Intelligent Fusion Server

Quick Start Guide

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. 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 this Document with the guidance and assistance of professionals trained in supporting the Product.

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.

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.

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 in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

- This device may not cause harmful interference.
- 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, 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: ***http://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: ***http://www.recyclethis.info***.

Industry Canada ICES-003 Compliance

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

Preface

Applicable Model

This manual is applicable to Intelligent Fusion Server.

Symbol Conventions

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

Symbol	Description
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Note	Provides additional information to emphasize or supplement important points of the main text.

Safety Instruction

- 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 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.

Contents

Chapter 1 Installation Preparation

Before installing operating system on the device, you should configure the IP address of iDRAC to make it accessible, and prepare a Java environment for further remote control.

1.1 Install Java Application

Java application can be served as a tool to control the server and conduct operation through your laptop.

Steps

1. Check if Java is installed on your laptop.
   1) Run **cmd** command line tool.
   2) Enter ***java -version*** to check if you can get Java version information.

Figure 1-1 Check Java Environment

   – If the Java version information is shown, you can skip the installation steps.
   – If no version information can be reached, follow Step 2 to 8.
2. Download and install Java application.

Note

JRE1.8 version or above recommended.

3. Go to **Control Panel** → **All Control Panel Items** → **System** → **Advanced system settings** → **Advanced** → **Environment Variables** → **System Variables** → **New**.

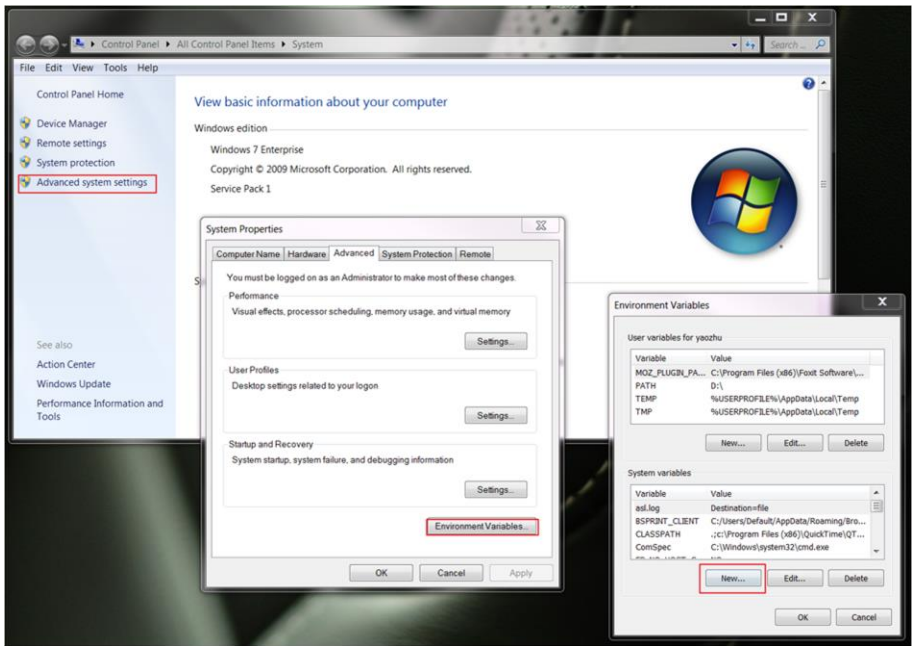

Figure 1-2 Add System Variable

4. Add a new system variable.

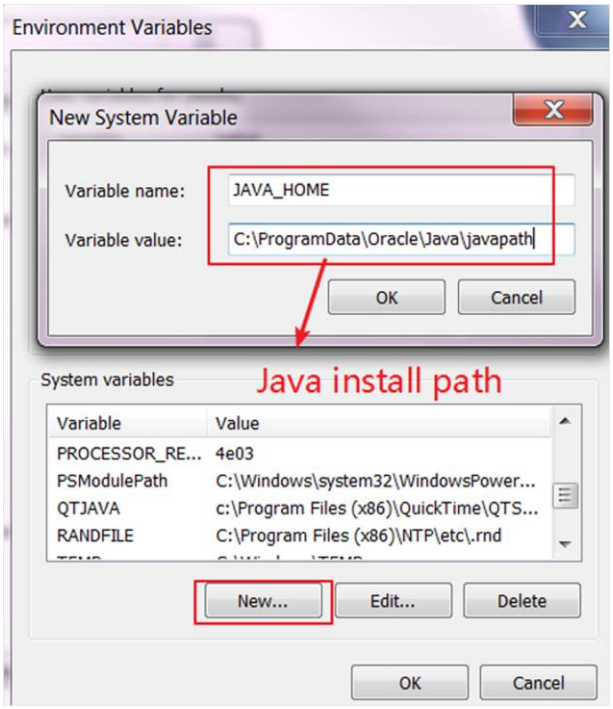

Figure 1-3 Configure System Variable

Variable name

Enter ***JAVA_HOME***.

Variable value

Copy the actual installation path to the text field.

5. Click **OK**.
6. Click **Path** variable, and then click **Edit**.
7. Enter ***%JAVA_HOME%\bin;%JAVA_HOME%\JRE\bin*** in **Variable value**.

Note

If other values already exist in the text field, enter the content at the forefront, and use a semicolon (;) to separate those values.

8. Click **OK**.

1.2 Configure iDRAC Network

Configure iDRAC network parameters to make it approachable through remote control.

Steps

1. Connect the device to your laptop with network cable.

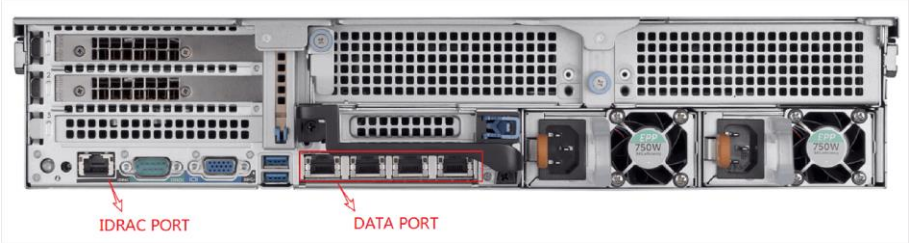

Figure 1-4 External Interfaces

2. Press the power button to turn the server on.
3. Press **F2** to enter system setup interface when the pop-up below appears.

Figure 1-5 System Setup

Note

The options vary from versions to versions. Please make your selection according to the actual prompts.

