# IPSAN Series
# Network Storage System
# Quick Guide

V1.07

# Contents


1 Introduction ..... 1

2 Hardware Installation ..... 2

2.1 Tool Reference ..... 2

2.2 Environment Requirements ..... 2

2.3 Installation Steps ..... 3

2.4 Cable Connection and Check ..... 6

3 Software Configuration ..... 12

3.1 Basic Concepts ..... 12

3.2 Configuration Workflow ..... 12

3.3 Device Login via Management Port ..... 13

3.4 Set the Service Port IP ..... 17

3.5 Configure Failover (For Dual Controller Device) ..... 17

3.6 Create a RAID Group/RAID LUN ..... 19

3.7 Create Logical Resources ..... 20

3.8 Create a Target and Add an Initiator ..... 21

3.9 Assign SAN Resources ..... 24

3.10 Configure the Initiator (with Windows Client as an Example) ..... 25

3.11 View Disks Assigned (with Windows 10 as an Example) ..... 29

4 (Optional) Video Management Server Configuration ..... 30

4.1 Product Introduction ..... 30

4.2 Basic Concepts ..... 31

4.3 Configuration Workflow ..... 31

4.4 Log in to the VMS' Web Client through Device IP Address ..... 32

4.5 Set the Service Port IP ..... 32

4.6 (Optional) Configure Primary Server IP Address ..... 33

4.7 Create and Format RAIDs ..... 34

4.8 Add IPCs and Recording Schedule (Primary) ..... 36

4.9 Recording Status and Playback (Primary) ..... 37

5 Appendix Disk Installation and Removal for the 60 Slots Products····· 38
Disclaimer and Safety Warnings····· 44

# 1 Introduction

IPSAN Series storage hosts include eleven types of products: single controller with 12 disk slots, single controller with 16 disk slots, single controller with 24 disk slots, single controller with 36 disk slots, single controller with 48 disk slots, single controller with 60 disk slots, single controller with 86 disk slots, single controller with 116 disk slots, dual controller with 24 disk slots, dual controller with 48 disk slots, and dual controller with 60 disk slots.

The storage product supports six types of DEUs: single controller DEUs with 24 disk slots, single controller DEUs with 48 disk slots, single controller DEUs with 60 disk slots, dual controller DEUs with 24 disk slots, dual controller DEUs with 48 disk slots, and dual controller DEUs with 60 disk slots.

For details about the supported DEUs, see the table below.

Table 1-1 Different products support different DEUs

| SCU disk slots | DEU disk slots |
|---|---|
| 12 (single controller) | 24 (single controller) |
| 16 (single controller) | |
| 24 (single controller) | |
| 36 (single controller) | |
| 48 (single controller) | 24 and 48 (both single controller) |
| 60 (single controller) | 60 (single controller) |
| 24 (dual controller) | 24 (dual controller) |
| 48 (dual controller) | 48 (dual controller) |
| 60 (dual controller) | 60 (dual controller) |
| 86 (single controller) | 24 and 48 (both single controller) |
| 116 (single controller) | |

**NOTE!**

- SCU (Storage Control Unit)
- DEU (Disk Expansion Unit)
- This manual takes the single controller with 24 disk slots for example. For more details, please see the latest product datasheet.
- The following illustrations are only for your reference. And may be different from the actual product and the actual software UI.

# 2 Hardware Installation

## 2.1 Tool Reference




## 2.2 Environment Requirements

| Temperature | Requirement |
|---|---|
| Operating temperature | 0°C~40°C<br>Recommended: 10°C~35°C |
| Storage temperature | Excluding battery modules: –20°C~+60°C<br>Including battery modules: –15°C~+40°C (storage within 1 month)<br>10°C~35°C (storage over 1 month) |
| **Humidity** | **Requirement** |
| Operating humidity | 20% to 80% (non-condensing) |
| Storage humidity | 10% to 90% (non-condensing) |

**NOTE!**

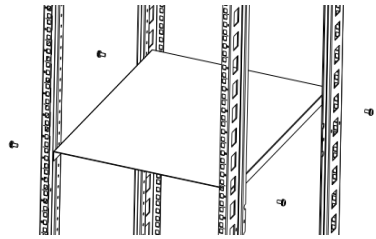
Corrosive gases and dust can cause damage to hard disks. For detailed requirements about the equipment room environment, please refer to Checking the Installation Environment section in User Manual.

## 2.3 Installation Steps

### 1 Other disk slots except for the 86 slots products

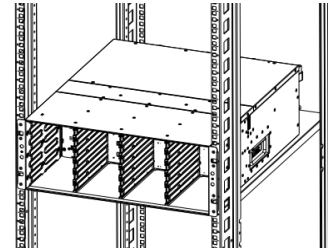
1. [Installing the tray on the cabinet](Optional)

   Align the four screw holes at the front and rear of the tray with the holes on the cabinet mounting rails.First tighten the thumb screws,then tighten the falt-head screws.



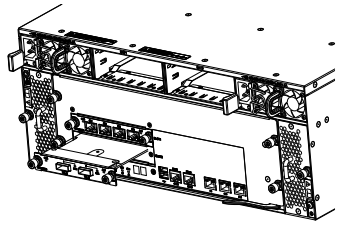
2. [Installing the chassis on the guide rail]

   Slowly push the main cabinet along the guide rail until the suspension loop is onto the front mounting hole, and use screws to secure the suspension loop to the front mounting bar.



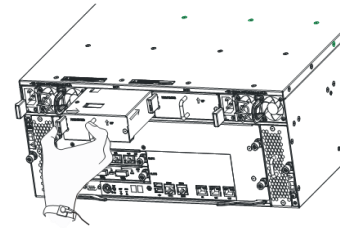
3. [Installing the expansion module]

   Face silkscreen of the expansion board forward, hold the middle of the expansion board, slowly insert the expansion board, and tighten the captive screws.



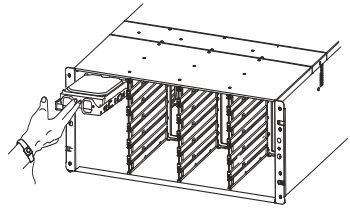
4. [Installing the battery module]

   Determine the direction of the battery case, insert the battery case slowly along the guide rail, until the lock spring piece is buckled.



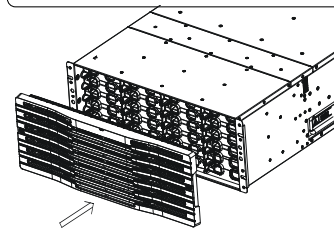
5. [Installing a disk]

   Hold the middle of the disk, but do not hold the handle bar. Slowly push the disk into the slot, until a clatter sound is heard, indicating that the disk is installed in position.



6. [Installing the front panels]

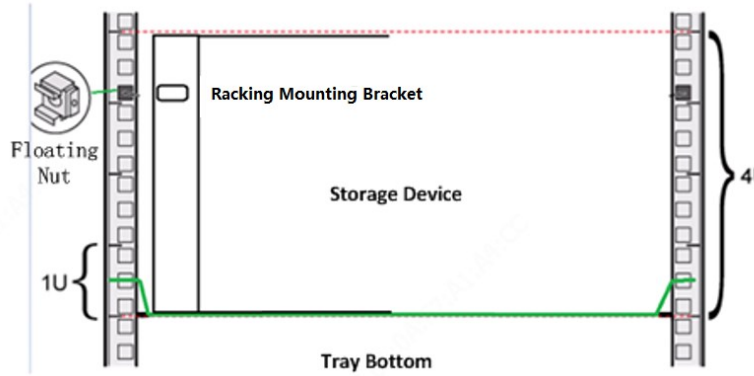
   Install the front panels of the storage controller and DEU, as shown in the following figure (DEU is used as an example).



**WARNING!**

- When installing a device, ensure that the device and the mark line on the square hole strip on the cabinet are properly aligned in 1U. Otherwise, you are not allowed to install the rack-mounting ear screws.

Figure 2-1 Correct installation




- If the rack-mounting ear screws are forcibly installed without the aligning procedure, a gap exists between the device and the tray and the device is hanging over the square hole strip. Consequently, the device is unstable, thereby affecting stability of the hard disks. If the hard disks are running for a long time in such situation, many problems, such as a high read/write error rate and a high damage rate, will arise.
- Besides, the depth of the equipment cabinet is generally greater than 0.8m, and it shall be selected according to different equipment.

**WARNING!**

- Incorrect installation manner:

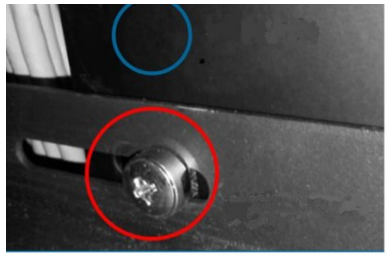


Figure 1

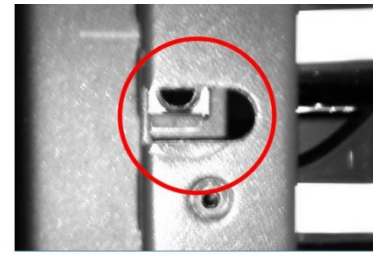


Figure 2

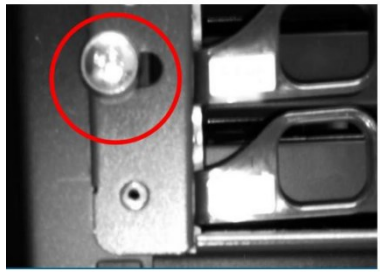


Figure 3

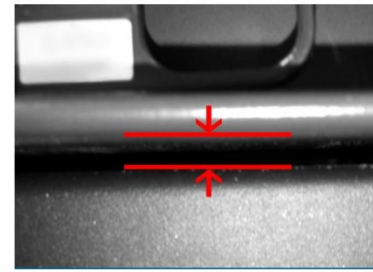


Figure 4

Figure 1: The tray is installed half-U downward.

Figure 2: The rack-mounting ear is not aligned properly.

Figure 3: The device is not aligned in one U and is hanging over the rack-mounting ear after the screws are installed.

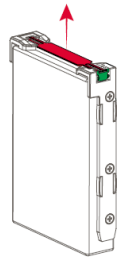
Figure 4: A gap exists between the device and the tray.

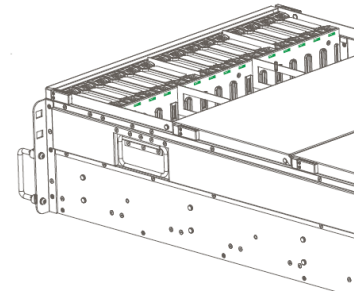
## 2 86 slots products

(1)Disk assembly and disassembly:

The steps to install the disk are as follows:

①Lift the handle in the direction of the arrow to release the locking structure of the buckle.
②Remove the hard drive.
③When installing the hard drive, the buckle should face the back of the device.
④Natural sinking until you hear a "click" sound or the hard drive is level with the slide rail to complete the hard drive installation.





(2)Device assembly and disassembly:

Please refer to the device installation instructions on the top cover of the chassis.

**NOTE!**

- Before extending the rack to the installation position, please read the installation instructions.
- Do not apply any load on the slide rail installation equipment in the installation position.

