Intelligent Micro Center Server

Deployment Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

This manual introduces the deployment of the server (hereinafter referred to as "the Server"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	February 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and car plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.

- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Transportation Requirements

Transport the server under allowed humidity and temperature conditions.

Storage Requirements

Store the server under allowed humidity and temperature conditions.

Installation Requirements

- Strictly comply with the local electrical safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the server.
- Do not expose the battery to environments with extremely low air pressure, or extremely high or low temperatures. Also, it is strictly prohibited for the battery to be exposed to extremely hot environments (such as direct sunlight or fire), and to cut or put mechanical pressure on the battery. This is to avoid the risk of fire and explosion.
- Use the standard power adapter. We will assume no responsibility for any problems caused by the use of a nonstandard power adapter.

- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Install the switch horizontally on a stable surface to prevent it from falling.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- Use power cords that conform to your local requirements, and are rated specifications.
- Before connecting the power supply, make sure the input voltage matches the server power requirement.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- Install the server in an area that only professionals can access.
- Extra protection is necessary for the device casing to reduce the transient voltage to the defined range.
- Install the device near a power socket for emergency disconnect.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.

Operation Requirements

WARNING

- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- The device is heavy and needs to be carried by several persons together to avoid personal injuries.

- Make sure that the power supply is correct before use.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drip or splash liquid onto the device, make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.
- Your configurations will be lost after performing a factory reset. Please be advised.
- Do not restart, shut down or disconnect the power to the device during an update.
- Make sure the update file is correct because an incorrect file can result in a device error occurring.
- The system cannot upgrade different types of AI modules at the same time.
- Do not frequently turn on/off the device. Otherwise, the product life might be shortened.
- Back up important data on a regular basis when using the device.
- Operating temperature: 10 °C to 35 °C (50 °F to 95 °F).

Maintenance Requirements

WARNING

- Make sure you use the same model when replacing the battery to avoid fire or explosion. Dispose the battery strictly following the instructions.
- Power off the device before maintenance.

- AI module does not support hot plug. If you need to install or replace the AI module, unplug the device power cord first. Otherwise, it will lead to file damage on the AI module.
- The device casing provides protection for internal components. Use a screwdriver to loosen the screws before detaching the casing. Make sure to put the casing back on and secure it in its original place before powering on and using the device.
- Clean the ventilation pipe regularly to avoid obstructions.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the device, first disconnect the appliance coupler.

Table of Contents

1 Initialization

For baseline server, you need to insert the permanent dongle to the USB port of the server and change the IP address with your laptop.

- Modification of the network configuration is based on the configuration that the network cable is connected to the first port of the left. If the device on site connects only 1 network cable, we recommend connect the first port of the left.
- If you want to reinstalling the system, you can skip this chapter, and for more information see"4 Reinstalling Server".

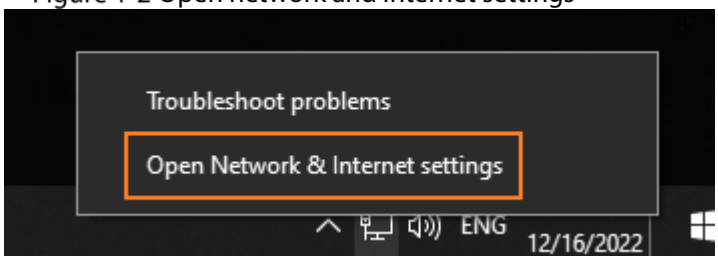
Step 1 Insert the permanent dongle to USB port of server.

Step 2 Connect the power supply and start up the server. Connect the laptop to the Ethernet port with network cable. We recommend you connect the network cable to the first port of the left side.

Step 3 Open the laptop, and then click the internet icon on the low right corner. Click **Open Network & Internet settings**".