4. Go to **iDRAC Settings** → **Network** to configure network parameters.

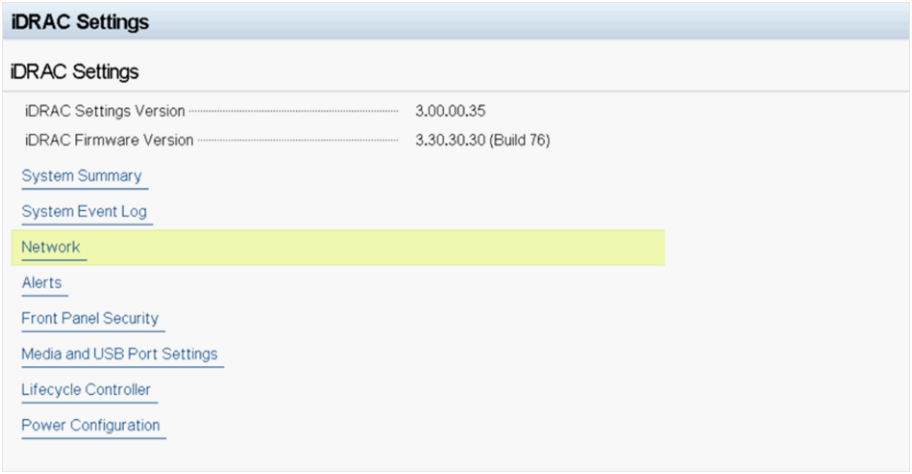

Figure 1-6 Configure iDRAC Network

5. Select **NIC Selection** as **Dedicated**.

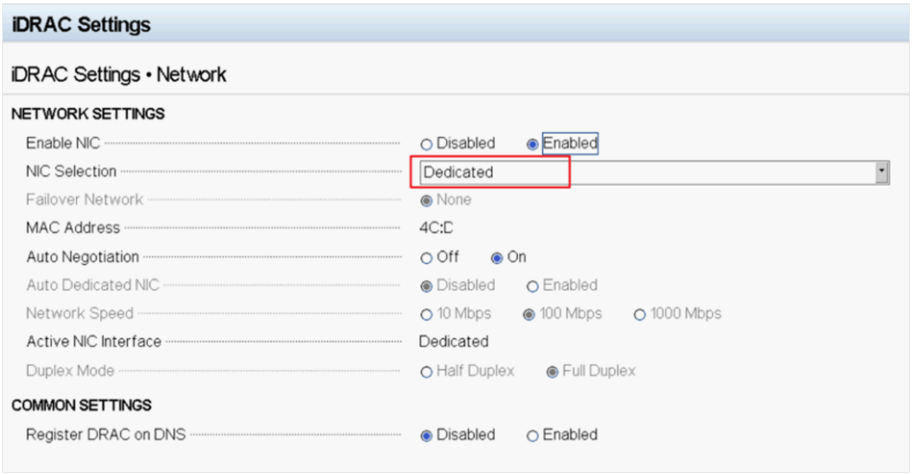

Figure 1-7 Set NIC Selection

6. Slide the slider down to configure **IPV4 Settings**.
   1) Enable IPv4 function.
   2) Disable DHCP function.
   3) Configure other parameters according to your actual IP address.

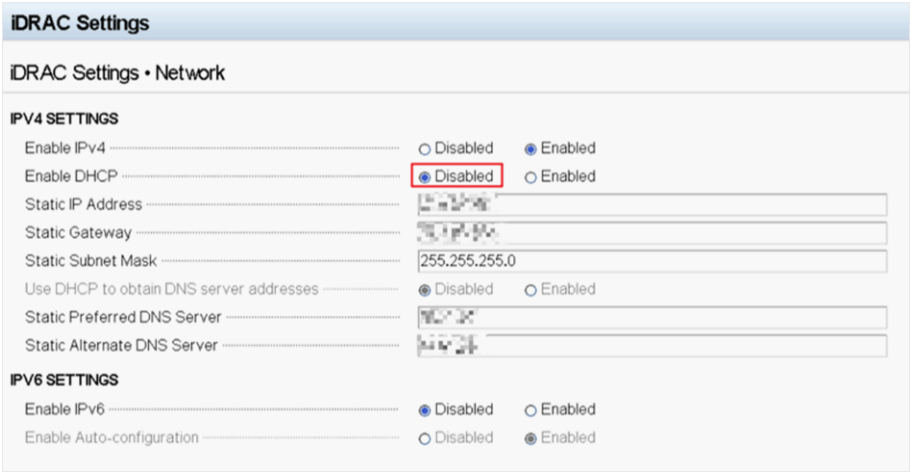

Figure 1-8 IPV4 Setting

7. Save and exit the setup.

1.3 Log in to iDRAC

The default login password can be found on the quick service label of the server. You can also change the default password after first-time login.

Before You Start

Ensure the server and your laptop are on the same subnet.

Steps

1. Check default root password.
   1) Pull the quick service label out form the front panel of the device.

Figure 1-9 Pull out Service Label

   2) Turn over the label, and the default password will be shown.

Figure 1-10 Check Default Password

2. Open your web browser, and enter the IP address of the server.

   It is recommended to use Google Chrome browser for better visualization.

3. Enter ***root*** in **Username** and the password on the quick service label.

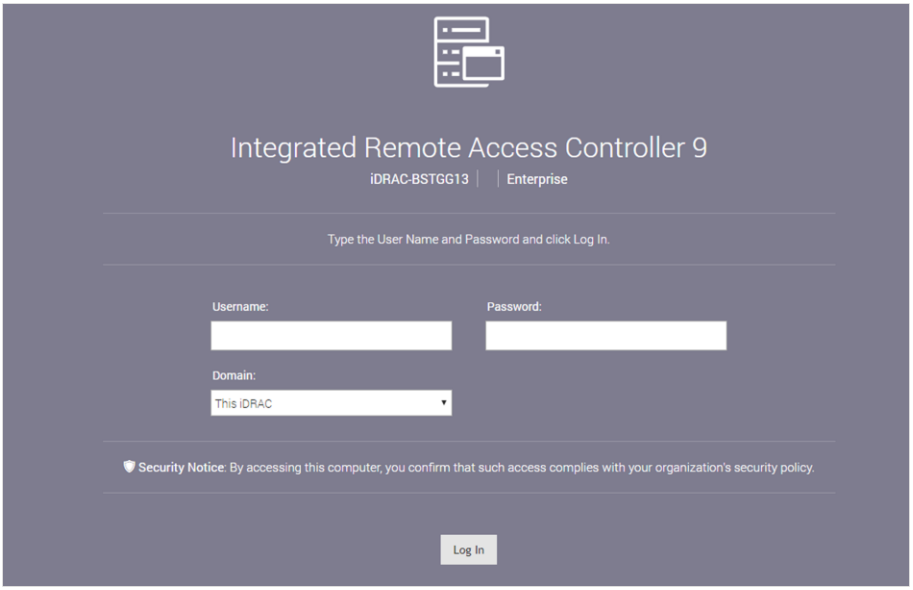

Figure 1-11 Login Interface

4. Click **Log in**.
5. Optional: You go to **iDRAC Settings** → **Users** → **Local Users** to change the password.

Chapter 2 OS Installation

This part introduces how to install operating system with an image file.

2.1 Enable Remote Control

Remote control can be achieved through iDRAC by different plug-ins. Here we introduce how to perform remote control by using Java as the tool.

Before You Start

- Ensure that you have logged in to iDRAC.
- Ensure a Java program (JRE1.8 version or above recommended) is installed.

Steps

1. Go to the homepage of iDRAC.

> **Note**
> You can check system information, health status, logs and other basic information.

2. Set virtual console.
1) Go to **Configuration** → **Virtual Console**.
2) Click **Settings** on the upper-right corner of the virtual console window.

Figure 2-1 Virtual Console Window

3. Select **Java** in **Plug-in Type**.

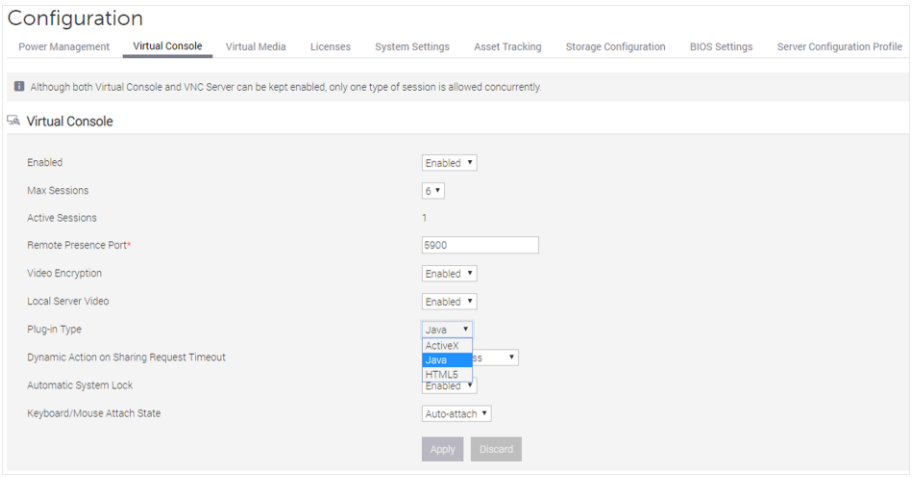

Figure 2-2 Set Plug-in Type

4. Click **Apply**.
5. Click **OK** in the pop-up.
6. Click **Launch Virtual Console** or the displaying area of the virtual console window.
   A file named **viewer. jnlp** will be downloaded automatically.
7. Save and open the file downloaded in step 6 when the prompt appears.