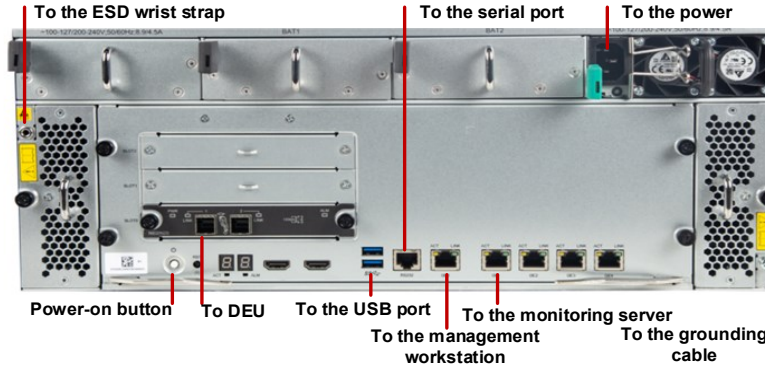
Please strictly follow the above precautions, otherwise the slide rail may pose a stability hazard and the rack may tip over, causing serious personal injury.

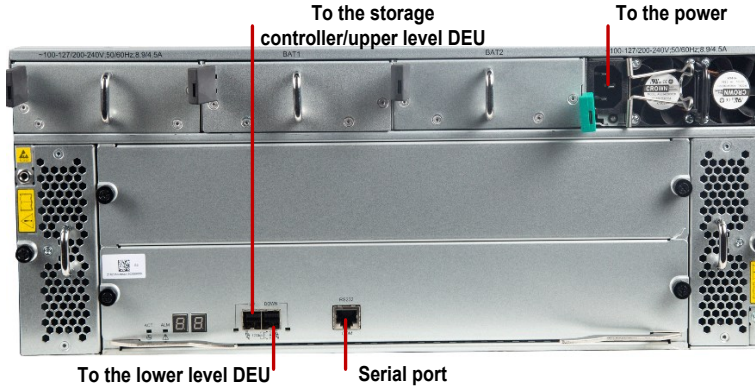
## 2.4 Cable Connection and Check

### 1 Cable Connection

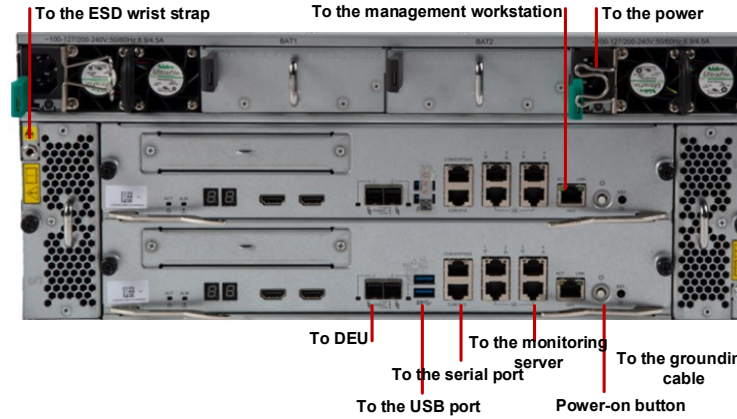
(1) Connect cables for the storage controller and DEU, as shown in the following figure.
(2) Power on the storage controller and DEU.
(3) Switch on the storage controller.

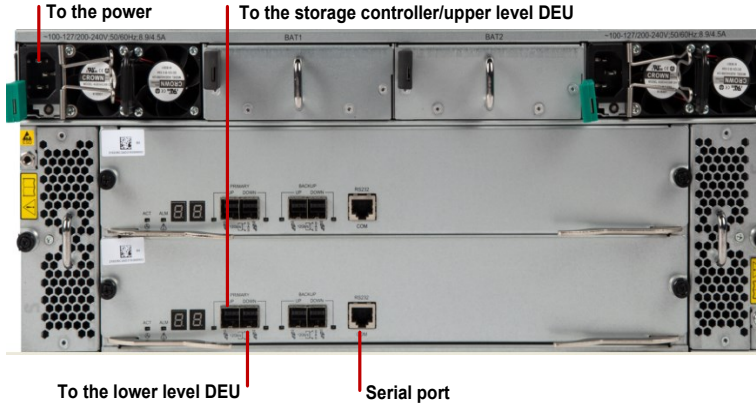
Single controller:




Dual controller:




## 2 Check

(1) Check the rear panel LED of the storage controller and DEU.

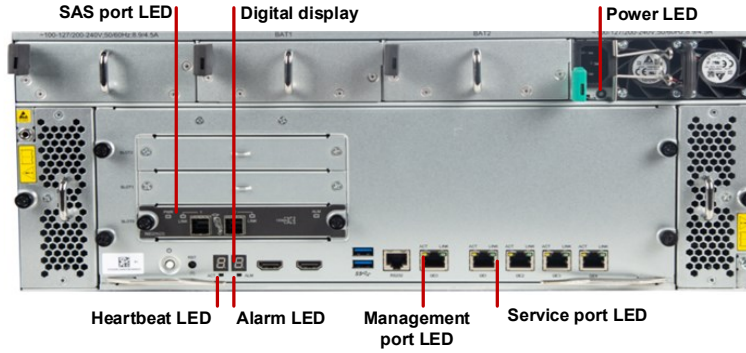
- Management port LED: Green on and yellow on
- Service port LED: Green or yellow on
- Alarm LED: Off; other LEDs: Green

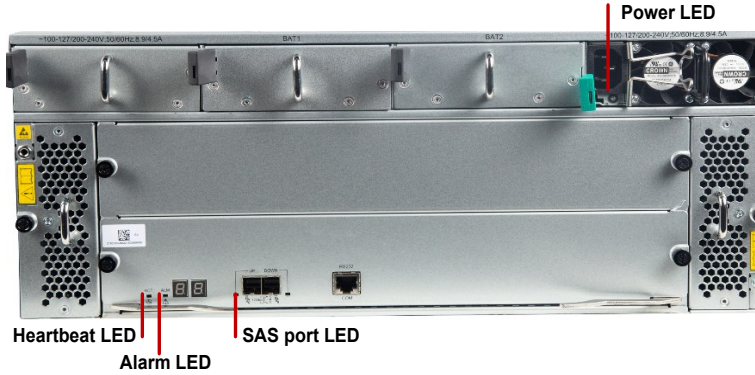
(2) Check the front panel LED of the storage controller and DEU (the illustration is omitted).

- Normally, the front panel LED is green.

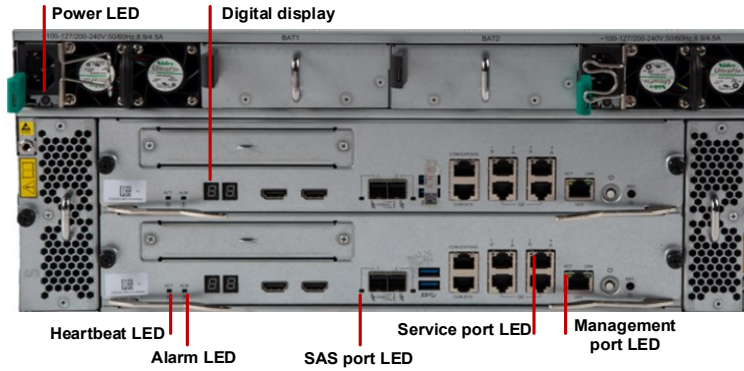
(3) Before using the device, it is necessary to remove the film from the silver sheet on both the chassis and the front panel.

Single controller:



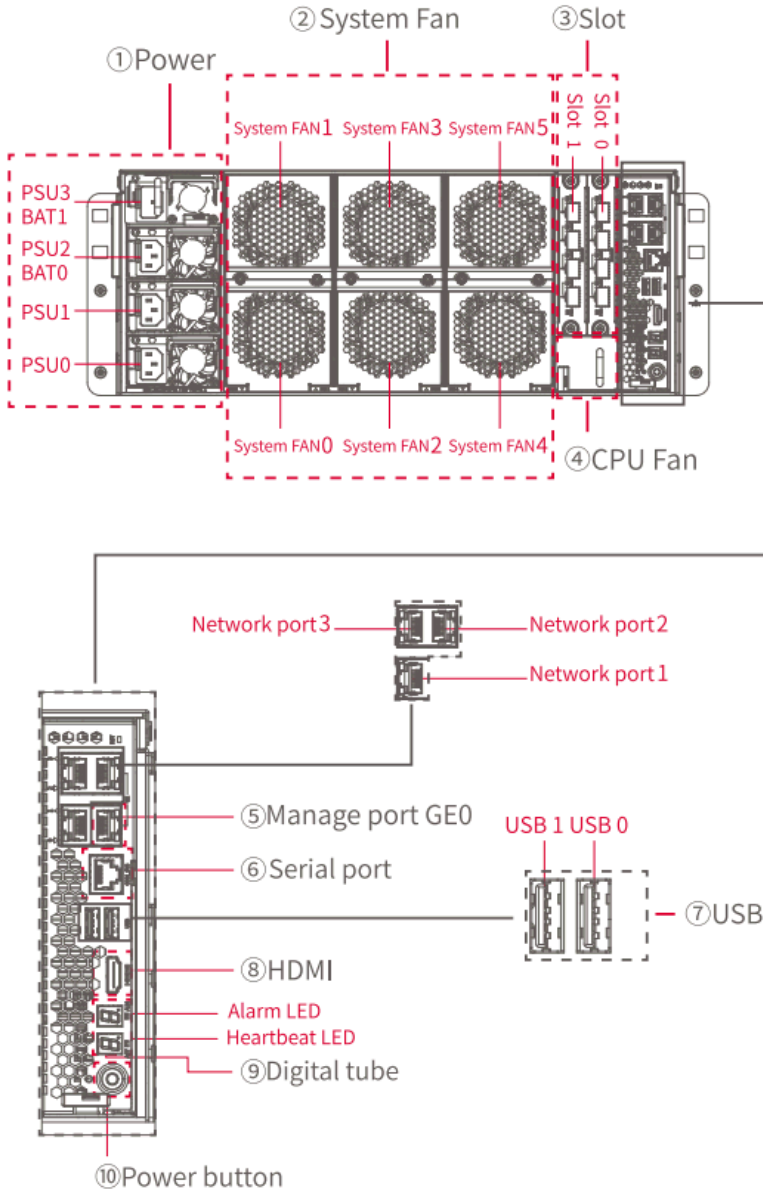




Dual controller:


Power LED
Digital display
Heartbeat LED
Alarm LED
SAS port LED
Service port LED
Management port LED


Power LED
Heartbeat LED
Alarm LED
SAS port LED

86 slots products:



# 3 Software Configuration

## 3.1 Basic Concepts

| Basic Concept | Description |
|---|---|
| Management workstation | Indicates the PC where the console is installed. |
| WEB | WEB client |
| VMS | VMS (Video Management Server) |
| RAID Group | Indicates a logical entity consists of multiple physical hard disks.<br>The logical entity is used to form the RAID of a specified level and provide physical resources for RAID Logical Unit Numbers (LUNs). |
| RAID LUN | Compared with a LUN, a RAID LUN indicates a smaller logical entity created in a RAID group.<br>After a RAID LUN is created in a RAID group, the RAID LUN directly inherits the RAID level of the RAID group. |
| Logical resource | Indicates a logical entity that is created on a RAID LUN for direct access from a client.<br>A client can access a logical resource after it is created on basis of a RAID LUN and assigned to a target. |
| Initiator | Indicates an entity that initiates an Internet Small Computer System Port (iSCSI) request. |
| Target | Indicates an entity that responds to an iSCSI request. An initiator can initiate a request to a target only after it is associated with the target. |
| Management port | 1000 Mbit/s port for device configuration and management. |
| Service port | 1000 Mbit/s port for data transfer. |

## 3.2 Configuration Workflow

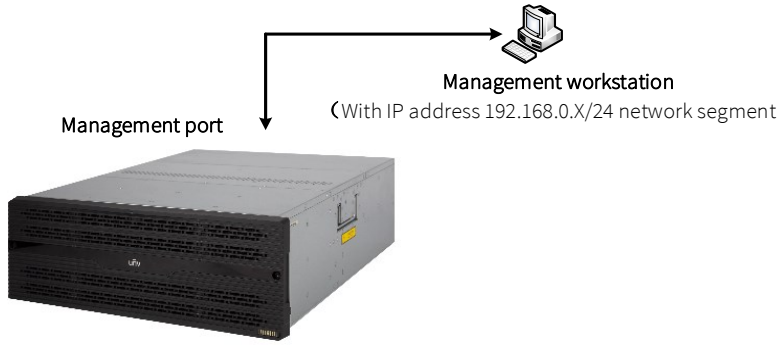
To complete most basic configurations, perform the following operations on the web client:

1. Log in to the device through the management port.
2. Set the service port IP.
3. Configure failover (for dual controller device).
4. Create a RAID group/RAID LUN.
5. Create logical resources.
6. Create a target and add an initiator.
7. Assign Storage Area Network (SAN) resources.
8. Configure the initiator (with Windows client as an example).
9. View disks assigned (with Windows 10 as an example).