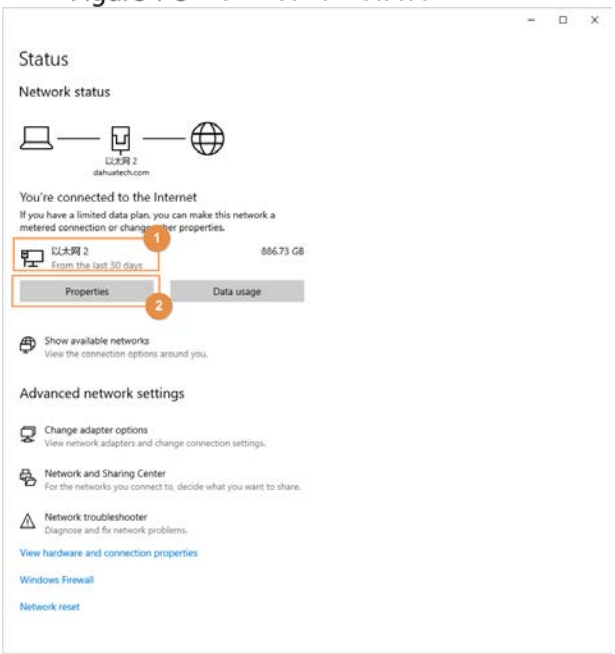
Figure 1-1 Internet icon

Figure 1-2 Open network and Internet settings



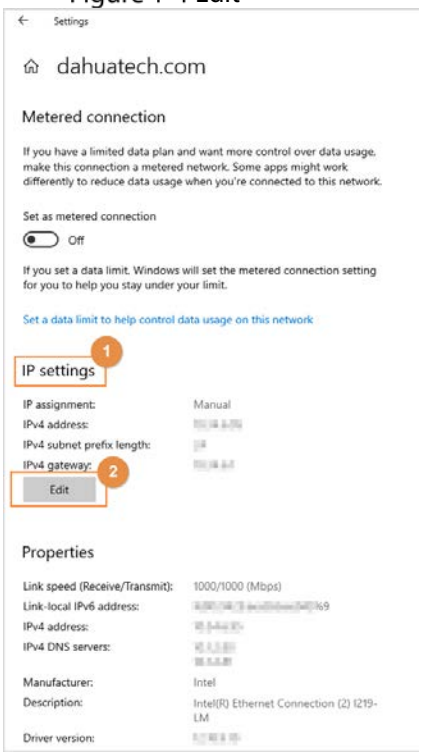
Step 4 On the **Open Network & Internet settings** page, click **Properties** of the online network connection.

Figure 1-3 View network status



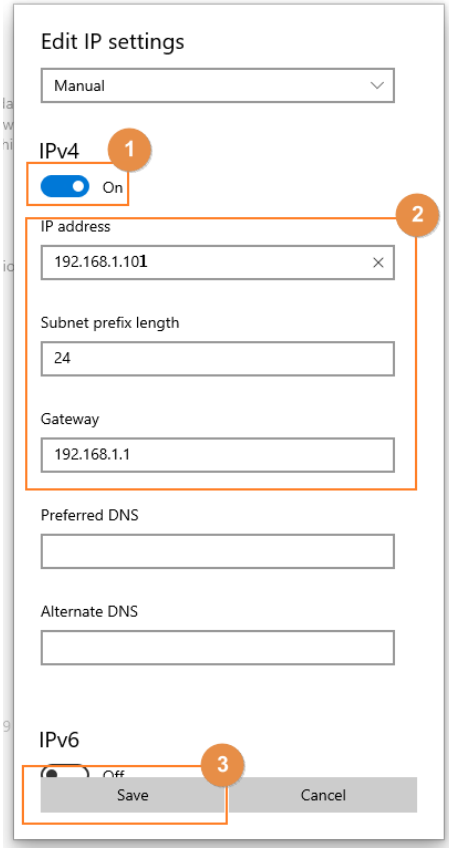
Step 5 On the **Open Network & Internet Settings** page, click **Edit**.

