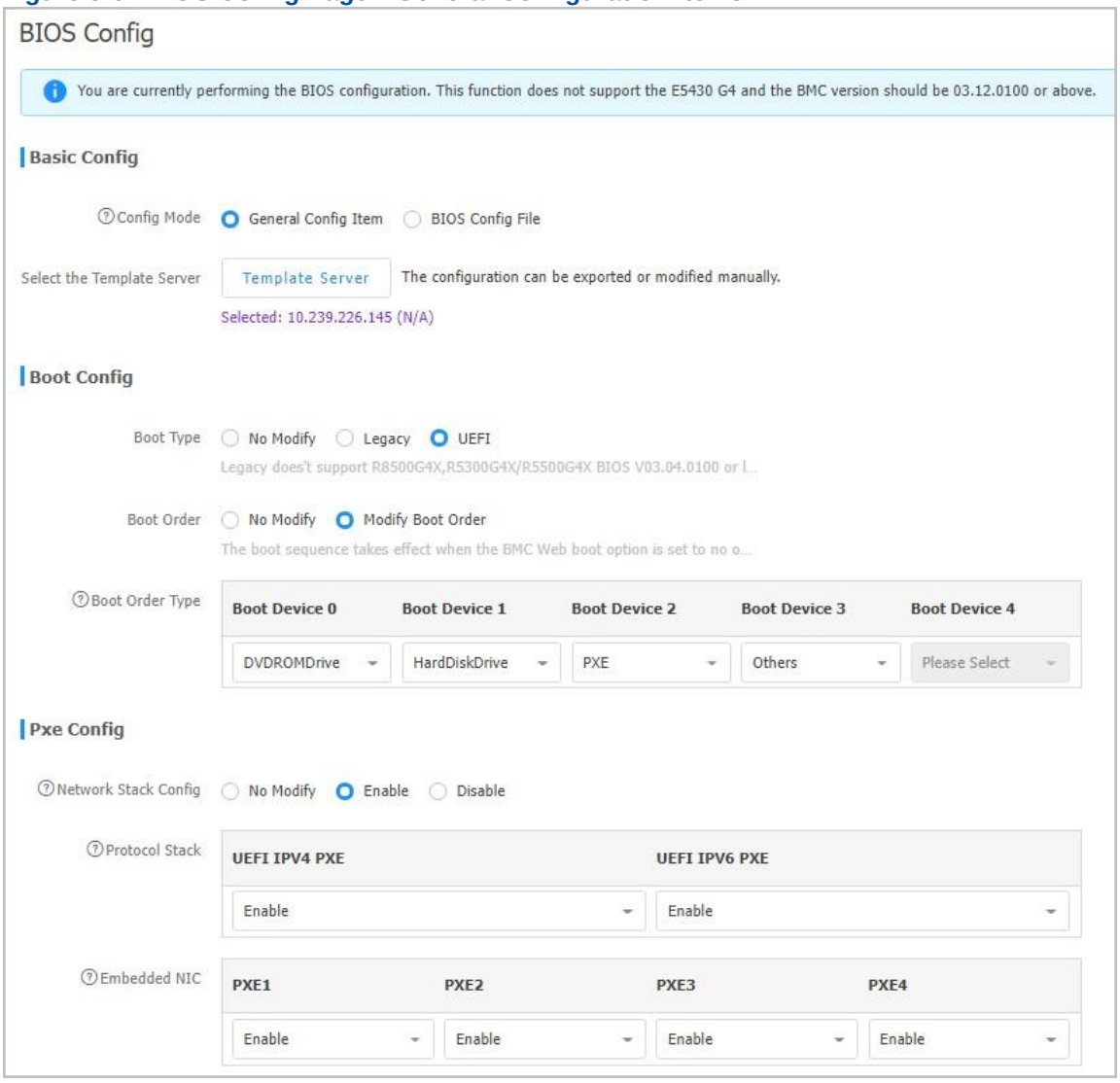
Abstract

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
Basic Config	
Config Mode	Select **General Config Item**.

Select the Template Server	Click **Template Server**, 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.

Parameter	Description
Boot Config	
Boot Type	Select the server boot mode. Options: ● **No Modify**: indicates not to modify the original server configuration. ● **Legacy**: indicates to boot the server in Legacy mode. ● **UEFI**: indicates to boot the server in UEFI mode.
Boot Order	Select whether to modify the boot order of the server. Options: ● **No Modify**: indicates not to modify the original server configuration. ● **Modify Boot Order**: indicates to modify the boot order. In this case, you need to set the boot devices in sequence in **Boot Order Type**.
Pxe Config	
Network Stack Config	Select whether to enable the PXE function. Options: ● **No Modify**: indicates not to modify the original server configuration. ● **Enable**: indicates to enable the PXE function. ● **Disable**: indicates to disable the PXE function. After the PXE function is enabled, you need to set **Protocol Stack** and **Embedded NIC**.
Virtual Config	
VT-D	Select whether to enable the virtualization function. Options: ● **No Modify**: indicates not to modify the original server configuration. ● **Enable**: indicates to enable the virtualization function. ● **Disable**: indicates to disable the virtualization function.
VMX(VT-X)	Select whether to enable the Vanderpool technology. Options: ● **No Modify**: indicates not to modify the original server configuration. ● **Enable**: indicates to enable the Vanderpool technology. ● **Disable**: indicates to disable the Vanderpool technology.
PCIe SR-IOV	Select whether to enable the SR-IOV function. Options: ● **No Modify**: indicates not to modify the original server configuration. ● **Enable**: indicates to enable the SR-IOV function. ● **Disable**: indicates to disable the SR-IOV function.

Power Config	
Custom Power Policy	Select the energy efficiency mode of power modules. Options: ● **No Modify**: indicates not to modify the original server configuration. ● **Efficiency**: 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. ● **Performance**: performance mode.

Parameter	Description
	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. ● **Custom**: user-defined mode. This mode is applicable to the scenarios where you need to customize the power management policy as required. ● **Load Balance**: 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. ● **IEM Power**: 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. ● **Latency Performance**: 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.

Turbo Mode	Select whether to enable the dynamic CPU acceleration function. Options: ● **No Modify**: indicates not to modify the original server configuration. ● **Enable**: indicates to enable the dynamic CPU acceleration function. ● **Disable**: indicates to disable the dynamic CPU acceleration function.
Processor Config	
CPU Hyper Thread	Select whether to enable the CPU hyper-threading function. Options: ● **No Modify**: indicates not to modify the original server configuration. ● **Enable**: indicates to enable the CPU hyper-threading function. ● **Disable**: indicates to disable the CPU hyper-threading function.
Memory Config	
NUMA	Select whether to enable the NUMA function. Options: ● **No Modify**: indicates not to modify the original server configuration.
Parameter	**Description**
	● **Enable**: indicates to enable the NUMA function. ● **Disable**: indicates to disable the NUMA function.
Console Config	
Serial Port Redirection	Select whether to enable the serial port redirection function. Options: ● **No Modify**: indicates not to modify the original server configuration. ● **Enable**: indicates to enable the serial port redirection function. ● **Disable**: indicates to disable the serial port redirection function. After the serial port redirection function is enabled, you need to set **Serial Port BaudRate**.
Security Config	
BIOS Password Operation	Select the BIOS password configuration mode. Options: ● **No Modify**: indicates not to modify the original server configuration. ● **Add/Modify**: indicates to create a new BIOS password or modify the existing BIOS password. In this case, you also need to set **Current BIOS Password**, **New BIOS Password**, and **Confirm New Password**. ● **Delete**: indicates to delete the BIOS password. In this case, you also need to set **Current BIOS Password**.
Configuration Mode	

Effective Mode	Select the validation mode. Options: ● **Manual Mode**: After the configurations are completed, you must manually restart the related host to apply the configurations. ● **Immediately Effect**: After the configurations are completed, the related hosts are automatically restarted to apply the configurations.
Server List	
Select Server	Click **Select Server** 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

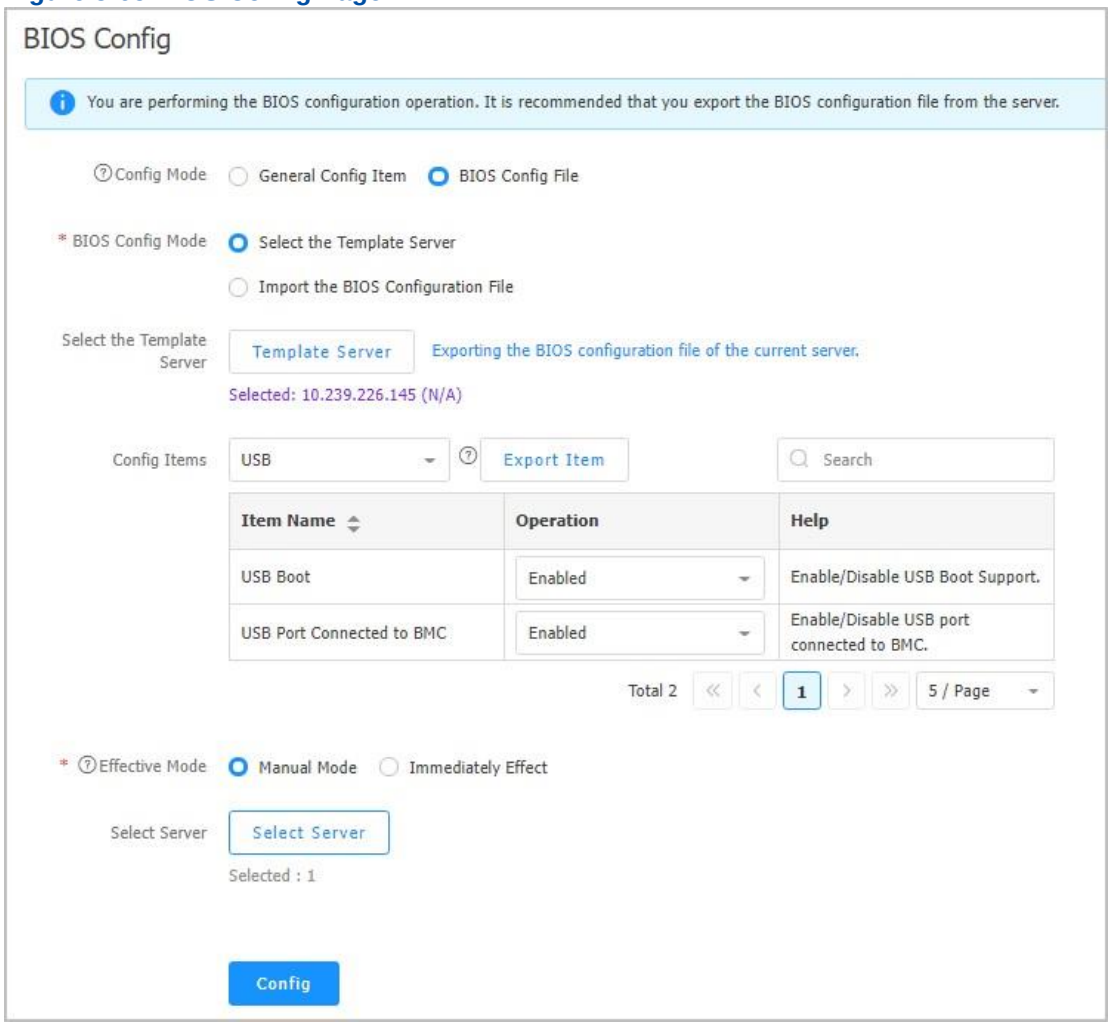
You can use either of the following methods for configuring the BIOS through a configuration file:

- **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



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 **BIOS Config File**.
BIOS Config Mode	Select **Select the Template Server**.
Select the Template Server	Click **Template Server**, 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 **Help** column.
Effective Mode	Select the validation mode. Options: → **Manual**: After the configurations are completed, you must manually restart the related hosts to apply the configurations.

Parameter	Description
	→ **Immediately Effect**: After the configurations are completed, the related hosts are automatically restarted to apply the configurations.
Select Server	Click **Select Server** 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.

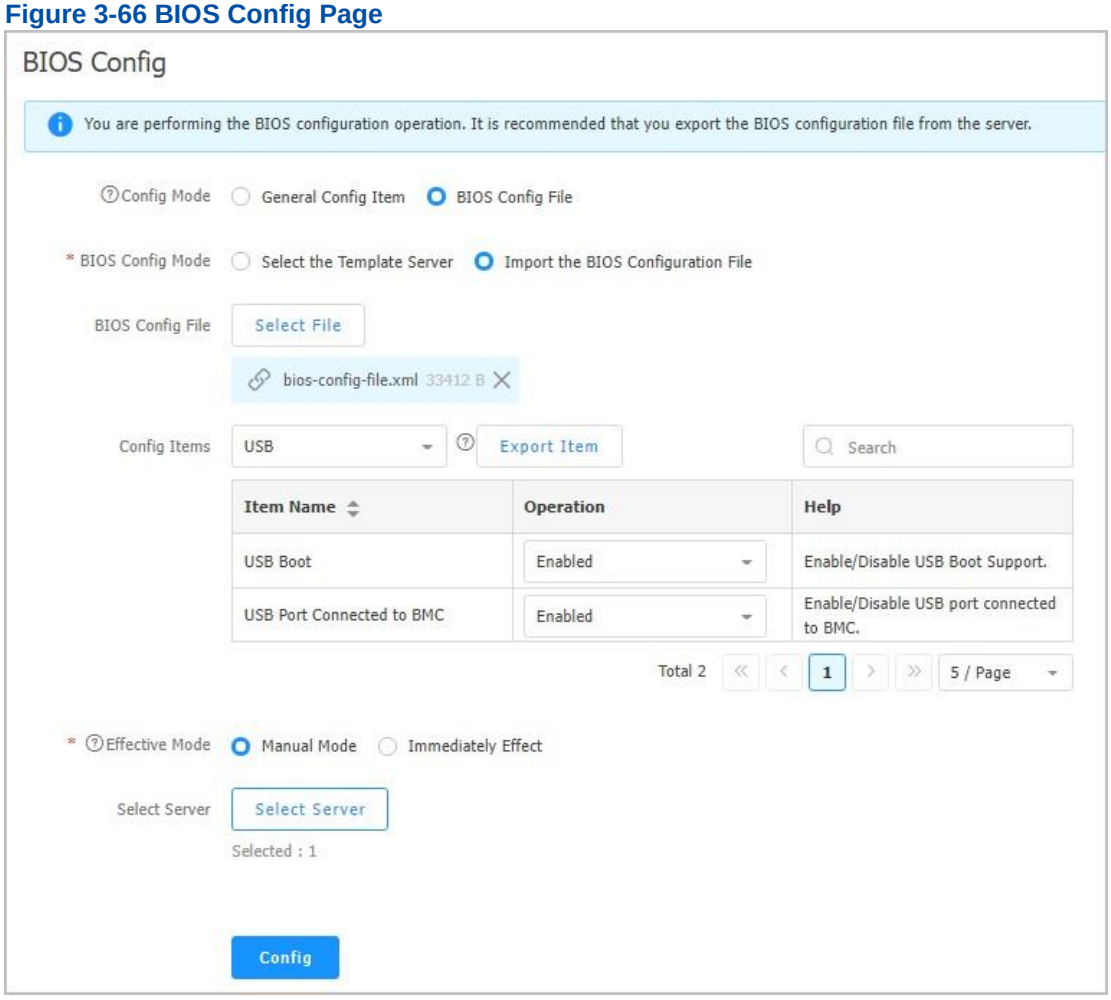
Note

→ 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



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 **BIOS Config File**.
BIOS Config Mode	Select **Import the BIOS Configuration File**.
BIOS Config File	Click **Select File**, 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 **Help** column.
Effective Mode	Select the validation mode. Options: → **Manual Mode**: After the configurations are completed, you must manually restart the related hosts to apply the configurations. → **Immediately Effect**: After the configurations are completed, the related hosts are automatically restarted to apply the configurations.
Select Server	Click **Select Server** 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.

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

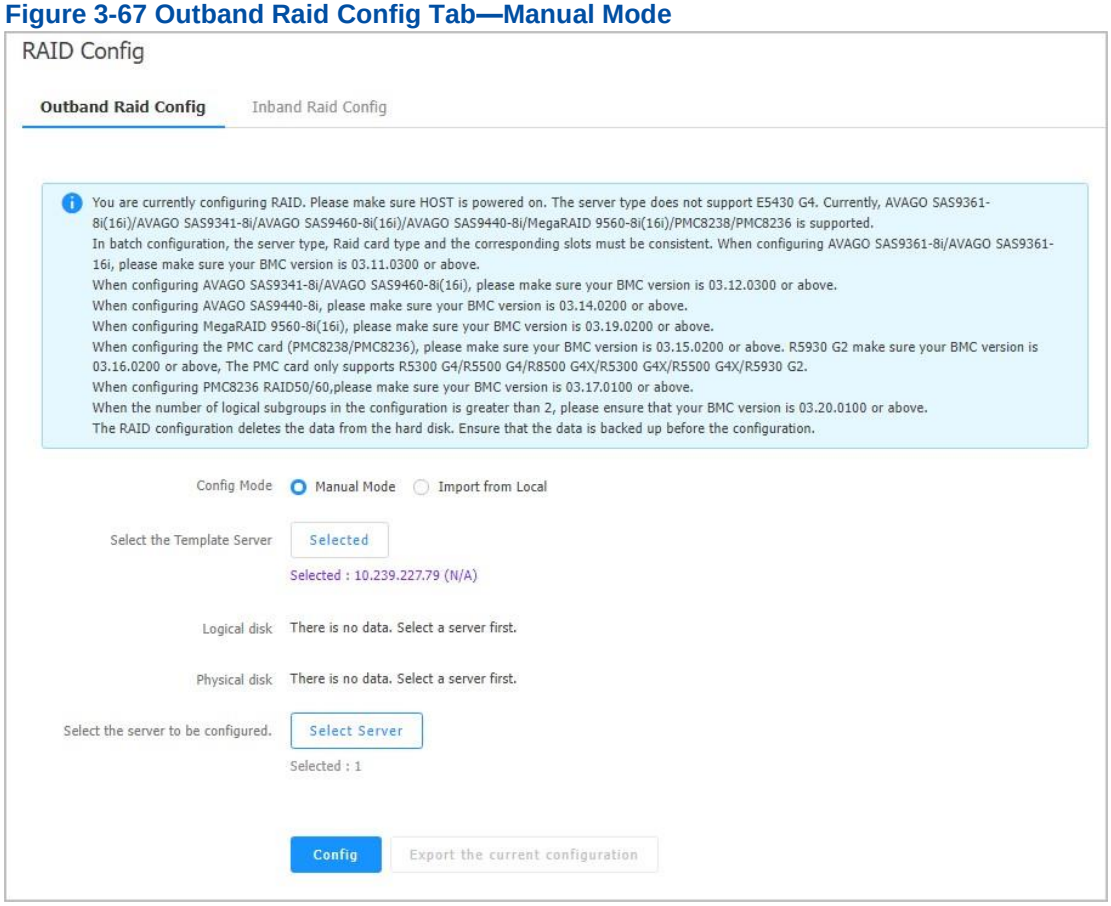
You can use either of the following methods for performing out-of-band RAID configuration:

- **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



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 **Manual Mode**.
Parameter	**Description**
Select the Template Server	Click **Select Server**, 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 **Add VD**. → To modify a logical disk, click **Modify** in the **Operation** column for the logical disk. → To delete a logical disk, click **Delete** in the **Operation** column for the logical disk. → To clear a logical disk, click **Clear**. → To enable forcible reconfiguration, turn on the **Forced reconfiguration** 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 **Forced reconfiguration** switch.
Select the server to be configured	Click **Select Server** 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.

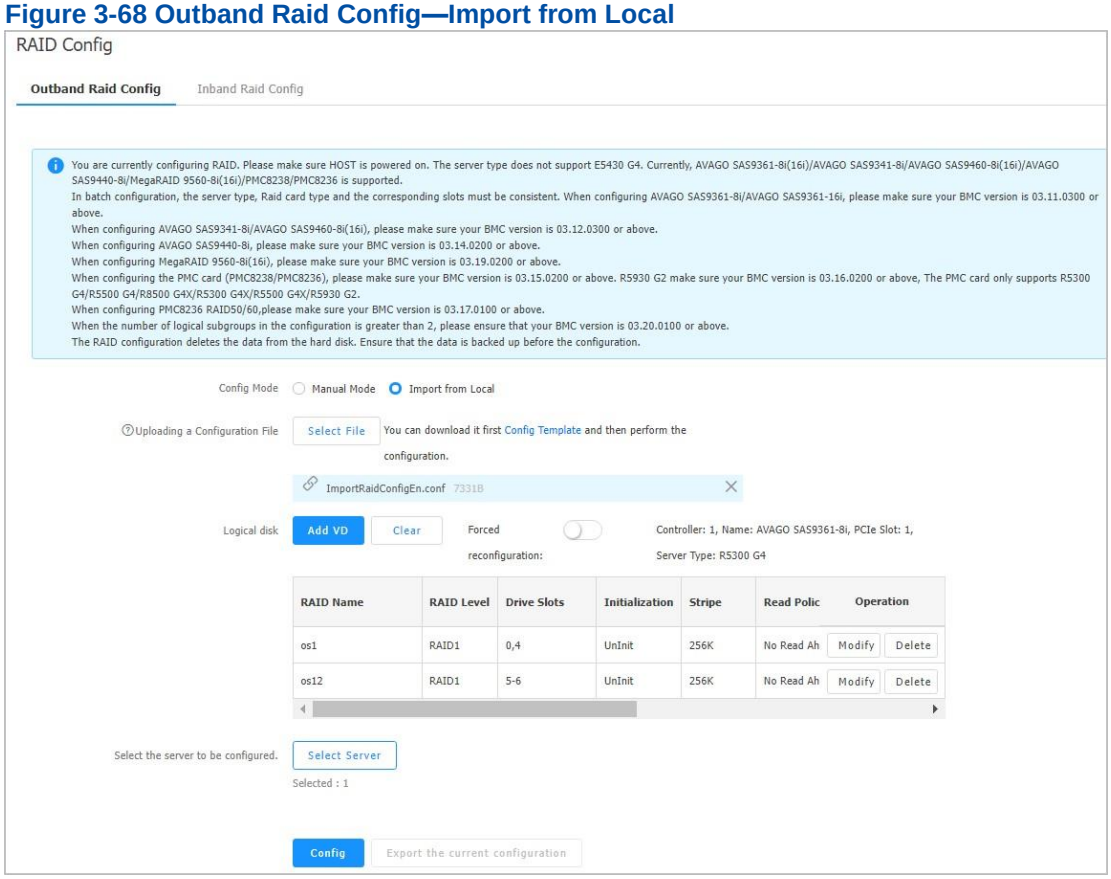
Note

→ 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 **Import from Local**.
Uploading a Configuration File	Click **Select File**, 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	Perform the following operations as required. → To add a logical disk, click **Add VD**. → To modify a logical disk, click **Modify** in the **Operation** column for the logical disk. → To delete a logical disk, click Delete in the **Operation** column for the logical disk. → To clear a logical disk, click Clear. → To enable forcible reconfiguration, turn on the **Forced reconfiguration** 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 **Forced reconfiguration** switch.
Parameter	**Description**
Select the server to be configured	Click **Select Server** 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.