## 3.3 Device Login via Management Port

1. Open your browser, enter the default storage management port IP address (eg. http://192.168.0.1) in the address bar to go to the WEB client.

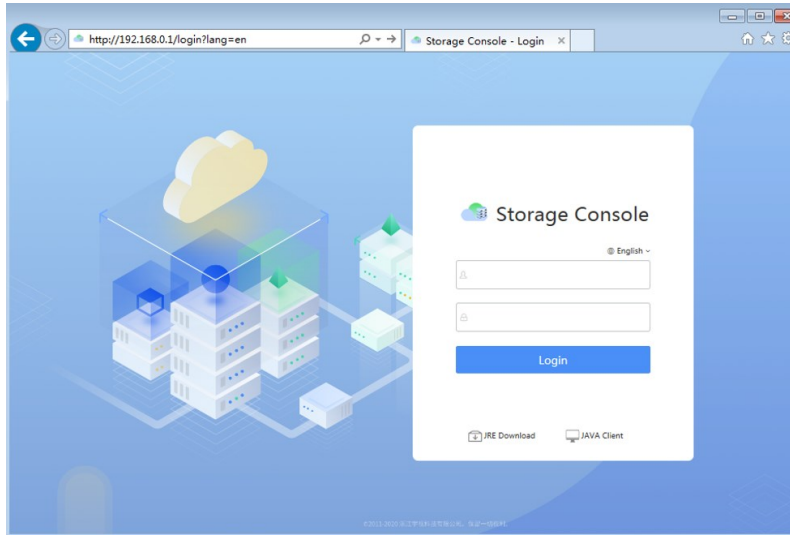
Figure 3-1 Login via Management Port



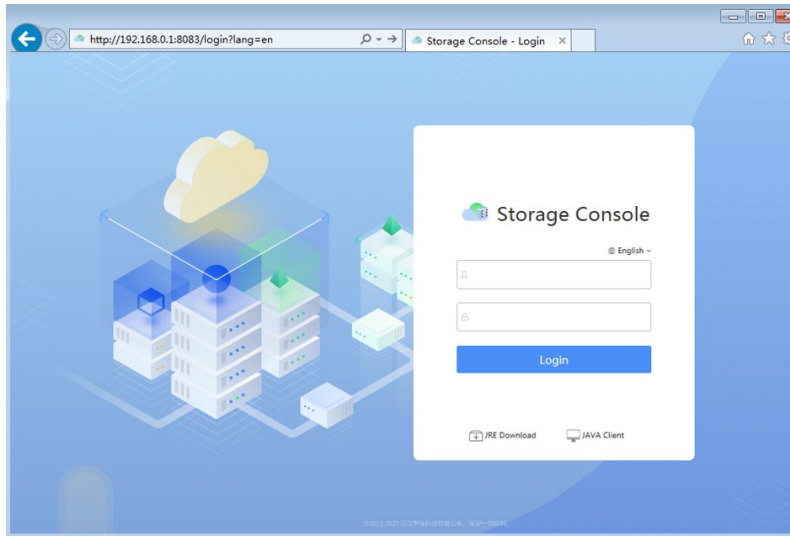

**NOTE!**

- Compatible browser versions: IE11, Chrome 60 or higher, Firefox 60 or higher, Edge 79 or higher.
- For a dual controller device, the default management port IP address for lower controller is http://192.168.0.1, for upper controller is http://192.168.0.2.

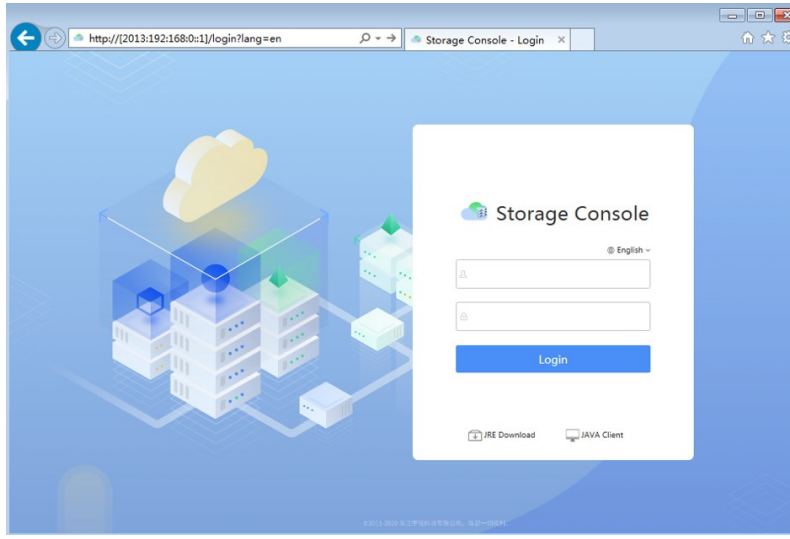
(1) If no VMS is installed, enter http://*Management port IP* in the address bar.



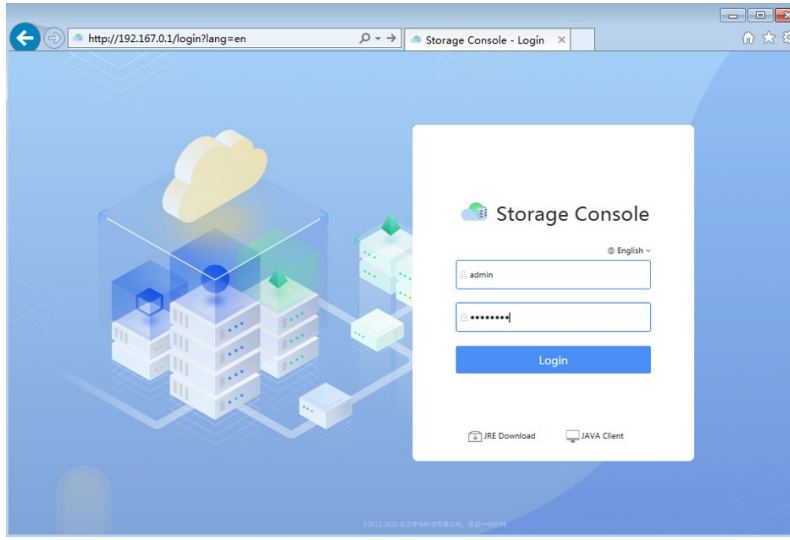

(2) If VMS is installed, enter http://*Management port IP*:8083 in the address bar. You will be directed to the VMS platform if you enter http://*Management port IP*.




(3) If the IP address is IPv6, enter http://[*IPv6*] in the address bar.




2. Enter the default username and password (admin/123456) to log in to the console.




3. After your first login, you will be prompted to change the password for the admin and root users.

Figure 3-2 Change User Password

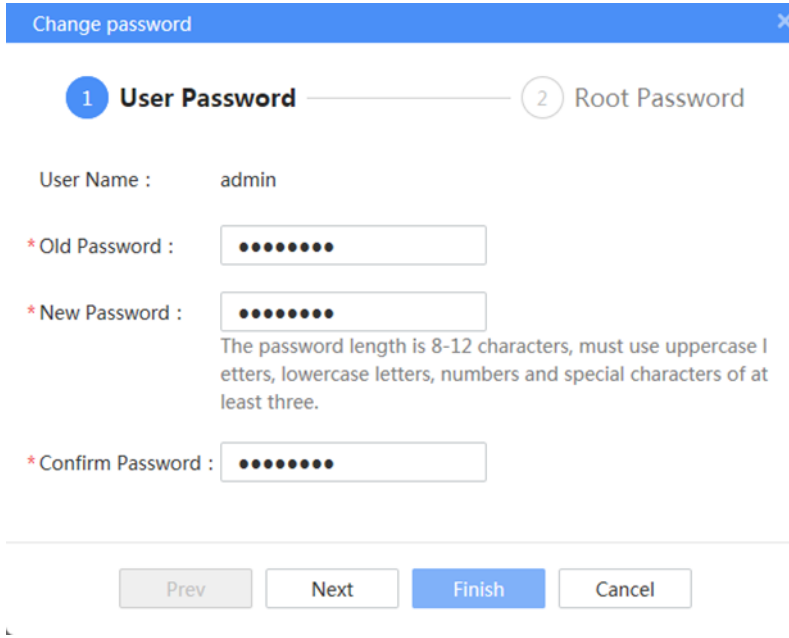
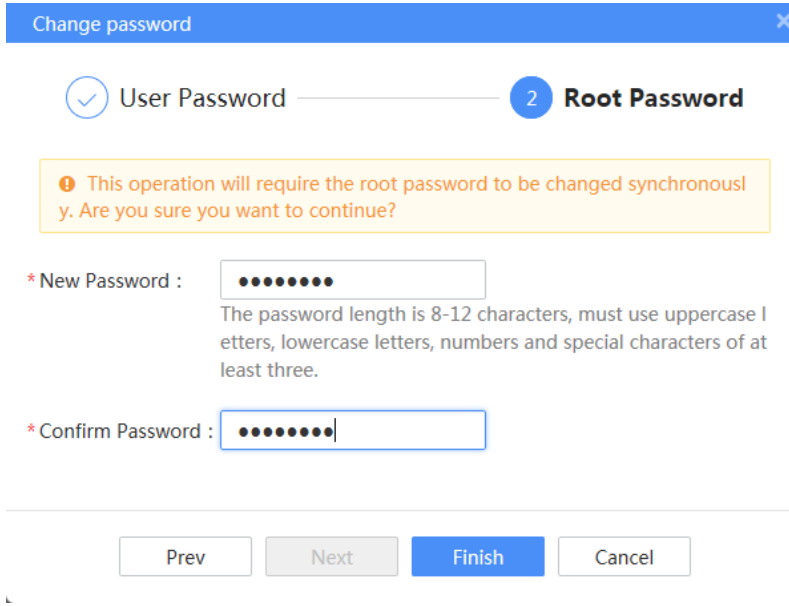



Figure 3-3 Change Root Password



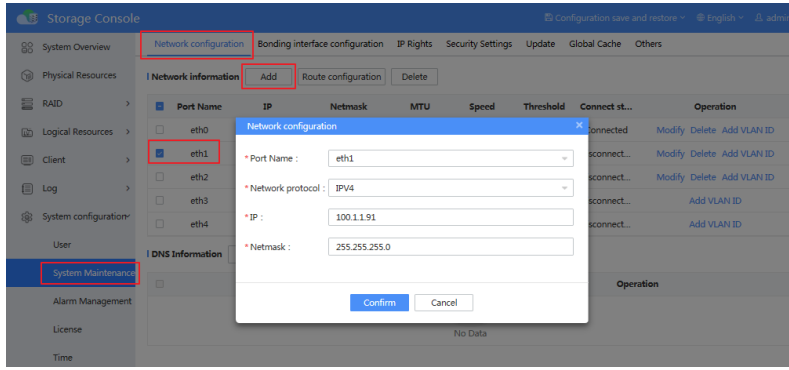
## 3.4 Set the Service Port IP

1. Choose **System Configuration** > **System Maintenance** > **Network Configuration**. Select the service port,then click **Add**.
2. Change the service port IP to **100.1.1.91** (configure this according to the actual situation).