Figure 1-4 Edit



Step 6 In the pop-up window that appears, enable IPv4, and then change the IP address, Subnet prefix length and Gateway to 192.168.1.101, 24 and 192.168.1.1 respectively. Click **Save.**

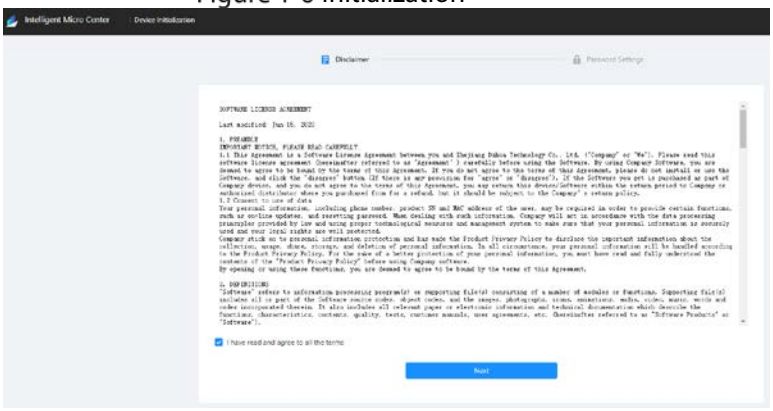
Figure 1-5 Edit IP settings



Step 7 Open the Chrome browser, enter the active IP address of the server (http://192.168.1.113 obtained in Step 5) in the address bar, and then press the Enter.

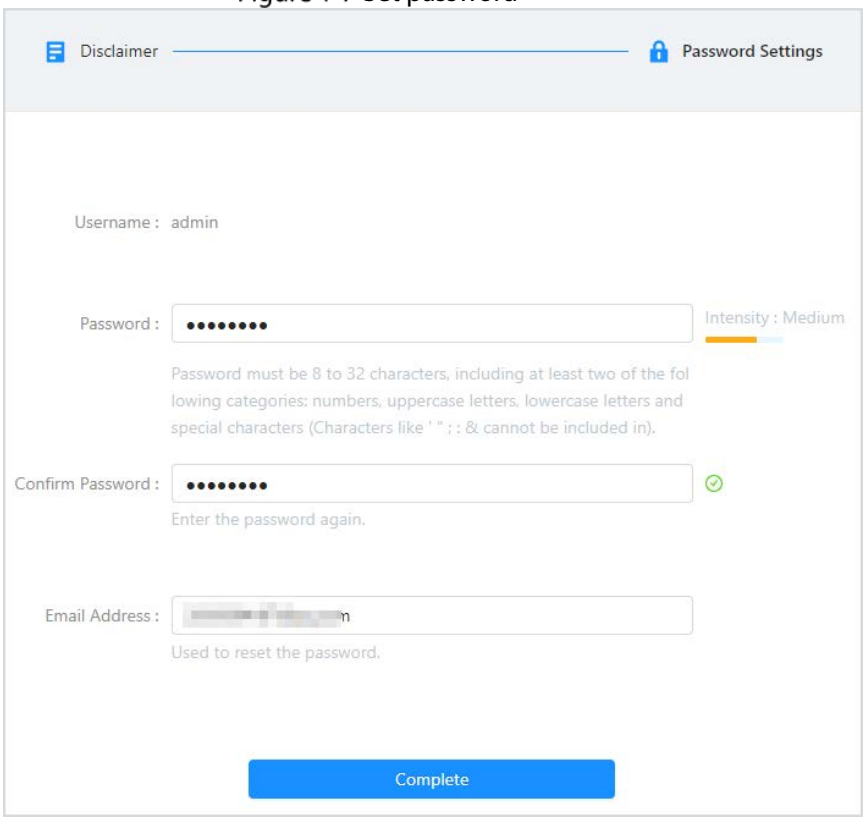
Step 8 Read the Software License Agreement and select I have read and agree to all the terms, and then click **Next**.

