



ICVS
User Manual

TABLE OF CONTENTS

Chapter 1 Login and Activation.....	7
1.1 Login.....	7
1.2 Device Activation.....	7
Chapter 2 Shortcut	9
Chapter 3 Overview	11
3.1 System Performance	11
3.1.1 View Performance	11
3.1.2 View CPU and Memory Usage	11
Chapter 4 Device	13
4.1 Node Tree.....	13
4.1.1 View Node Tree.....	13
4.1.2 Map	13
4.2 Node Status	13
4.3 Device Overview.....	14
4.3.2 Locate Device	14
4.3.3 Mute Device.....	15
4.3.4 Reboot and Shut down Device	15
4.3.5 More Operations.....	15
4.4 Device Graph of a Node.....	15
4.4.1 Device Indicator.....	15
4.4.2 HDD Slot Graph.....	16
4.4.3 Information Overview	17
Chapter 5 Log.....	25
5.1 Search Log	25
5.2 Download Log	25
5.3 Clear Log	26
Chapter 6 Maintenance	27
6.1 Version Information	27
6.2 System Upgrade	27
6.3 Disk Management	28
6.4 Password Management.....	28
6.5 Time Management.....	29
6.5.1 Synchronize Time Manually	29
6.5.2 Synchronize Time by NTP	30
6.6 Default Settings.....	31

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.
- **HDMI**™ The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Symbol Conventions

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

Symbol	Description
 NOTE	Provides additional information to emphasize or supplement important points of the main text.
 WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

Preventive and Cautionary Tips

Before connecting and operating your device, please be advised of the following tips:

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

Chapter 1 Login and Activation

1.1 Login

Purpose:

You can get access to the device via web browser. The recommended web browser includes Internet Explorer 8 to 11.

Before you start:

- Use a network cable to connect Ethernet port of your computer and the Management LAN of the device.
- Configure your computer IP address. Ensure it is in the same network segment with the Management LAN of the device (the default IP address of Management LAN is 10.254.254.254).

Step 1 Enter the device IP address (https://IP Address:2004) in web browser.

Step 2 Press Enter. Then login interface appears.

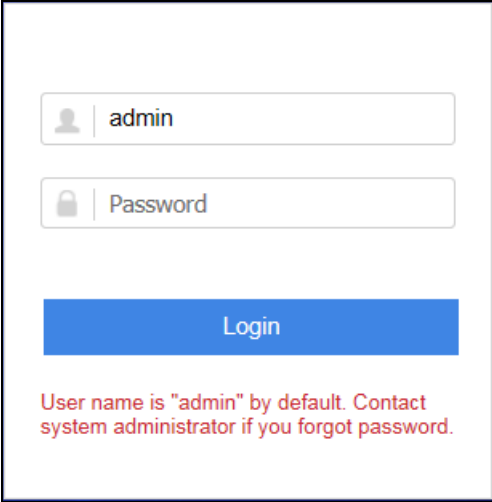
A screenshot of the login interface. It features two input fields: the first is labeled 'admin' with a user icon, and the second is labeled 'Password' with a lock icon. Below these fields is a blue 'Login' button. At the bottom, a red text message reads: 'User name is "admin" by default. Contact system administrator if you forgot password.'

Figure 1-1 Login

Step 3 Enter **User Name** and **Password**.

Step 4 Click **Login**.

1.2 Device Activation

Purpose:

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation.

Step 1 Access device via web browser.

Step 2 Enter the same password in **Create New Password** and **Confirm New Password**.

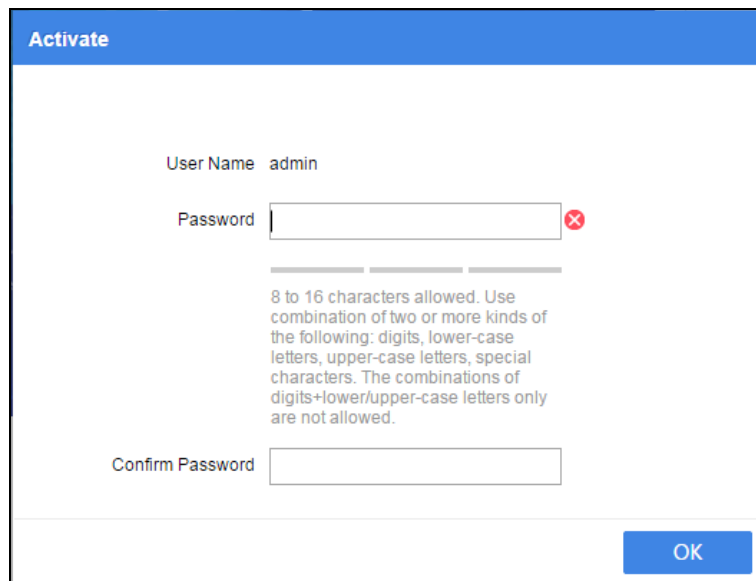


Figure 1-2 Activation

Step 3 Click **OK**.



STRONG PASSWORD RECOMMENDED—We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Chapter 2 Shortcut

The bar on top right corner of device webpage shows the shortcut buttons for quick configuration.

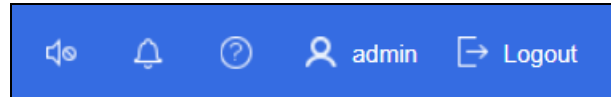


Figure 2-1 Shortcut

- : Mute alarm sound for alarm events. Only valid for current alarm events.
- : Show the exception alarm information. You can search alarm information by specifying alarm level, computing, and keyword.

Alarm Center ✕

Level Level (all) ▼

Search

Export History Alarm

Error Code	Level	Description	Details
0x502a	● Serious	Failed to detect CPU temperature. (equipment...	...
0x5024	● Serious	Failed to detect device temperature. (equipme...	...
0x1000	● Serious	Port Status Exception (Data network interface:...	...
0x5012	● Serious	Case Fan Loss (equipment:0x5000cba656136...	...
0x5012	● Serious	Case Fan Loss (equipment:0x5000cba656136...	...
0x5012	● Serious	Case Fan Loss (equipment:0x5000cba656136...	...
0x5012	● Serious	Case Fan Loss (equipment:0x5000cba656136...	...
0x5001	● Serious	Power Exception (equipment:0x5000cba6561...	...
0x5022	● Serious	Failed to detect system temperature. (equipm...	...
0x5022	● Serious	Failed to detect system temperature. (equipm...	...
0x5022	● Serious	Failed to detect system temperature. (equipm...	...