Note

If Java plug-in does not pop up, go to **Java Control Panel** → **Security** → **Edit Site List**, and add the IP address of iDRAC to **Exception Site List**.

Figure 2-3 Add Exception Site

The interface will redirect to virtual console window.

2.2 Install OS with Image File

The operating system can be installed to the device by mapping image file.

Before You Start

- Enable virtual console.
- Ensure that the image file has been saved in local storage.

Steps

1. Go to **Virtual Media** → **Connect Virtual Media**.

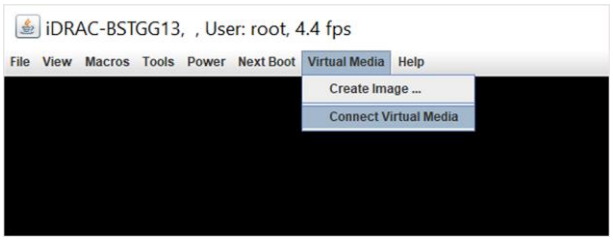

Figure 2-4 Connect Virtual Media

2. Click **Map CD/DVD**.

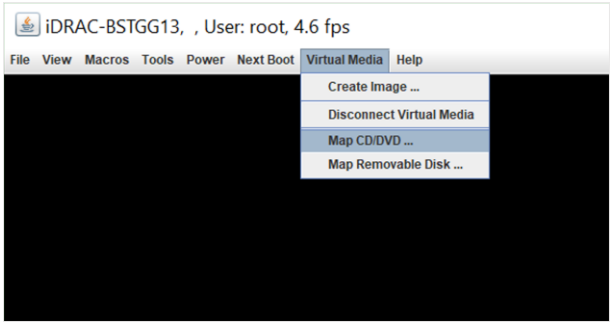

Figure 2-5 Map ISO File

3. Click **Browse** in the pop-up.
4. Select an image file in your local storage.

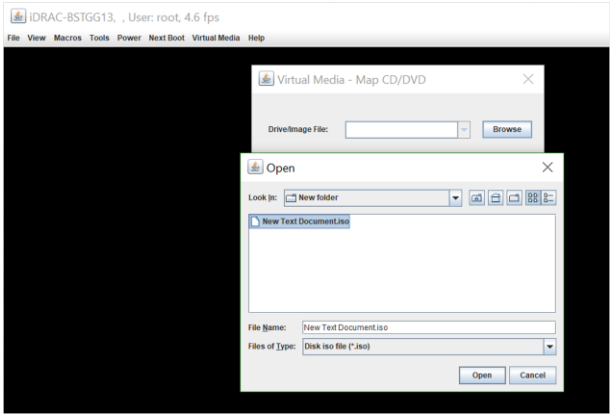

Figure 2-6 Open ISO File

5. Click **Open**
6. Click **Map Device** in the pop-up.
   The selected image file will be mapped to CD/DVD.
7. Click **Next Boot**, and then select **Virtual CD/DVD/ISO**.

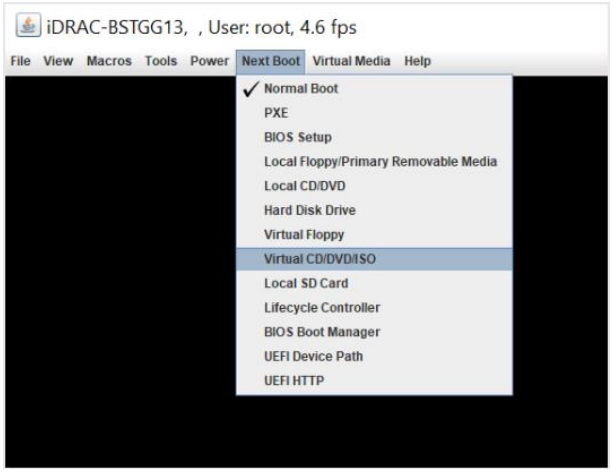

Figure 2-7 Set Reboot Mode

8. Click **Power**, and then select **Reset System (warm boot)**.

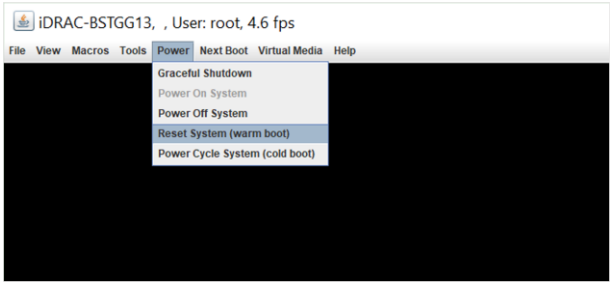

Figure 2-8 Reset System

The operating system will be installed automatically.

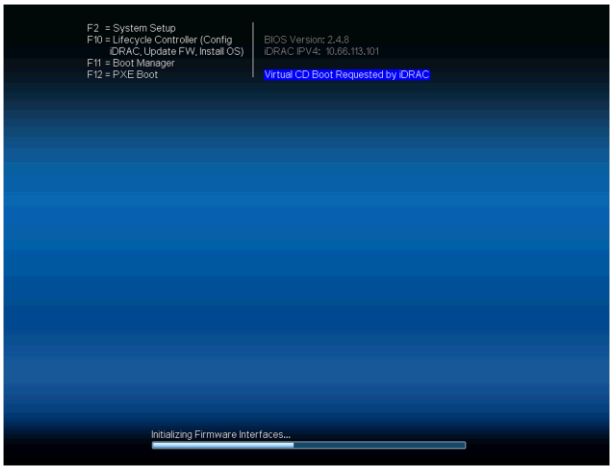

Figure 2-9 Boot by Virtual ISO

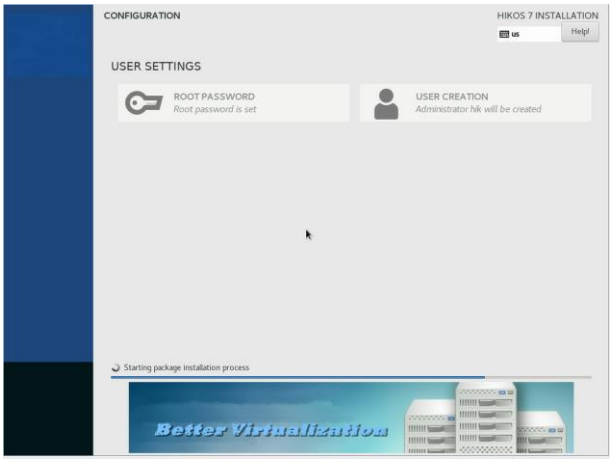

Figure 2-10 Install OS

Chapter 3 LIGHTSYSTEM Installation (Optional)

LIGHTSYSTEM software is installed automatically during the process of OS installation. You can log in to the web interface of intelligent fusion server via its IP address. Hereinafter the manual installation and uninstallation of LIGHTSYSTEM software are introduced.