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.

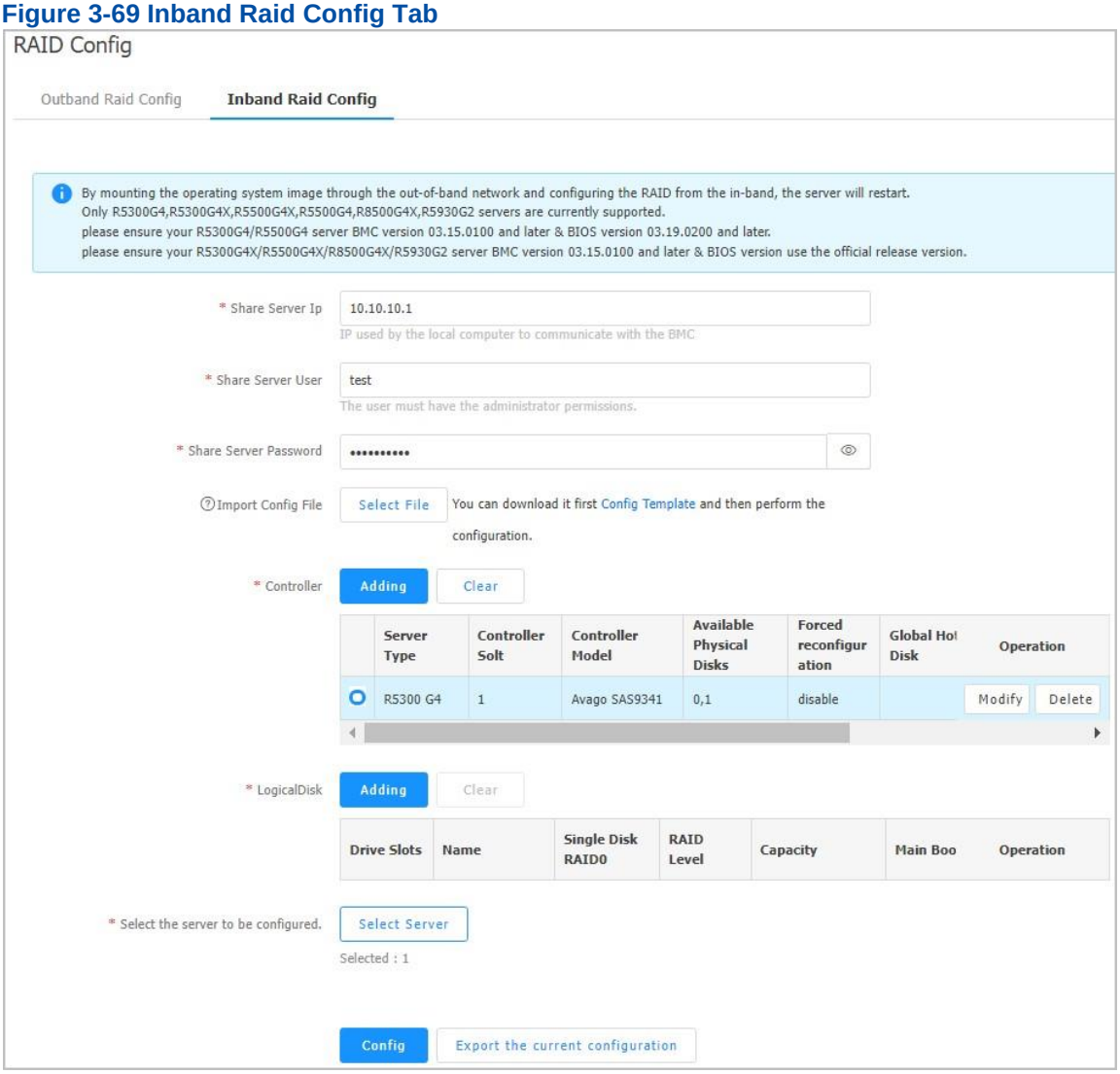
Prerequisite

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



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 **Select Server**, 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.
   - Importing a configuration file
     a. (Optional) If there is no RAID configuration file, click **Config Template** to download and fill in the configuration template.
     b. Click **Select File**, and select the edited RAID configuration file.
     c. Click **Submit**.

     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.

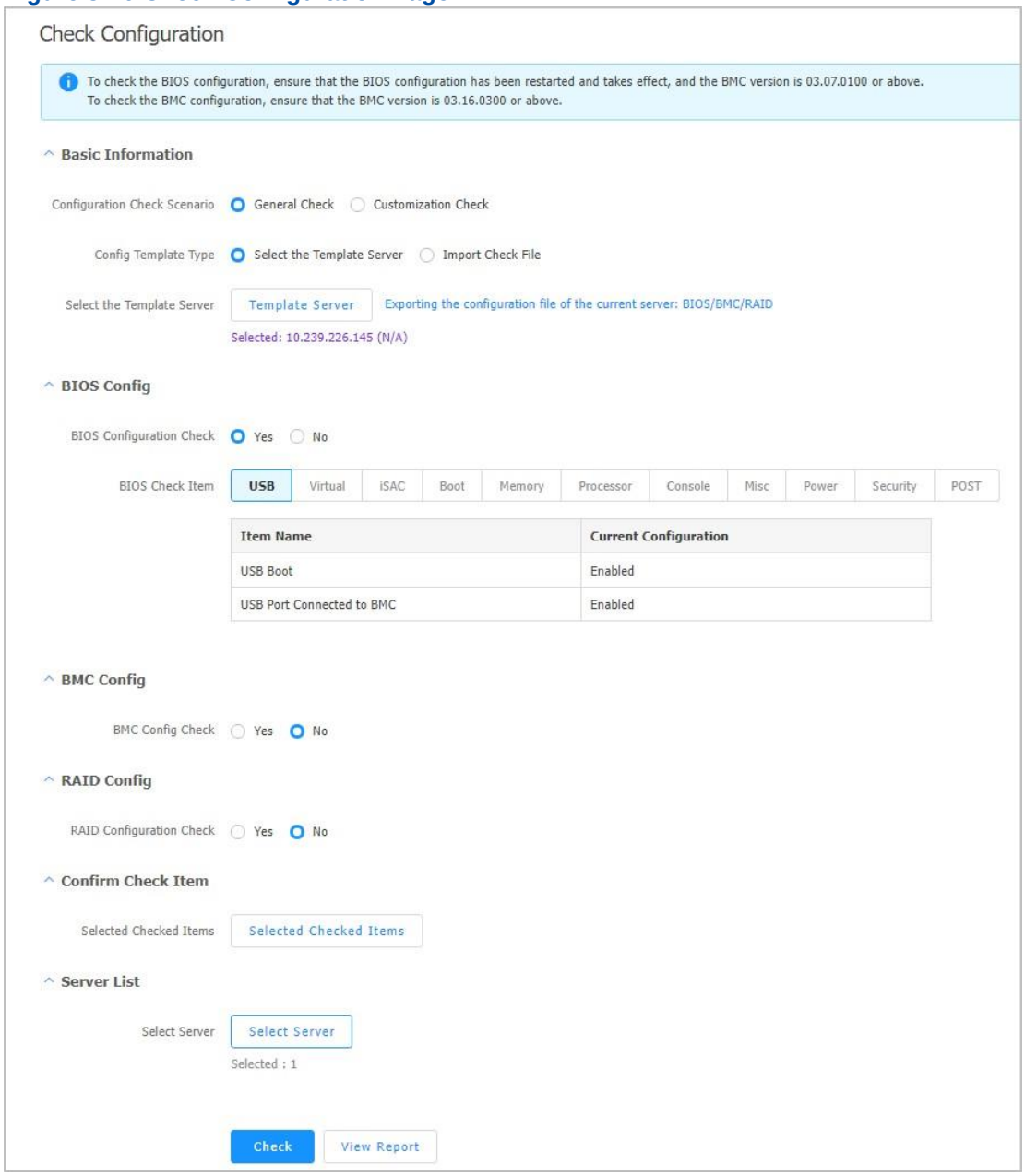
You can check general configurations through either of the following ways:

- **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



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
Basic Information	
Configuration Check Scenario	Select **General Check**.
Config Template Type	Select **Select the Template Server**.

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

Parameter	Description
	a. Click **Template Server**. The **Select the exported configuration** dialog box is displayed. b. Select the configurations to be exported, including **BIOS Config**, **BMC Config**, and **RAID Config**. c. Click **Next Step**. The **Select Server** dialog box is displayed. d. Select a server as the template server, and click **Export**. After **Export** is clicked, the configuration parameters of the current server are obtained from the template server. After the configurations of the template server are successfully exported, the **Exporting the configuration file of the current server: BIOS/BMC/RAID** button is activated. To export the configurations from the template server to a local `*.json` file, click **Exporting the configuration file of the current server: BIOS/BMC/RAID**.
BIOS Config	
BIOS Configuration Check	Select whether to check BIOS configurations.
BIOS Check Item	→ If **BIOS Configuration Check** is set to **Yes**, the current BIOS configurations on the template server are displayed. → If **BIOS Configuration Check** is set to **No**, this parameter is not displayed.
BMC Config	
BMC Config Check	Select whether to check BMC configurations.
BMC Check Item	→ If **BMC Config Check** is set to **Yes**, the current BMC configurations on the template server are displayed. → If **BMC Config Check** is set to **No**, this parameter is not displayed.
RAID Config	
RAID Configuration Check	Select whether to check RAID configurations.
RAID Check Item	→ If **RAID Configuration Check** is set to **Yes**, the current RAID configurations on the template server are displayed. → If **RAID Configuration Check** is set to **No**, this parameter is not displayed.
Confirm Check Item	

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

3. Click **Check**.

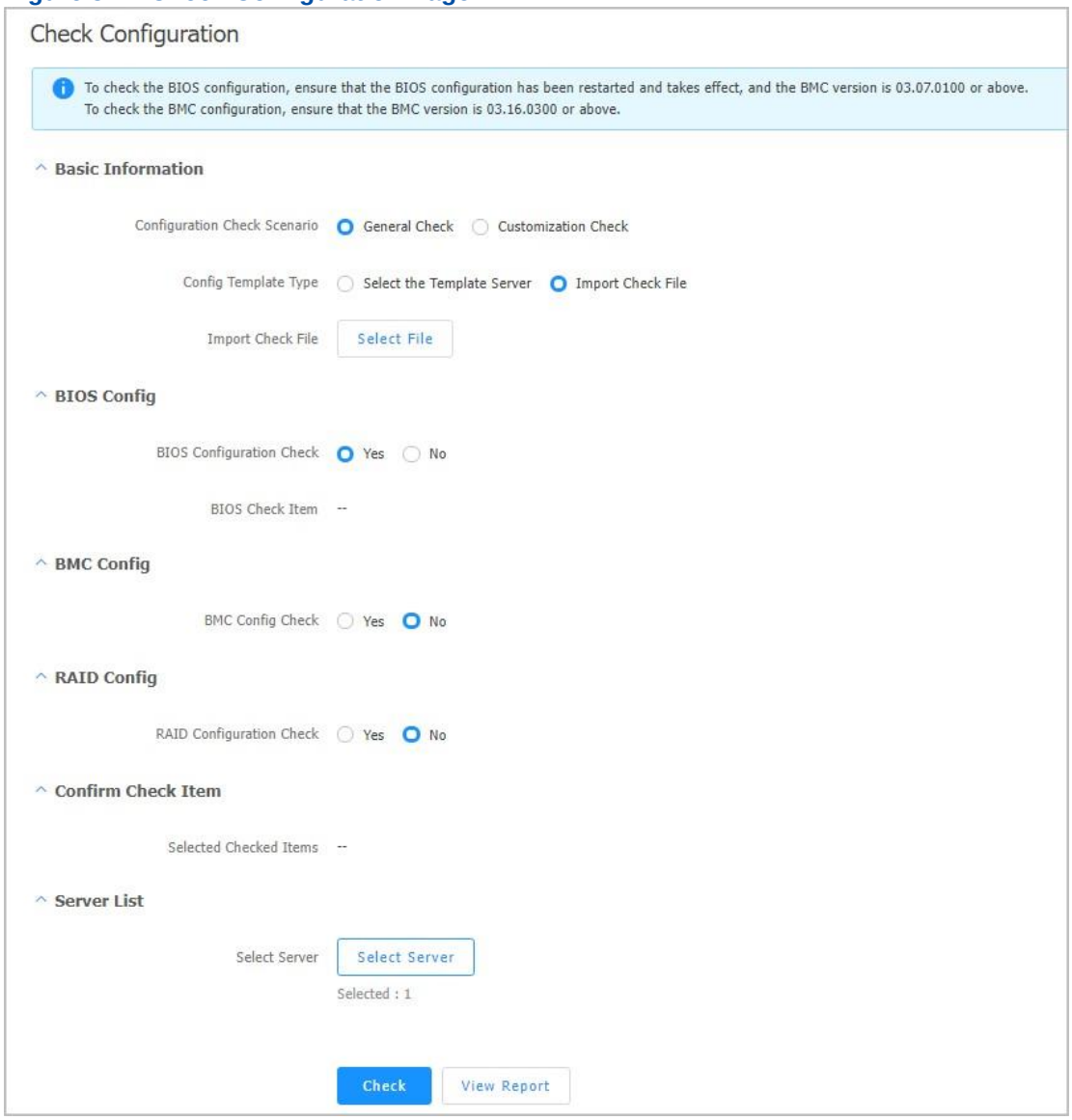
Note

→ 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



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
Basic Information	
Configuration Check Scenario	Select **General Check**.
Config Template Type	Select **Import Check File**.
Import Check File	Click **Select File**, and select the desired check file.

BIOS Config	
Parameter	**Description**
BIOS Configuration Check	Select whether to check BIOS configurations.
BIOS Check Item	→ If **BIOS Configuration Check** is set to **Yes**, the current BIOS configurations on the template server are displayed. → If **BIOS Configuration Check** is set to **No**, this parameter is not displayed.
BMC Config	
BMC Config Check	Select whether to check BMC configurations.
BMC Check Item	→ If **BMC Config Check** is set to **Yes**, the current BMC configurations on the template server are displayed. → If **BMC Config Check** is set to **No**, this parameter is not displayed.
RAID Config	
RAID Configuration Check	Select whether to check RAID configurations.
RAID Check Item	→ If **RAID Configuration Check** is set to **Yes**, the current RAID configurations on the template server are displayed. → If **RAID Configuration Check** is set to **No**, this parameter is not displayed.
Confirm Check Item	
Selected Checked Items	Confirm the items to be checked. To do this, perform the following operations: a. Click **Selected Checked Items**. The **Selected Checked Items** dialog box is displayed. b. Confirm the items to be checked, and click **Submit**.
Server List	
Select Server	Click **Select Server** 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.

Related Tasks

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

To...	Do...
Recheck the configurations	1. Click **ReCheck**. A dialog box is displayed. 2. Click **Submit** to return to the **Check Configuration** page. 3. Reconfigure the check parameters. 4. Click **Check**.
Perform a secondary check	1. Select the server for which you want to perform a secondary check. 2. Click **Second Check**.
Export the check report	Click **Exporting Check Summary Result** to export the configuration report to a local `*.csv` file.
Export the details of the comparison between a server and the template server	1. Select the server that you want to compare with the template server. 2. Click **Exporting Check Summary Details**.

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.

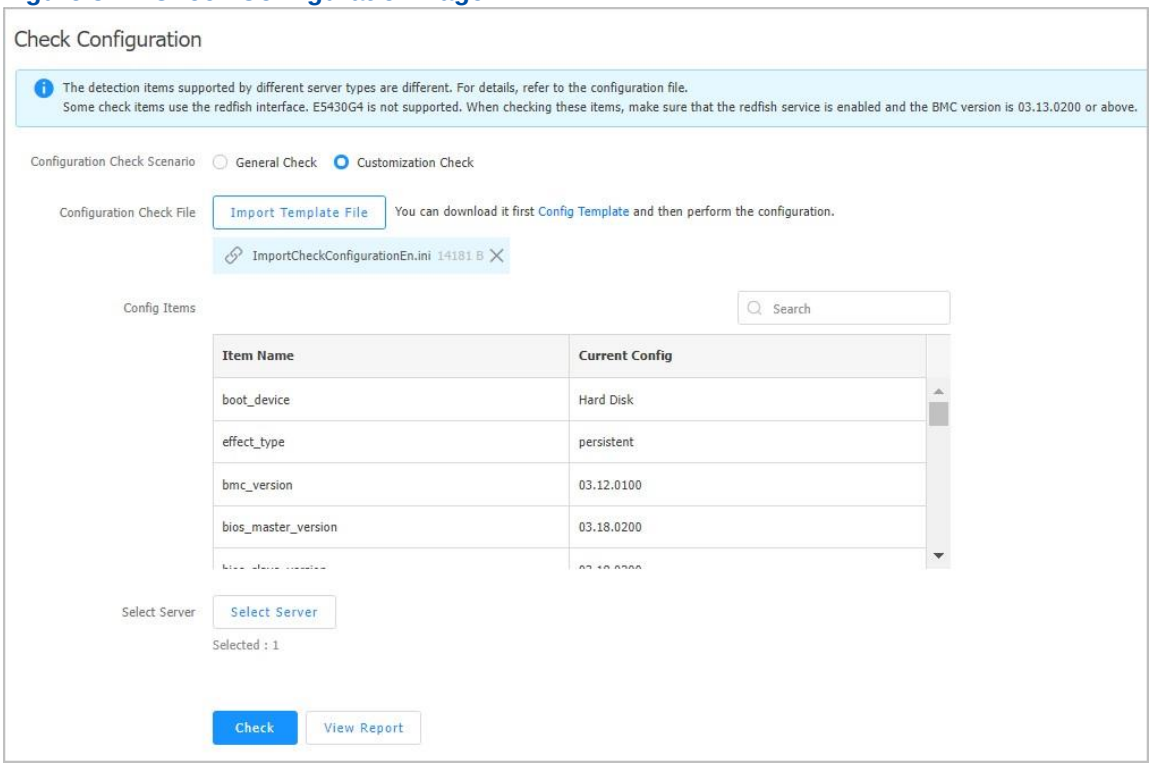
Note

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



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 **Customization Check**.
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 **Config Template** to download and fill in the configuration template. b. Click **Select File**, and select the desired check file. c. Click **Submit**.
Config Items	After the check file is selected, the configuration items in the file are displayed in the configuration item list.
Select Server	Click **Select Server** 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.

Related Tasks

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

To...	Do...
Recheck the configurations	1. Click **ReCheck**. A dialog box is displayed. 2. Click **Submit** to return to the **Check Configuration** tab. 3. Reconfigure the check parameters. 4. Click **Check**.
Export the check report	Click the **Export Report** 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.

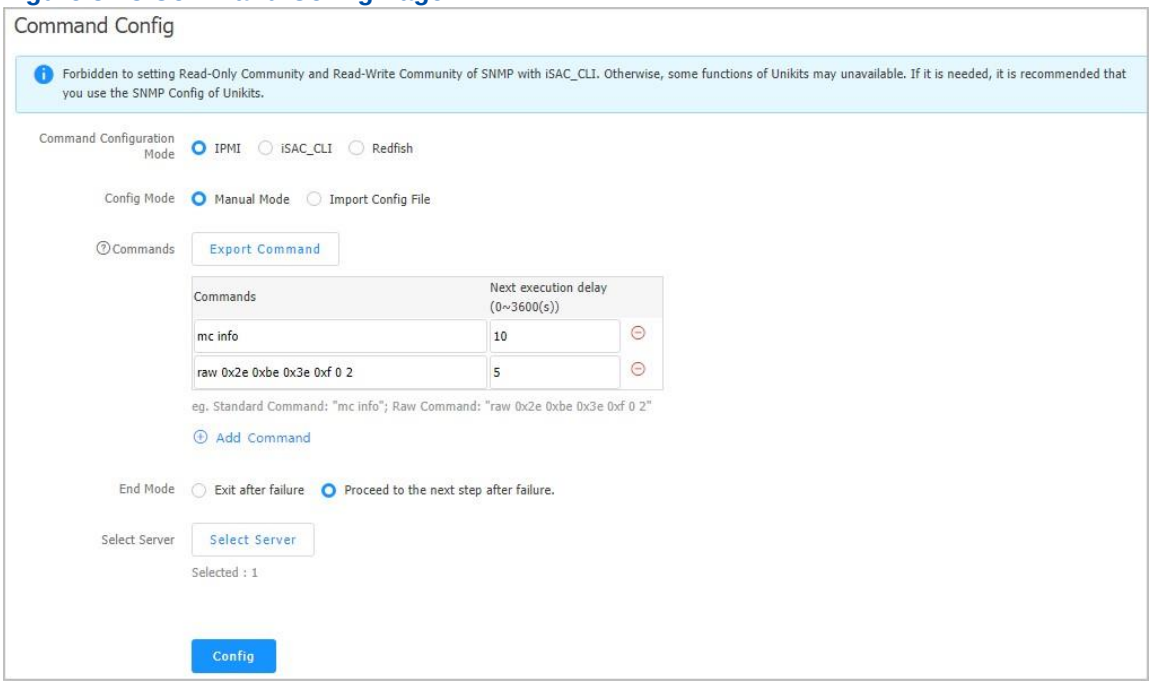
Note

This function does not support interactive commands.

Steps

1. Select **Device Mgmt > Deployment > Command Config**. The **Command Config** page is displayed, as shown in Figure 3-73.

Figure 3-73 Command Config Page



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	Select a command type. Options: ● **IPMI**: 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 SNMP read-only community or read-write community. ● **iSAC_CLI**: 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. ● **Redfish**: indicates to execute Redfish commands on a server. Redfish commands support four request methods: Get, Post, Patch, and Delete.
Config Mode	Select a command configuration mode. Options: ● **Manual Mode**: A maximum of 10 commands can be configured manually. In this case, you need to set **Commands** and **Next execution delay**. For Redfish commands, you also need to set **Request Mode** and **Request Body**. The **Next execution delay** parameter sets the time interval between two commands. It is used to prevent command execution failure be-

Parameter	Description
	cause two mutually associated commands need to be executed at the specified interval. Range: 0–3600, unit: seconds. The **Request Body** parameter supports the JSON format only. ● **Import Config File**: Commands are imported through a command script file. If there is no command script file, click **Config Template** to download the template, edit the template, and import it. Click **Select File**, and select the command configuration file.
End Mode	Select a command termination mode. Options: ● **Exit after failure**: If a command fails to be executed, the command execution process stops immediately and the execution result is returned. ● **Proceed to the next step after failure**: 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. The termination mode is valid for only a single server. For example, when **Exit after failure** 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.
Select Server	Click **Select Server**, and select the servers to be configured in the displayed dialog box.