Total 11 item(s)

<<

<

1/1

>

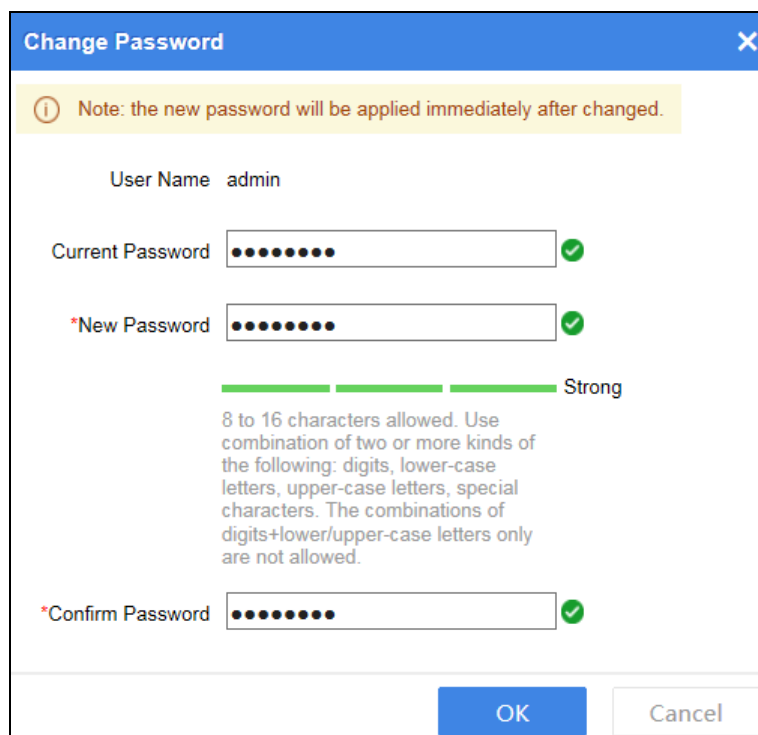
>>

page

Go

Figure 2-2 Alarm Center

- : View quick start guide, user manual, and download Command Line Tool.
- : Change admin password.



The image shows a 'Change Password' dialog box with a blue title bar and a close button (X) in the top right corner. Below the title bar is a yellow note box with an information icon and the text: 'Note: the new password will be applied immediately after changed.' The main area contains the following fields and elements:

- 'User Name' label followed by the text 'admin'.
- 'Current Password' label followed by a password input field (masked with dots) and a green checkmark icon.
- '*New Password' label followed by a password input field (masked with dots) and a green checkmark icon.
- A green progress bar below the 'New Password' field, followed by the word 'Strong'.
- Text below the progress bar: '8 to 16 characters allowed. Use combination of two or more kinds of the following: digits, lower-case letters, upper-case letters, special characters. The combinations of digits+lower/upper-case letters only are not allowed.'
- '*Confirm Password' label followed by a password input field (masked with dots) and a green checkmark icon.

At the bottom right, there are two buttons: 'OK' (blue) and 'Cancel' (grey).

Figure 2-3 Change Password

- : Log out system. At next login, you will automatically enter the page of last login.

Chapter 3 Overview

3.1 System Performance

3.1.1 View Performance

Go to **Overview** to view system performance.

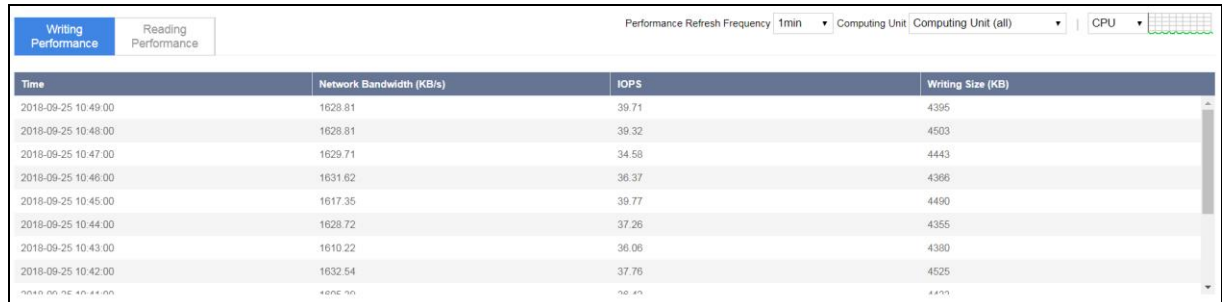


Figure 3-1 System Performance

Table 3-1 Performance Description

Status	Description
Writing/reading performance	Shows the time, network bandwidth, IOPS, and writing/reading size.

You can set the **Performance Refresh Frequency** and **Computing Unit** (only available for dual-controller device) to filter performance to show.

3.1.2 View CPU and Memory Usage

Purpose:

You can view the CPU and memory usage, number of cores, and total memory.

Step 1 Go to **Overview**.

Step 2 Select **CPU** or **Memory** to view.

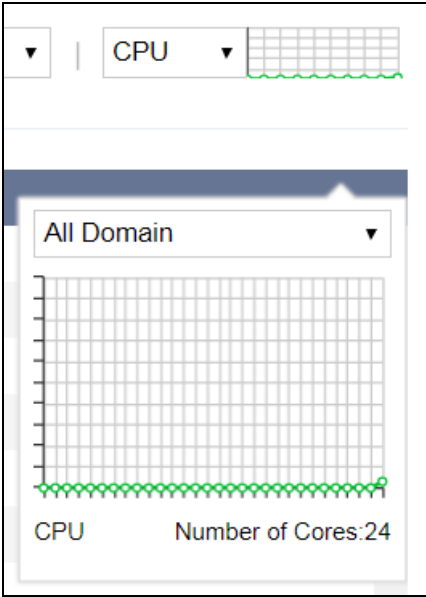


Figure 3-2 View CPU and Memory Performance

Chapter 4 Device

4.1 Node Tree

4.1.1 View Node Tree

Step 1 Go to **Device**.

Step 2 Click  of node tree dropdown list.

Step 3 Click  to show device name.

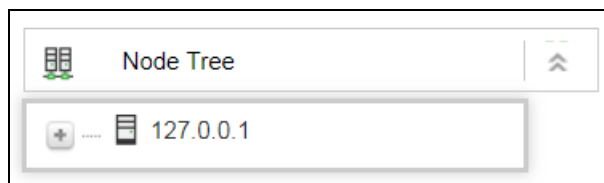


Figure 4-1 Node Tree

4.1.2 Map

Step 1 Go to **Device**.

Step 2 Click a node in node tree to refresh the topological graph of network switch node and the topological graph of specified device.