**NOTE!**

- The default IP addresses of the service ports are empty.
- If expansion boards are inserted, the corresponding default IP addresses are empty too.

Figure 3-4 Change the IP Address

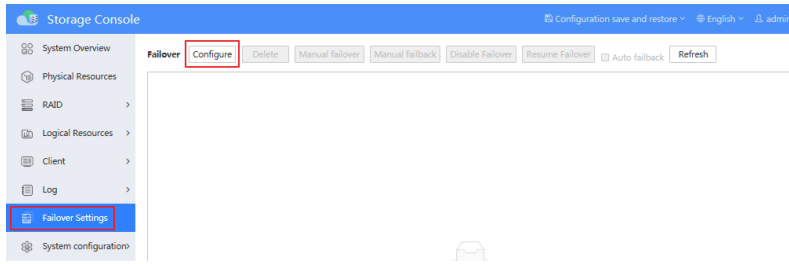



3. Click **Confirm**.

## 3.5 Configure Failover (For Dual Controller Device)

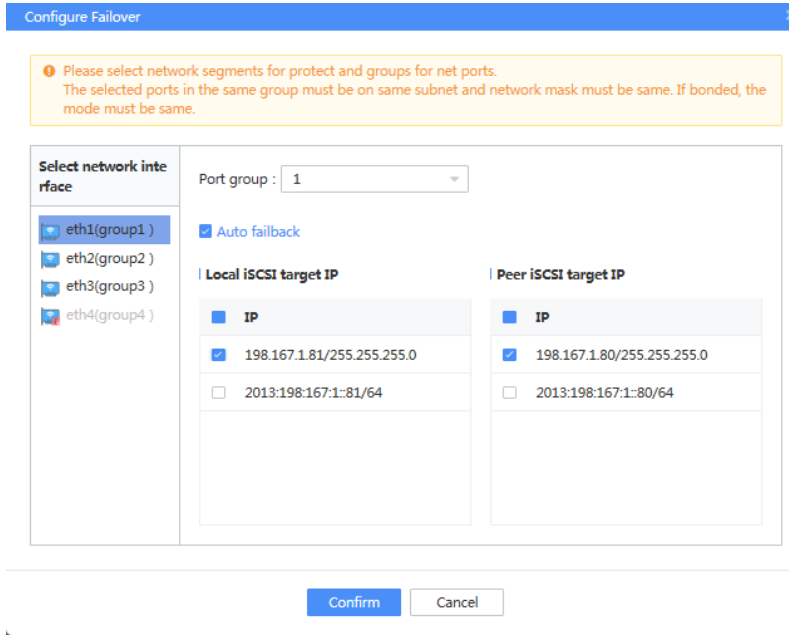
1. Choose **Failover Settings** > **Configure**.

Figure 3-5 Configure Failover Settings



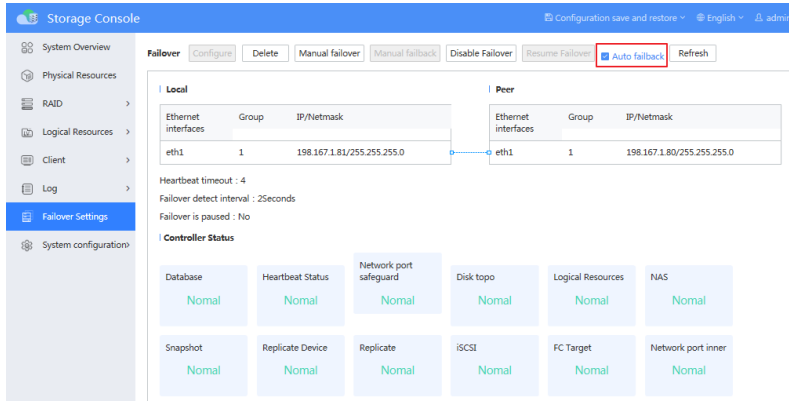
2. A dialog box appears as below. In the left column, each eth (or bond) corresponds to an actual network interface. Select the network interfaces for protection and the network segments accordingly.

Figure 3-6 Select Network Interface




3. Select whether to enable **Auto failback**. By default, it is selected.

Figure 3-7 Set Auto Failback



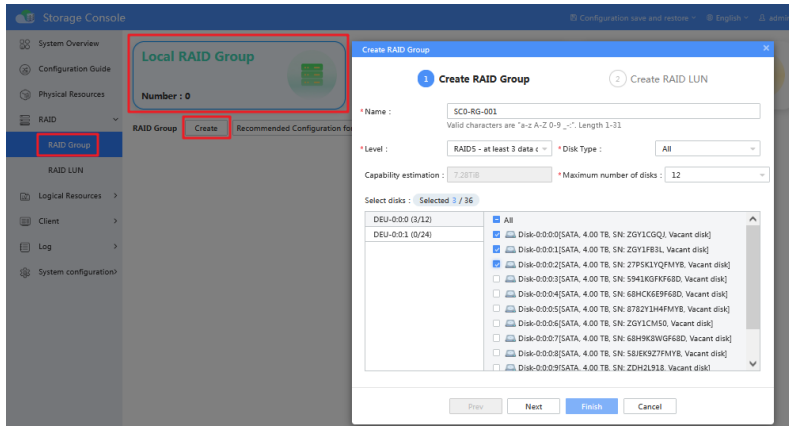
## 3.6 Create a RAID Group/RAID LUN

1. Choose **RAID** > **RAID Group** > **Local RAID Group**, then click **Create**.
2. Create a RAID group. Check whether the number of disks under **Physical Resources** is consistent with the actual number.

Recommend number of disks:

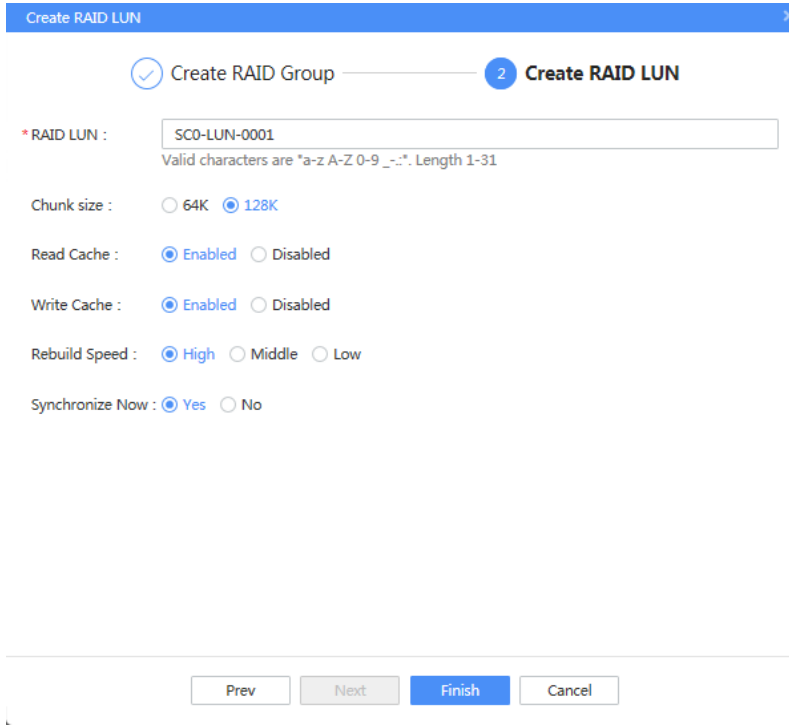
| |
|---|
| 11 (RAID5) + 1 (hot standby) + 11 (RAID5) + 1 (hot standby) |
| 11 (RAID5) + 12 (RAID5) + 1 (hot standby) |

Figure 3-8 Create a RAID Group




3. Click **Next**. Check the information of the RAID LUN.

Figure 3-9 Check the Information of the RAID LUN

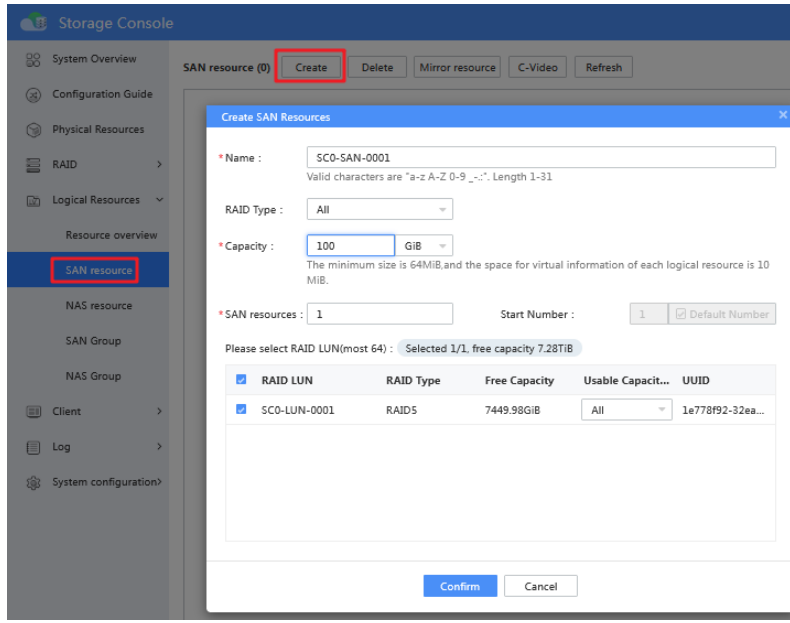



4. Click **Finish**.

## 3.7 Create Logical Resources

1. Choose **Logical Resources** > **SAN resource**, then click **Create**.
2. Set the SAN resource name and size, and select its RAID LUN.

Figure 3-10 Create the SAN Resource

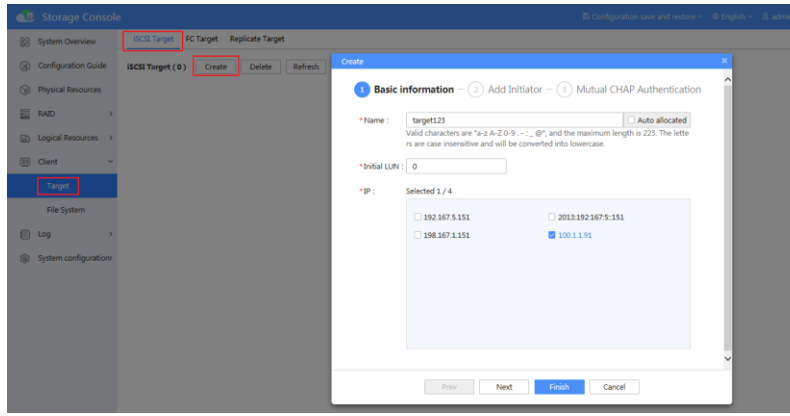



3. Click **Confirm**.

## 3.8 Create a Target and Add an Initiator

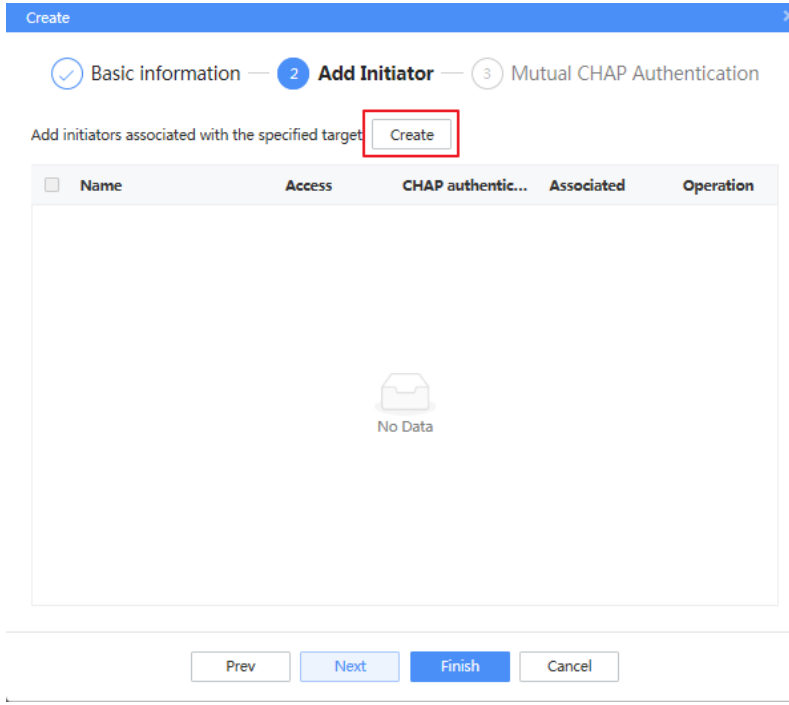
1. Choose **Client** > **Target** > **iSCSI Target**, then click **Create**.
2. Deselect **Auto allocated,** and customize the name (eg. target123). Select the IP address of the target, then click **Next**.