3.1 Install LIGHTSYSTEM

Steps

1. Enter ***cd /opt***, and press **Enter**.
2. Enter ***ls***, and press **Enter**.

Figure 3-1 Run Installation File

Note

If the software is disable to function, enter ***chmod +x DC_LIGHTSYSTEM****** to authorize the software.

3. Enter ***./DC_DC_LIGHTSYSTEM_******, and press **Enter**.

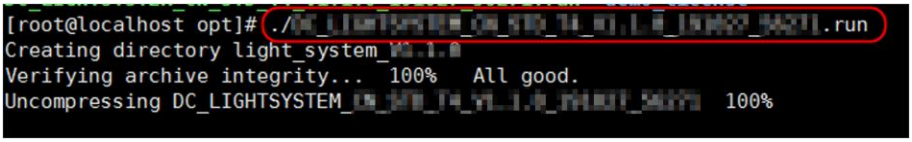

Figure 3-2 Install Software

Note

- Replace *** with the actual name of installation package.
- It takes a while to install, and the server will restart after the process completed.

3.2 Uninstall LIGHTSYSTEM

Steps

1. Enter ***cd /opt***, and press **Enter**.
2. Enter ***ls***, and press **Enter**.

Figure 3-3 Run Uninstall File

Note

If the software does not function, enter ***chmod +x DC_LIGHTSYSTEM****** to authorize the software.

3. Enter ***./DC_DC_LIGHTSYSTEM_*** run uninstall***, and press **Enter**.

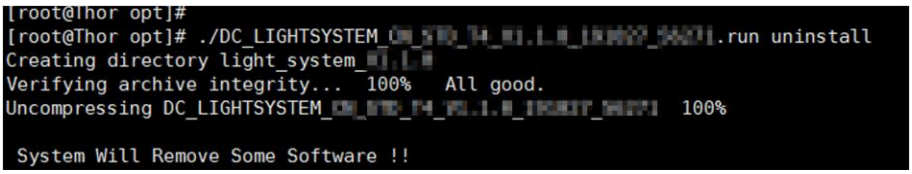

Figure 3-4 Uninstall Software

Note

- Replace *** with the actual name of installation package.
- The micro video cloud will also be uninstalled during this process.
- It takes a while to uninstall, and the server will restart after the process completed.

Chapter 4 Micro Video Cloud Installation (Optional)

Micro video cloud is installed automatically during the process of OS installation. You can log in to the web interface of intelligent fusion server via its IP address. Hereinafter the manual installation and uninstallation of micro video cloud are introduced.

4.1 Install Micro Video Cloud

Before You Start

Ensure an SSH tool is installed, such as Xshell.

Steps

1. Open Xshell tool, enter ***ssh IP 2343*** and press **Enter**

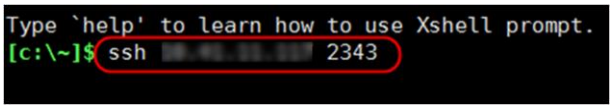

Figure 4-1 Set SSH Connection

Note

IP refers the actual IP address of your device.

2. Enter ***root*** as user name, and enter your password.
3. Enter ***cd /yunstorage***, and press **Enter** to enter **/yunstorage** folder.
4. Enter **rm –rf *** to clear the folder out.
5. Enter **cd /opt**, and press **Enter**.
6. Enter **./DC_LIGHTSYSTEM_*.run –noexec**, and press **Enter** to decompress the file.

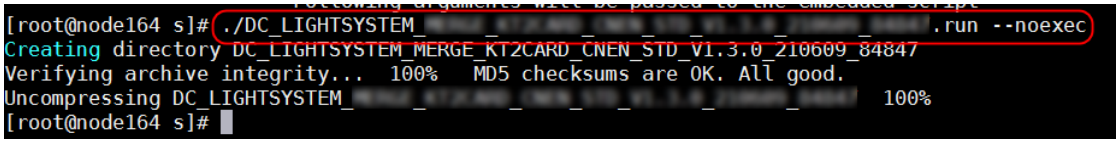

Figure 4-2 Decompress File

7. Enter **cp * /yunstorage**, and press **Enter** to copy the decompressed files to **/yunstorage** directory.
8. Enter **cd /yunstorage**, and press Enter.
9. Enter **chmod 755 ***, and press **Enter** to authorize.

Note

Replace ***yunstorage*** with the actual directory name of the installation package.

4. Enter ***./install.sh***, and press **Enter**.

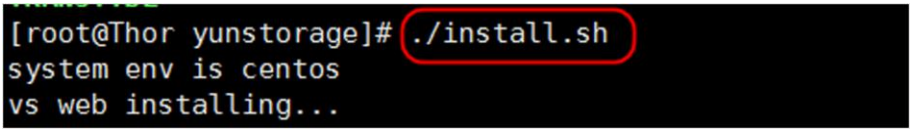

Figure 4-3 Install Script

4.2 Uninstall Micro Video Cloud

Uninstall micro video cloud before re-installation.

Steps

1. Open Xshell tool, enter ***ssh IP 2343***, and press **Enter**.

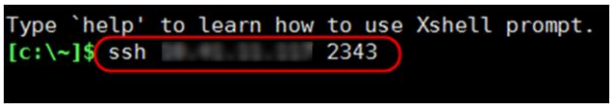

Figure 4-4 Set up ssh Connection

Note

IP refers the actual IP address of your device.

2. Enter ***root*** as user name, and enter your password.
3. Enter ***cd /yunstorage***, and press **Enter**.

Figure 4-5 Check Uninstallation Script

4. Enter ***/b_iscsi/bn_cli/resolve_bios *** bin***, and press **Enter** to uninstall script.

Figure 4-6 Uninstall Script

Note

- Replace ********* with the actual name of the script.
- Press **Tab** to obtain system command prompt.

Chapter 5 Activation and Login

5.1 Tools Preparation

- SADP Software.
- Xshell.
- Java Environment (JER 1.8 or above version).

5.2 PC Requirements

You can get access to the server by IE browser. The requirements for your PC are shown as below.

Table 5-1 PC Requirements

Operating System	CPU	Memory	Resolution	Browser
Microsoft Windows 7, Microsoft Windows 10	Intel® Pentium IV 3.0 GHz or more advanced version	1 GB or larger	1024 × 768 or higher	IE8 to IE11

Note

The interface varies from version to version.

5.3 Activation

The server is available only after being activated.

5.3.1 Activate via SADP Software

Before You Start

- Obtain and install SADP software.
- Your PC should be in the same subnet with the device.

Steps

1. Run the SADP software.

Note

The IP address is set as 192.168.1.64 by default.

The server will search all online devices in the same subnet. Detailed information such as device type, IP address, activation status and device serial number.