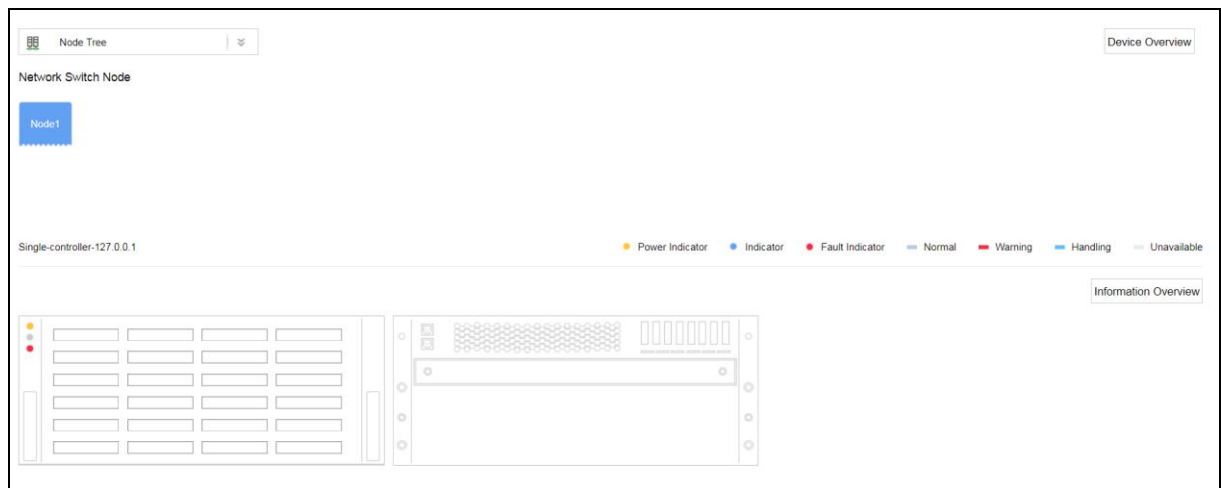


Figure 4-2 Node Mapping

4.2 Node Status

Step 1 Go to **Device**.

Step 2 Position the mouse on a node to show node status, including **Device Name**, **Device Status**, **Serial No.**, and **Product Model**.

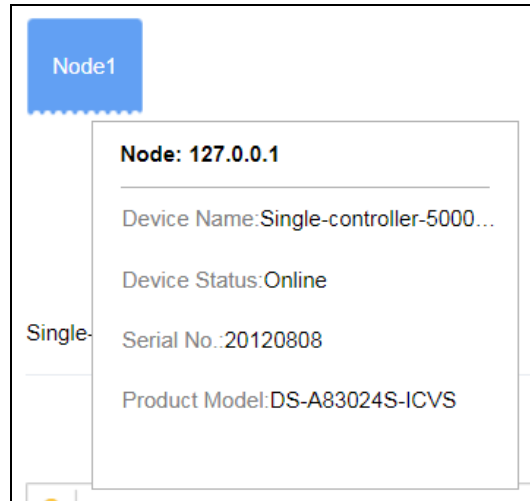


Figure 4-3 Node Status

4.3 Device Overview

Purpose:

Go to **Device** and click **Device Overview** to view device name, IP address, port, status, etc.

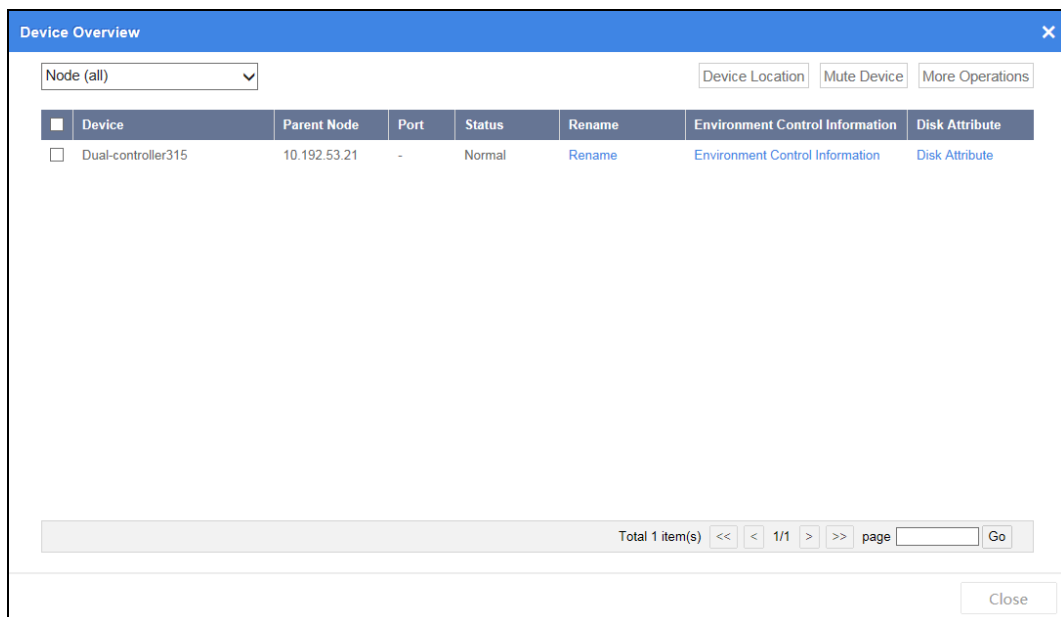


Figure 4-4 Device Overview

4.3.2 Locate Device

Purpose:

To find a device, turn on FN indicator on its front panel.

Step 1 Check the device.

Step 2 Click **Device Location**. FN indicator of the selected device will keep flashing for 10 minutes.

4.3.3 Mute Device

Purpose:

Turn off alarm sound of a device.

Step 1 Check the device.

Step 2 Click **Mute Device**. Device alarm sound will be turned off.

4.3.4 Reboot and Shut down Device

Purpose:

Restart or shut down a device.

Step 1 Check the device.

Step 2 Click **More Operations**.

Step 3 Select **Device Restart** or **Device Shutdown**.

Step 4 Enter **Password** and **Verification Code** to confirm the operation.

4.3.5 More Operations

- Rename a device .For details, refer to *Rename Device*.
- Modify device network parameters. For details, refer to *View Environment and Control Information*.
- Modify HDD property. For details, refer to *Manage Disk*.

4.4 Device Graph of a Node

The bottom half of the **Device** page shows the device graph, device name, and device indicators.

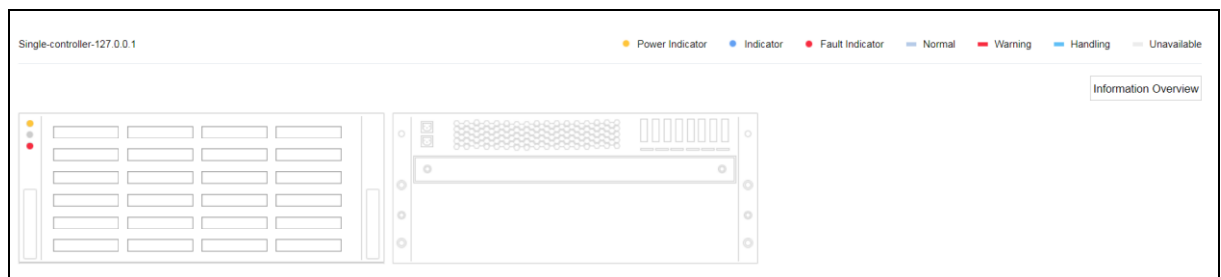


Figure 4-5 Device Graph

4.4.1 Device Indicator

Purpose:

Device indicator includes status indicator and HDD indicator.