Figure 3-11 Create a Target



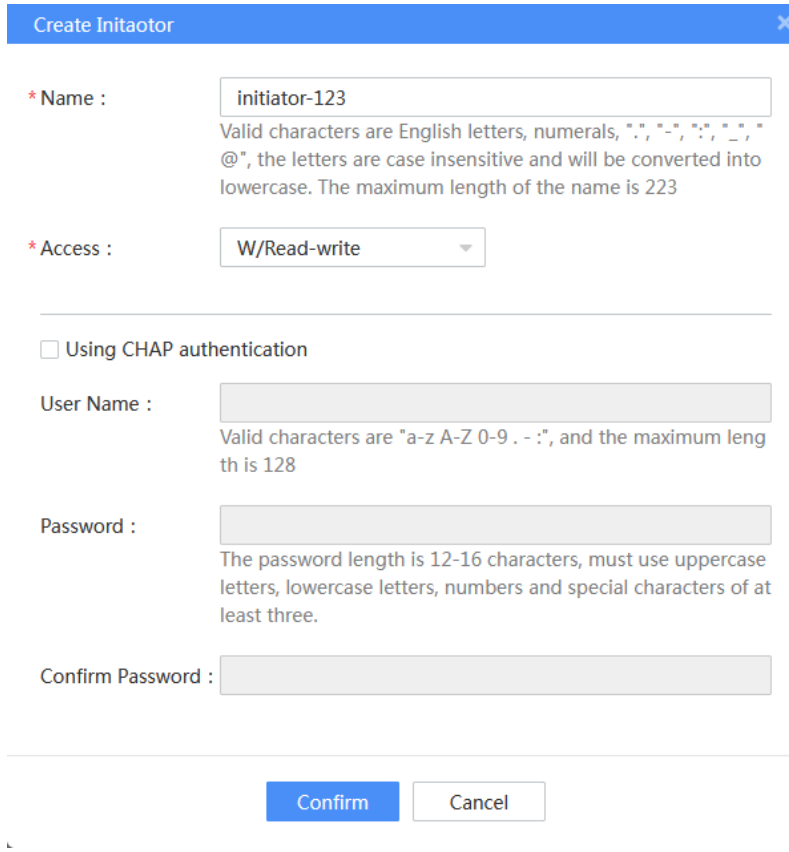
3. Click **Create** to add an initiator.

Figure 3-12 Add an Initiator



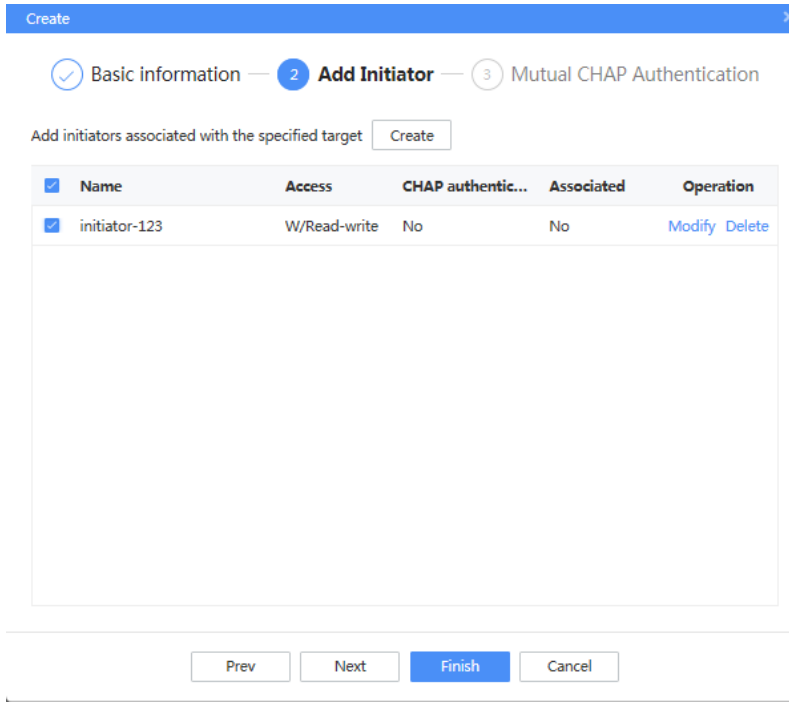

4. Set the name of the initiator, then click **Confirm**.

Figure 3-13 Set the Name of the Initiator




5. Select initiators associated with the target.

Figure 3-14 Associate Initiator with Target

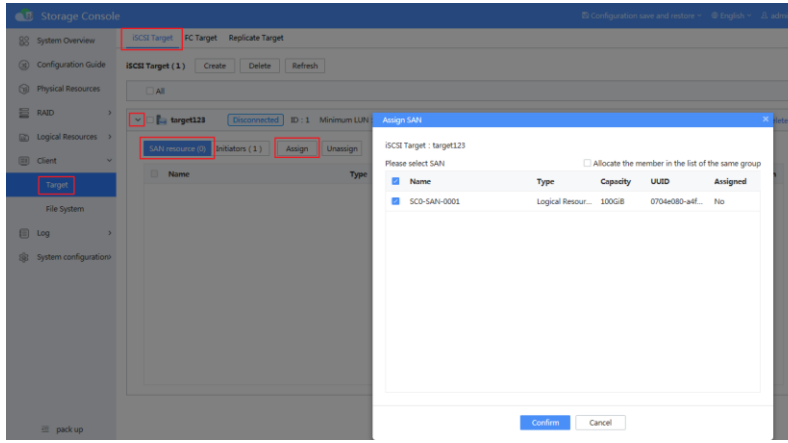



6. Click **Finish**.

## 3.9 Assign SAN Resources

1. Choose **Client** > **Target** > **iSCSI Target**, select the target (eg. **target123**), then click **SAN resource** > **Assign**.
2. Select resources to be assigned to a target.

Figure 3-15 Assign SAN Resources

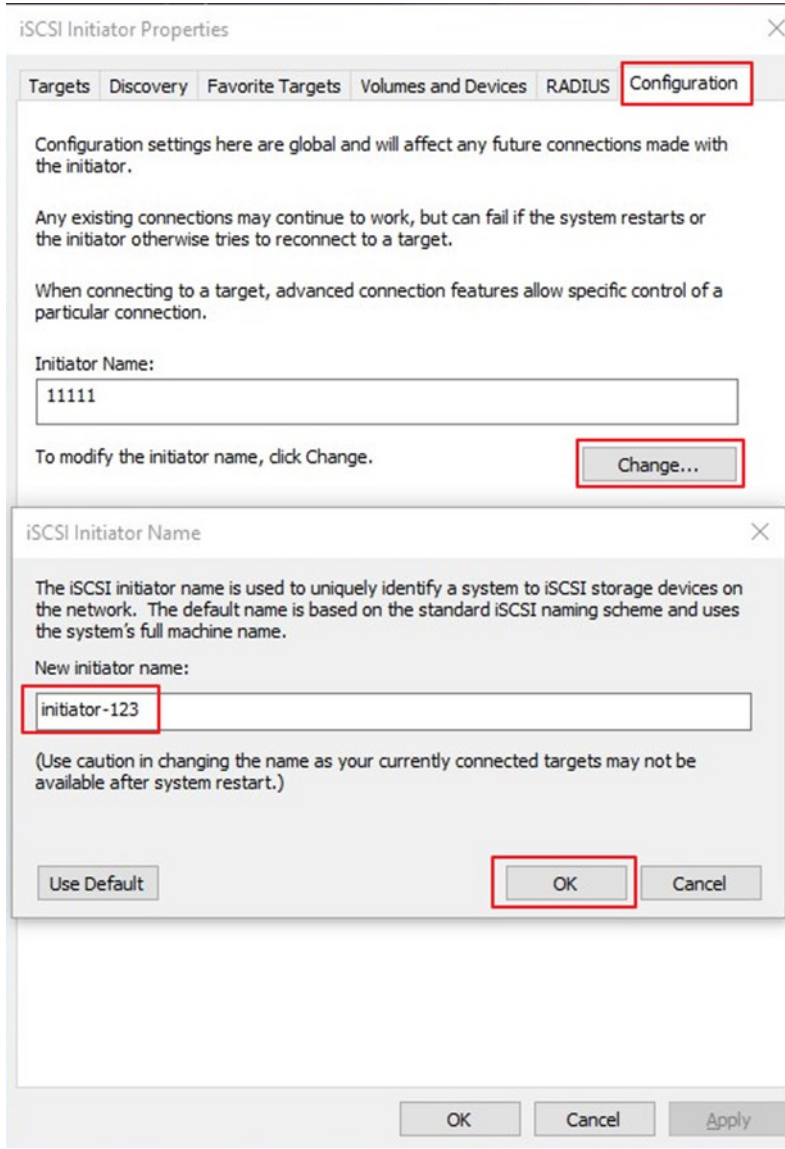



3. Click **Confirm**.

## 3.10 Configure the Initiator (with Windows Client as an Example)

1. Choose **Configuration** > **Change…**, enter the initiator name, and then click **OK**.

Figure 3-16 Change the Initiator Name

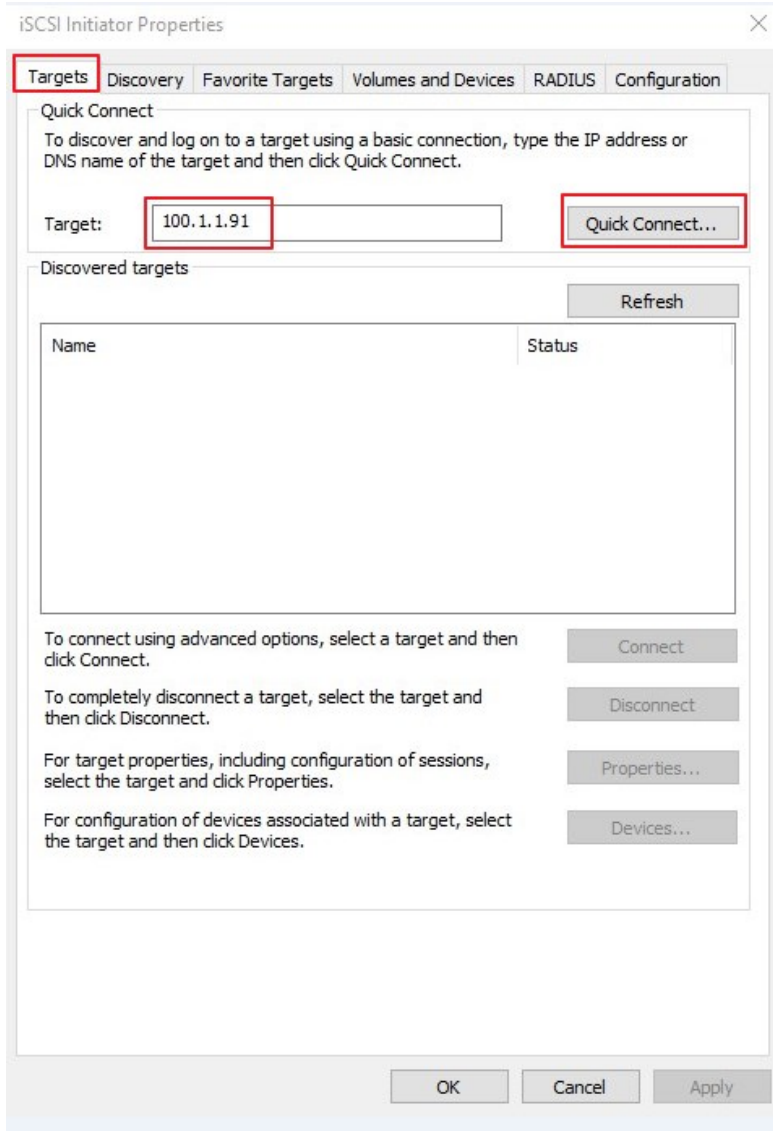



**NOTE!**

- The **New initiator name** configured on the windows client must be the same as that configured on the storage.