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

Note

- 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

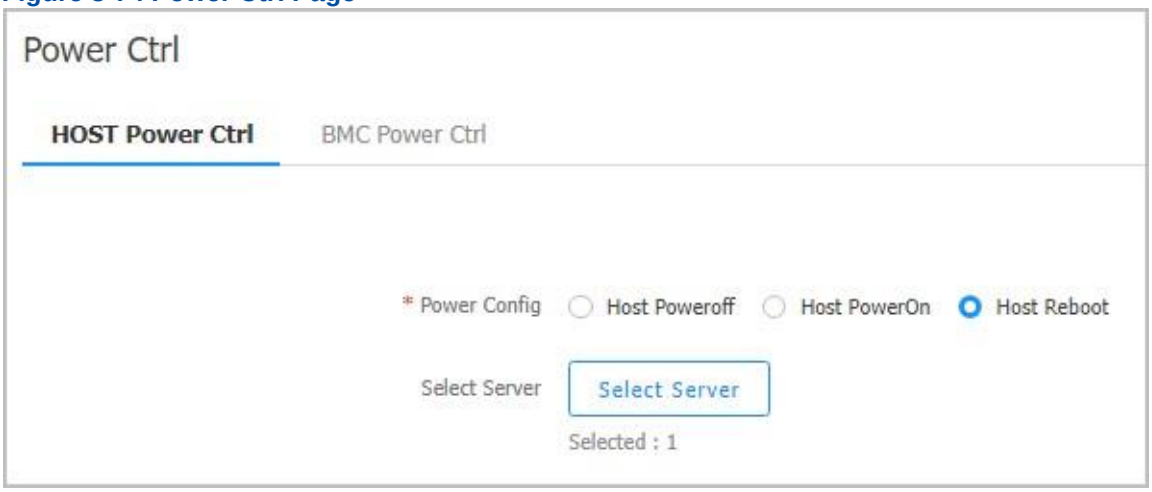
Notice

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	a. Select **Host Poweroff**. b. Click **Select Server** and select the servers to be powered off. c. (Optional) If the selected servers are of different models, enter **yes** in the displayed dialog box and select **I have read it and know the influence**. d. Click **Config**. In the displayed dialog box, enter **yes** and select **I have read it and know the influence**. e. Click **Submit**.
Power on hosts	a. Select **HOST PowerOn**. b. Click **Select Server** and select the servers to be powered on. c. (Optional) If the selected servers are of different models, enter **yes** in the displayed dialog box and select **I have read it and know the influence**. d. Click **Config**. In the displayed dialog box, click **Submit**.

Restart hosts	a. Select **Host Reboot**. b. Click **Select Server** and select the servers to be restarted.
To...	**Do...**
	c. (Optional) If the selected servers are of different models, enter **yes** in the displayed dialog box and select **I have read it and know the influence**. d. Click **Config**. In the displayed dialog box, enter **yes** and select **I have read it and know the influence**. e. Click **Submit**.
Restart the BMC	a. Click **BMC Power Ctrl**. The **BMC Power Ctrl** tab is displayed. b. Select **BMC Reboot**. c. Click **Select Server** and select the BMCs to be restarted. d. (Optional) If the selected BMCs are of different models, enter **yes** in the displayed dialog box and select **I have read it and know the influence**. e. Click **Config**. In the displayed dialog box, enter **yes** and select **I have read it and know the influence**. f. Click **Submit**.

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

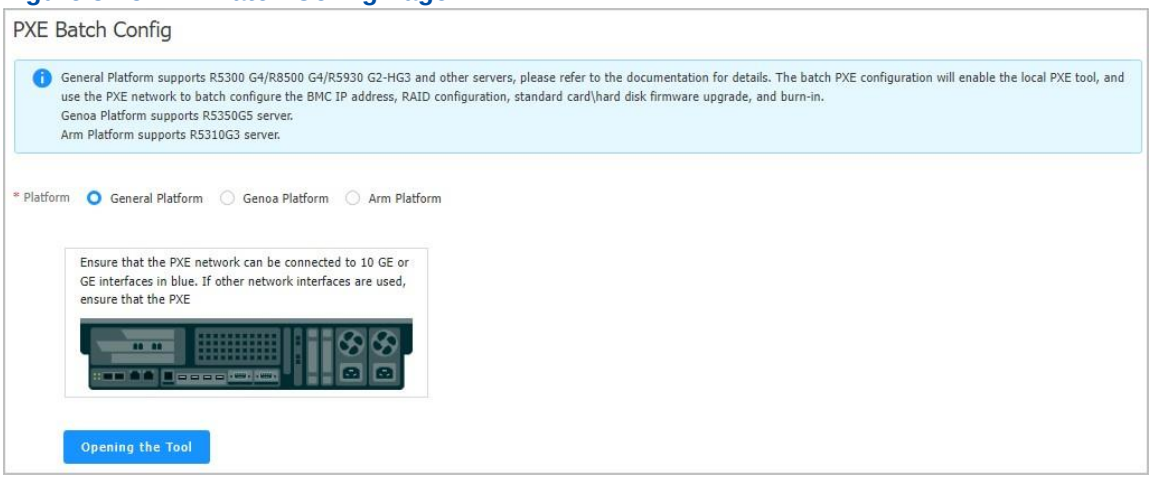
Notice

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.

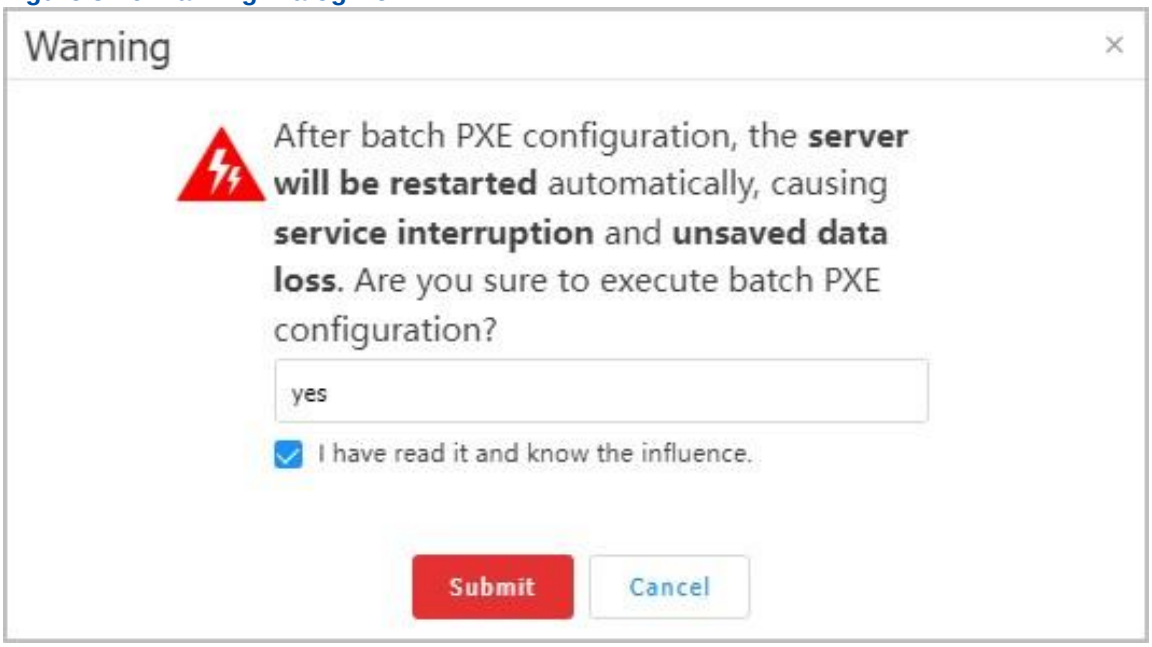
Figure 3-75 PXE Batch Config Page



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

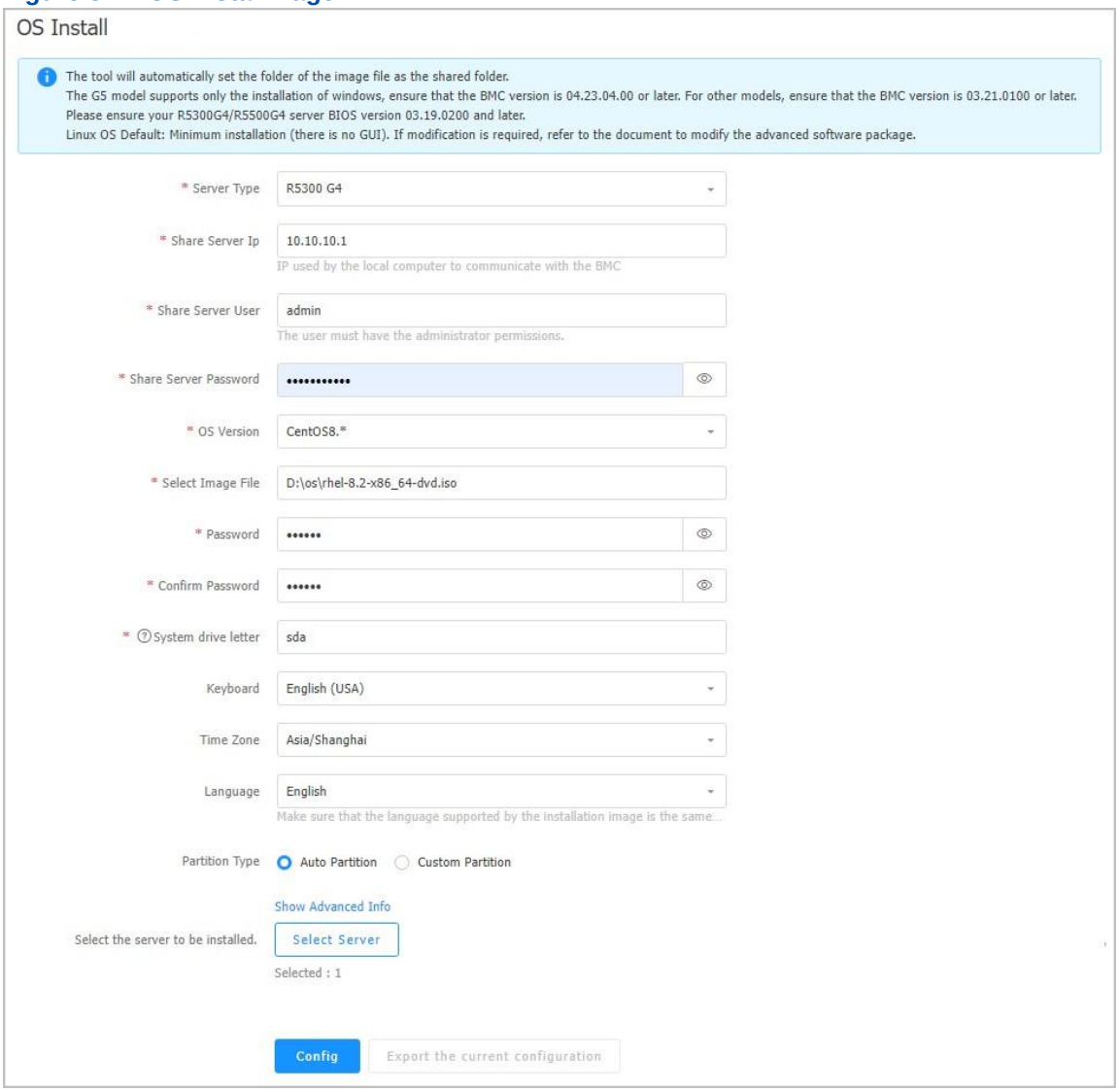
Prerequisite

- 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



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: **sda**.
Keyboard	Default: **English (USA)**.
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 **Custom Partition**, click **Add Partition** to add a partition.
Show Advanced Info	
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 DMA interface, enter *ide=nodma*.
Installation Mode	Select the OS installation mode.
Module of the software package	This parameter is required when **OS Version** is set to **SUSE15.2–SUSE15.4** and **Installation Mode** is set to **Customized Installation**. Enter the module where the installation package is located.

Install Software Package	This parameter is required when **Installation Mode** is set to **Customized Installation**. Enter the information about the software package that you want to install.
Script After Installation	● For CentOS or RHEL, this parameter does not need to be set by default.
Parameter	**Description**
	● For SUSE, enter the shell script that is automatically executed immediately after the installation is completed.
Select the server to be installed	Click **Select Server** 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

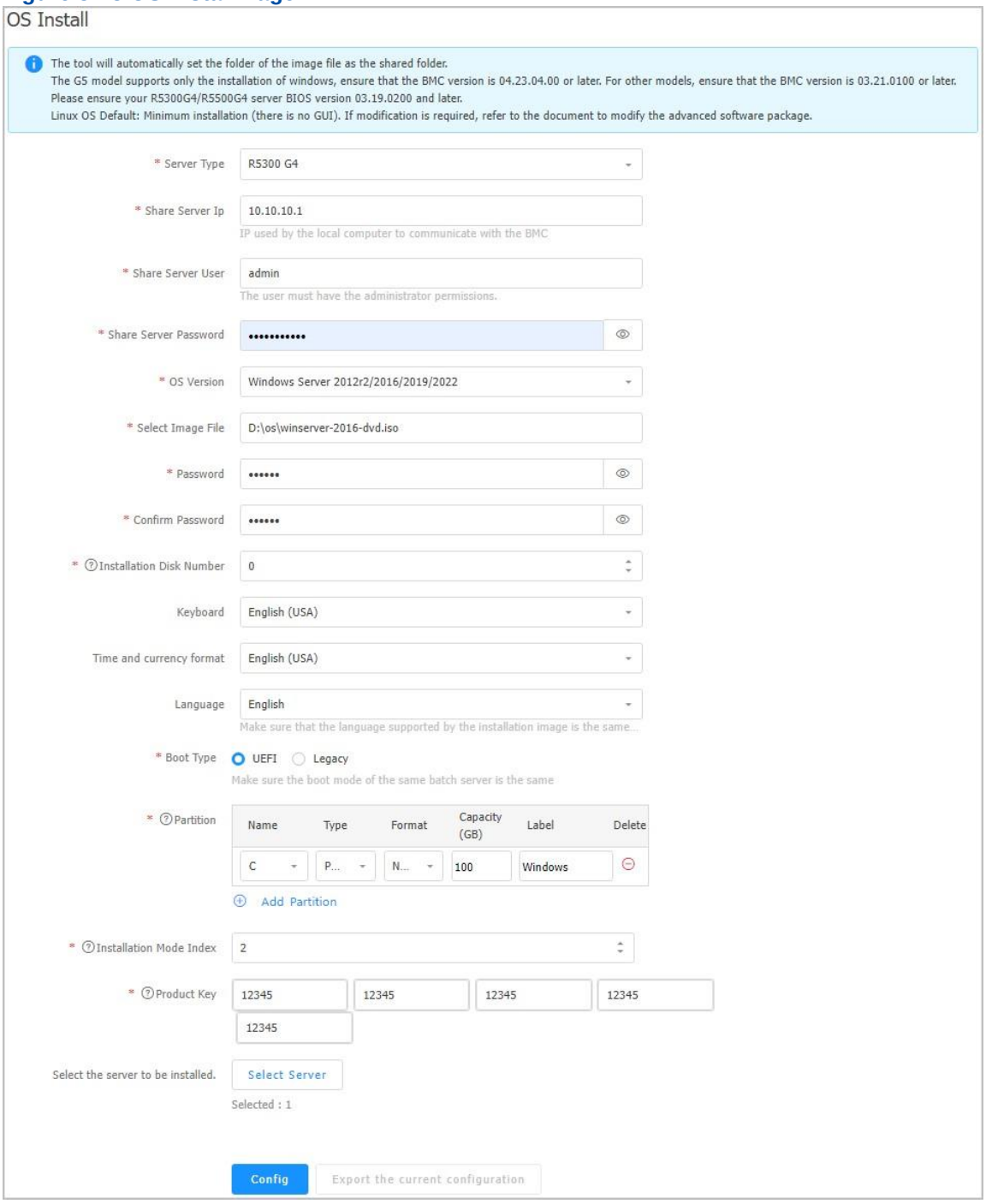
Prerequisite

- 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



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: **English (USA)**.
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	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. If you need to add a partition, click **Add Partition**. 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.
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 **IMAGE INDEX** in the *sources\install.wim\[1].xml* file.
Product Key	Enter the product key.
Select the server to be installed	Click **Select Server** 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

Note

PSU firmware upgrade is supported on only G5 models.

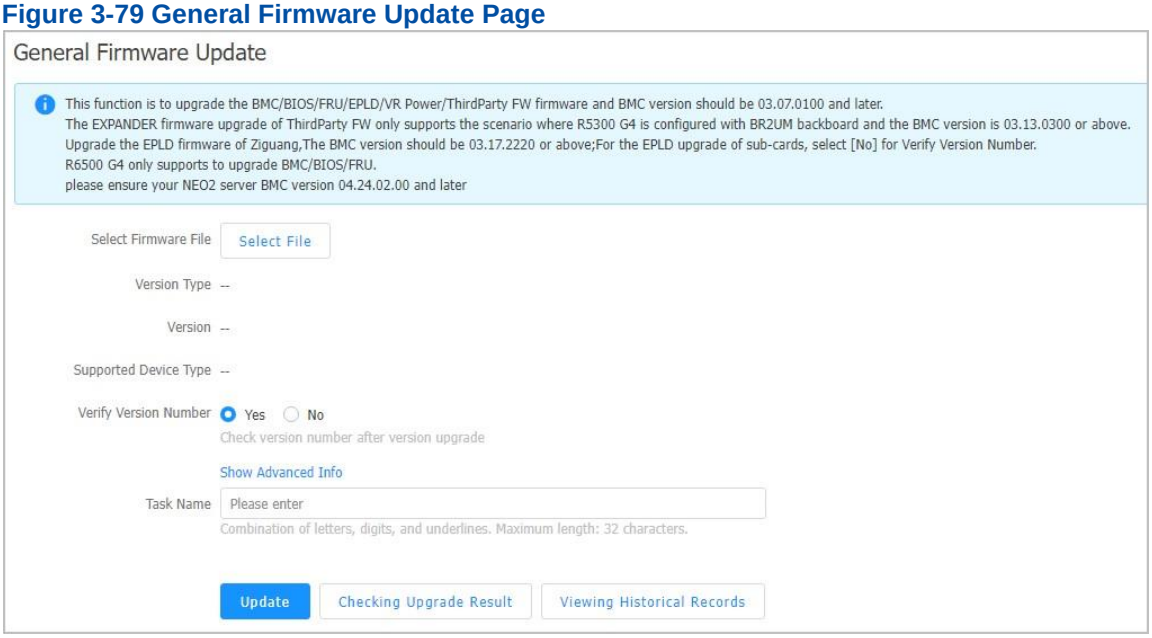
Prerequisite

The firmware to be upgraded is already obtained.

Steps

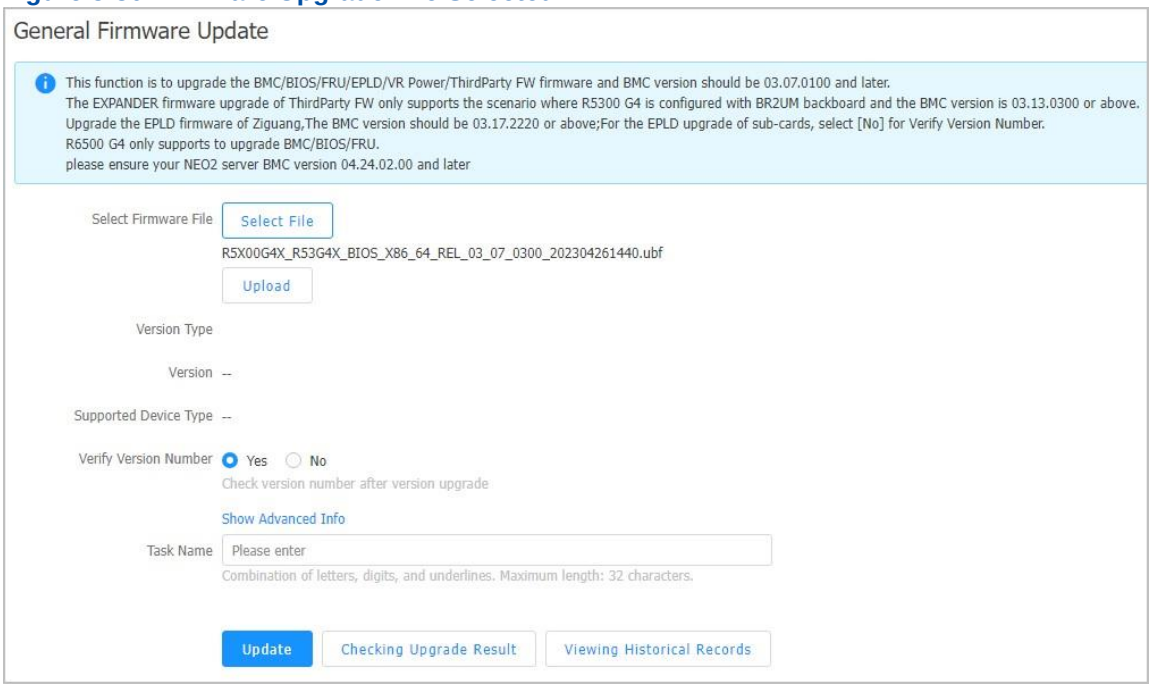
1. Select **Device Mgmt > Firmware Update > General Firmware Update**. The **General Firmware Update** page is displayed, see Figure 3-79.