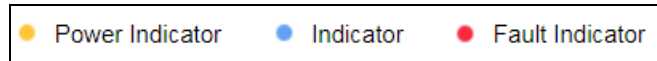


Figure 4-6 Status Indicator

Table 4-1 Indicator Description

No.	Description
Power indicator	● Yellow: Default. ● Grey: Device is powered off or shut down.
FN indicator	Blue.
Fault indicator	Red: Device is abnormal.



Figure 4-7 HDD Indicator

Table 4-2 Indicator Description

No.	Description
Normal	Blue: HDD detection is normal.
Warning	Red: HDD is not available instantly after HDD detection. Only after repair can you decide if the HDD is normal or not.
Handling	Light blue: HDD is being detected or located.
Unavailable	Grey: HDD detection fails and HDD cannot be repaired.

4.4.2 HDD Slot Graph

Purpose:

HDD slot graph shows the HDD working status.

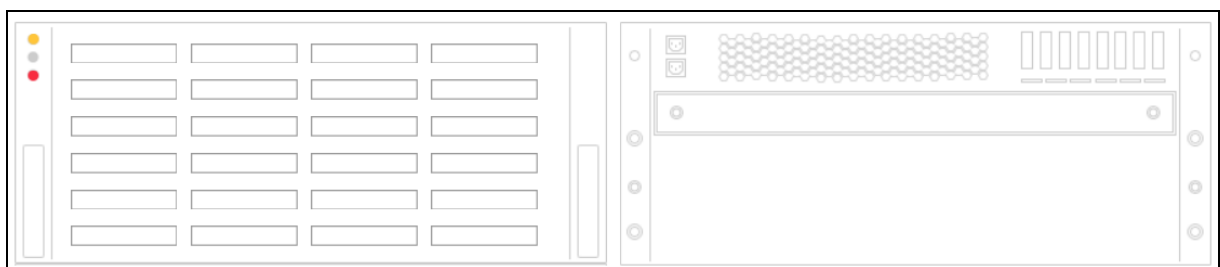


Figure 4-8 HDD Slot Graph

Step 1 Go to **Device**.

Step 2 Click an HDD slot. Then the disk information window will pop up.

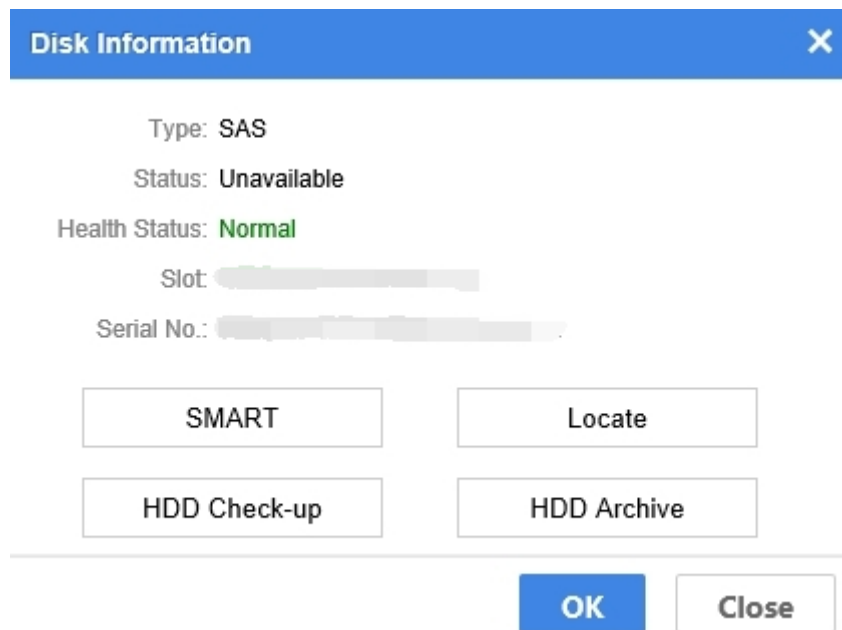


Figure 4-9 Disk Information

- **S.M.A.R.T.:** Click it to show HDD S.M.A.R.T. information.

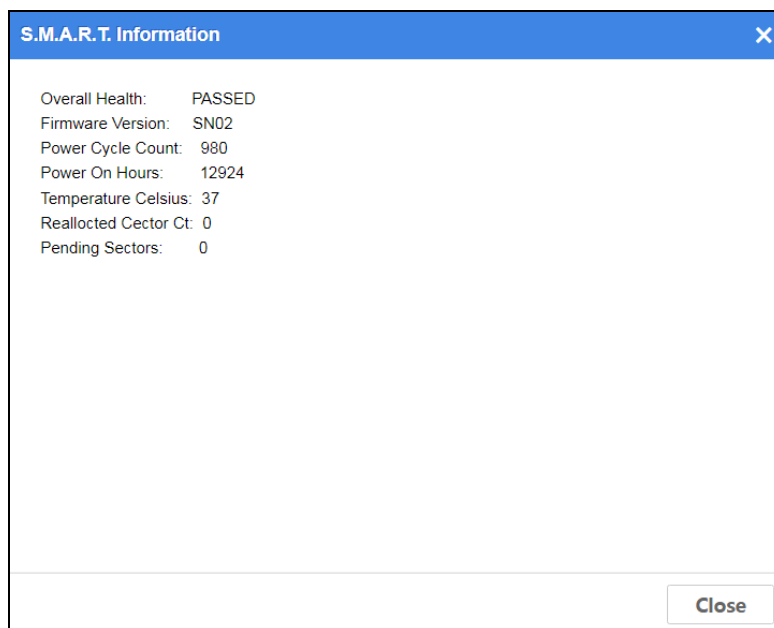


Figure 4-10 S.M.A.R.T. Information

- **Locate:** Click it to turn on FN indicator of the selected HDD. The indicator will keep flashing (default flashing time is 600 seconds).

4.4.3 Information Overview

Purpose:

View environment and control information, manage disks, mute device, etc.

View Environment and Control Information

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 View environment and control information.

- **Temperature:** Temperature of backboard, HBA card, CPU, etc.
- **Fan:** Working status of chassis fan, backboard fan, and power fan.
- **Power:** Power module working status.