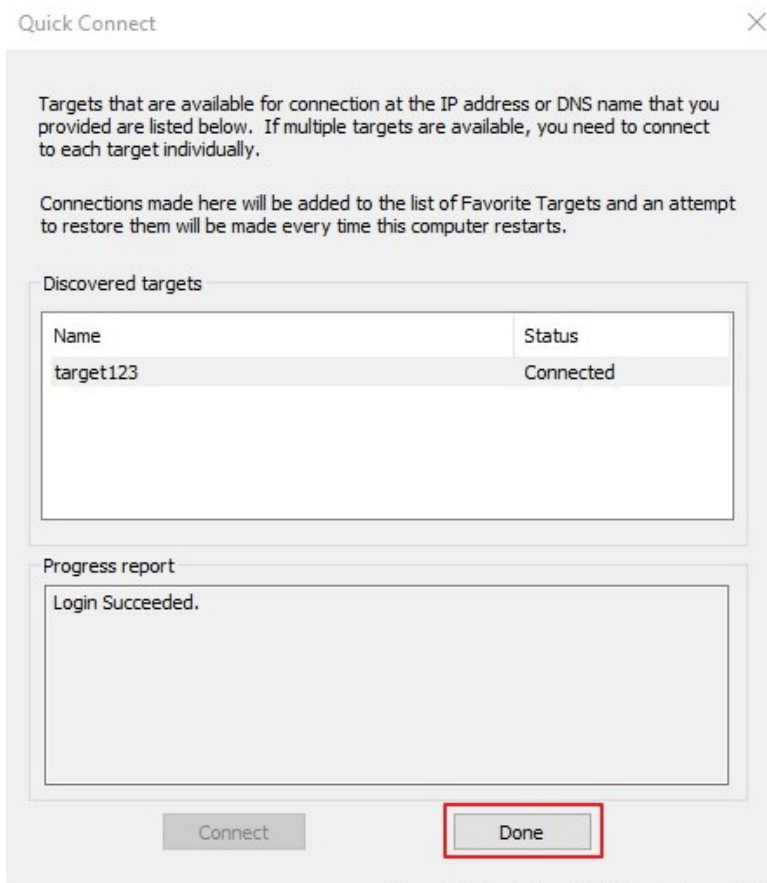
2. Select **Targets**, enter the IP address, then click **Quick Connect…**.

Figure 3-17 Quick Connect to the Target



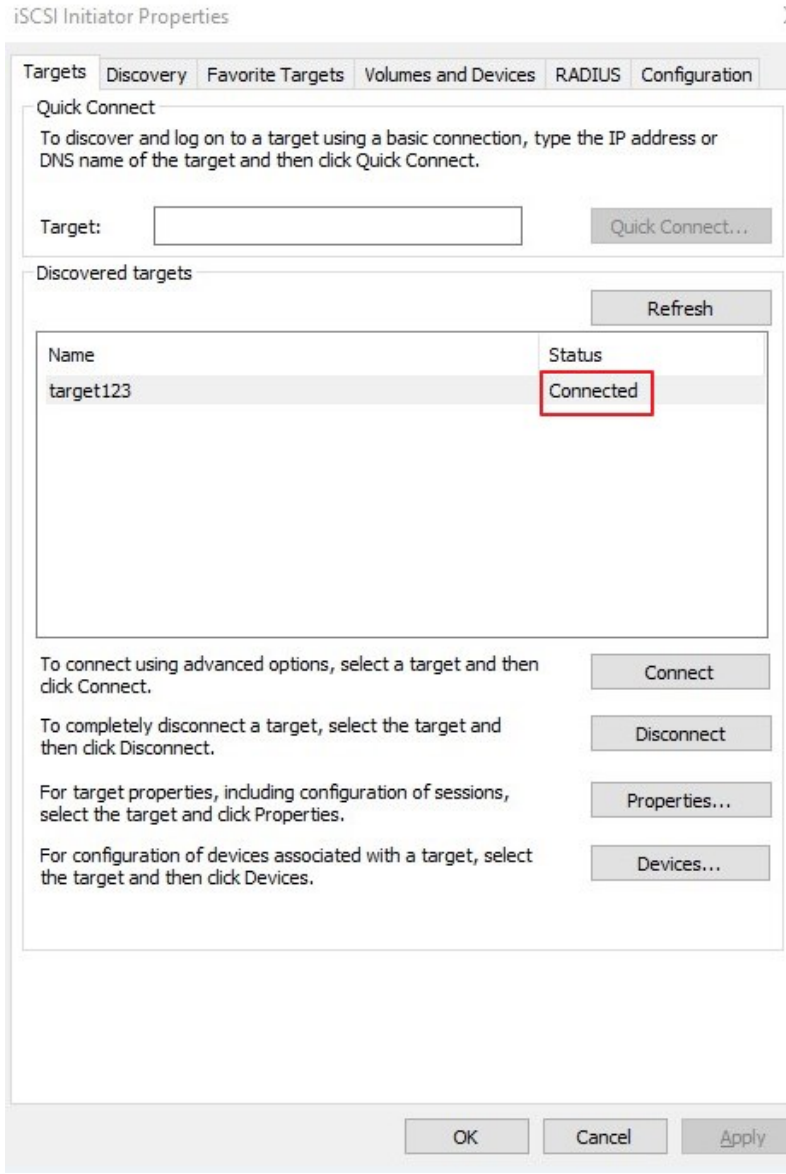

3. Click **Done**.

Figure 3-18 Finish Quick Connect




4. You can see that the target is connected.

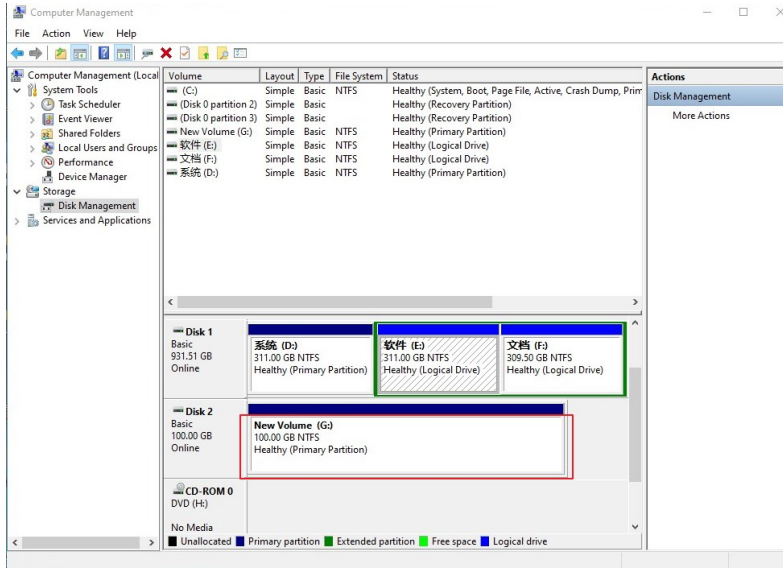
Figure 3-19 Check the Status




## 3.11 View Disks Assigned (with Windows 10 as an Example)

1. Right-click **My Computer**, then choose **Computer Management**.

Figure 3-20 Check the Added Disk Space




2. View the added disk space (as shown in the red box in the figure above).

# 4 (Optional) Video Management Server Configuration

## 4.1 Product Introduction

The Video Management Server is a smart integrated video technology platform with video input, storage, forward and device management functions designed specifically for digital video technology applications. The Unicorn has adopted audio/video compression and decompression, embedded system, storage, network, and smart technologies and it is suitable for security video technology scenarios such as residential areas, buildings, campus, hotels, and shopping malls etc.

**NOTE!**

- The following illustrations are only for your reference. And may be different from the actual product and the actual software UI.
- The manual takes VX16-EB Series with VMS installed by default for example.

## 4.2 Basic Concepts

| Basic Concept | Description |
|---|---|
| Management workstation | Indicates the PC where the console is installed. |
| VMS | VMS (Video Management Server) |
| DM | DM (Data Management) |
| MS | MS (Media Switch) |
| Management port | 100/1000 Mbit/s port for device configuration and management. |
| Service port | 1000 Mbit/s port for data transfer. |

**NOTE!**

IPSAN (VX16-EB Series) is installed with VMS by default, and does not support direct installation of DM and MS. Please uninstall the VMS first before installing DM and MS.

## 4.3 Configuration Workflow

To complete most basic configurations, perform the following operations on the web client (with Firefox browser as an example):

1. Log in to the VMS' web client through device IP address.
2. Set the service port IP.
3. (Optional) Configure primary server IP address
4. Create and format RAIDs.
5. Add IPCs and configure a recording schedule (primary).
6. View recording status and playback (primary).

## 4.4 Log in to the VMS' Web Client through Device IP Address

1. Enter the device IP address in the browser address bar of the management workstation (should be the same network segment with the server), then press **Enter**.
2. Enter the correct username and password to log in to the VMS' web client.
3. The default username/password: **admin**/**123456**. The default server IP address: **192.168.0.1** (management port: **eth0**).

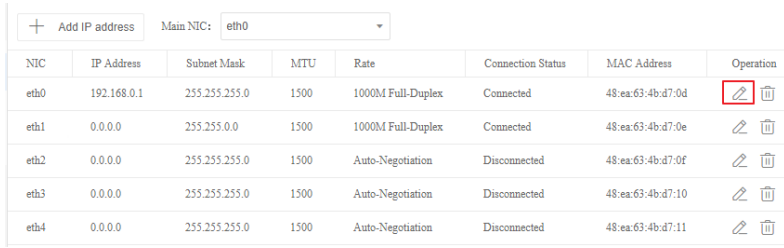
**NOTE!**

- The default password **123456** is only for first login and should be changed to a strong one with at least nine characters including uppercase and lowercase letters, digits and special characters of at least three.
- Compatible browser versions: Edge 79 or higher, Chrome 60 or higher, Firefox 60 or higher.