Figure 1-6 Initialization



Step 9 Configure and confirm the password, and then enter your email address, after that click **Complete**.

Figure 1-7 Set password



Step 10 Enter username and password, and then click **Login**.

Figure 1-8 Log in to the page

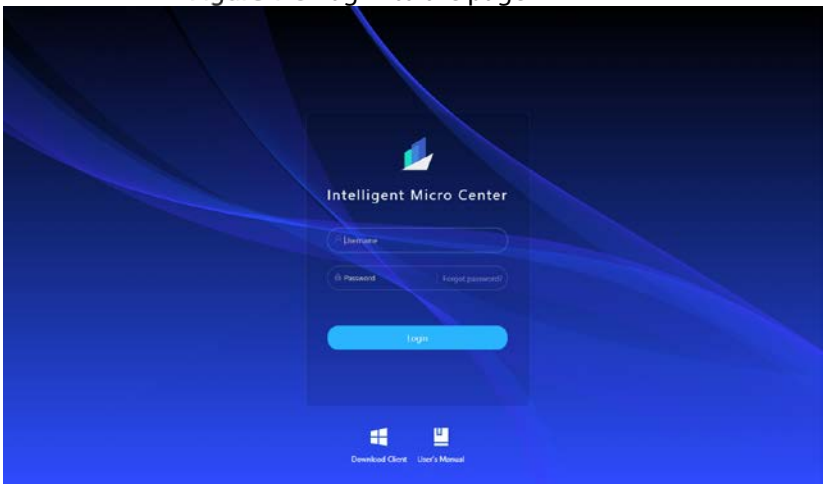
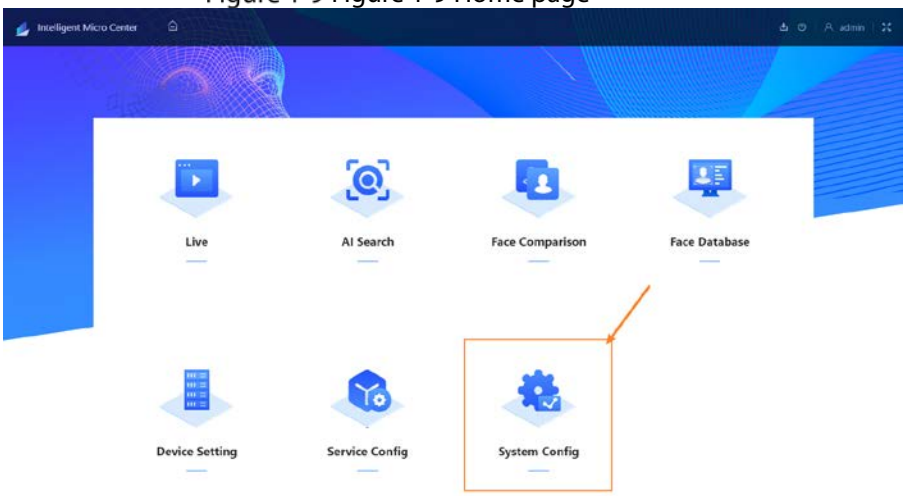
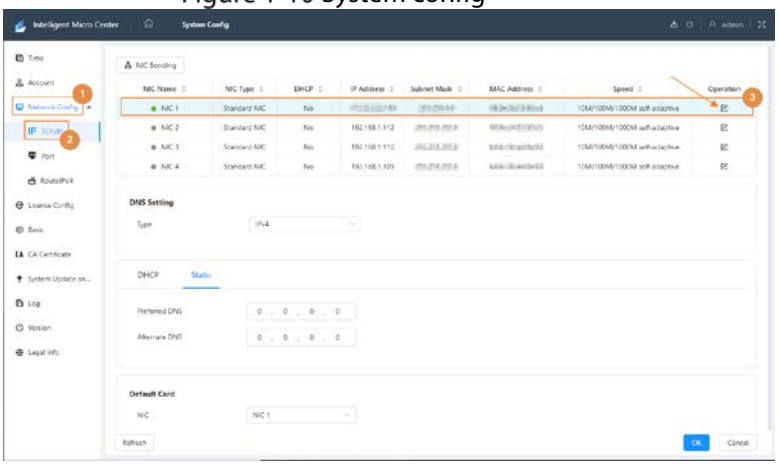