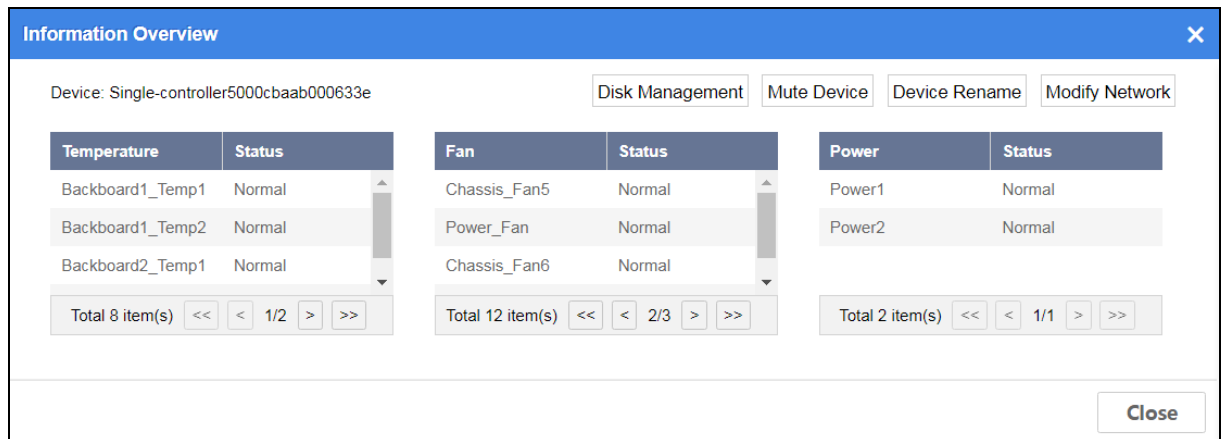


Figure 4-11 Information Overview

Manage Disk

Purpose:

You can search the information of all the HDDs in storage device.

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Disk Management**.

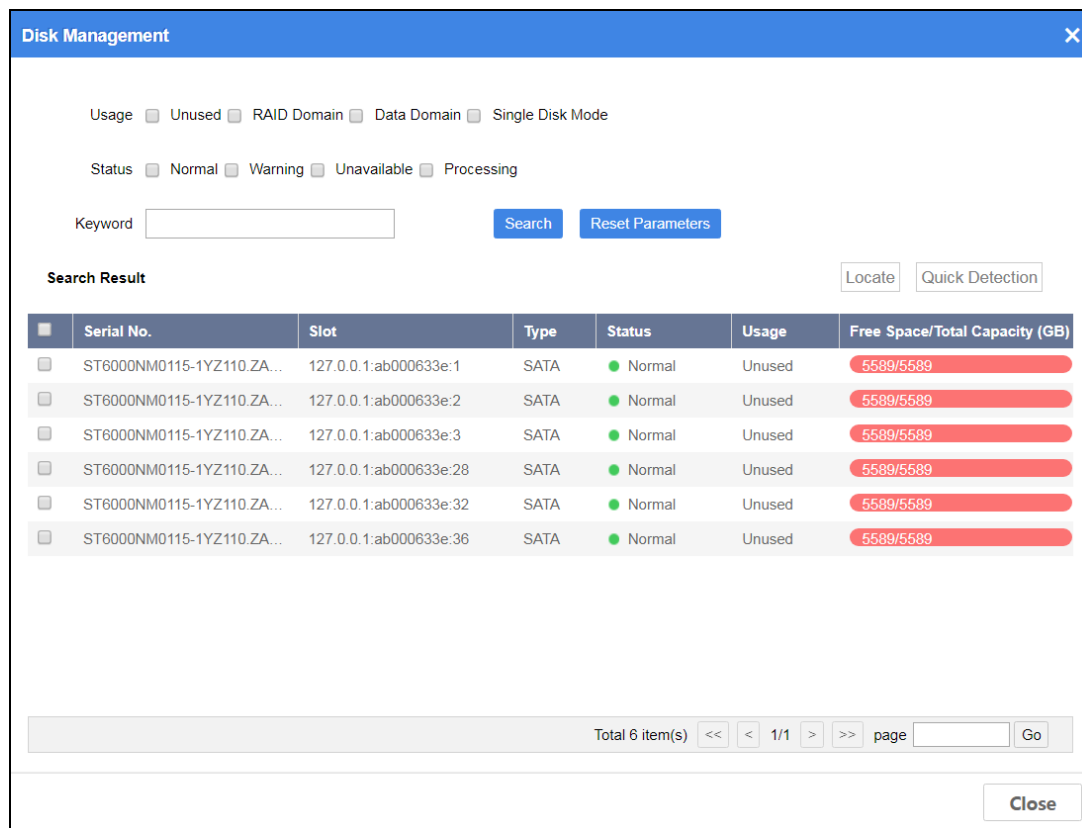


Figure 4-12 Disk Management

Step 4 Specify search conditions.

- **Usage:**
 - **Unused:** Disk not used by any RAID domain.
 - **Single Disk Mode:** Reserved.
- When disk **Usage** is set as **Unused**, **Status** description is shown as follows:
 - **Normal:** Disk is normal in all online nodes.
 - **Warning:** Disk is normal in some online nodes. Or bad sector exists in the disk.
 - **Unavailable:** Disk is abnormal in all the online nodes. Disk will be removed from resource pool.
 - **Processing:** Disk is being detected, located, repaired, moved, or maintained.

Step 5 Click **Search**.

When disk status is warning, unavailable, or processing, click the status in status column to show help. You can follow the help to recover disk.

Step 6 Optionally, to locate a disk, check the disk and click **Locate** to turn on FN indicator of the disk. FN indicator will keep flashing (default flashing time is 600 seconds).

Step 7 Optionally, to detect a disk, check the disk and click **Quick Detection**. Detection progress will be shown in **Status** column.

Mute Device

Purpose:

When device is abnormal and sending alarm sound, you can mute it.

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Mute Device**.

Rename Device

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Device Rename**.

Step 4 Enter **New Name** and click **OK**.



Device name must be unique in the domain. Valid name contains 1 to 16 characters and only digits, lowercase, and uppercase are allowed.

Modify Network

You can view port name, status, speed, IP address, subnet mask, gateway IP, and Jumbo frame size, bound ports, and modify network parameters.

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Modify Network**.