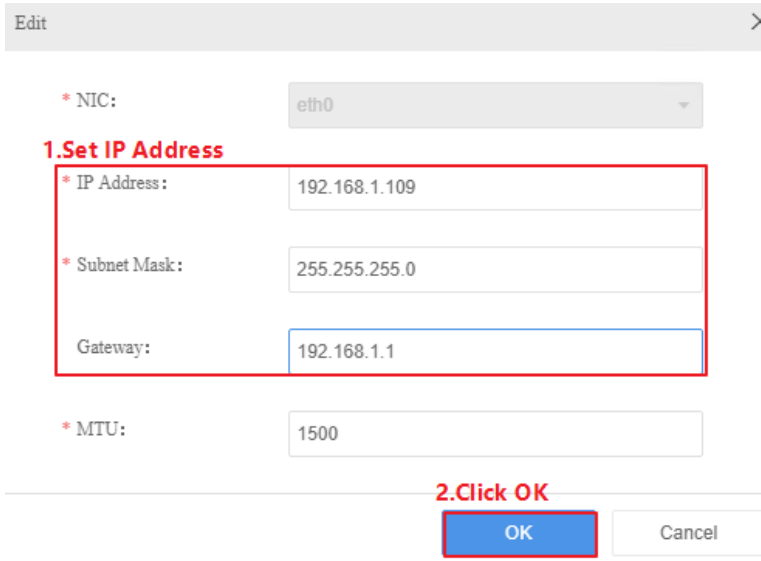
## 4.5 Set the Service Port IP

1. Choose **System** > **Network** >**TCP/IP** > **Network**, then click  under **Operation**. Change the IP address of the service port to **192.168.1.109** (configure this according to the actual situation).

Figure 4-1 Change IP Address




| NIC | IP Address | Subnet Mask | MTU | Rate | Connection Status | MAC Address | Operation |
|---|---|---|---|---|---|---|---|
| eth0 | 192.168.0.1 | 255.255.255.0 | 1500 | 1000M Full-Duplex | Connected | 48:ea:63:4b:d7:0d | |
| eth1 | 0.0.0.0 | 255.255.0.0 | 1500 | 1000M Full-Duplex | Connected | 48:ea:63:4b:d7:0e | |
| eth2 | 0.0.0.0 | 255.255.255.0 | 1500 | Auto-Negotiation | Disconnected | 48:ea:63:4b:d7:0f | |
| eth3 | 0.0.0.0 | 255.255.255.0 | 1500 | Auto-Negotiation | Disconnected | 48:ea:63:4b:d7:10 | |
| eth4 | 0.0.0.0 | 255.255.255.0 | 1500 | Auto-Negotiation | Disconnected | 48:ea:63:4b:d7:11 | |

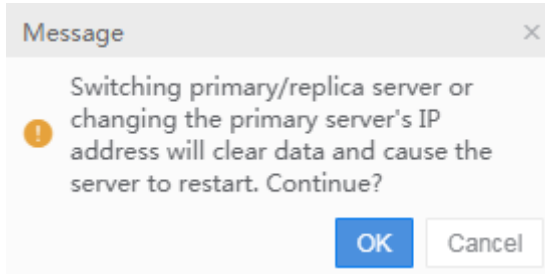



2. Click **OK**

## 4.6 (Optional) Configure Primary Server IP Address

1. Choose **System** > **Primary/Replica Switch**.
2. Enter the primary server IP address (eg. **192.169.1.110**), then click **Save**.
3. A message appears as below, then click **OK** to restart.

Figure 4-2 Restart Message



**NOTE!**

The VMS installed on VX16-EB Series is in **Replica mode** by default. You can switch to the **Primary mode** according to the actual situation, or connect other VMS hosts to expand the storage capacity of the primary server.

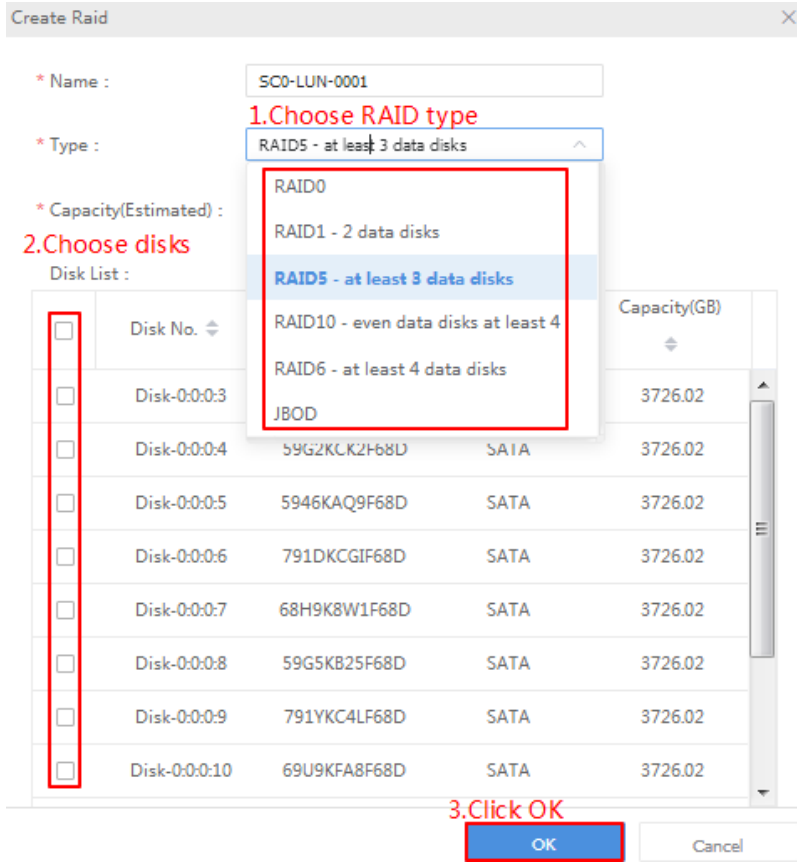
## 4.7 Create and Format RAIDs

1. Choose **System > Disk > RAID Manage > Physical Disk**. Check whether the number of disks under **DEU** is consistent with the actual number.
2. Click **Manual Create** to create RAIDs.

Recommend number of disks:

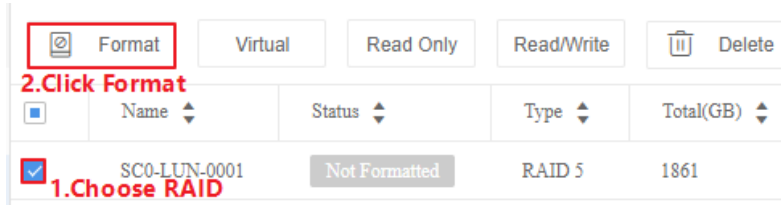
| |
|---|
| 11 (RAID5) + 1 (hot standby) + 11 (RAID5) + 1 (hot standby) |
| 11 (RAID5) + 12 (RAID5) + 1 (hot standby) |
| 7 (RAID5) + 8 (RAID5) +1 (hot standby) |

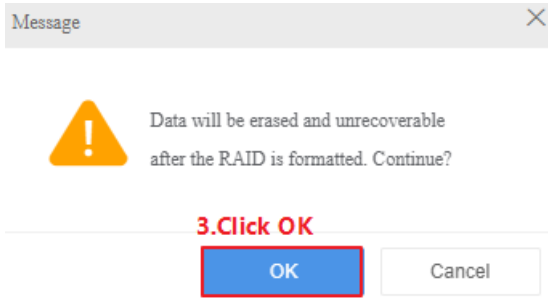
Figure 4-3 Create RAID




3. Choose System > Disk > RAID Manage > RAID. Choose the RAID to format, click Format, and then click OK.

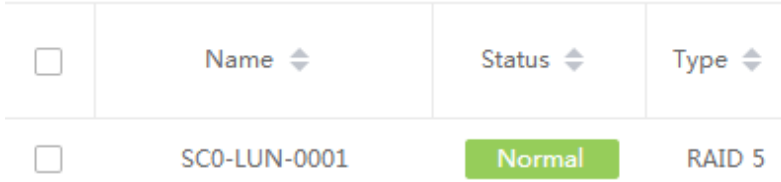
Figure 4-4 Format RAID






4. Check the formatting results. Ensure the status is normal.

Figure 4-5 Normal RAID Status



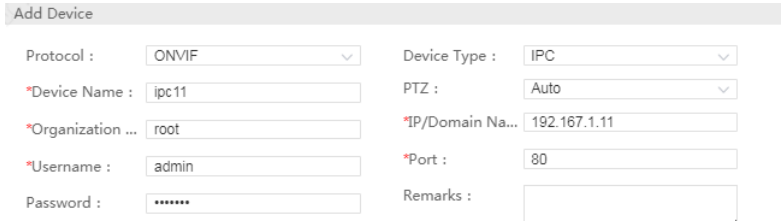

## 4.8 Add IPCs and Recording Schedule (Primary)

Make sure RAID has been added and formatted successfully before you start configuring a recording schedule.

The following steps take ONVIF as an example. You may add the IPCs with other protocols.

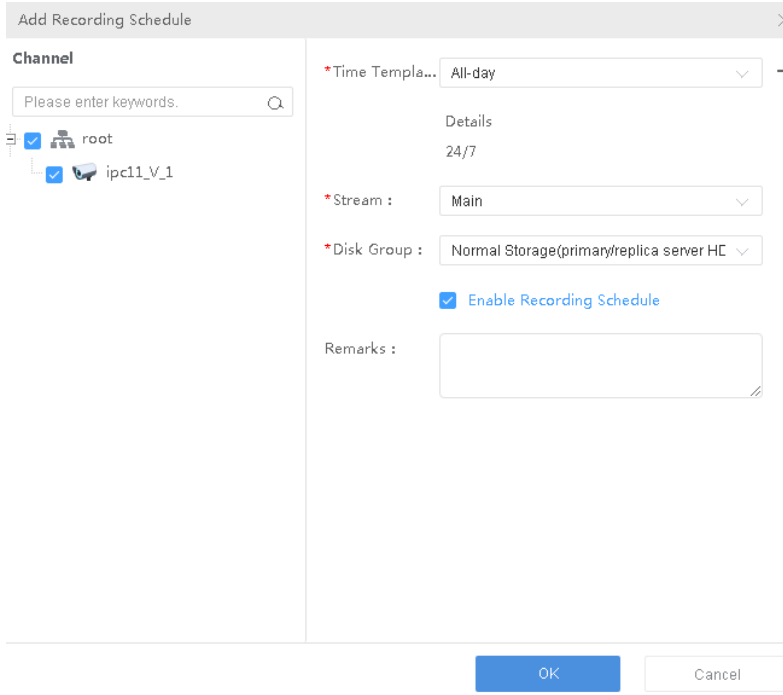
1. Choose **Basic** > **Device** > **Encoding Device**, click **+Add**. The following takes **ipc11** for example.

Figure 4-6 Add Device




2. Choose **Basic** > **Recording Schedule**, click **+Add**, select **ipc11_V_1**, then click **OK**.

Figure 4-7 Add Recording Schedule

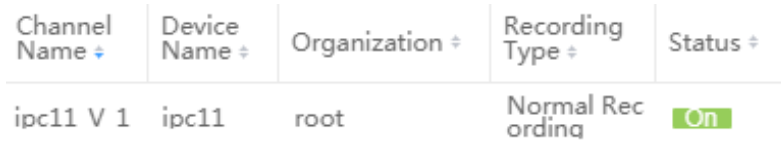



## 4.9 Recording Status and Playback (Primary)

Make sure recording schedule have been added before you view the recording status and playback.