Figure 1-9 Figure 1-9 Home page



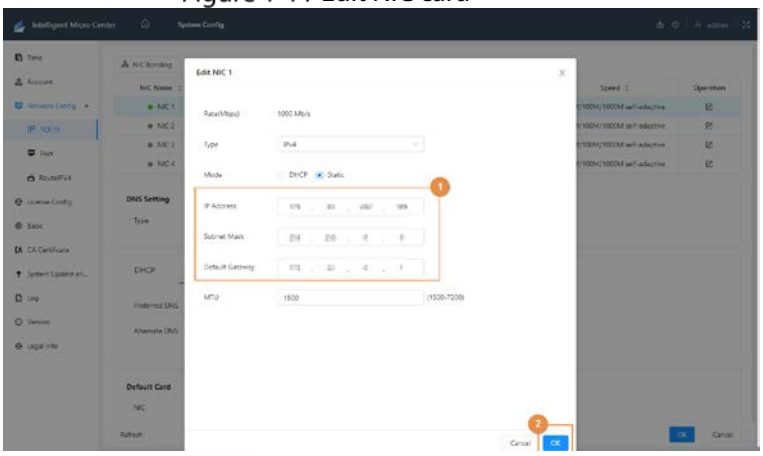
Step 11 On home page, select **System Config** > **Network Config** > **TCP/IP**, and then click corresponding to the active NIC card.

Figure 1-10 System config



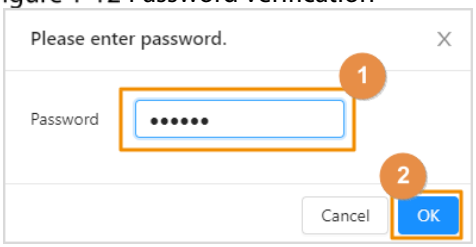
Step 12 Configure the IP address, subnet mask and gateway according to your actual needs, and then click **OK**.

Figure 1-11 Edit NIC card



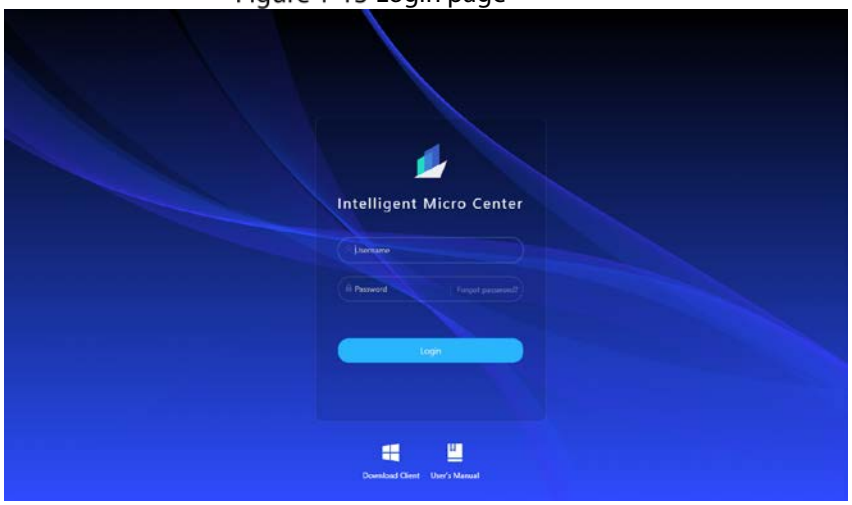
Step 13 Change the default NIC card to the active NIC card, of which the IP address has been edited before (If there are multiple active NIC cards, you can select any of the online NIC cards), and then click **OK**. Enter the login password and then click **OK** to save TCP/IP the configuration.