Figure 3-79 General Firmware Update Page



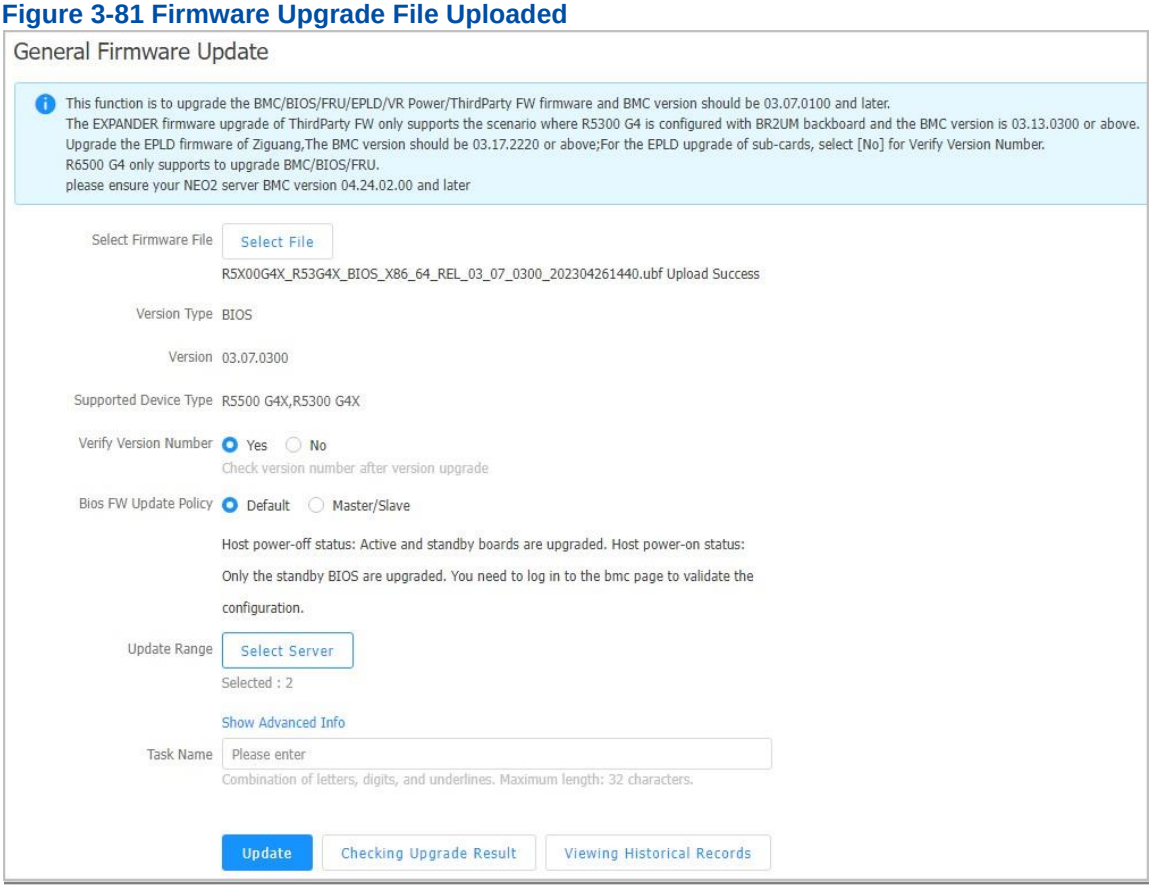
2. Click **Select File**, and select the desired firmware upgrade file. The file is selected, see Figure 3-80.

Figure 3-80 Firmware Upgrade File Selected



3. Click **Upload**. The file is uploaded, see Figure 3-81.

Figure 3-81 Firmware Upgrade File Uploaded



Note

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

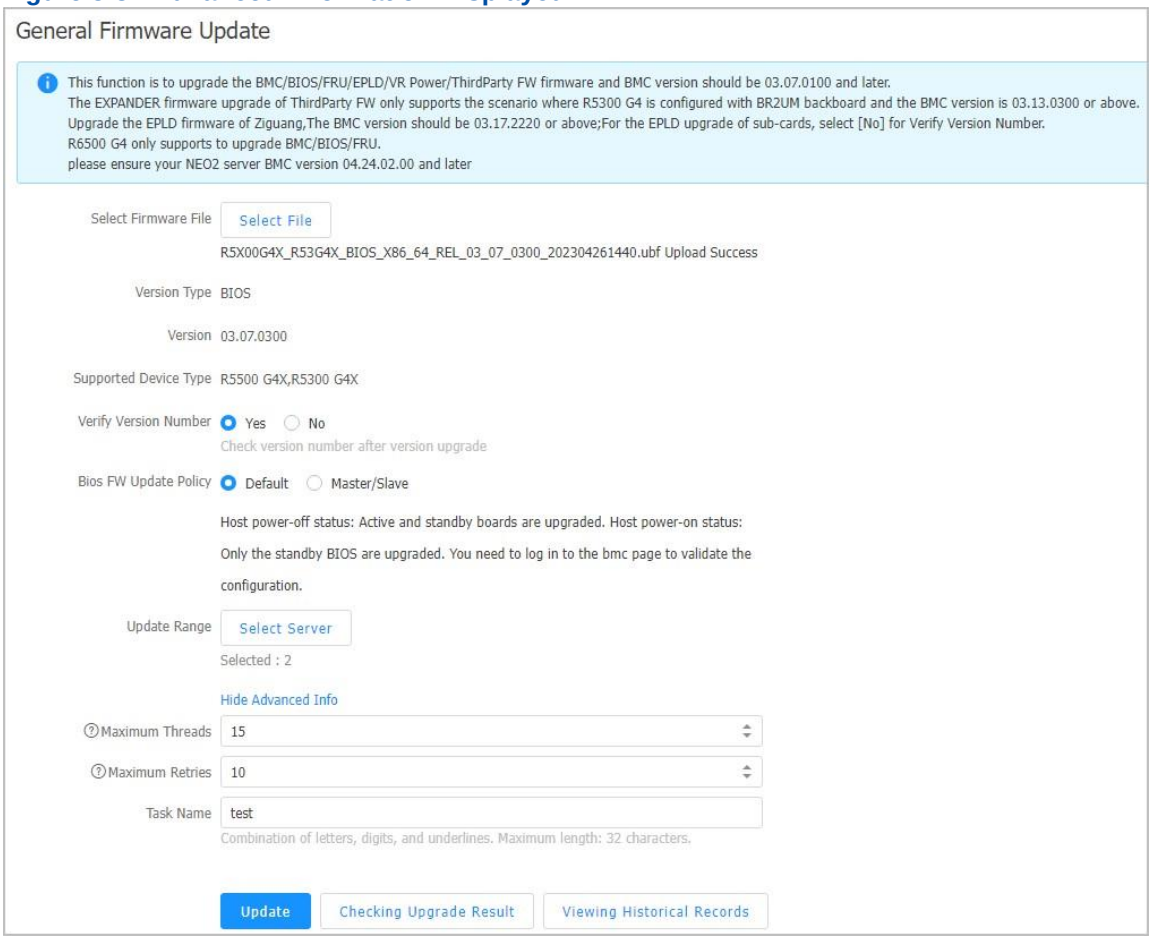
Host Power-on Status	BIOS Upgrade Policy	
-	Default	Upgrade both the active BIOS and the standby BIOS.
Powered off	Upgrade both the active BIOS and the standby BIOS	Upgrade both the active BIOS and the standby BIOS.
Powered on	Upgrade the standby BIOS	a. Power off the host. b. Upgrade both the active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



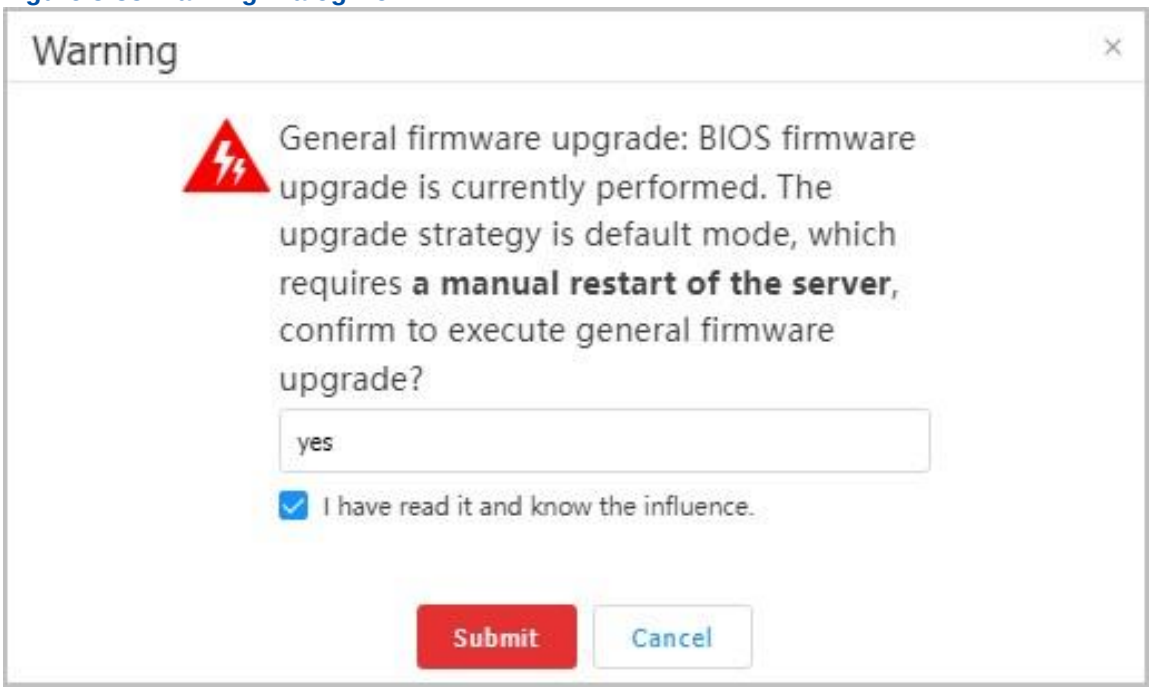
8. Configure upgrade parameters. For a description of the parameters, refer to Table 3-53.

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 **View Report** to view the upgrade result of general firmware.
Reconfigure the parameters for upgrading general firmware	1. Click **Reconfiguration**. A message box is displayed. 2. Click **Submit**.
Export the report	Click **Export Report** 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.

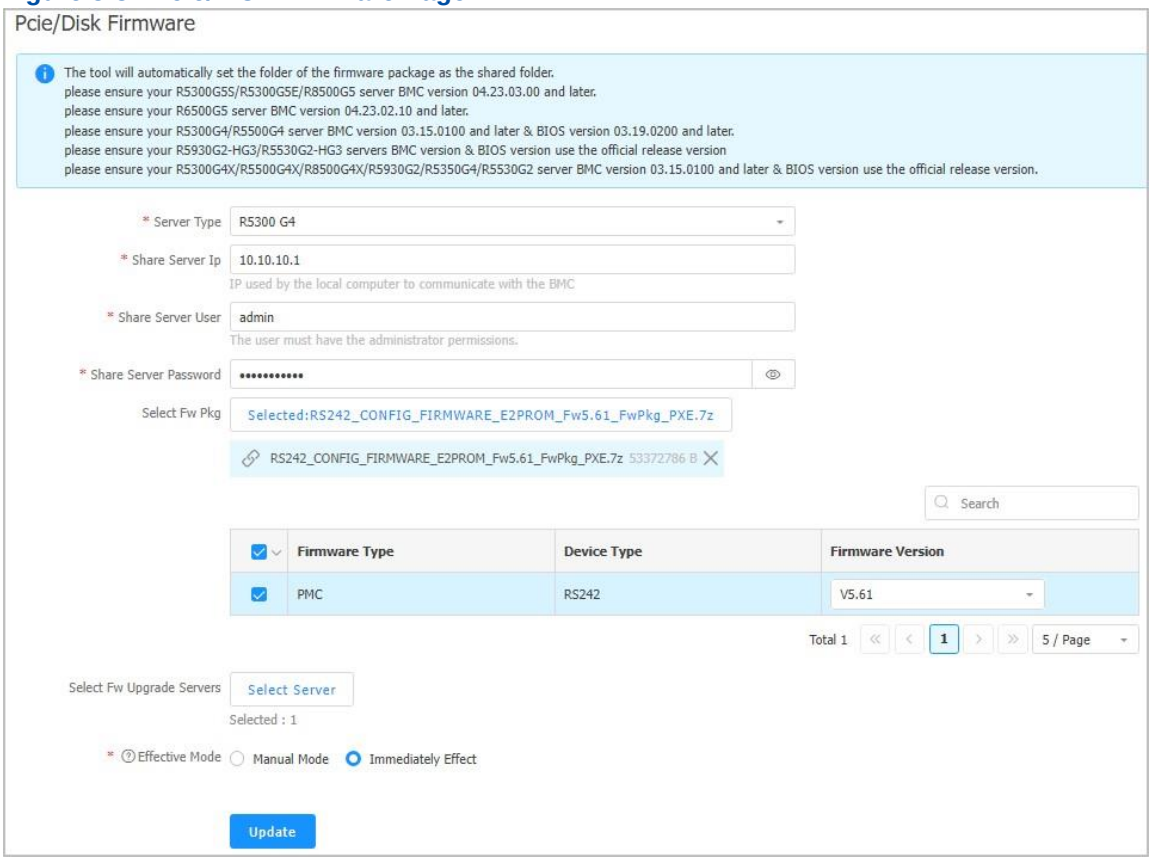
Prerequisite

- 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



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 **Select File**, and select the desired firmware file.
Select Fw Upgrade Servers	Click **Select Server**, and select the servers whose firmware needs to be upgraded.
Effective Mode	Select a validation mode. Options: ● **Manual Mode**: After the configurations are completed, you must manually restart the related hosts to apply the configurations. ● **Immediately Effect**: After the configurations are completed, the related hosts are automatically restarted to apply the configurations.

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

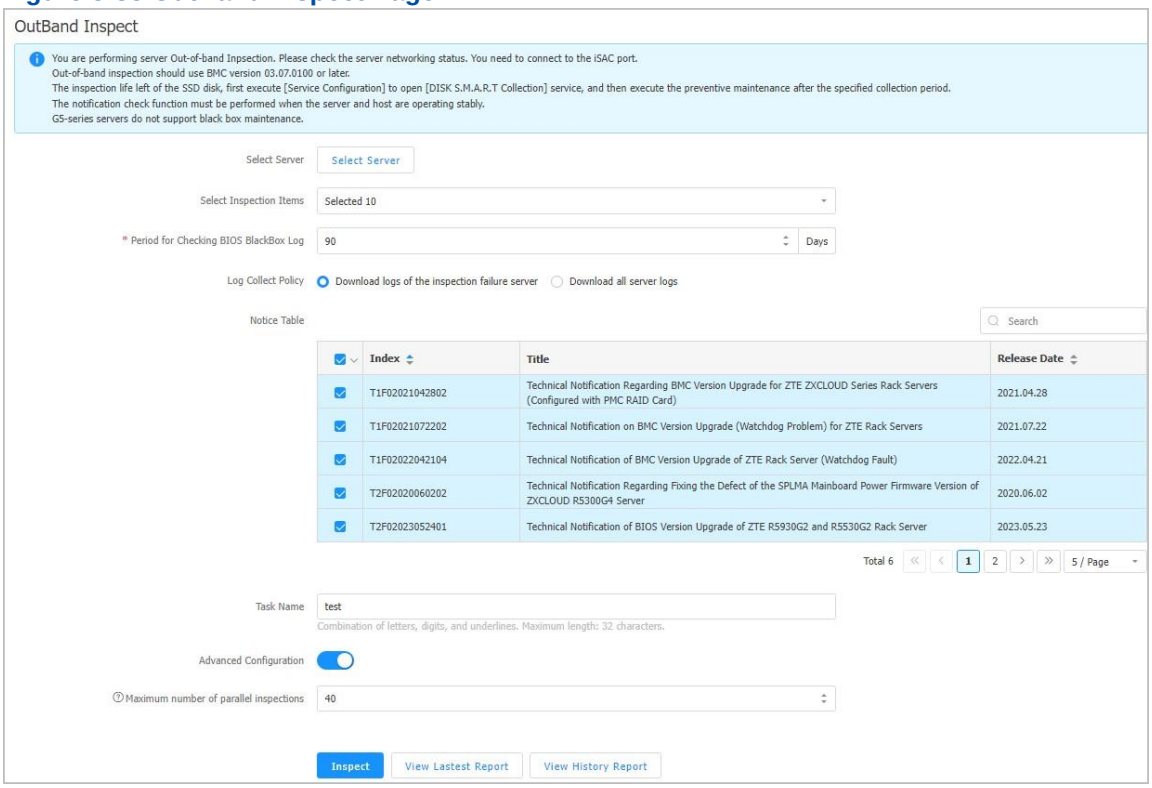
- The network status of the server is proper and the iSAC network port is connected.

- 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



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 **Select Server**, and select the server that you want to inspect.

Select Inspection Items	Select the desired inspection items. The inspection parameters displayed in the lower part of the page vary with the selected inspection items. ● If **BIOS black box** is selected, you need to set **Period for Checking BIOS BlackBox Log**. ● If **Asset Inspection** is selected, you can set **Disk Inspection Threshold**. The **Disk Inspection Threshold** switch can be enabled only after the corresponding license is imported. ● If **Notice Check** is selected, you need to select notices in the **Notice Table** list to check whether the operations described in the notices are performed on the selected servers.
Parameter	**Description**
Period for Checking BIOS BlackBox Log	This parameter is displayed and required when **BIOS black box** is selected from the **Select Inspection Items** list. 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.
Log Collect Policy	Select the log collection policy. Options: ● **Download logs of the inspection failure server**: downloads log files from only the servers that fail the inspection. ● **Download all server logs**: downloads log files from all the servers involved in the inspection.
Notice Table	This parameter is displayed and required when **Notice Check** is selected from the **Select Inspection Items** list. Select the desired notices from the list.
Task Name	Enter the name of the inspection task.
Maximum number of parallel inspections	Click the **Advanced Configuration** toggle button to enable this parameter. Set **Maximum number of parallel inspections**. Range: 30–60. Default: 40. 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.

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 **Show Detail**. The detailed information about the out-of-band inspection is displayed.
Perform inspection again	1. Click **Re-Inspection** to return to the **OutBand Inspect** page. 2. Set the out-of-band inspection parameters again. 3. Click **Inspect**.
To...	**Do...**
View alarms	1. Click in the **Details** column. The alarm causes and handling suggestions of the corresponding alarm are displayed. 2. (Optional) Click **OutBand Inspect . Detailed Inspection** in the upper left corner to return to the out-of-band inspection result page.

3.6.2 Performing In-Band Inspection

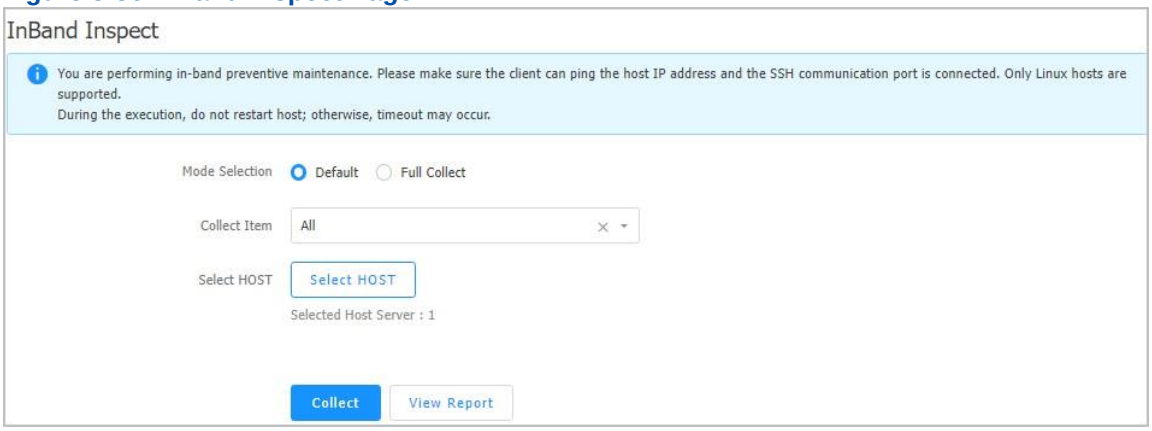
Abstract

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: ● **Default**: collects the information of the specified modules. The collected information does not include large files and files that are time-consuming to be collected. ● **Full Collect**: collects the information of the specified modules. The collected information includes large files and files that are time-consuming to be collected.
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 **Select HOST** 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 **Re-Collection** to return to the **InBand Inspect** page. 3. Set the in-band inspection parameters again. 4. Click **Collect**.
Export logs	1. Select the servers for which the collected logs need to be exported. 2. Click **Export Log**.
Perform a secondary collection	1. Select the server for a secondary collection. 2. Click **Second Collect**.