2. Select the desired device, set your password in **Activate Device** and click **Activate**.

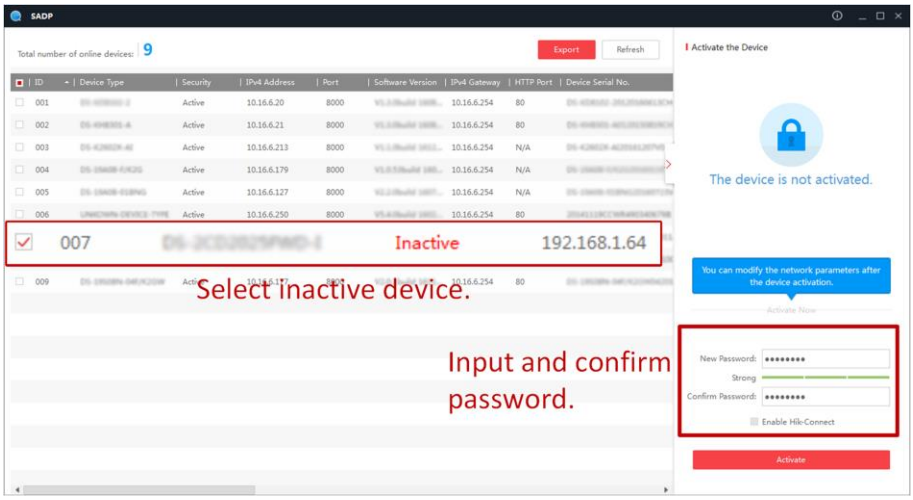

Figure 5-1 Activate via SADP Software

Note

- We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.
- We recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

The **Activation Status** will change to be **Activated** after the device is activated.

3. Modify network parameters of the device.
   1) Select an activated device, and enter information such as **IP Address**, **Subnet Mask** and **Gateway** in the **Modify Network Parameter**.
   2) Enter your password and click **modify**.
   The prompt information of "Network parameters modified." indicates that those settings will take effects.

5.3.2 Activate via Web Browser

The device can be activated via Web browser. The default IP address is 192.168.1.64.

Before You Start

- Make sure your PC connects to the Internet.

- Modify the IP address of your PC to make sure the PC and the server are in the same subnet.

Steps

1. Double click the IE browser and enter the default IP address (192.168.1.64) of the server.
2. Press **Enter** to enter the activation interface.

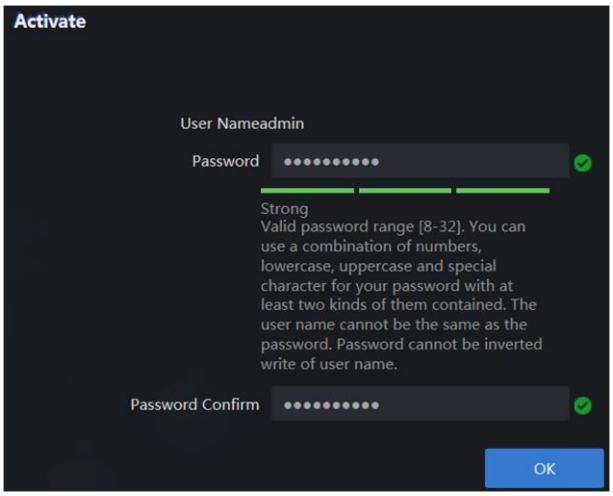

Figure 5-2 Activation Interface

Note

The password of root user will be changed when the activation password is set. As a result, the password of root user will be the same as that of admin user.

3. Enter password and confirm.
4. Click **OK**.

5.3.3 Import Authorization File

All-in-one devices are equipped with the authorization file by default. For those devices which are installed with a new OS, it is necessary to import an authorization file manually for normal operation. Contact our technical support staff for authorization file application.

The system goes to the authorization interface after activation. Move the mouse to **Operation**

guide, and follow the steps to import the authorization file.

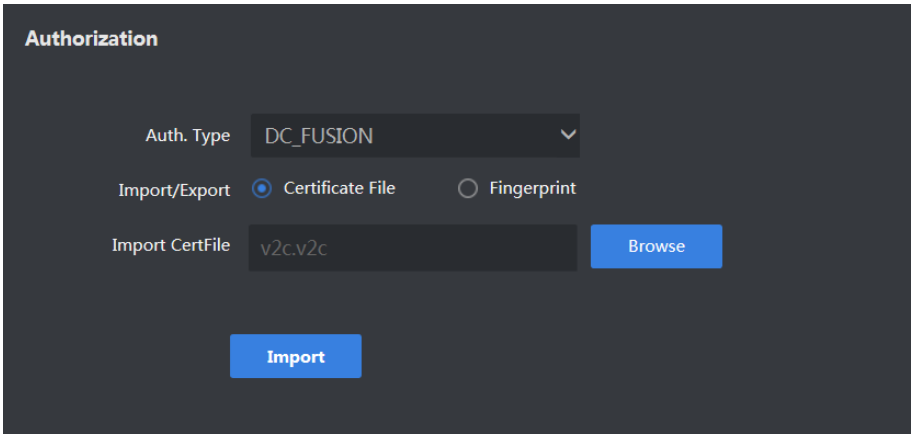

Figure 5-3 Import Authorization File

5.4 Log In

You can get access to the server by web browser.

Note

You shall acknowledge that the use of the product with Internet access might be under network security risks. For avoidance of any network attacks and information leakage, please strengthen your own protection. If the product does not work properly, please contact with your dealer or the nearest service center.

Steps

1. Open Web browser, enter the IP address of the server and then press **Enter**.

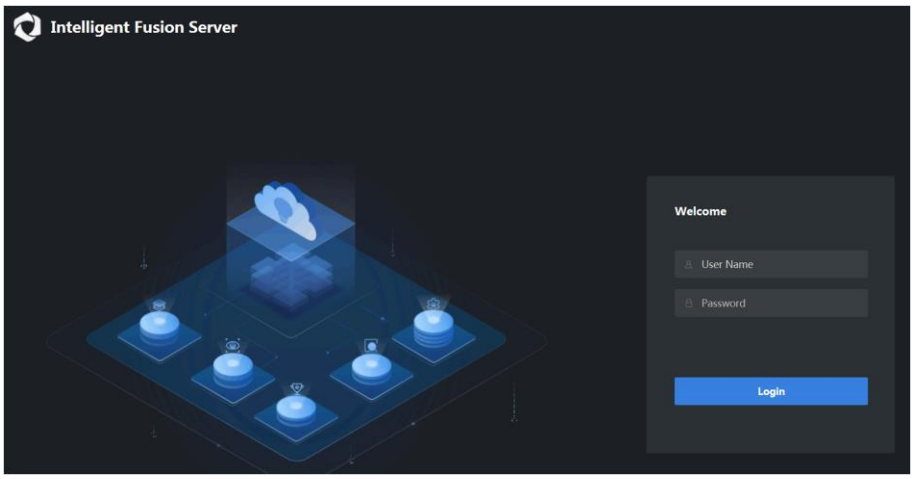

Figure 5-4 Login Interface

2. Enter **User Name** (admin) and **Password** (set for activation).
3. Click **Login**.

Note

- If the server is inaccessible, go to **Internet Options** → **Advancement**, check **Enable TLS1.1** and **Enable TLS1.2**.
- The specific interface varies from product to product.

Chapter 6 Configuration Wizard

6.1 Configure IP Address

Configure the IP address of the server to make it connectable to on-site devices.

Steps

1. Execute the command of ***ifconfig*** to check the network card.

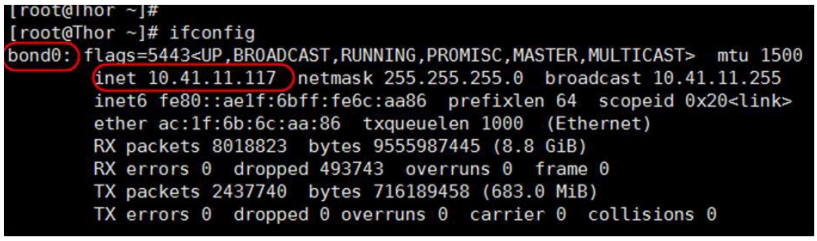

Figure 6-1 Check Network Card

2. Execute the command of ***cd /etc/sysconfig/network-scripts*** to enter the directory of network card configuration files.
3. Execute the command of ***ls*** to check the configuration file of network card.