Figure 1-12 Password verification



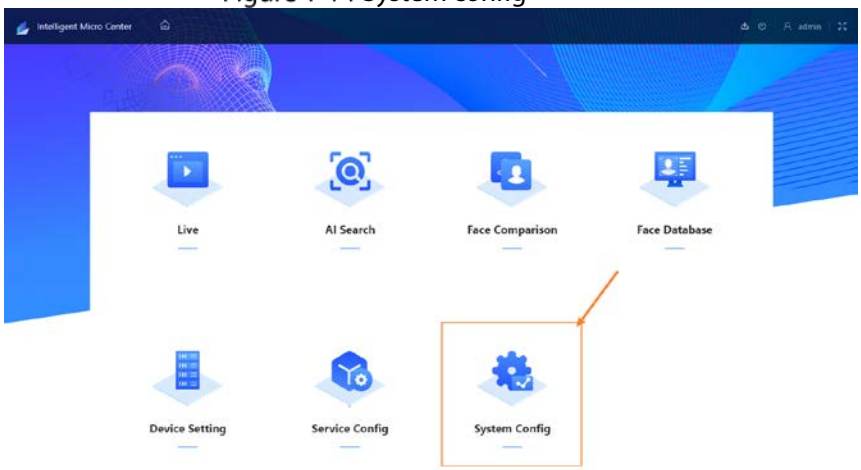
Step 14 After completing the NIC configuration, open the Chrome browser, and then enter the IP address (http:// *server IP*) in the address bar to enter Intelligent Micro Center.

Figure 1-13 Login page



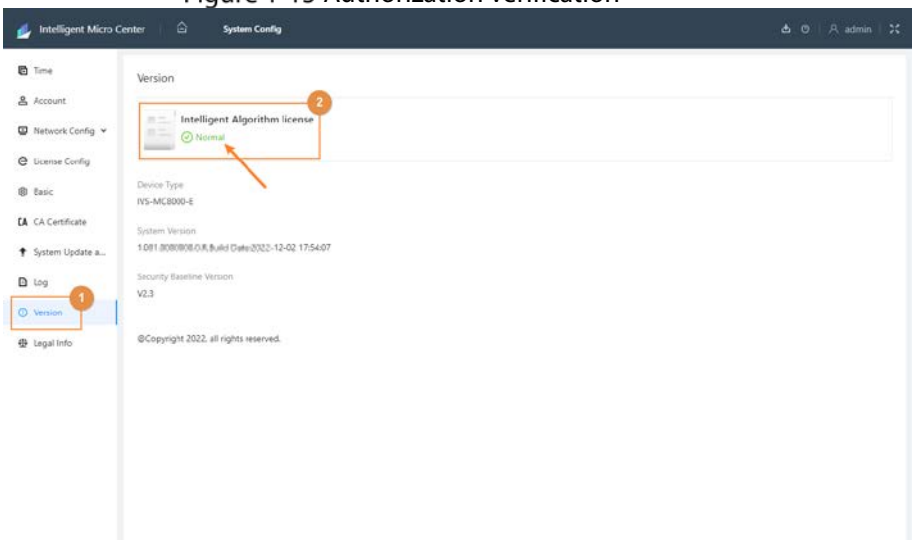
Step 15 Enter the username and password to log in to the Intelligent Micro Center webpage, and then click **System Config**.

Figure 1-14 System config



Step 16 Select **System Config** > **Version**. If the **Intelligent Algorithm License** displays **Normal**, it means the authorization has taken effect. For follow up operations, see "2 Service Status Verification".