3.6.3 Collecting Asset Information

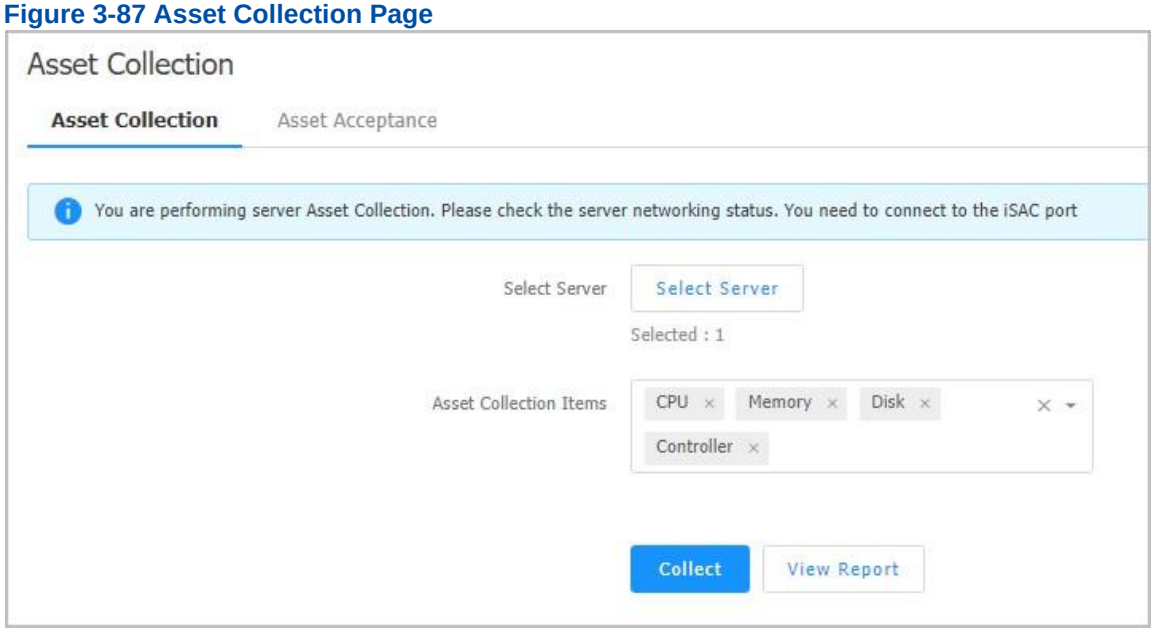
Abstract

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 **Select Server**, 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

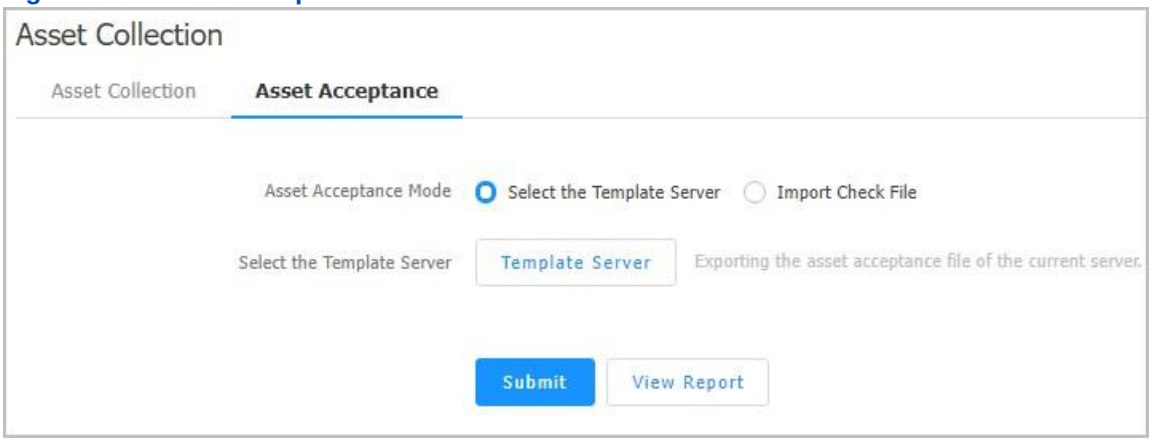
Abstract

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



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

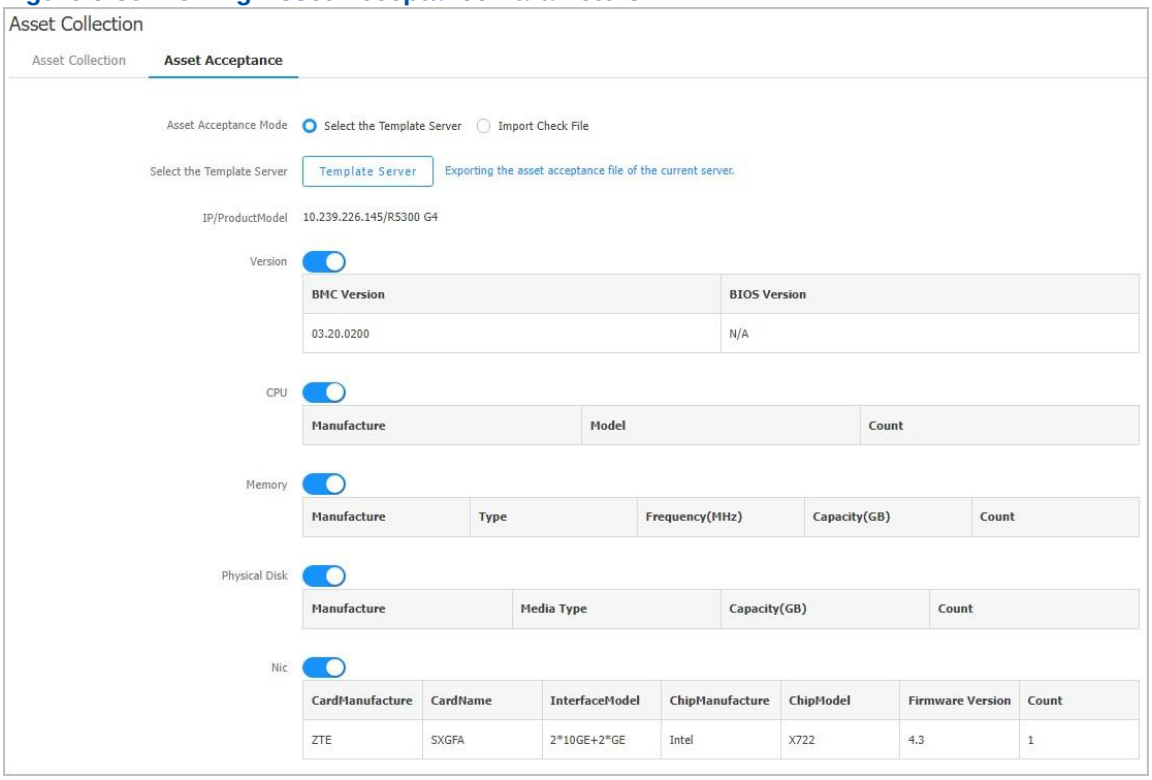
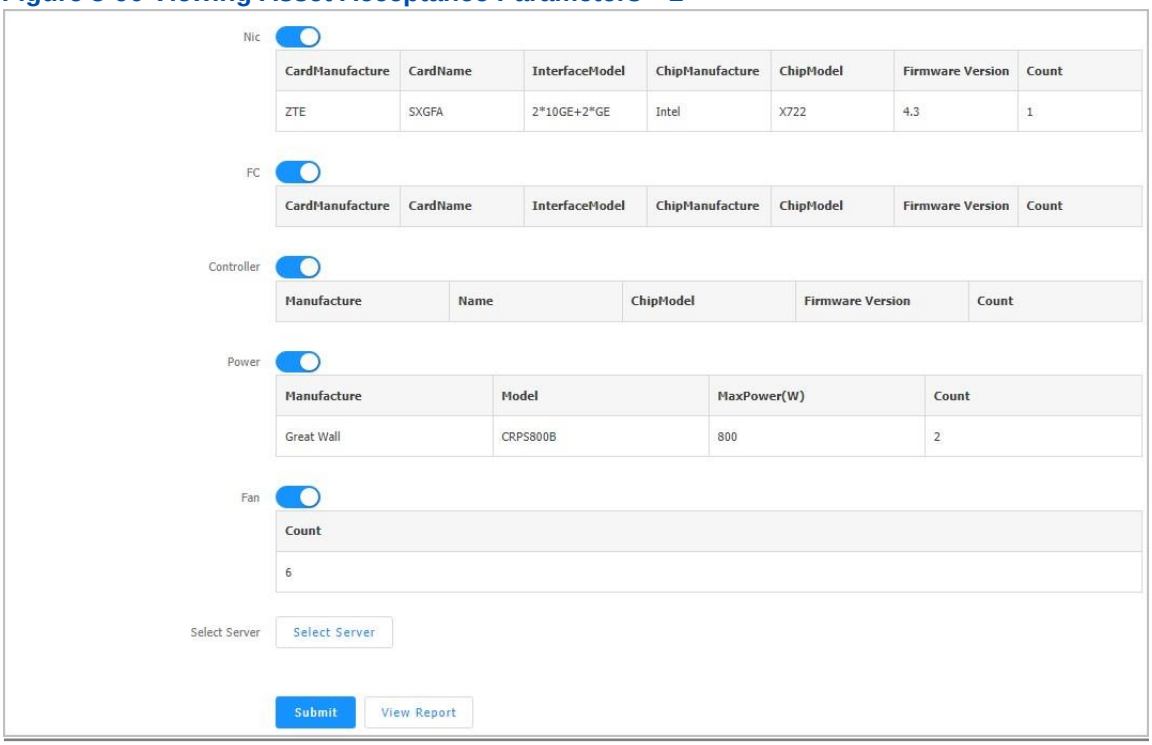


Figure 3-90 Viewing Asset Acceptance Parameters—2



Note

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 **View Details**. The detailed asset acceptance information is displayed.
Perform asset acceptance again	1. Click **ReAcceptance**. The **ReAcceptance** dialog box is displayed. 2. Click **Submit**.
Export a statistical report	Click **Export Statistic Report**. The acceptance report is exported and saved to a local `*.csv` file.

3.6.4.2 Performing Asset Acceptance Through a Check File

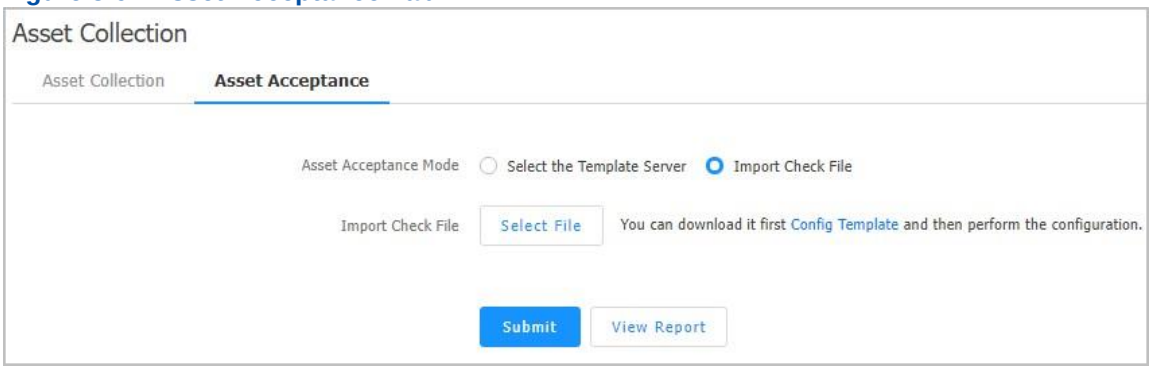
Abstract

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.

Note

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.

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 **View Details**. The detailed asset acceptance information is displayed.
Perform asset acceptance again	1. Click **ReAcceptance**. The **ReAcceptance** dialog box is displayed. 2. Click **Submit**.

To...	Do...
Export a statistical report	Click **Export Statistic Report**. 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

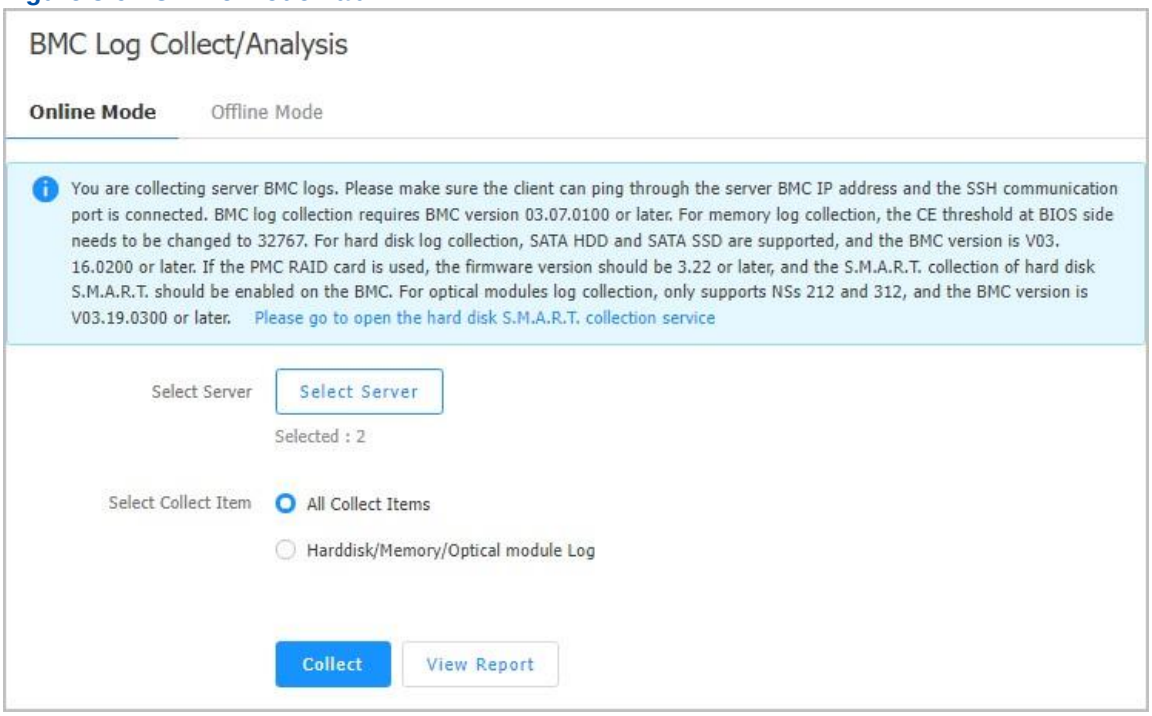
If you need to collect hard disk logs, enable the **DISK S.M.A.R.T.Collection** service. For details, refer to "3.4.2.12 Configuring Services".

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



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.

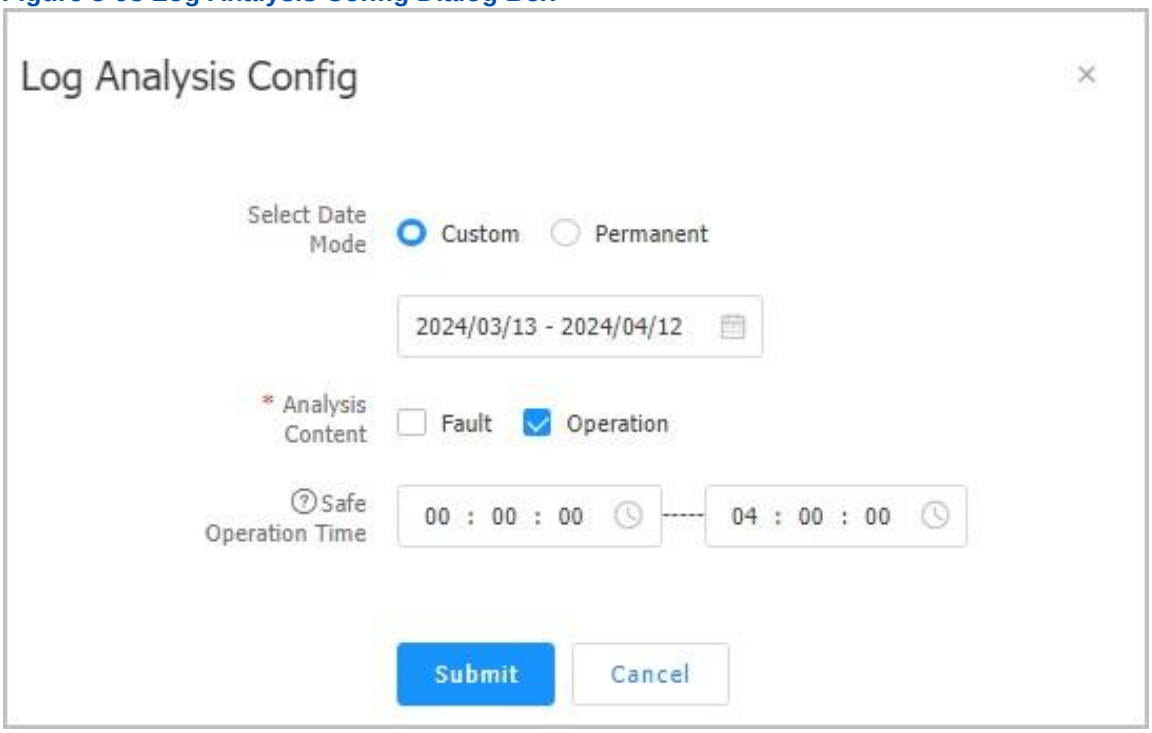
Note

- 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
	● **Custom**: Logs generated within the specified time period are analyzed. You need to select the start date and end date. ● **Permanent**: Logs generated at any time are analyzed.
Analysis Content	Select the objects for log analysis. Options: ● **Fault**: analyzes fault logs. ● **Operation**: analyzes the logs about the operations such as power-on and power-off that are not performed within the allowed operation time. After **Operation** is selected, you also need to set **Safe Operation Time**.
Safe Operation Time	This parameter is required when **Analysis Content** is set to **Operation**. Select the allowed operation period. Default: 00:00:00–04:00:00.

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	1. Click **Re-Collection** to return to the **BMC Log Collect/Analysis** page. 2. Set the collection parameters again. 3. Click **Collect**.
Export logs	1. Select the servers for which the collected logs need to be exported. 2. Click **Export Log**.
Perform a secondary collection	1. Select the server for which you want to collect logs for the second time. 2. Click **Second Collect**.

3.7.2 Analyzing BMC Logs Offline

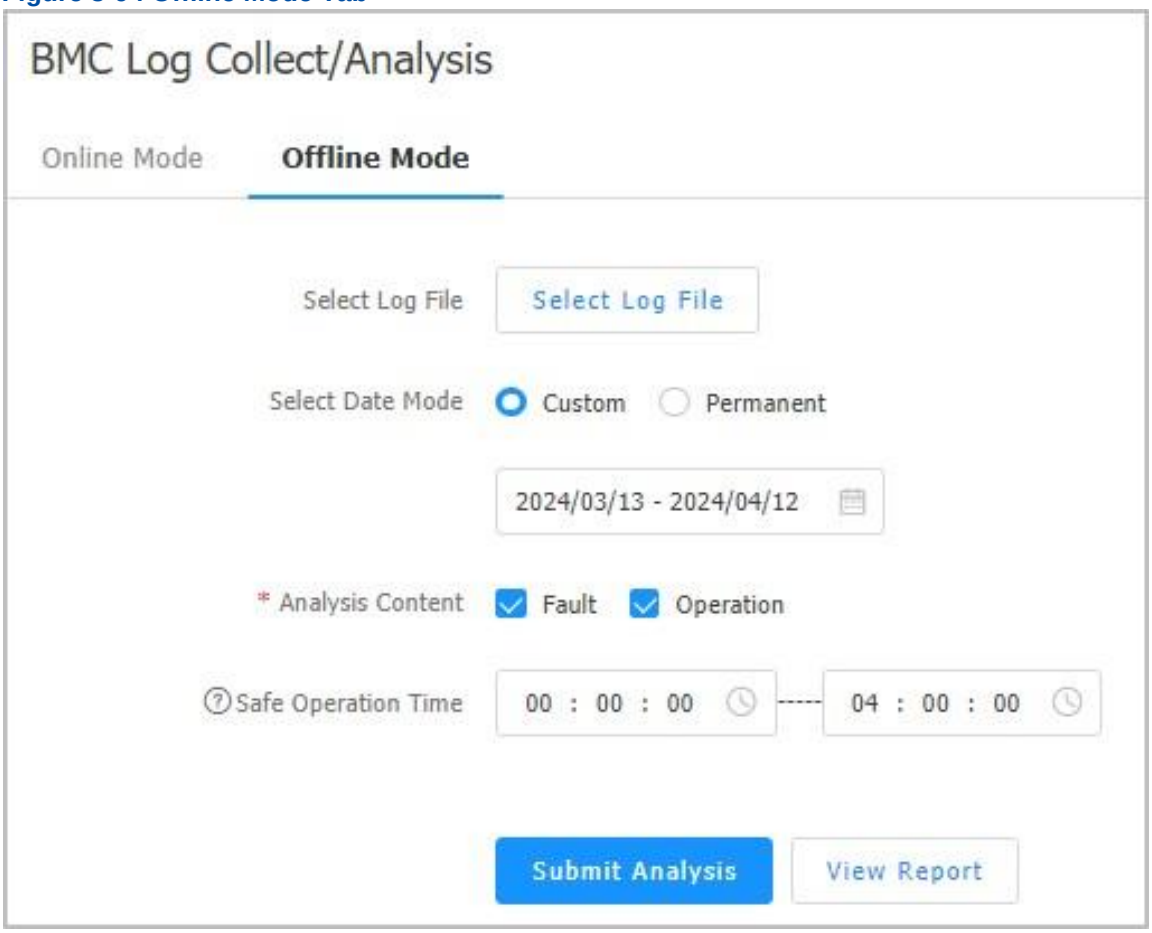
Abstract

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



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 **Select Log File** to select the log file that you want to analyze. Log files can be exported in the following ways: ● UniKits ● Web portal of the BMC
Select Date Mode	Select a time period within which the logs to be analyzed were generated. Options: ● **Custom**: Logs generated within the specified time period are analyzed. You need to select the start date and end date.

Parameter	Description
	● **Permanent**: Logs generated at any time are analyzed.
Analysis Content	Select the objects for log analysis. Options: ● **Fault**: analyzes fault logs. ● **Operation**: analyzes the logs about the operations such as power-on and power-off that are not performed within the allowed operation time. After **Operation** is selected, you also need to set **Safe Operation Time**.
Safe Operation Time	This parameter is required when **Analysis Content** is set to **Operation**. 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

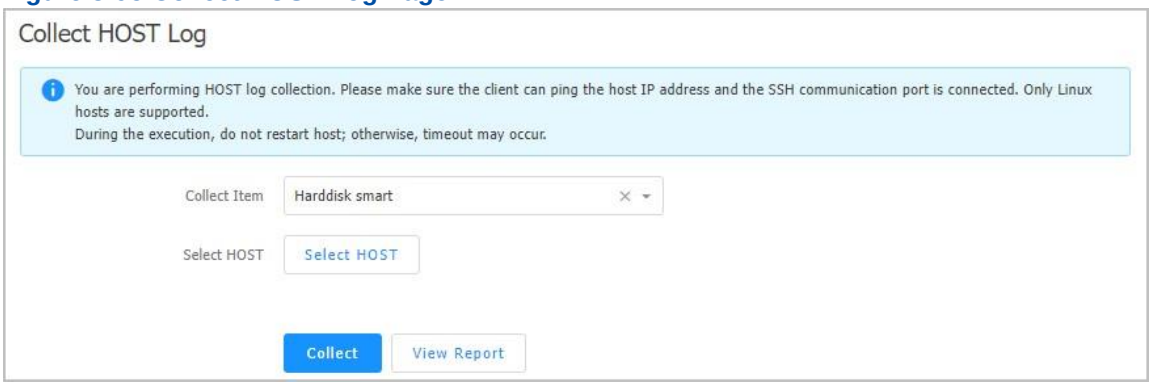
Abstract

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	1. Click **Re-Collection** to return to the **Collect HOST Log** page. 2. Set the collection parameters again. 3. Click **Collect**.
Export logs	1. Select the servers for which the collected logs need to be exported. 2. Click **Export Log**.
Perform a secondary collection	1. Select the servers for which you want to perform a secondary collection. 2. Click **Second Collect**.

3.7.4 Programming a UUID and Serial Number

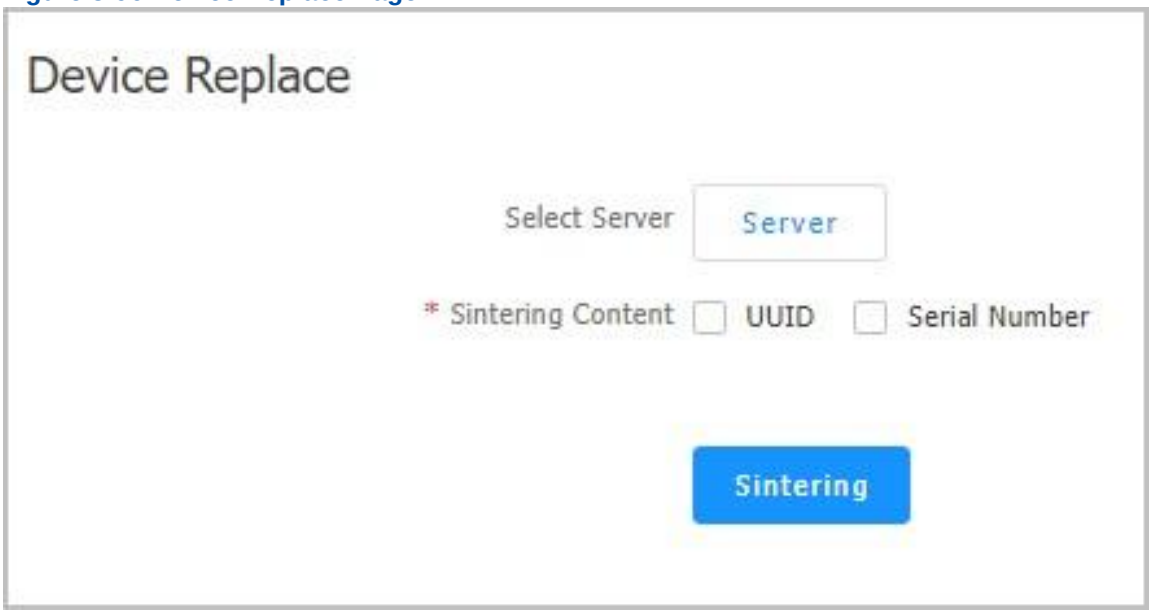
Abstract

After replacing a mainboard, you need to program the UUID and serial number of the original main board to the new mainboard.