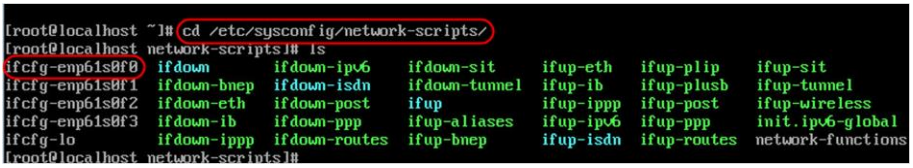

Figure 6-2 Check Network Card Configuration File

4. Execute the command of ***vim ifcfg-****.

Note

Replace ***** with the actual name of the default network card.

Example

You can enter ***vim ifcfg-enp61s0f0***.

5. Press **I** to enter the editable mode, and configure your network parameters.
   - BOOTPROTO: enter ***static***.
   - IPADDR: enter the actual IP address of the server.
   - PREFIX: set as ***24***.
   - GATEWAY: enter the actual gateway address of the server.

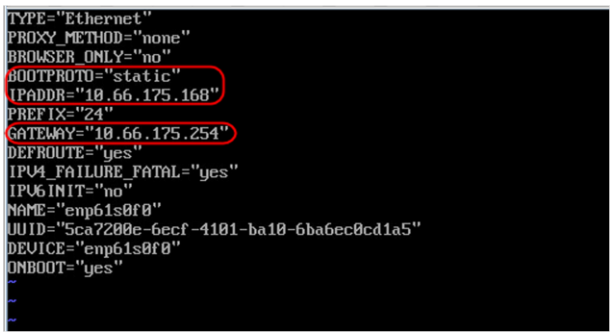

Figure 6-3 Edit Network Parameters

6. Press **Esc** to exit the editable mode.
7. Execute the command of ***:wq*** to save the changes and exit the configuration file.
8. Execute the command of ***reload_NetworkManager*** to restart network service.

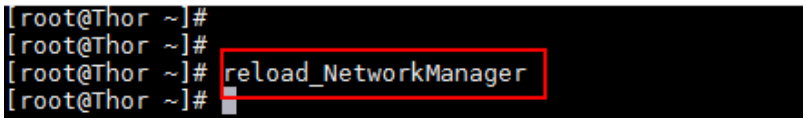

Figure 6-4 Reboot Network Service

9. Optional: Execute the command of ***ifconfig*** to check network parameters of the device.

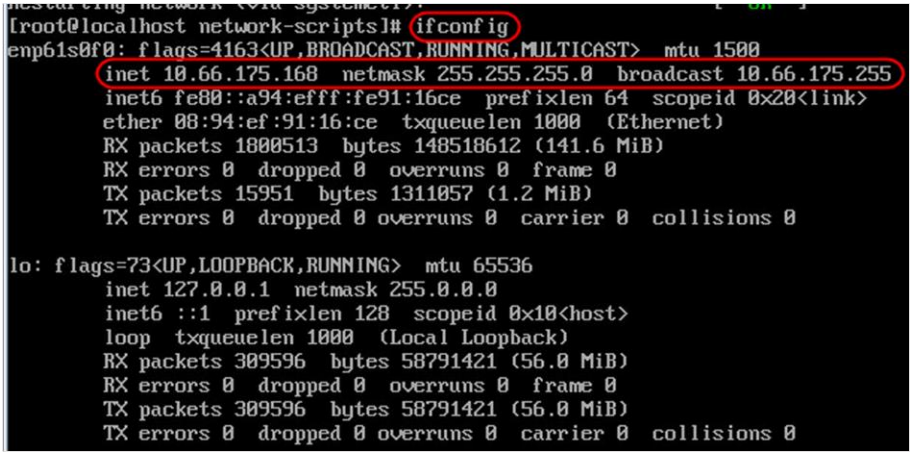

Figure 6-5 Check Device Network Parameters

What to do next

After the IP address is modified, you can manage the server through X-shell, X-ftp or Web browsers.

6.2 Deploy Micro Video Cloud

Micro video cloud is used to store human face pictures and uploaded videos.

6.2.1 Create Micro Video Cloud Cluster

Note

The nodes that create micro video cloud cluster should be the same with that of creating analysis cluster. Otherwise, exception may occur.

Steps

1. Enter ***https://IP:5120*** in IE browser, and press **Enter** to enter the platform.

   Note

   IP refers the actual IP address of the device.

2. When logging in for the first time, you should set the password of administrator and create an account.

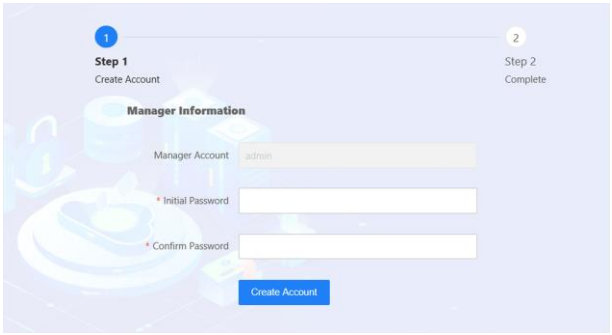

Figure 6-6 Create Account

3. Enter user name (admin) and the activation password, and click **Login**.

Figure 6-7 Log In

Note

Hereinafter this interface will be referred as 5120 interface.

4. Click **Build**.

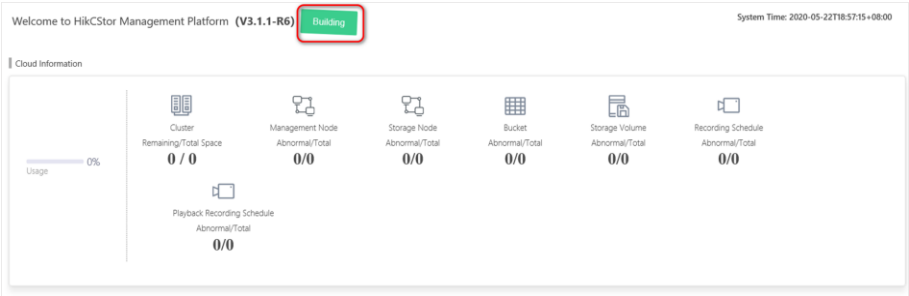

Figure 6-8 Build Cluster

Note

- A stand-alone micro video cloud: 1 node.
- A cluster of micro video cloud: 2 to 5 nodes.
- Select a deployment mode according to your actual needs.

Create Stand-alone Micro Video Cloud

Steps

1. Select **Standalone**, and click **OK**.

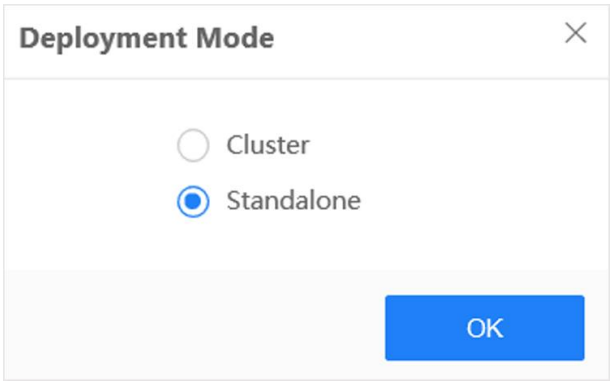

Figure 6-9 Select Deployment Mode_Standalone

The cluster will be created automatically.