Modify Network

Create Bond

	Port Name	Status	Speed	IP Address	Subnet Mask	Gateway IP	Jumbo Frame Size	Set Port
☐	Network interfac...	Connect	1000	0.0.0.0	0.0.0.0		1500	Settings
☐	Network interfac...	Connect	1000	0.0.0.0	0.0.0.0		1500	Settings

Total 2 item(s) << < 1/1 > >> page Go

Delete Bond

	Port Name	Status	Speed	IP Address	Subnet Mask	Gateway IP	Jumbo Frame Size	Set Port	Attribute
☐	Bond network in...	Connect	4000Mb/s	10.192.52.8	255.255.255.0	10.192.52.254	1500	Settings	Attribute

Total 1 item(s) << < 1/1 > >> page Go

Close

Figure 4-13 Modify Network

Set Bound Port

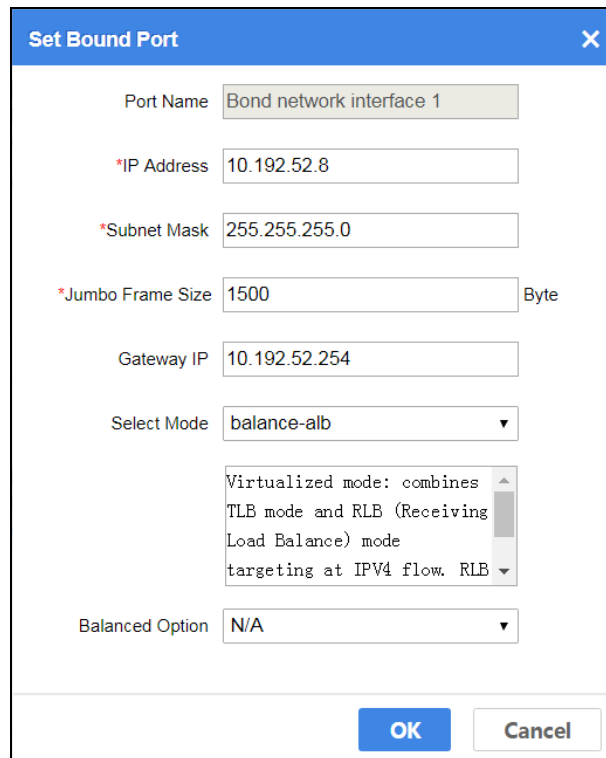
Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Modify Network**.

Step 4 Click **Settings** of a bound port.

- **Port Name**: Not editable.
- **Jumbo Frame Size**: Default value is 1500. Default value is recommended.
- **Select Mode**: Seven bound mode is selectable. Default mode is balance-alb.



The 'Set Bound Port' dialog box contains the following fields and controls:

- Port Name:** Bond network interface 1
- *IP Address:** 10.192.52.8
- *Subnet Mask:** 255.255.255.0
- *Jumbo Frame Size:** 1500 Byte
- Gateway IP:** 10.192.52.254
- Select Mode:** balance-alb (dropdown menu)
- Virtualized mode:** combines TLB mode and RLB (Receiving Load Balance) mode targeting at IPV4 flow. RLB (text area)
- Balanced Option:** N/A (dropdown menu)
- Buttons:** OK and Cancel

Figure 4-14 Set Bound Port



- Management port does not support port binding.
- Connect all bound ports to network.

View Bound Port Attribute

Purpose:

View bound port attribute, including port name, port attribute, binding mode, etc.

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Modify Network**.

Step 4 Click **Attribute** of a bound port.

Bound Port Attribute

Port Name

Bond network interface 1

Port Attribute

Not Configured

Binding Mode

balance-alb

Port Name	Status	Speed
Network interfac...	Connect	1000Mb/s
Network interfac...	Connect	1000Mb/s
Network interfac...	Connect	1000Mb/s
Network interfac...	Connect	1000Mb/s

Close

Figure 4-15 Bound Port Attribute

Delete Bound Port

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Modify Network**.

Step 4 Check bound port to delete.

Step 5 Click **Delete Bond**.

Step 6 Click **OK** in message box to confirm the operation.



NOTE

Unbounded ports will be listed in top half of the page.

Set Port Parameters

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Modify Network**.

Step 4 Click **Set** of unbounded port to configure its network parameters.

- **Port Name:** Not editable.
- **Jumbo Frame Size:** Default value is 1500. Default value is recommended.

Create Bond

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Modify Network**.

Step 4 Select ports to bind and click **Create Bond**.

- **Select Mode:** **Rotating Mode**, **Active-standby Mode**, **XOR Mode**, **Broadcasting Mode**, **802.3ad Mode**, **TLB Mode**, and **Virtualized Mode** are selectable.
- **Balanced Option:** **L2**, **L3**, and **L4** are selectable. **L2** is default one and recommended one.



NOTE

- Bound port will be listed in lower half of the page.
- IP address of bound port is the same with the IP address of the first port.

Chapter 5 Log

5.1 Search Log

Step 1 Go to **Log**.

Step 2 Specify search conditions.

Step 3 Click **Search**.

Computing Unit	Level	Time	Description
10.192.52.8	Normal	2018-09-29 11:14:42	Admin logged in (IP:10.25.220.107)
10.192.52.8	Normal	2018-09-29 10:33:22	Admin logged in (IP:10.192.45.159)
10.192.52.8	Normal	2018-09-29 10:02:31	Admin logged in (IP:10.192.44.129)
10.192.52.8	Normal	2018-09-29 09:57:54	The maintenance log is downloaded.
10.192.52.8	Normal	2018-09-29 09:55:34	Admin logged in (IP:10.192.36.203)
10.192.52.8	Normal	2018-09-29 09:49:51	The maintenance log is downloaded.
10.192.52.8	Normal	2018-09-29 09:49:19	The maintenance log is downloaded.
10.192.52.8	Normal	2018-09-29 09:40:51	Admin logged in (IP:10.8.99.23)

Figure 5-1 Log

5.2 Download Log

Before you start:

Enable web browser file download permission by going to **Options > Security > Internet > Custom Level Download**.

Step 1 Go to **Log**.

Step 2 Click **Download Log**.

Step 3 Select log type in **Downloads** drop-down list.

Step 4 Check the computing unit to download.

Step 5 Click **Download**.

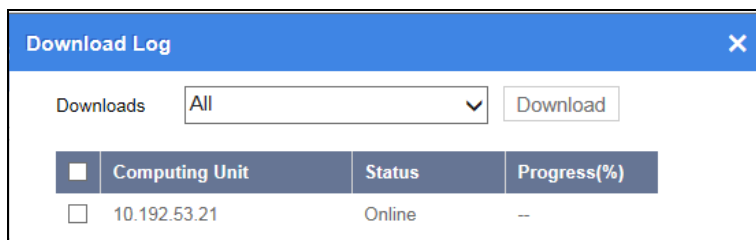


Figure 5-2 Download Log

5.3 Clear Log

Step 1 Go to **Log**.

Step 2 Click **More Operations** and select **Clear Log**.

Step 3 Enter **Password** and **Verification Code**.

Step 4 Click **OK** to confirm the operation.



NOTE

The operation will clear all logs in device. You are recommended to back up logs before clearing.