Steps

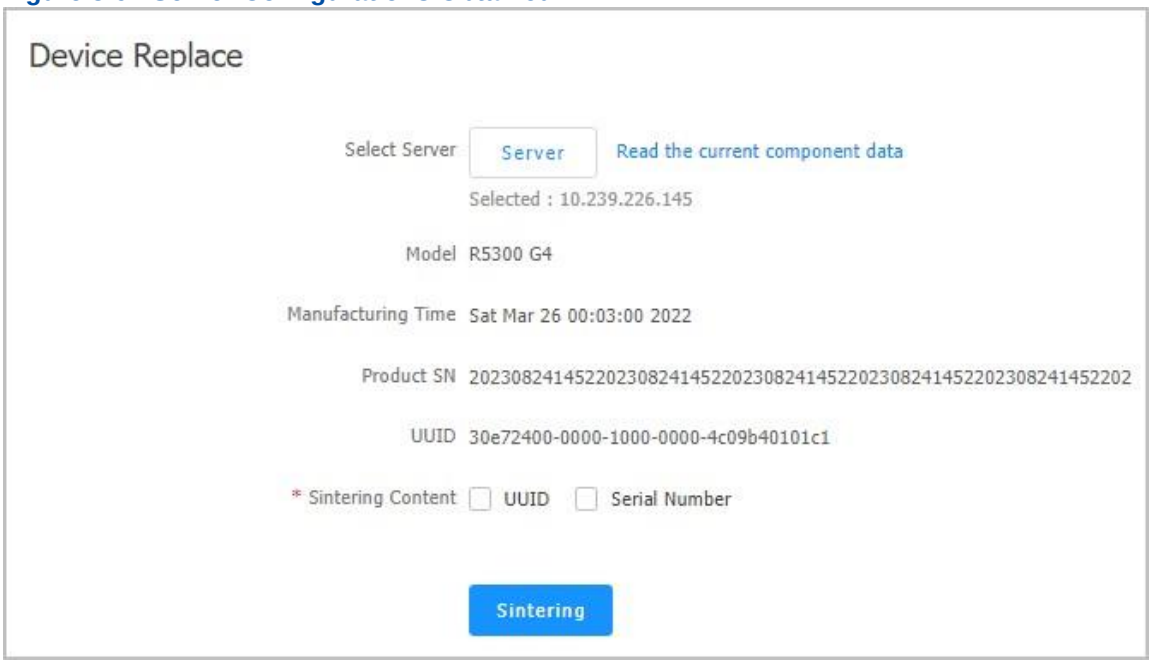
1. Select **Device Mgmt > Troubleshooting > Device Replace**. The **Device Replace** page is displayed, see Figure 3-96.

Figure 3-96 Device Replace Page



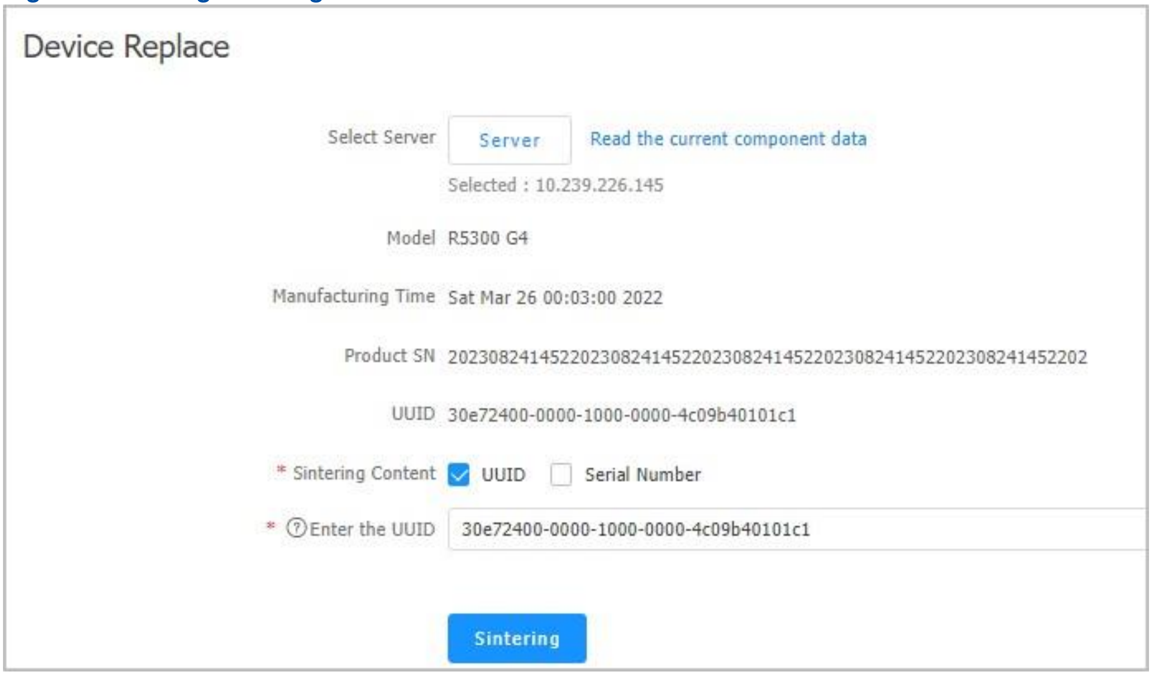
2. Click **Server**. The **Select Server** dialog box is displayed.
3. Select the server where the mainboard has been replaced.
4. Click **Get Config**. The configurations of the server are obtained, see Figure 3-97.

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



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

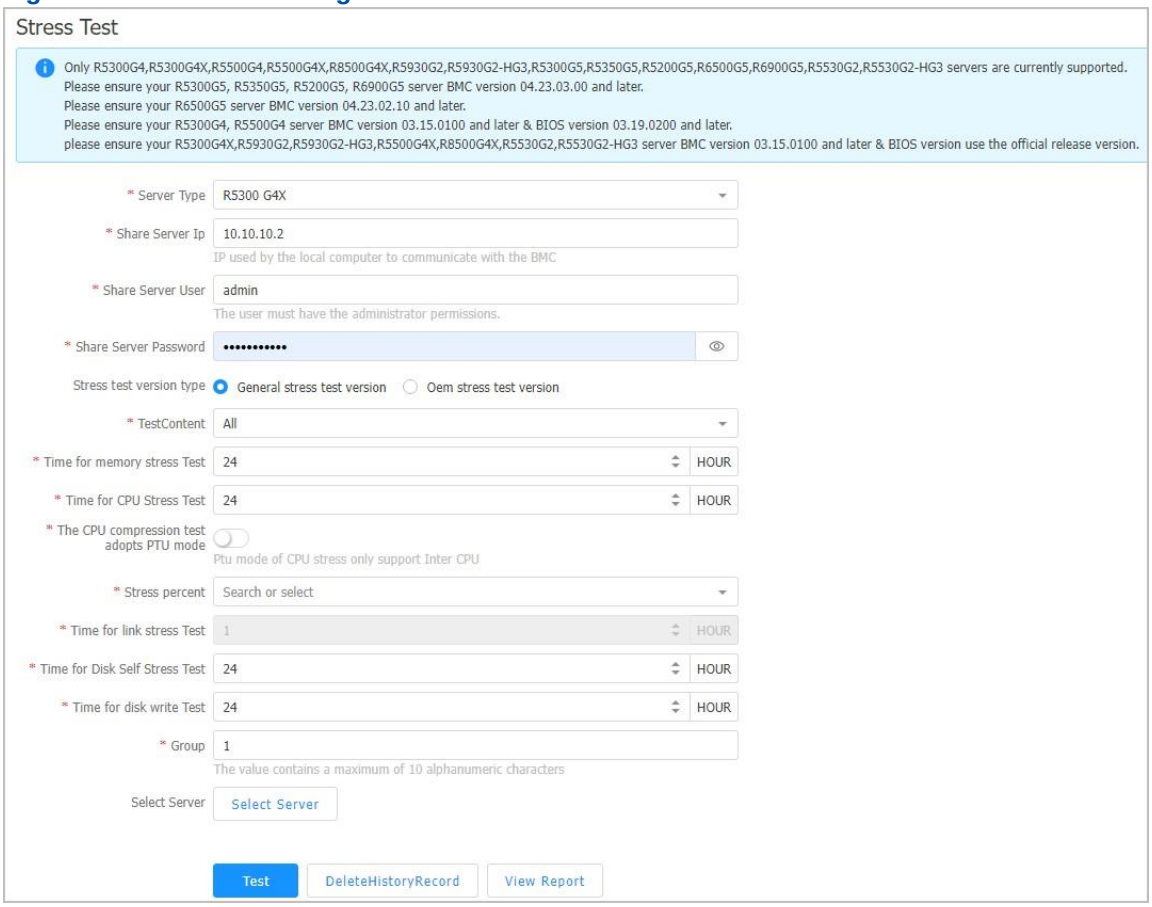
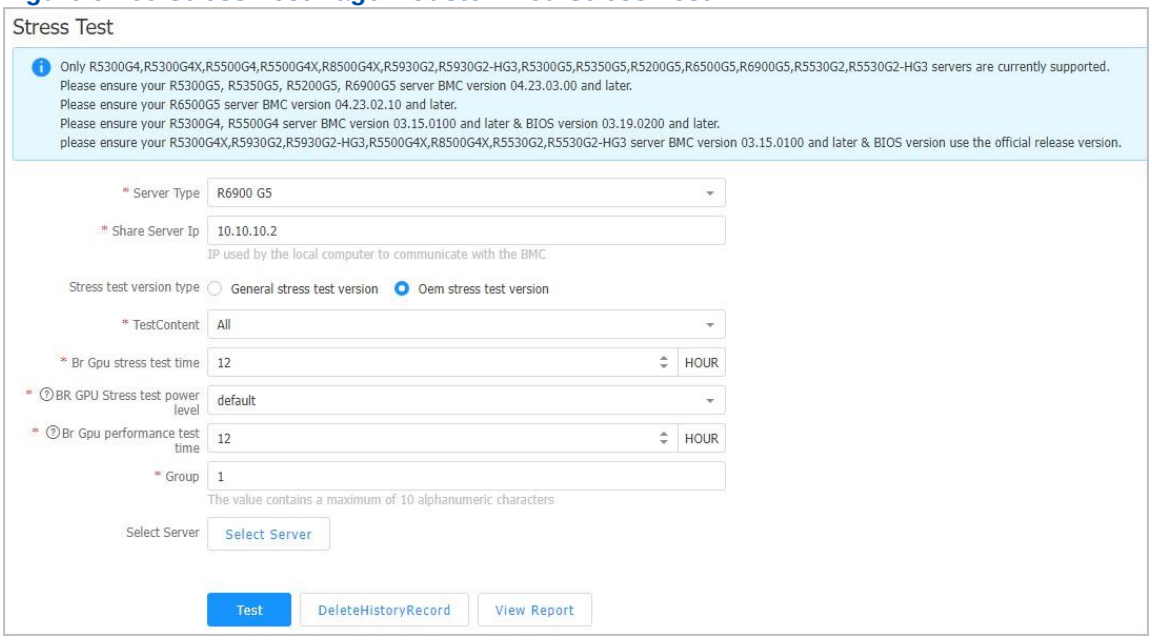


Figure 3-100 Stress Test Page—Customized Stress Test



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 **General stress test version**.
TestContent	Select the desired test items. Options: ● **Memory stress Test** ● **CPU stress Test** ● **Link error code Test** ● **Hard disk self-check** ● **Hard disk write Test**

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 PTU 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 iSAC management interface in each batch must be unique.
Select Server	Click **Select Server**, and select the servers for which you want to conduct stress tests.

Table 3-61 Parameter Descriptions for Customized Stress Tests

Parameter	**Description**
Server Type	Select the server model for which you want to conduct customized stress tests.
Share Server Ip	Enter the IP address of the installation PC.
Stress test version type	Select **Oem stress test version**.
TestContent	Select the desired test items. Options: ● **BR GPU Stress Test** ● **BR GPU Performance Test**
Br Gpu stress test time	Enter the GPU stress test duration. Range: 0.5–48 hours.

BR GPU Stress test power level	Select a desired power consumption level. Options: ● **default** ● **50** ● **60** ● **70** ● **80** ● **90** ● **100**
Parameter	**Description**
	The default option is **default**, indicating that consumption levels from **50** to **100** are set in sequence. When conducting a stress test, the test time of each power consumption level is: **Br GPU stress test time** ÷ 6. 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 × the current power consumption level. For example, if the following error message is displayed when the test item is **board power**, it only indicates that the power exceeds the upper limit during the test. The displayed error message is irrelevant to the hardware. `max should less than xxx`
Br Gpu performance test time	Enter the GPU performance 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 iSAC management interface in each batch must be unique.
Select Server	Click **Select Server**, 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 **View Report** to view the progress and result of the previous or current stress test.
Reconduct a stress test	Click **ReTesting** to conduct the stress test again.
View the progress of a batch of tests	Click **Show Detail** in the **Operation** column for the desired batch.
View the progress of multiple batches of tests.	1. Select the desired batches. 2. Click **CheckProgress**.
Export a stress test report	1. Select the batch of tests for which the report needs to be exported.
To...	**Do...**
	2. Click **Export Report**.

3.7.6 Setting a UID Indicator State

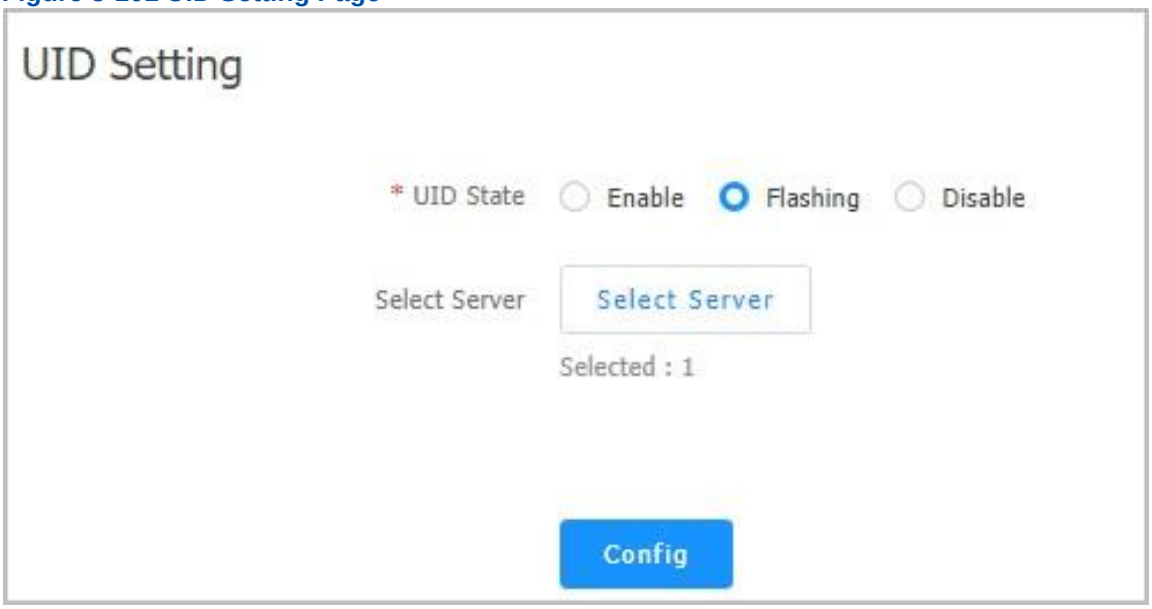
Abstract

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



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: ● **Enable**: The UID indicator is turned on. ● **Flashing**: The UID indicator is flashing. ● **Disable**: The UID indicator is turned off.
Select Server	Click **Select Server** 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

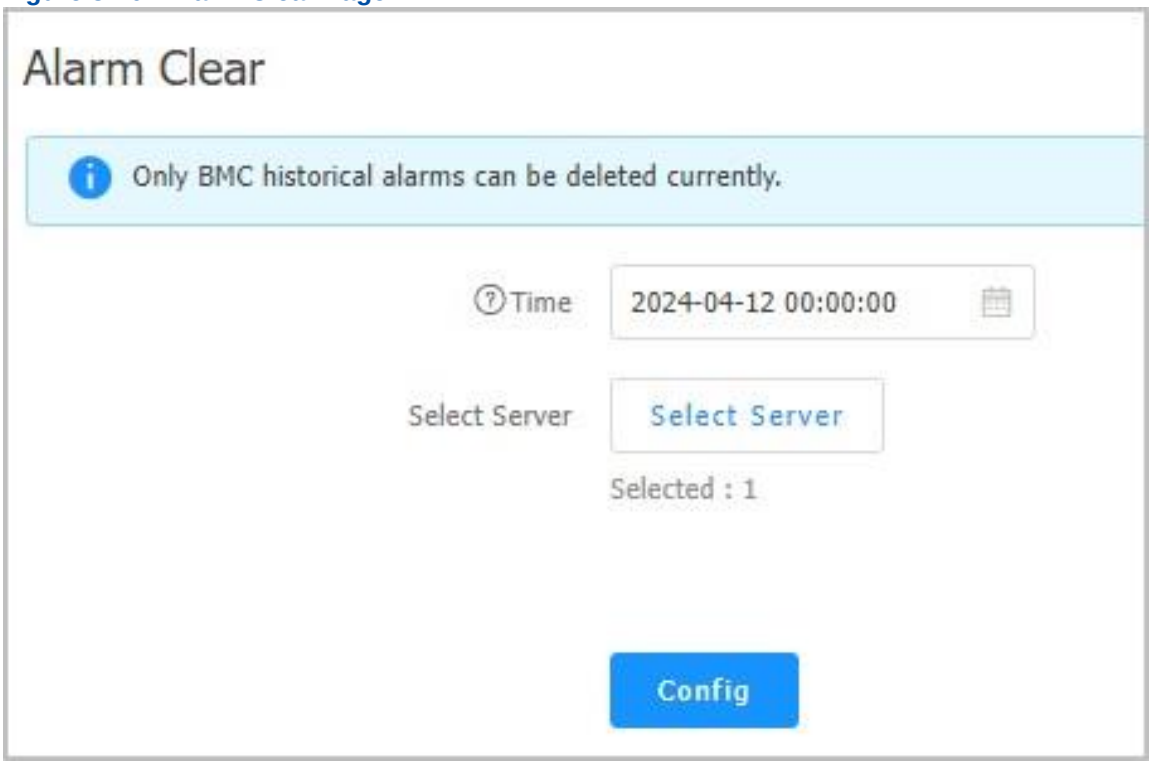
Abstract

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 **Time** is set to **2024-04-12 00:00:00**, the alarms raised before 00:00:00 on April 12, 2024 are cleared.
Select Server	Click **Select Server** 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

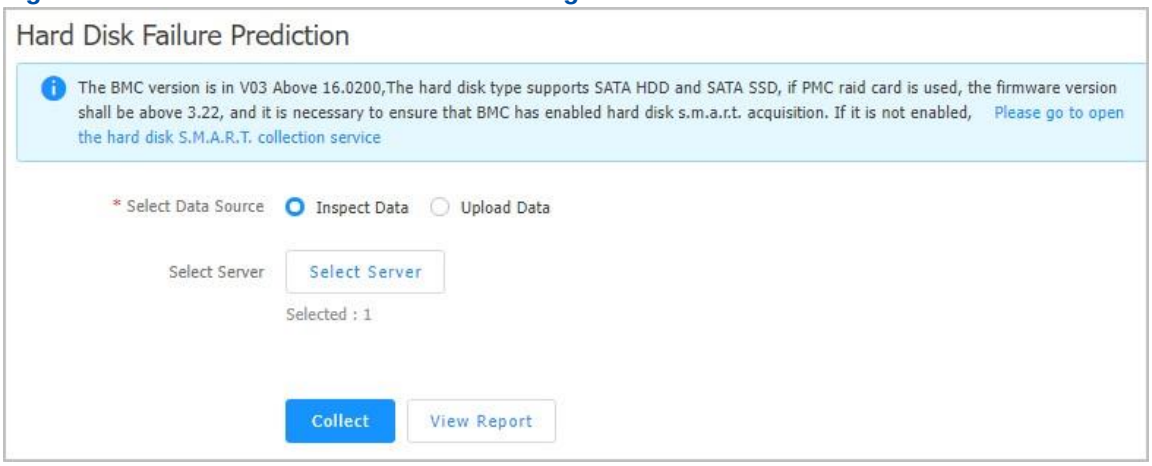
Abstract

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 **Inspect Data**.
Select Server	Click **Select Server**, and select the server for which you want to predict hard disk faults.

3. Click **Collect** to deliver the collection command.

Note

After the collection is completed, the collection results are displayed automatically.

4. Click **Start Forecasting**.

Note

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.

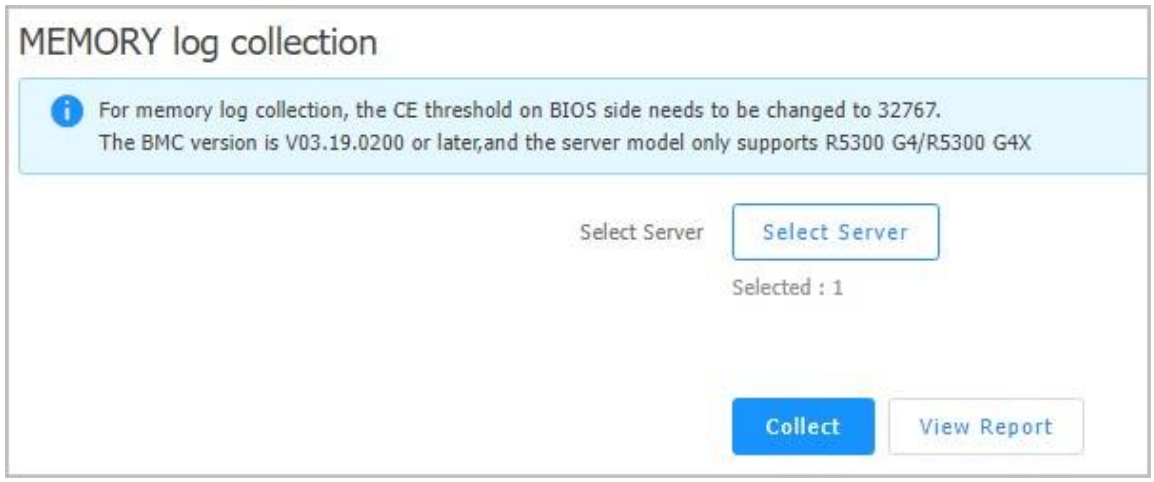
3.8.2 Predicting Memory Faults

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**



2. Click **Select Server**, and select the server for which you want to predict memory faults.
3. Click **Collect** to deliver the collection command.