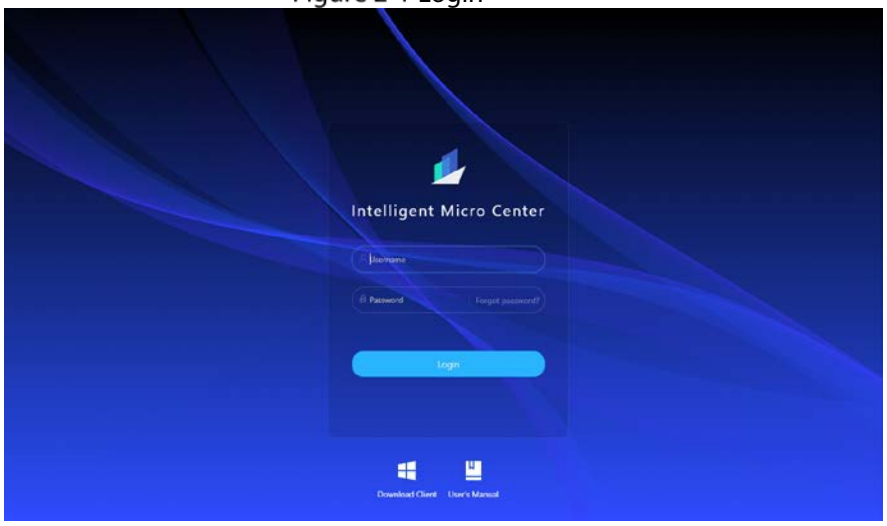
Figure 1-15 Authorization verification



2 Service Status Verification

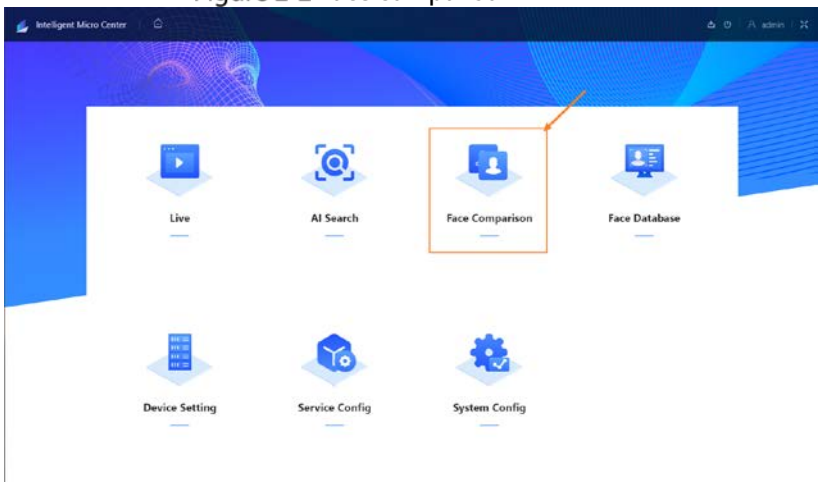
Step 1 Open the Chrome, and then enter http:// *server IP* in the address bar, and then press Enter. Enter the admin and its responding password to log in.

Figure 2-1 Login



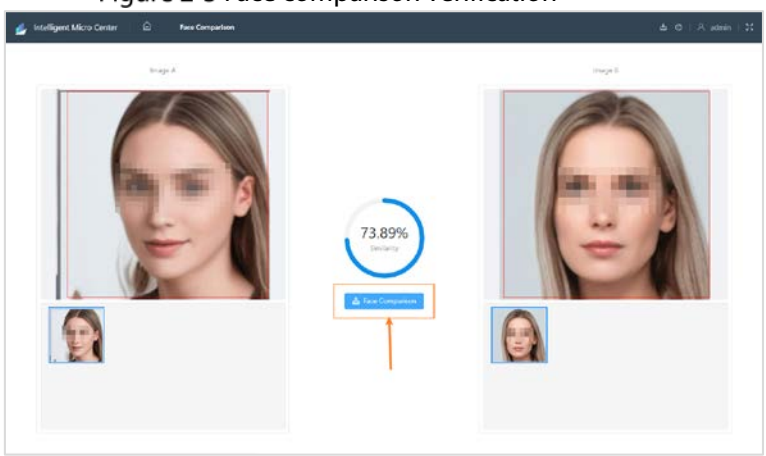
Step 2 On home page, click **Face Comparison**.