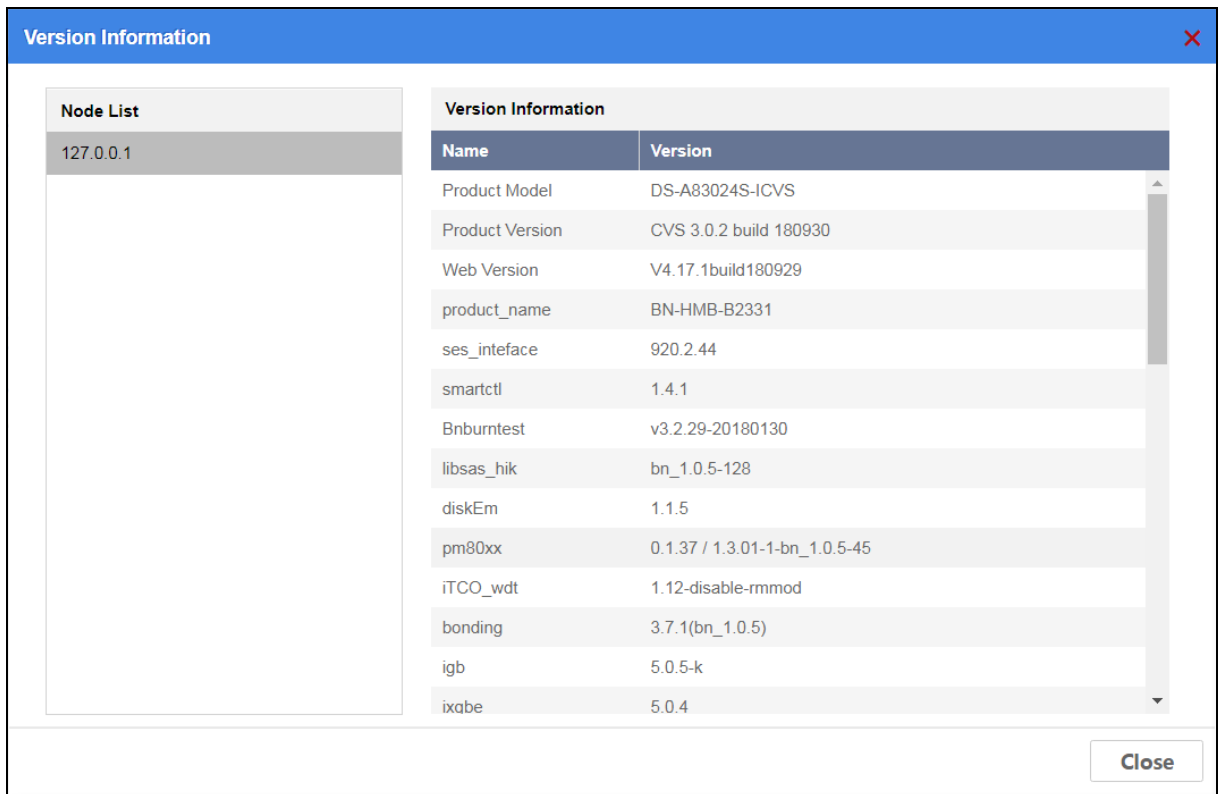
Chapter 6 Maintenance

6.1 Version Information

Step 1 Go to **Maintenance**.

Step 2 Click **Version Information**.

Step 3 Select a node in **Node List**.



Version Information	
Name	Version
Product Model	DS-A83024S-ICVS
Product Version	CVS 3.0.2 build 180930
Web Version	V4.17.1build180929
product_name	BN-HMB-B2331
ses_interface	920.2.44
smartctl	1.4.1
Bnburntest	v3.2.29-20180130
libsas_hik	bn_1.0.5-128
diskEm	1.1.5
pm80xx	0.1.37 / 1.3.01-1-bn_1.0.5-45
iTCO_wdt	1.12-disable-rmmod
bonding	3.7.1(bn_1.0.5)
igb	5.0.5-k
ixabe	5.0.4

Figure 6-1 Version Information

6.2 System Upgrade

Step 1 Go to **Maintenance**.

Step 2 Click **Upgrade**.

Step 3 Click **Browse** to select upgrade file.

Step 4 Select the computing unit to upgrade.

Step 5 Click **Upgrade**.

Step 6 Reboot the computing unit after upgrade finishes.

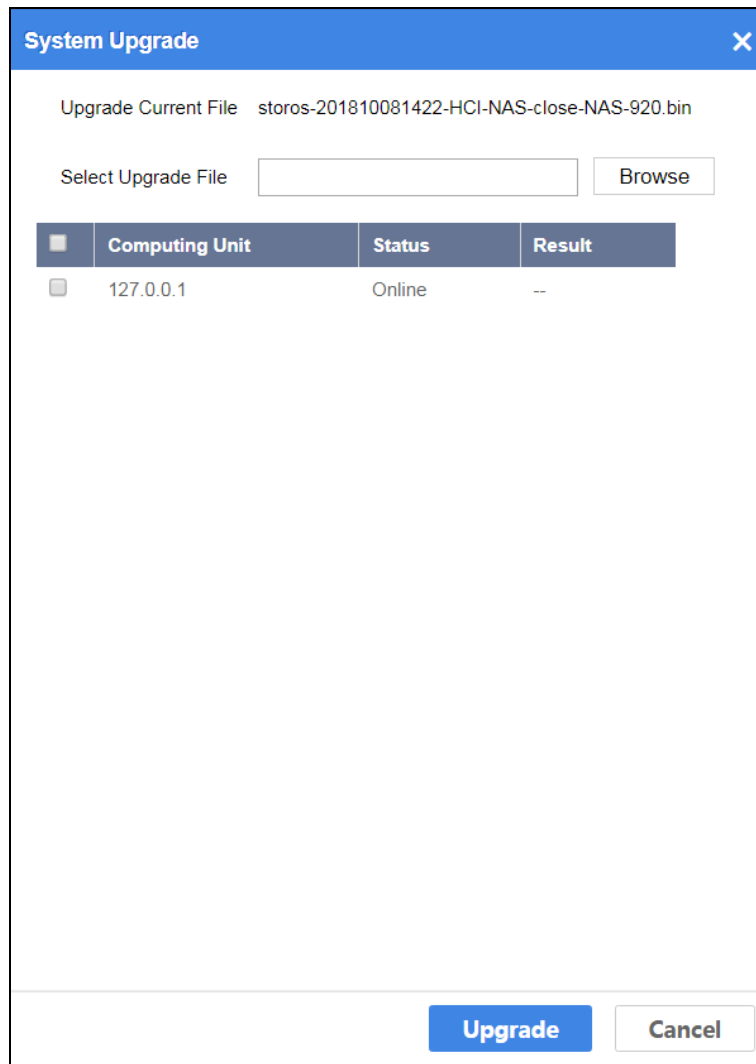


Figure 6-2 System Upgrade

6.3 Disk Management

For details, refer to *Manage Disk*.

6.4 Password Management

Step 1 Go to **Maintenance**.

Step 2 Click **Password Management**.

Step 3 Enter **Current Password**.

Step 4 Enter the same password in **New Password** and **Confirm Password**.

**WARNING**

STRONG PASSWORD RECOMMENDED—We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 5 Click **OK**.

Figure 6-3 Change Password

6.5 Time Management

6.5.1 Synchronize Time Manually

Step 1 Go to **Maintenance**.