Note

After the collection is completed, the collection results are displayed automatically.

4. Click **Start Forecasting**.

Note

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

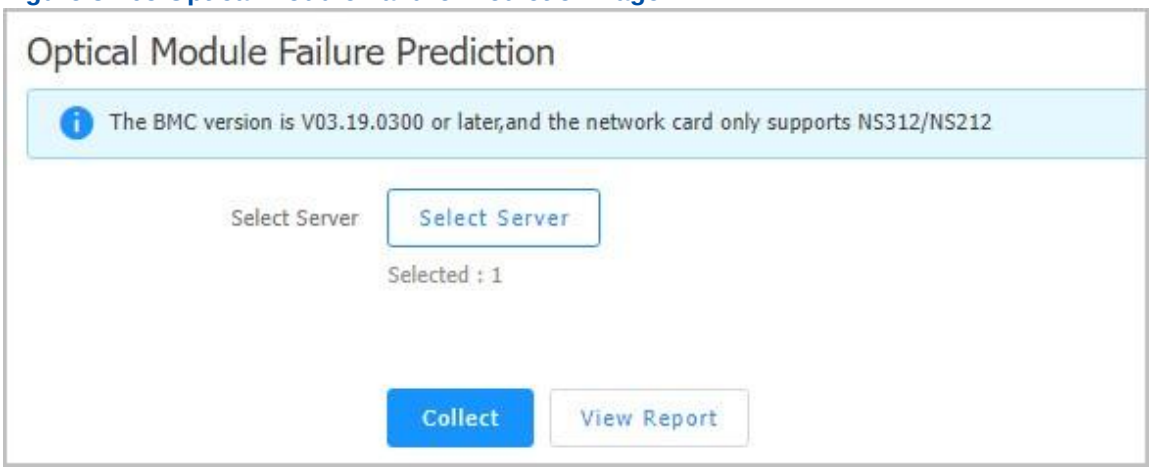
Abstract

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.

Note

After the collection is completed, the collection results are displayed automatically.

4. Click **Start Forecasting**.

Note

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.

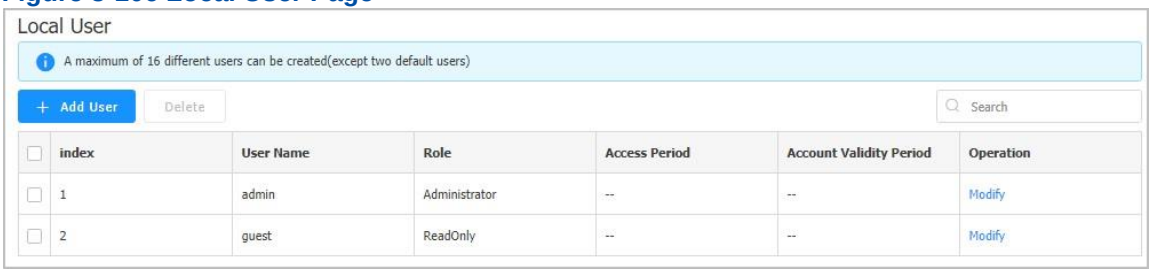
Notice

The **admin** and **guest** users cannot be deleted from the local users.

Steps

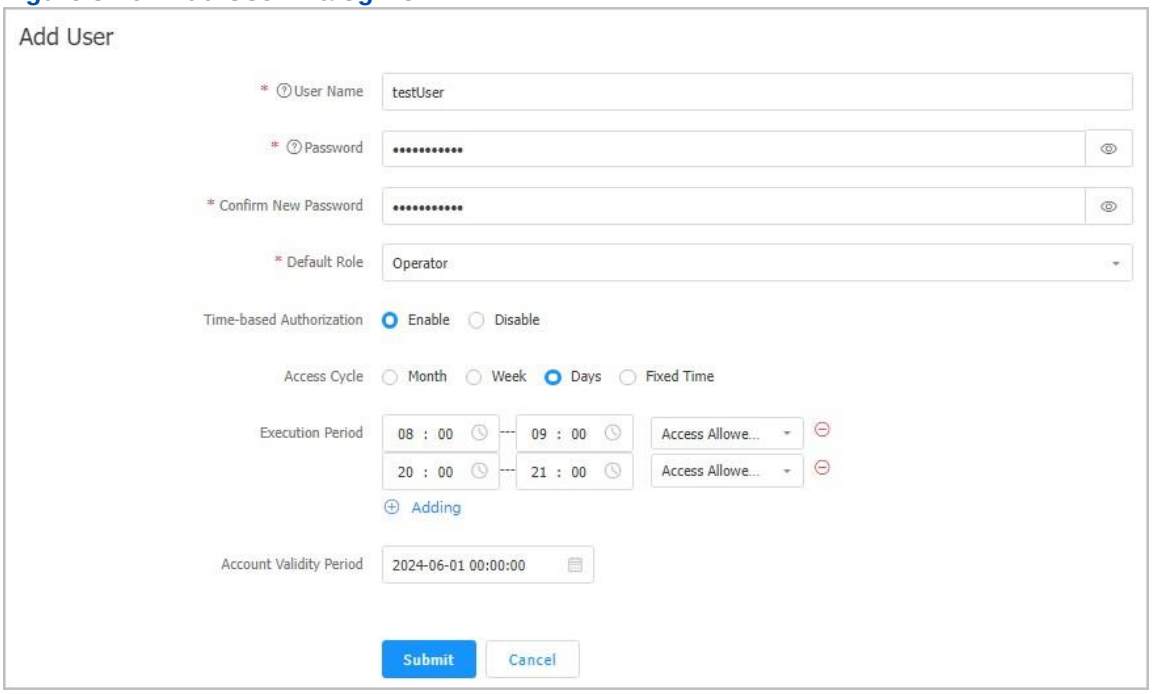
1. Select **System Mgmt > User Mgmt > Local User**. The **Local User** page is displayed, see Figure 3-106.

Figure 3-106 Local User Page



2. Click **Add User**. The **Add User** dialog box is displayed, see Figure 3-107.

Figure 3-107 Add User Dialog Box



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: ● A string of 4–16 digits and letters ● Case sensitive ● Allowed special characters: -, _, and @.
Password	Enter the password of the local user. The requirements for the password are as follows: ● The password cannot be the same as the username. ● The length is 8–20 characters. ● The password must contain four types of characters (uppercase letters, lowercase letters, digits, and symbols). ● The password must not contain spaces or tabs.
Confirm Password	Enter the password again.
Default Role	Select the role of the local user. Options: ● **Administrator**: indicates that the local user has permissions on all functions. ● **Operator**: indicates that the local user has permissions on collection inspection and configuration delivery (except the configurations related to user management and LDAP), and the local user has no permission on

Parameter	Description
	user management (including adding or deleting a user, and modifying user permissions and password). ● **ReadOnly**: 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.
Time-based Authorization	Select whether to enable the time-based authorization function. Options: ● **Enable**: indicates to enable the time-based authorization function. After the function is enabled, **Access Cycle** and **Execution Period** should be configured to specify the permissions of the newly added user within a fixed period. ● **Disable**: indicates to disable the time-based authorization function.
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	1. Click **Modify** in the **Operation** column for the local user. The **Change User** dialog box is displayed. 2. Modify the parameters for the local user. 3. Click **Submit**.
Delete a local user	1. Click **Delete** in the **Operation** column for the local user. The **Delete Local User** dialog box is displayed. 2. Click **Submit**.
Delete local users in batches	1. Select the local users that you want to delete. 2. Click **Delete**.

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.

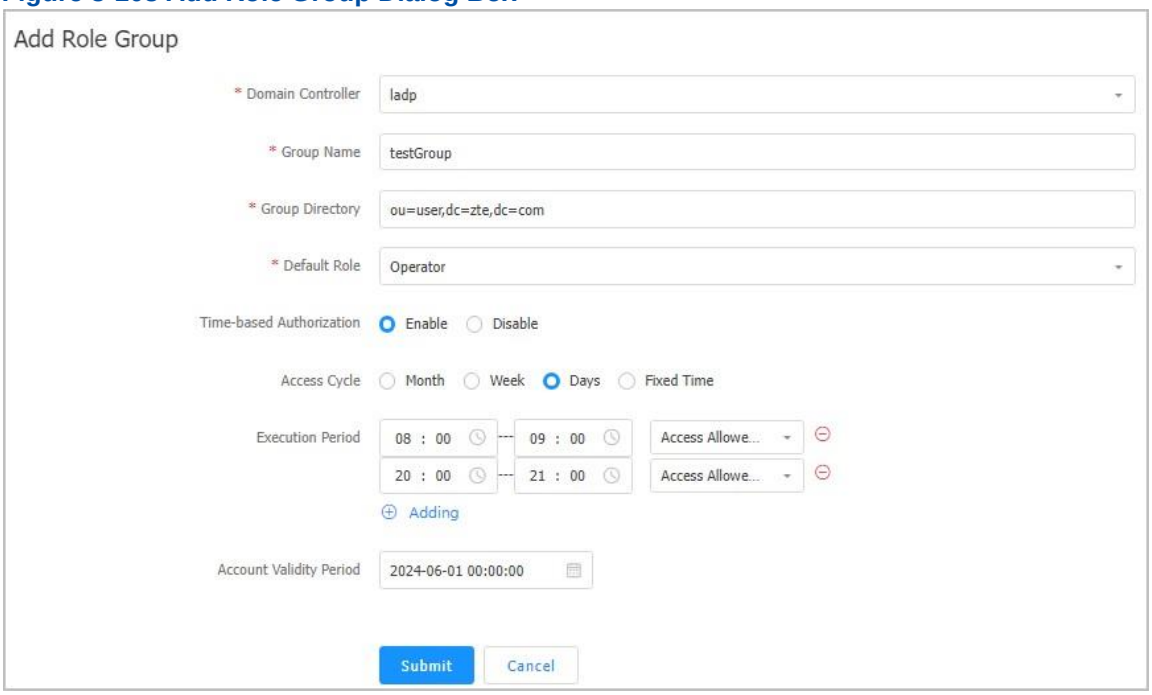
Prerequisite

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



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: ● **Administrator**: indicates that the domain user has permissions on all functions. ● **Operator**: 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). ● **ReadOnly**: indicates that the domain user only has permissions on collection inspection.
Time-based Authorization	Select whether to enable the time-based authorization function. Options:
Parameter	**Description**
	● **Enable**: indicates to enable the time-based authorization function. After the function is enabled, **Access Cycle** and **Execution Period** should be configured to specify the permissions of the newly added user within a fixed period. ● **Disable**: indicates to disable the time-based authorization function.
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 **Modify** in the **Operation** column for the domain user. The **Change User** dialog box is displayed. 2. Modify the parameters for the domain user. 3. Click **Submit**.
Delete a domain user	1. Click **Delete** in the **Operation** column for the domain user. The **Delete Domain User** dialog box is displayed. 2. Click **Submit**.
Delete domain users in batches	1. Select the domain users that you want to delete. 2. Click **Delete**.

3.9.3 Adding an LDAP Server

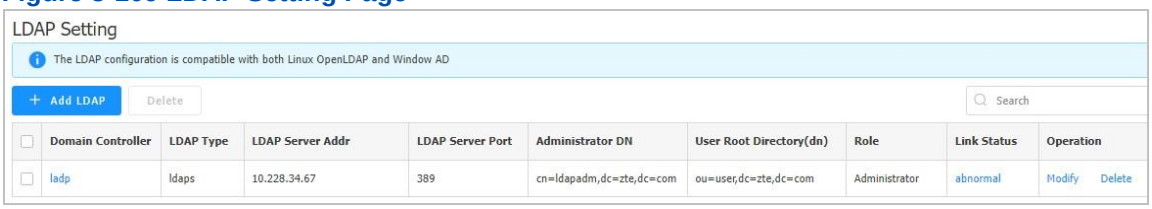
Abstract

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

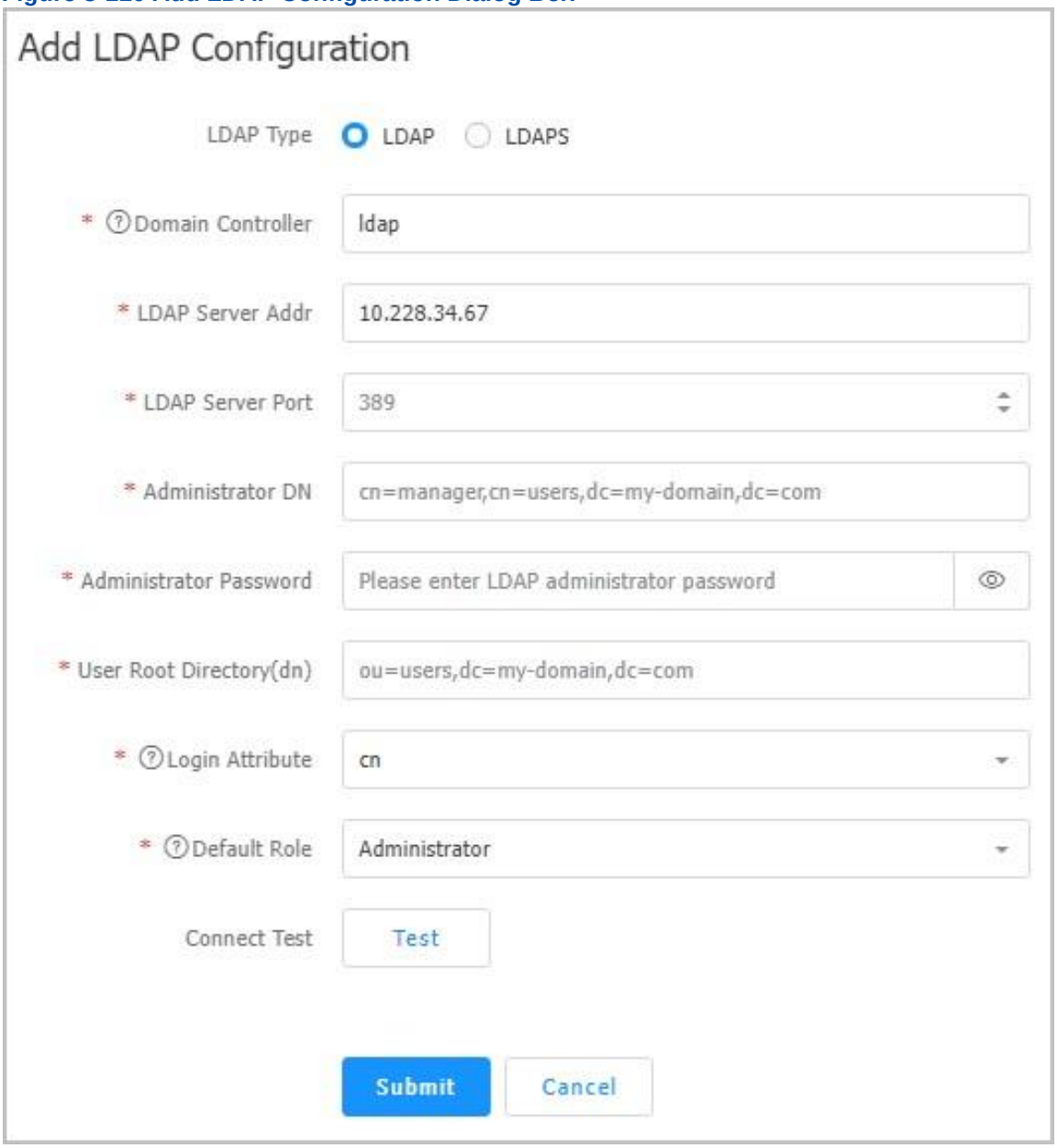
1. Select **System Mgmt > System Setting > LDAP Setting**. The **LDAP Setting** page is displayed, see Figure 3-109.

Figure 3-109 LDAP Setting Page



2. Click **Add LDAP**. The **Add LDAP Configuration** dialog box is displayed, see Figure 3-110.

Figure 3-110 Add LDAP Configuration Dialog Box



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: ● **LDAP**: indicates that communications are not encrypted. ● **LDAPS**: indicates that communications are encrypted.
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 IP address of the LDAP server. Both the IPv4 address and domain name are supported.
LDAP Server Port	Enter the port number of the LDAP server. For example: ● LDAP port number: 389 ● LDAPS port number: 636
Administrator DN	Enter the DN with the administrator permissions on the LDAP server. For example, cn=ldapadm,dc=NETAŞ,dc=com. DNs are unique and used for distinguishing between users. A DN has three attributes: CN, DC, and OU.
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, ou=user,dc=NETAŞ,dc=com.
Login Attribute	Select a user login attribute. Options: ● **cn**: The common name of a user is used for login. ● **uid**: The user ID of a user is used for login. ● **mail**: The email address of a user is used for login.
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 **Test** 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 **Domain Controller** column. The LDAP configuration details are displayed.
Modify the information about an LDAP server	1. Click **Modify** in the **Operation** column for the LDAP server. The **Update LDAP Configuration** dialog box is displayed. 2. Modify the LDAP configurations. 3. Click **Submit**.
Delete an LDAP server	Click **Delete** in the **Operation** column for the LDAP server.
Delete LDAP servers in batches	1. Select the LDAP servers that you want to delete. 2. Click **Delete**.

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.

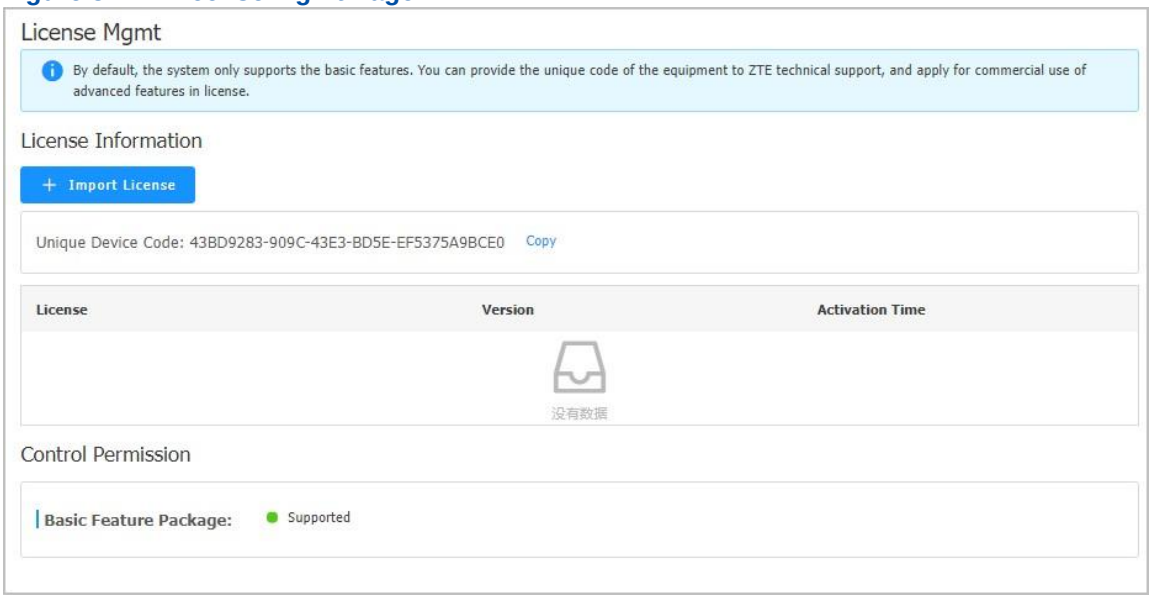
Prerequisite

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.

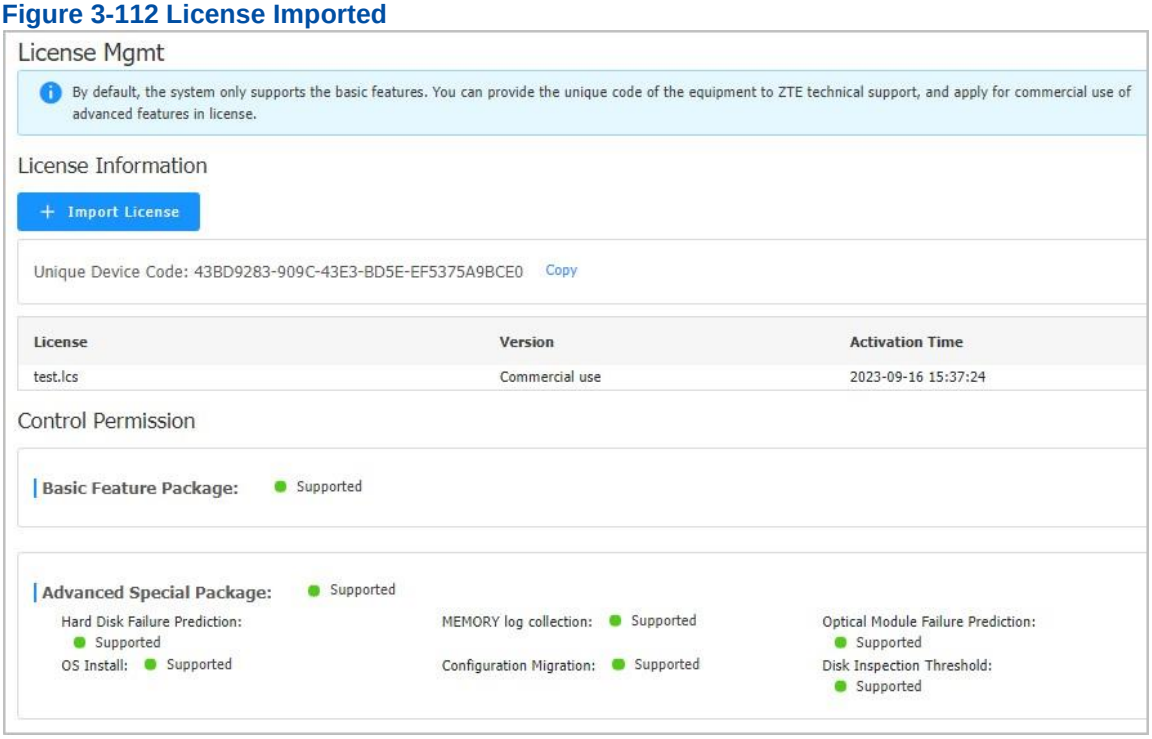
Figure 3-111 License Mgmt Page



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



3.9.5 Querying Management Logs

Abstract

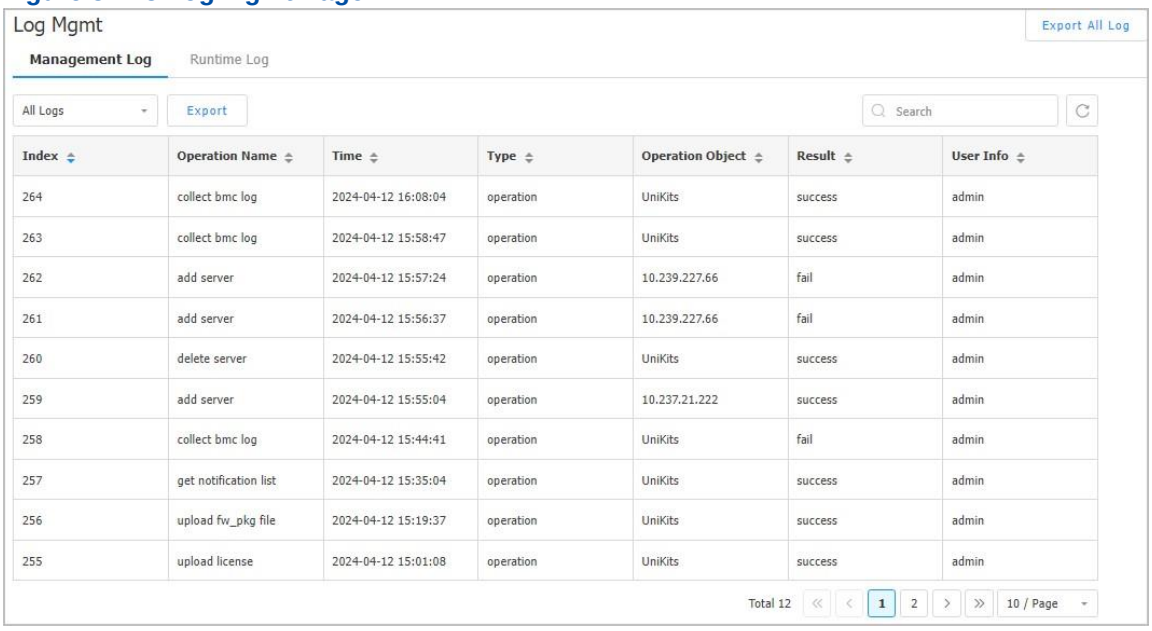
Management logs record your operations in the UniKits, including operation logs and login logs.