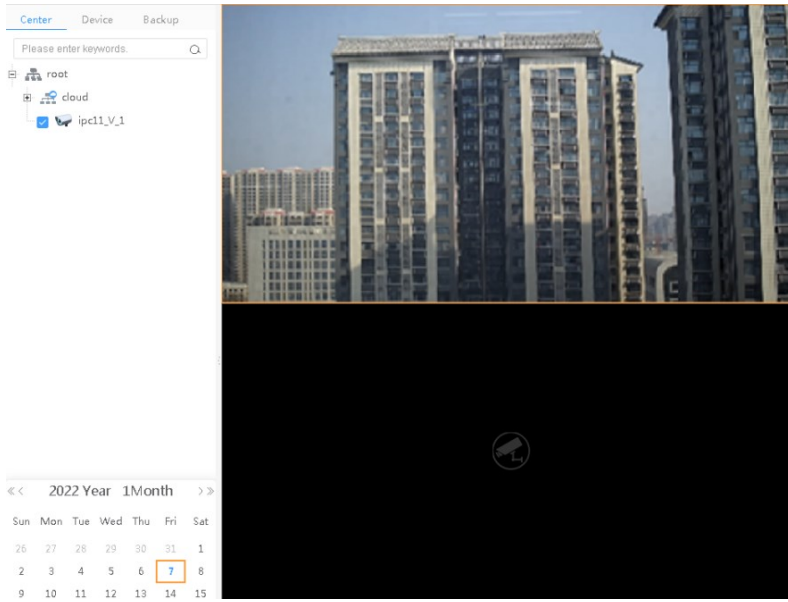
1. Choose **Statistics** > **Server** > **Recording**.

Figure 4-8 Check Recording Status




2. Choose **Video Service** > **Playback** > **Center**, select **ipc11_V_1**, then click **Search**.

Figure 4-9 Playback




# 5 Appendix Disk Installation and Removal for the 60 Slots Products

For the 60 slots products, the installation and removal of the disk are slightly different from other slots. Here is a separate introduction.

Do not touch the Printed Circuit Board (PCB) of the disk.

Verify that the handle and screws on both sides of the disk case are secure.

## Installing a Disk

The steps to install the disk are as follows:

1. Unplug the disk subrack. Turn the screw (counter clockwise, please refer to the blue mark in the figure below). When the screws are loose, pull out the disk subrack with both hands at the same time (like pulling a drawer).

**NOTE!**

- The disk subrack cannot be completely unplugged. You only need to extract it to the appropriate position to install the disk.
- No. 0-3 slot of each disk subrack must be full before using other slots to install the disk.



2. Put the disk into the disk subrack (hold the middle position on both sides of the disk), and put the rotating shaft on the disk into the disk support (as shown in the corresponding position of the blue area in the figure below).



3. If the frame is not fully loaded with hard disks, make sure each subrack is installed with at least 4 hard disks; the hard disks are always installed from the outermost row toward inside and in the order as shown below (from slot 0 to slot 3). As shown in the figure below, No. 0-3 slot of each disk subrack must be full before using other slots to install the disk.




4. After putting the disk into the slot one by one, press the handle to install the disk in place (following the blue arrow radian in the figure below).



5. After all the disks are installed, push the disk subrack back into place to let the handle bar fit the panel. Turn the screws on the panel clockwise (as shown in the figure below), and lock the screws of the disk insert frame.



## Removing a Disk

The steps to remove the disk are as follows:

1. Turn the screw of the disk subrack (counter clockwise, please refer to the blue mark below). After the screws are loose, pull out the disk insert frame (like pulling a drawer) with both hands at the same time.



2. Hook out the disk pull ring. Find the location of the disk to be pulled out, and use your fingers to hook out the pull ring on the disk (see the blue part in the figure below).



3. Pull the pull ring with your finger, pull out the disk (along the blue arc direction shown in the figure below), and take out the disk by holding the middle position on both sides of the disk.



4. Disk subrack reset. Make sure that the disk insert frame is pushed back in place, the handle bar is connected with the panel, turn the screws on the panel (clockwise, as shown in the figure below), and lock the screws.



# Disclaimer and Safety Warnings

## Copyright Statement

©2012-2026 Zhejiang Uniview Technologies Co., Ltd. All rights reserved.
No part of this manual may be copied, reproduced, translated or distributed in any form or by any means without prior consent in writing from Zhejiang Uniview Technologies Co., Ltd (referred to as Uniview or us hereafter).
The product described in this manual may contain proprietary software owned by Uniview and its possible licensors. Unless permitted by Uniview and its licensors, no one is allowed to copy, distribute, modify, abstract, decompile, disassemble, decrypt, reverse engineer, rent, transfer, or sublicense the software in any form or by any means.

## Trademark Acknowledgements

unv uniarch are trademarks or registered trademarks of Uniview.

HDMI HIGH-DEFINITION MULTIMEDIA INTERFACE The terms HDMI, HDMI High-Definition Multimedia Interface, HDMI Trade dress and the HDMI Logos are trademarks or registered trademarks of HDMI Licensing Administrator, Inc.

All other trademarks, products, services and companies in this manual or the product described in this manual are the property of their respective owners.

## Export Compliance Statement

Uniview complies with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abides by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described in this manual, Uniview asks you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

## EU Authorised Representative

UNV Technology EUROPE B.V. Treubstraa 1, 2288 EG, Rijswijk, Netherlands.
If you have any feedback, please contact us at service@uniview.com.

## Privacy Protection Reminder

Uniview complies with appropriate privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information. Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

## About This Manual

- This manual is intended for multiple product models, and the photos, illustrations, descriptions, etc, in this manual may be different from the actual appearances, functions, features, etc, of the product.
- This manual is intended for multiple software versions, and the illustrations and descriptions in this manual may be different from the actual GUI and functions of the software.
- Despite our best efforts, technical or typographical errors may exist in this manual. Uniview cannot be held responsible for any such errors and reserves the right to change the manual without prior notice.
- Users are fully responsible for the damages and losses that arise due to improper operation.
- Uniview reserves the right to change any information in this manual without any prior notice or indication. Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

## Disclaimer of Liability

- To the extent allowed by applicable law, in no event will Uniview be liable for any special, incidental, indirect, consequential damages, nor for any loss of profits, data, and documents.
- The product described in this manual is provided on an "as is" basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. Uniview strongly recommends that users take all necessary measures to enhance the protection of network, device, data and personal information. Uniview disclaims any liability related thereto but will readily provide necessary security related support.
- To the extent not prohibited by applicable law, in no event will Uniview and its employees, licensors, subsidiary, affiliates be liable for results arising out of using or inability to use the product or service, including, not limited to, loss of profits and any other commercial damages or losses, loss of data, procurement of substitute goods or services; property damage, personal injury, business interruption, loss of business information, or any special, direct, indirect, incidental,

consequential, pecuniary, coverage, exemplary, subsidiary losses, however caused and on any theory of liability, whether in contract, strict liability or tort (including negligence or otherwise) in any way out of the use of the product, even if Uniview has been advised of the possibility of such damages (other than as may be required by applicable law in cases involving personal injury, incidental or subsidiary damage).

- To the extent allowed by applicable law, in no event shall Uniview's total liability to you for all damages for the product described in this manual (other than as may be required by applicable law in cases involving personal injury) exceed the amount of money that you have paid for the product.

## Network Security

Please take all necessary measures to enhance network security for your device.

**The following are necessary measures for the network security of your device:**

- **Change default password and set strong password**: You are strongly recommended to change the default password after your first login and set a strong password that includes at least 9 characters including uppercase letter, lowercase letter, digit and special character.
- **Keep firmware up to date**: It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit Uniview's official website or contact your local dealer for the latest firmware.

**The following are recommendations for enhancing network security of your device:**

- **Change password regularly**: Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.
- **Enable HTTPS/SSL**: Use SSL certificate to encrypt HTTP communications and ensure data security.
- **Enable IP address filtering**: Allow access only from the specified IP addresses.
- **Minimum port mapping**: Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- **Disable the automatic login and save password features**: If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- **Choose username and password discretely**: Avoid using the username and password of your social media, bank, email account, etc, as the username and password of your device, in case your social media, bank and email account information is leaked.
- **Restrict user permissions**: If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- **Disable UPnP**: When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage. Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.
- **SNMP**: Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.
- **Multicast**: Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- **Check logs**: Check your device logs regularly to detect unauthorized access or abnormal operations.
- **Physical protection**: Keep the device in a locked room or cabinet to prevent unauthorized physical access.
- **Isolate video surveillance network**: Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.

**Learn More**

You may also obtain security information under Security Response Center at Uniview's official website.

## Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

**Storage, Transportation, and Use**

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Protect the device from liquid of any kind.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.
- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting Uniview first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.
- This equipment is not suitable for use in locations where children are likely to be present.
- Always disconnect the device from power before attempting to move the device.



CAUTION!SHOCK HAZARD!

Power Requirements

- Installation and use of the device must be in strict accordance with your local electrical safety regulations.
- Use the battery properly. Improper use of the battery may cause risks of fire and explosion. Replace only with an identical battery. Dispose the used battery according to your local regulations or the battery manufacturer's instructions. Never dispose of the battery in fire.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded by a skilled person.
- If the equipment is not used for a long time, disconnect the equipment from outlet.

Battery Use Caution

- When battery is used, avoid:
  - Extremely high or low temperature and air pressure during use, storage and transportation.
  - Battery replacement.
- Use the battery properly. Improper use of the battery such as the following may cause risks of fire, explosion or leakage of flammable liquid or gas.
  - Replace battery with an incorrect type;
  - Dispose of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery;
- Dispose of the used battery according to your local regulations or the battery manufacturer's instructions.

Avertissement de l'utilisation de la batterie

- Lorsque utiliser la batterie, évitez:
  - Température et pression d'air extrêmement élevées ou basses pendant l'utilisation, le stockage et le transport.
  - Remplacement de la batterie.
- Utilisez la batterie correctement. Mauvaise utilisation de la batterie comme cellesmentionnées ici, peut entraîner des risques d'incendie, d'explosion ou de fuite liquide de gaz inflammables.
  - Remplacer la batterie par un type incorrect;
  - Disposer d'une batterie dans le feu ou un four chaud, écraser mécaniquement ou couper la batterie;
- Disposer la batterie utilisée conformément à vos règlements locaux ou aux instructions du fabricant de la batterie.
- Personal safety warnings:
  - Chemical Burn Hazard. This product contains a coin cell battery. Do NOT ingest the battery. It can cause severe internal burns and lead to death.
  - Keep new and used batteries away from children.
  - If the battery compartment does not close securely, stop using the product and keep it away from children.
  - If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- Avertissements de sécurité personnelle:
  - Risque de brûlure chimique. Ce produit contient une batterie de cellules. N'ingérer pas la batterie. Si la batterie de cellule est avalée, elle peut causer de graves brûlures internes en seulement 2 heures et peut entraîner la mort.
  - Gardez les batteries nouvelles ou utilisées à l'écart des enfants.
  - Si le compartiment de la batterie ne se ferme pas en toute sécurité, cessez d'utiliser le produit et gardez-le à l'écart des enfants.
  - Si vous pensez que des piles ont pu être avalées ou placées à l'intérieur d'une partie du corps, consultez immédiatement un médecin.

## Regulatory Compliance

FCC Statements

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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Compliance Information Statement refer to:

http://en.uniview.com/Support/Download_Center/Product_Installation/Declaration/

**Caution:** The user is cautioned that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

**NOTE:** 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.

LVD/EMC Directive

This product complies with the European Low Voltage Directive 2014/35/EU and EMC Directive 2014/30/EU.

WEEE Directive–2012/19/EU



The product this manual refers to is covered by the Waste Electrical & Electronic Equipment (WEEE) Directive and must be disposed of in a responsible manner.

Battery Directive-2013/56/EC



Battery in the product complies with the European Battery Directive 2013/56/EC. For proper recycling, return the battery to your supplier or to a designated collection point.

Better Security, Better World

www.uniview.com

globalsupport@uniview.com