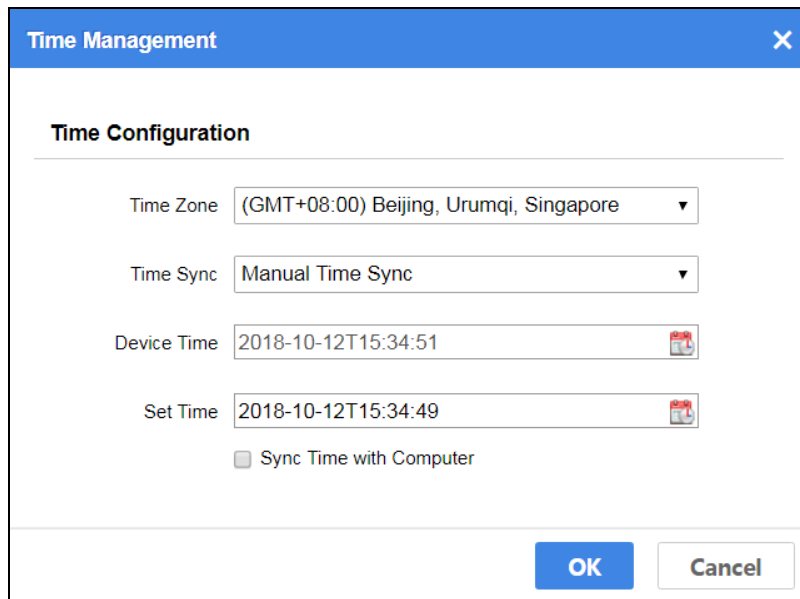
Step 2 Click **Time Management**.

Step 3 Select **Time Zone**.

Step 4 Select **Time Sync** as **Manual Time Sync**.

Step 5 Optionally, you can set time or check **Sync Time with Computer**.

Step 6 Click **OK**.



The dialog box titled "Time Management" contains a "Time Configuration" section. It features four input fields: "Time Zone" set to "(GMT+08:00) Beijing, Urumqi, Singapore", "Time Sync" set to "Manual Time Sync", "Device Time" showing "2018-10-12T15:34:51", and "Set Time" showing "2018-10-12T15:34:49". Below these fields is an unchecked checkbox labeled "Sync Time with Computer". At the bottom right are "OK" and "Cancel" buttons.

Figure 6-4 Manual Time Sync

6.5.2 Synchronize Time by NTP

Step 1 Go to **Maintenance**.

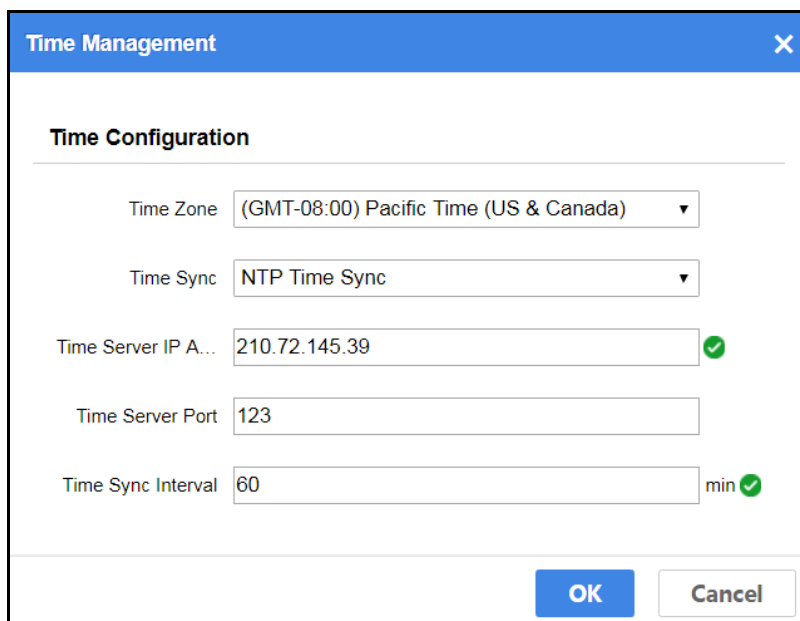
Step 2 Click **Time Management**.

Step 3 Select **Time Zone**.

Step 4 Select **Time Sync** as **NTP Time Sync**.

Step 5 Enter **Time Server IP Address**, **Time Server Port**, and **Time Sync Interval**.

Step 6 Click **OK**.



The dialog box titled "Time Management" contains a "Time Configuration" section. It features five input fields: "Time Zone" set to "(GMT-08:00) Pacific Time (US & Canada)", "Time Sync" set to "NTP Time Sync", "Time Server IP A..." set to "210.72.145.39" with a green checkmark, "Time Server Port" set to "123", and "Time Sync Interval" set to "60" with "min" and a green checkmark. At the bottom right are "OK" and "Cancel" buttons.

Figure 6-5 NTP Time Sync

6.6 Default Settings

Purpose:

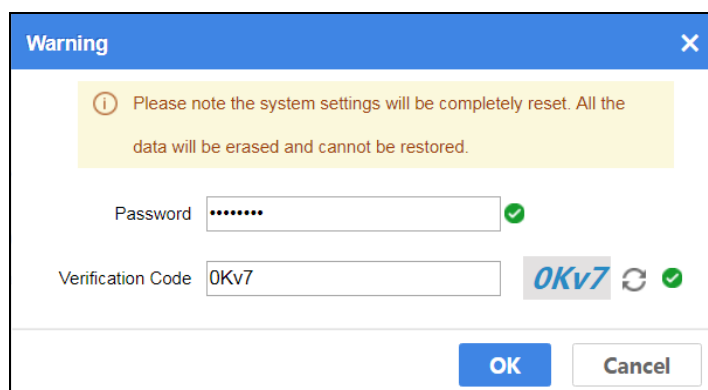
Restore all parameters to default settings.

Step 1 Go to **Maintenance**.

Step 2 Click **All system settings reset**.

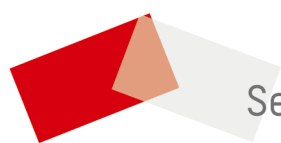
Step 3 Enter admin **Password** and **Verification Code**.

Step 4 Click **OK**.



A warning dialog box titled "Warning" with a close button (X) in the top right corner. The dialog contains a yellow warning box with an information icon (i) and the text: "Please note the system settings will be completely reset. All the data will be erased and cannot be restored." Below this, there are two input fields: "Password" with a masked password "*****" and a green checkmark icon to its right, and "Verification Code" with the code "0Kv7" and a green checkmark icon to its right. To the right of the verification code input, there is a blue button labeled "0Kv7" with a refresh icon and a green checkmark icon. At the bottom right of the dialog, there are two buttons: "OK" (blue) and "Cancel" (white).

Figure 6-6 Restore Default Settings



See Far, Go Further