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.

Note

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.

Note

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

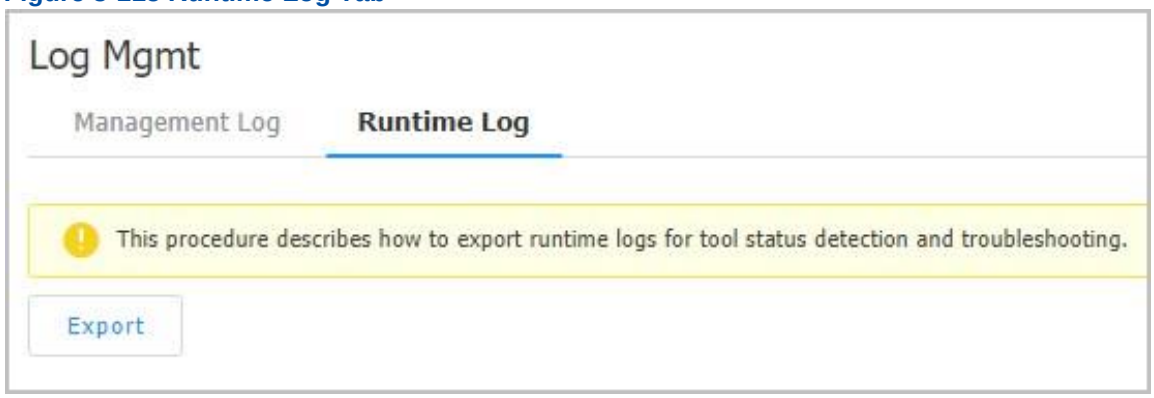
Abstract

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.

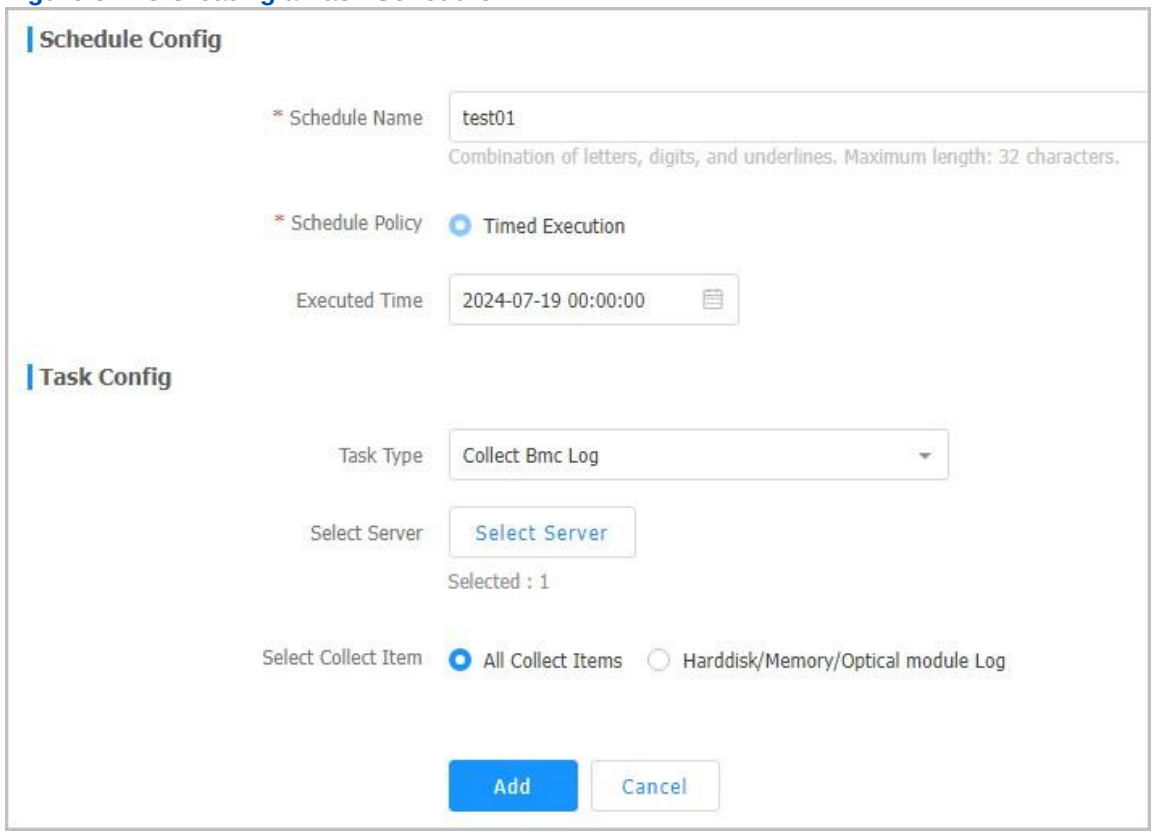
Steps

1. Select **Task Center > Task Schedule**. The **Task Schedule** page is displayed, as shown in Figure 3-117.

Figure 3-117 Task Schedule Page

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



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
Schedule Config	
Schedule Name	Name of the schedule. It consists of letters, digits, and underscores. A maximum of 32 characters are supported.
Schedule Policy	By default, **Timed Execution** is selected.
Executed Time	Click to set the start time of the task.
Task Config	
Task Type	By default, **Collect Bmc Log** is selected.
Select Server	Click **Select Server**, and select a server on which the scheduled task will be executed.

Select Collect Item	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	1. Click **Show Detail** in the **Operation** column to view the schedule details. 2. Check the schedule details and task execution result.
Delete task schedules	1. Select the task schedules to be deleted. 2. Click **Delete**.

3.10.2 Viewing Task Execution Records

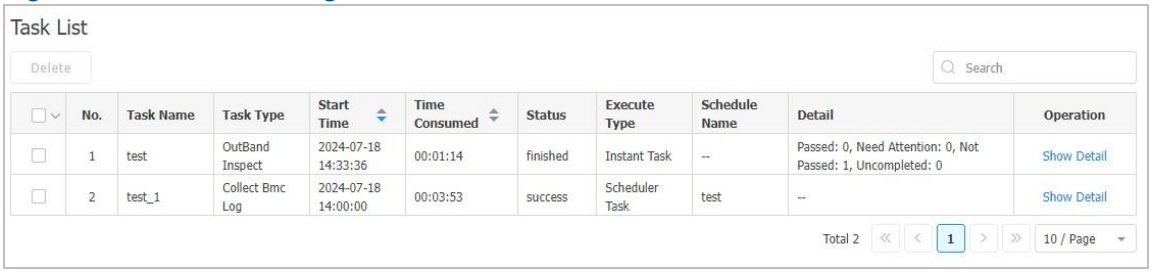
Abstract

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

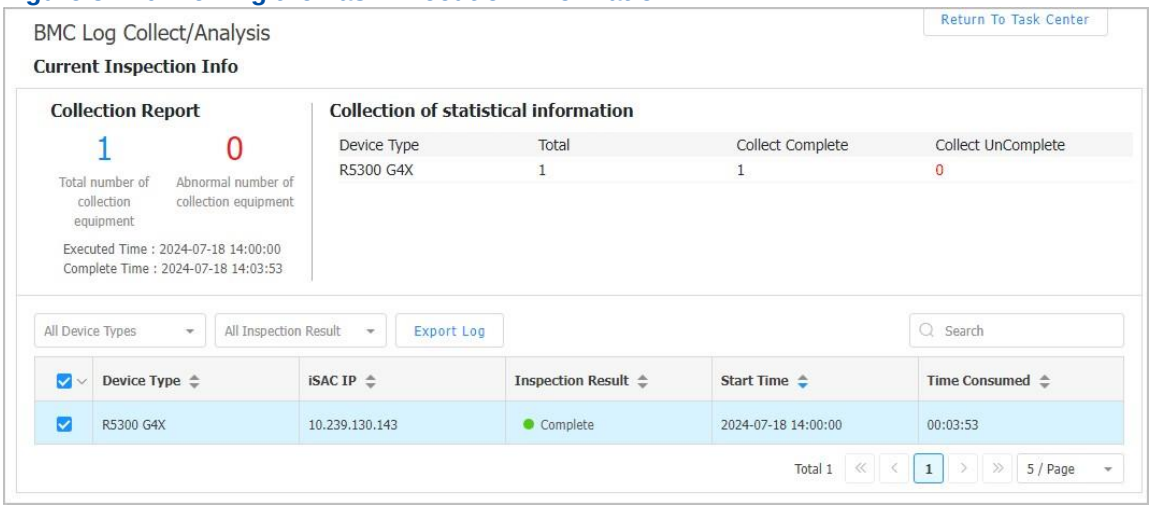
1. Select **Task Center > Task List**. The **Task List** page is displayed, as shown in Figure 3-119.

Figure 3-119 Task List Page



2. Click **Show Detail** in the **Operation** colum to view the detailed task execution information, as shown in Figure 3-120.

Figure 3-120 Viewing the Task Execution Information



Chapter 4
Troubleshooting

Table of Contents

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	a. Start the control panel of the operating system. b. Click **Appearance and Personalization**. The **Appearance and Personalization** window is displayed. c. Click **Display**. The **Display** window is displayed. d. Select **Smaller (S)-100%(default)**. e. Click **Apply**.
Windows 10 is used	a. Right-click the desktop and select **Display settings**. The **Display** window is displayed. b. Select **100% (Recommended)** for **Change the size of text, apps, and other items**.

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 **ViewShow 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:

   - 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 NETAŞ 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=NETAŞ, 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.

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 *Windows8.1- 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 *Windows8.1- KB2999226-x64.msu* patch package, install the *Windows8.1-KB2919355- x64.msu* patch package first and then the *Windows8.1KB2999226-x64.msu* patch package.
The *Windows8.1-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.

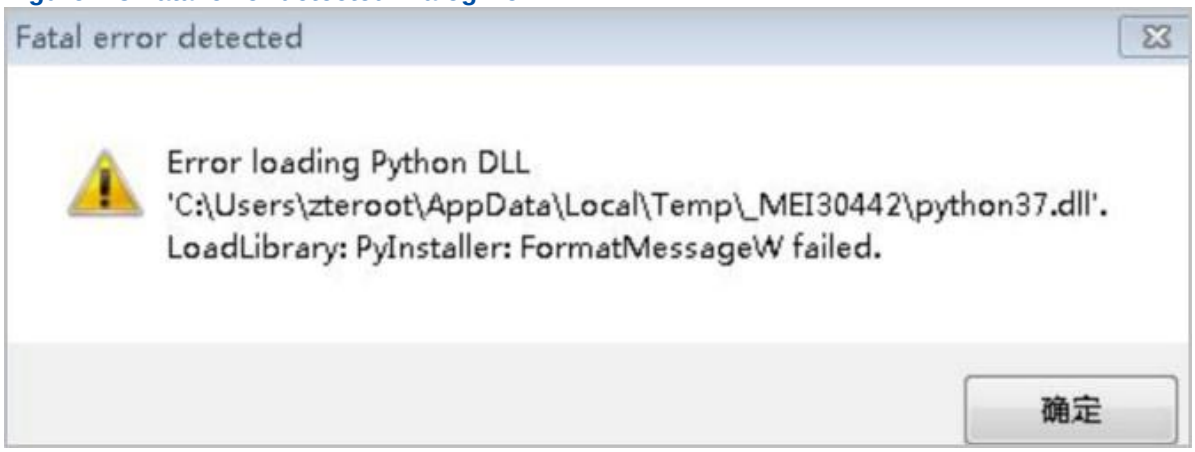
4.9 UniKits Operation Failure in the 64-Bit Windows 7 OS

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 *Windows6.1- KB2999226-x64.msu* patch package.

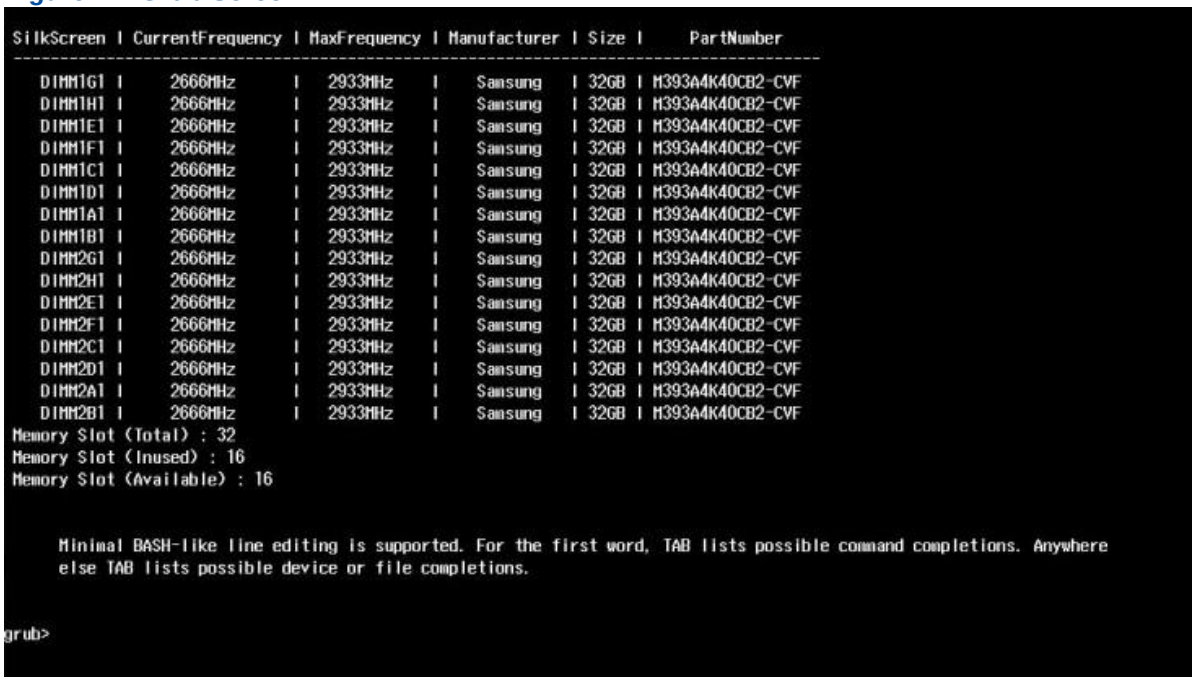
   The patch package is downloaded at https://www.microsoft.com/zh-cn/download/details.aspx?id=49062&751be11f-ede8-5a0c-058c-2ee190a24fa6=True. If the link is unavailable, you can search for and download the patch package.
2. Uninstall the UniKits.
3. Reinstall the UniKits.

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



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 NETAŞ 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

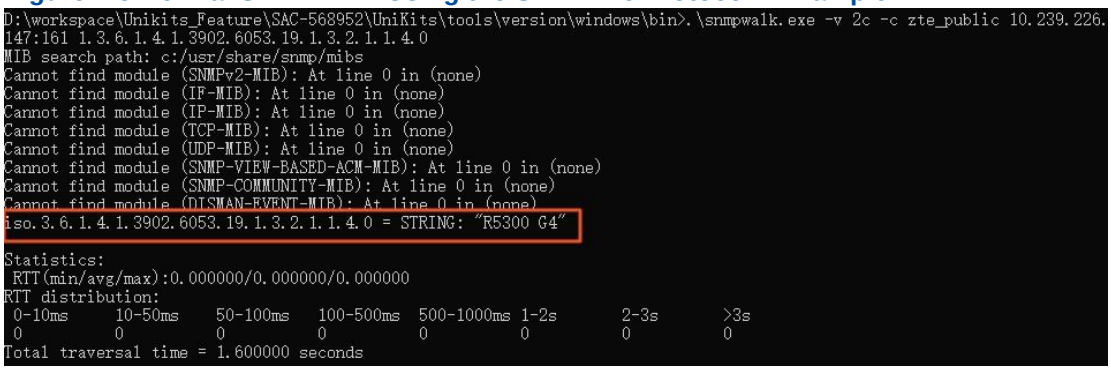
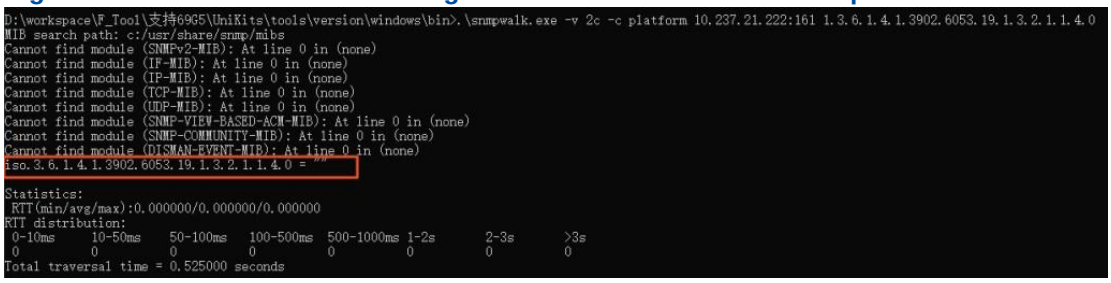


Figure 4-6 Normal SNMP Link Using the SNMPv2c Protocol—Example 2

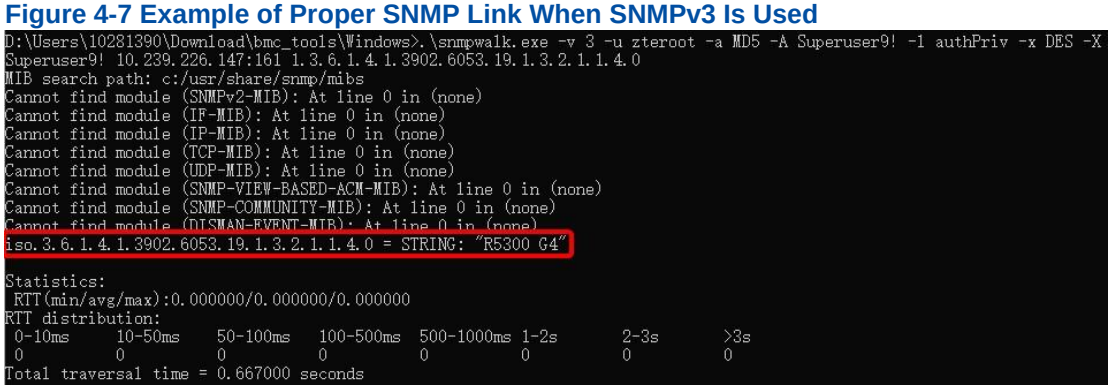


- If SNMPv3 is used, run the following command.

  .\snmpwalk.exe -v 3 -u NETAŞroot -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



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 outof-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
Service Type	**Default Port Number**
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 KVM.
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
IPMI link error	1. Check whether the network connection is proper. For example, run the **`ping`** command to check connectivity. 2. Check whether the username and password are correct. 3. Check whether the IPMI link is proper. For details, refer to "4.4 IPMI Link Error". 4. (Optional) If the fault persists, contact NETAŞ technical support.

SNMP link error	1. Check whether the network connection is proper. For example, run the **`ping`** command to check connectivity. 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. 3. Check whether the SNMP link is proper. For details, refer to "4.11 SNMP Link Check". 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 3.2.1 Manually Adding a BMC. 5. (Optional) If the fault persists, contact NETAŞ technical support.

Error Type	**Operation Suggestions**
Internal SNMP error	1. Check whether the SNMP link is proper. For details, refer to "4.11 SNMP Link Check". 2. (Optional) If the fault persists, contact NETAŞ technical support.
HTTP network connection error	1. Check whether the network connection is proper. For example, run the **`ping`** command to check connectivity. 2. Try to log in to the Web portal of the BMC of the server. 3. (Optional) If the fault persists, contact NETAŞ technical support.
SSH link error	1. Check whether the network connection is proper. For example, run the **`ping`** command to check connectivity. 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. 3. Try to log in to the BMC of the server through SSH. 4. (Optional) If the fault persists, contact NETAŞ technical support.
Redfish interface execution error	In accordance with the operation type, select the corresponding handling method: ● If the ISO file fails to be mounted during the following operations, refer to "4.5 ISO File Mounting Failure". → Standard card or disk firmware upgrade → In-band RAID configuration → Stress test ● 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. → If not, upgrade the BMC version of the server and then configure the BIOS. → If yes, contact NETAŞ technical support. ● If other functions fail to be implemented, contact NETAŞ technical support.

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

Tables

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**IPv4**

- 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