2. Optional: Edit cluster information as needed.

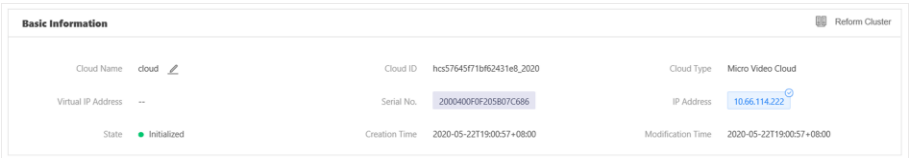

Figure 6-10 Edit Basic Information_Standalone

Note

Restart the device and deploy the resource again if the creation fails.

Create Cluster Micro Video Cloud

Steps

1. Select **Cluster**.

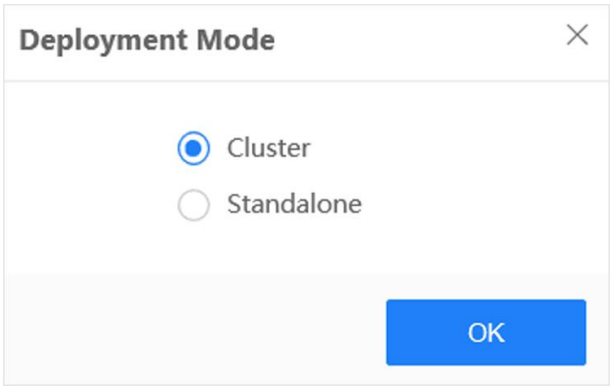

Figure 6-11 Select Deployment Mode_Cluster

2. Add management nodes.

Note

Management node refers to those devices which are used to create micro video cloud cluster.

1) Enter the IP address of each node.
2) Click **Detect and add**.
3) Repeat the steps above to add more nodes.

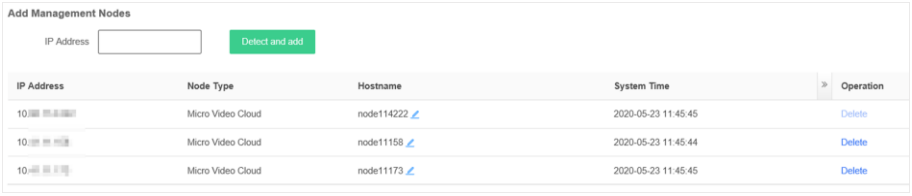

Figure 6-12 Add Management Nodes_Cluster

3. Add storage nodes.
   1) Click **Download Template**.
   2) Open the file, and enter all the IP addresses of nodes.

Note

The IP address should be entered as the format of IP-IP.

Example

10.41.63.77-10.41.63.77
10.41.63.207-10.41.63.207
10.41.63.208-10.41.63.208

3) Save the file to your local storage.
4) Click **Select** to upload the file.

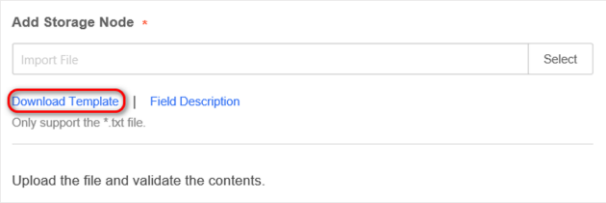

Figure 6-13 Add Storage Node_Cluster

4. Add cluster information.
   1) Enter an unused IP address on the same subnet of your device in **Virtual IP**.
   2) Click **Detect** to test whether it is accessible.
   3) Enter **Cloud Name** as needed.

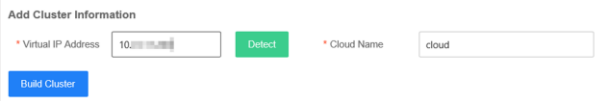

Figure 6-14 Add Cluster Information

5. Click **Build Cluster**.
   The cluster will be created automatically.

6.2.2 Create Domain

Domain refers to a cluster of multiple storage devices.

Steps

1. Go to **Resource** → **Domain**.
2. Click **Create**.

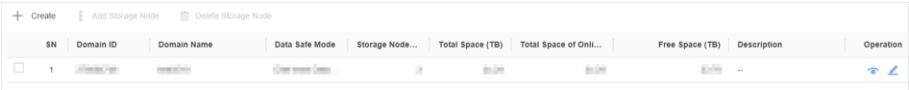

Figure 6-15 Create Domain

3. Configure domain parameters.
   1) Enter a name in **Domain Name**.
   2) Select a **Data Safe Mode**.

Device-level Data Safe

Data will be stored in multiple devices.

Disk-level Data Safe

Data will be stored in a single device.

3) Optional: Enter desired information in **Description**.

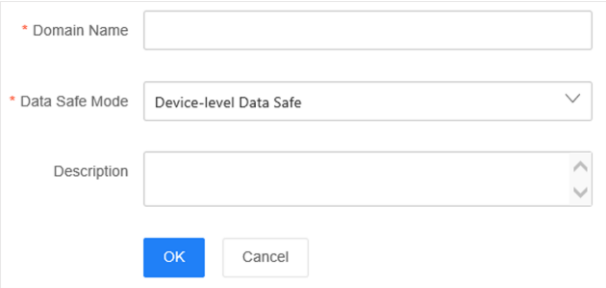

Figure 6-16 Configure Domain Parameters

4. Click **OK**.
5. Click **Storage** to format storage volume and memory volume.

Note

This step is necessary as the storage volume can not be directly applied if the device has been deployed with micro video cloud before.

6.2.3 Add Storage Node to Domain

Steps

1. Check the desired domain, and click **Add Storage Node**.

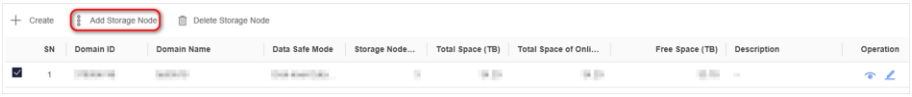

Figure 6-17 Add Storage Node to Domain

2. Check the desired storage nodes, and click **OK**.

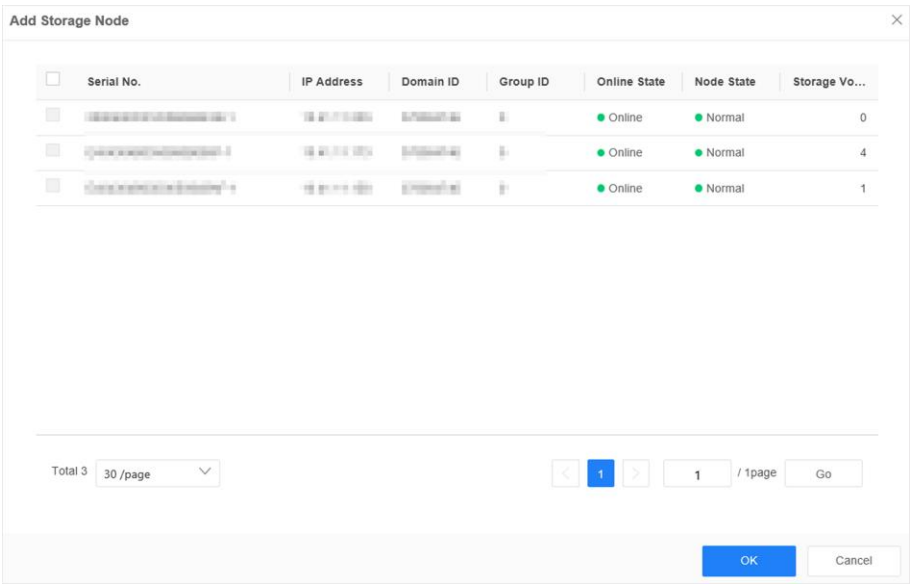

Figure 6-18 Check Desired Storage Nodes

The selected nodes will be added to the domain automatically.

6.2.4 Create Bucket

The bucket refers to the storage space allocated for users. It is required to create 3 buckets for storing list pictures, captured pictures and videos respectively.

Before You Start

Ensure that the device has never been installed with micro video cloud before. Otherwise, you need to format the storage volume first.

Steps

1. Go to **Resource** → **Bucket**.
2. Click **Create Bucket**.

Figure 6-19 Create Bucket

3. Configure general information.
   1) Select a desired domain name.
   2) Enter a unique bucket name.

> **Note**
>
> Digits only.

   3) Select **admin** as **User Name**.

4) Set **Redundancy Level** as ***2+1:1***.
5) Set the storage space of bucket as **Capacity** according to actual condition.

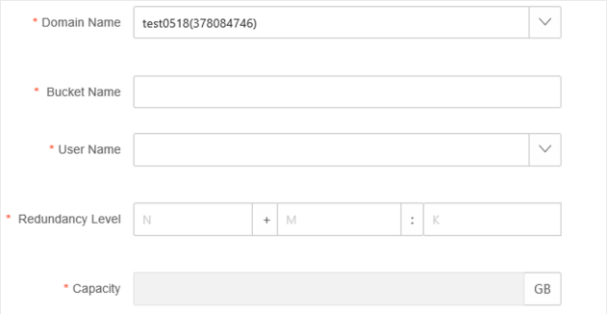

Figure 6-20 Configure Bucket Parameters

4. Select a coverage strategy according to actual condition.

Not Overwrite

Under this strategy, the data will not be overwritten when the storage is full. But related functions will not be accessible.

Capacity Overwrite

Under this strategy, the earliest data will be overwritten by the latest data when the storage is full.

Period Overwrite

Under this strategy, the earliest data will be overwritten by the latest data according to the period set.

Note

Please ensure that the storage space is sufficient during the period you set.

Note

The configuration of **Coverage Strategy** varies from different buckets. Please refer to ***Create Static Pool***, ***Create Dynamic Pool***, and ***Create Video Pool*** for further information.

Create Static Pool

Static pool is used to storage human face picture of list library.

Before You Start

Ensure that the general parameters in ***Create Bucket*** have been configured.

Steps

1. Select **Not Overwrite** in **Coverage Strategy**.

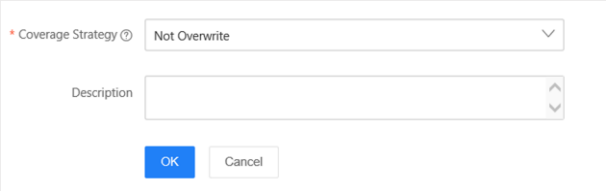

Figure 6-21 Select Coverage Strategy_Static Pool

2. Optional: Enter desired description.
3. Click **OK**.

Create Dynamic Pool

Dynamic pool is used to storage the human face pictures that are captured by the camera.

Before You Start

Ensure that the general parameters in ***Create Bucket*** have been configured.

Steps

1. Select **Capacity Overwrite** in **Coverage Strategy**.

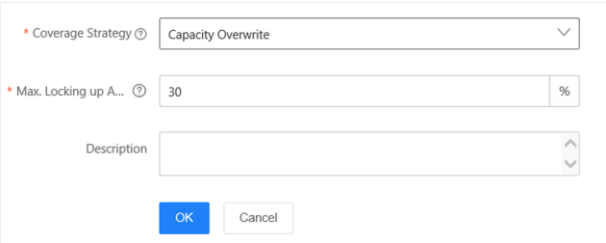

Figure 6-22 Select Coverage Stategy_Dynamic Pool

2. Set **Max. Locking up Attempts**.

Note

The reserved ratio of storage space.

Example

If you enter ***10***, 10 percent of storage space will be reserved. When the other 90 percent of storage space is occupied, the storage will be in a full status.

3. Optional: Enter desired description.
4. Click **OK**.

Create Video Pool

Video pool is used to storage video files that are manually uploaded.

Before You Start

Ensure that the general parameters in ***Create Bucket*** have been configured.

Steps

1. Select **Capacity Overwrite** in **Coverage Strategy**.

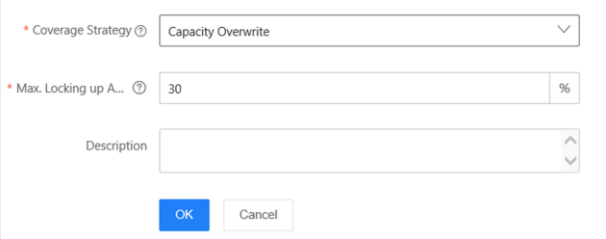

Figure 6-23 Select Coverage Stategy_Video Pool

2. Set **Max. Locking up Attempts**.

Note

The reserved ratio of storage space.

Example

If you enter ***10***, 10 percent of storage space will be reserved. When the other 90 percent of storage space is occupied, the storage will be in a full status.

3. Optional: Enter desired description.
4. Click **OK**.

6.2.5 Add Micro Video Cloud

Steps

1. Enter ***https://IP***, and press **Enter**.

Note

IP refers the actual IP address of device.

2. Go to **System Management** → **System Config** → **Cloud Storage**.
3. Click **Add**.
4. Configure parameters of **Smart Storage Unit**.
   1) Enter a desired name.
   2) Enter an IP address in **Smart Storage Unit IP**.

Note

- For cluster micro video cloud, enter the virtual IP address.
- For stand-alone micro video cloud, enter the IP address of itself.

   3) Enter **Dynamic Resource Pool ID**, **Static Resource Pool ID**, and **Video Resource Pool ID**.

Note

- ID refers to the bucket name of each pool you set in ***Create Bucket***.
- Go to the homepage of micro video cloud platform, and go to **Resource** → **Bucket** to check bucket name.

4) Keep the default values of **Port** and **Download Port**.
5) Enter ***admin*** in **User Name**.
6) Enter the login password of micro video cloud platform in **Password**.
7) Click **User**, and click to download **Access Key** and **Secret Key**.

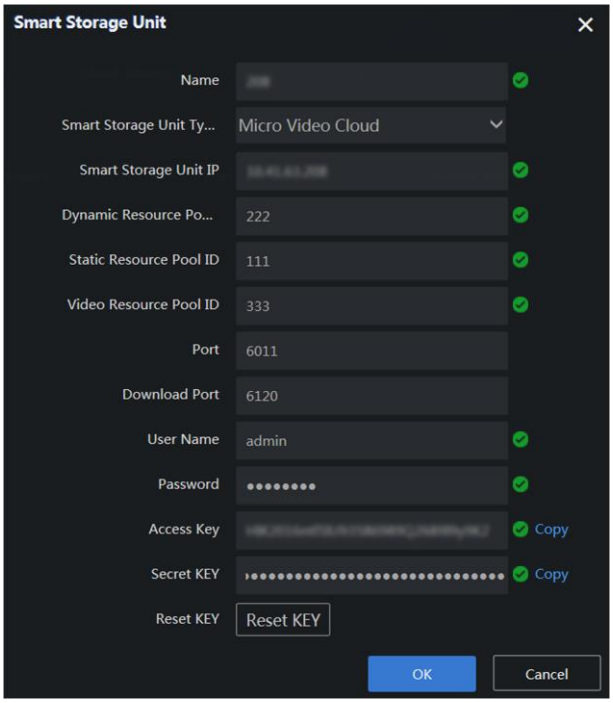

Figure 6-24 Add Smart Storage Unit

5. Click **OK**.


See Far, Go Further