Figure 2-2 Face comparison



Step 3 On **Face Comparison** page, upload 2 face images and then click **Face Comparison**, if the similarity results are displayed, it means that the server is working normally.

Figure 2-3 Face comparison verification



3 (Optional) Program Update Guide

Intelligent Micro Center supports two update methods: web update and background update. You need to prepare the installation package before update. the file name varies with version and release date.

Step 1 Open the Chrome browser. Enter the http://*Server IP* in the address bar and then press Enter. Enter the username and password to login.

Figure 3-1 Login

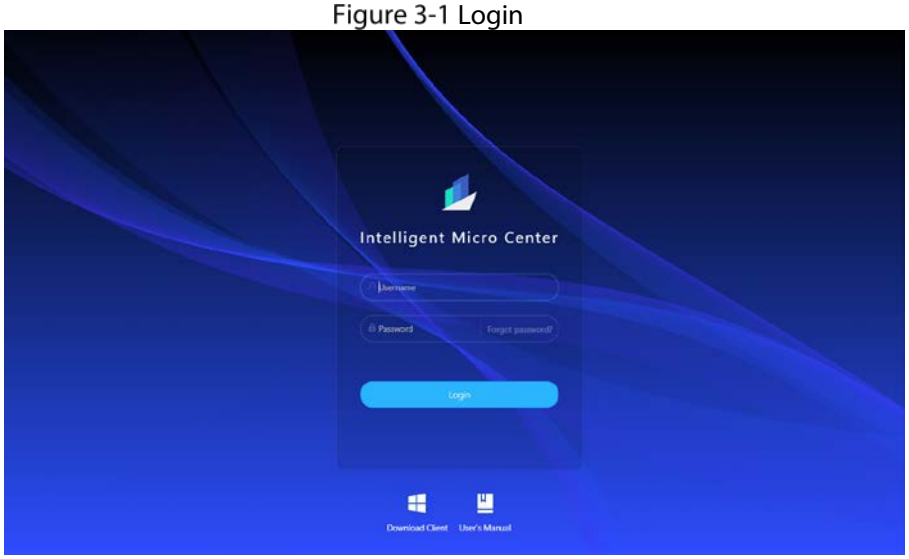
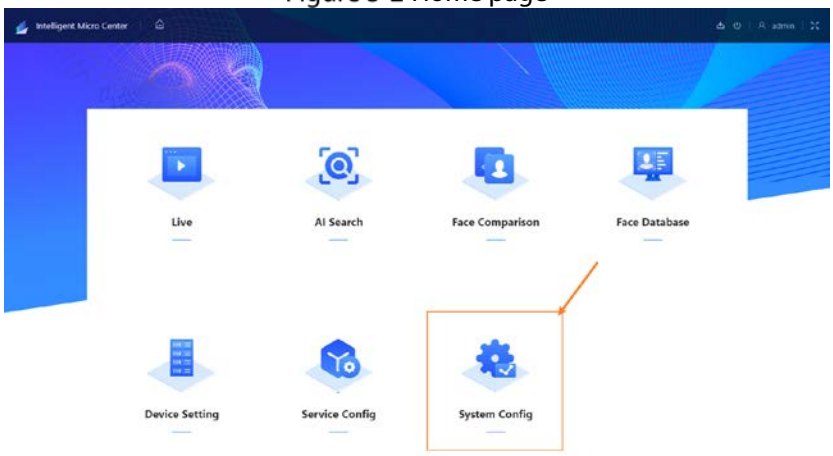
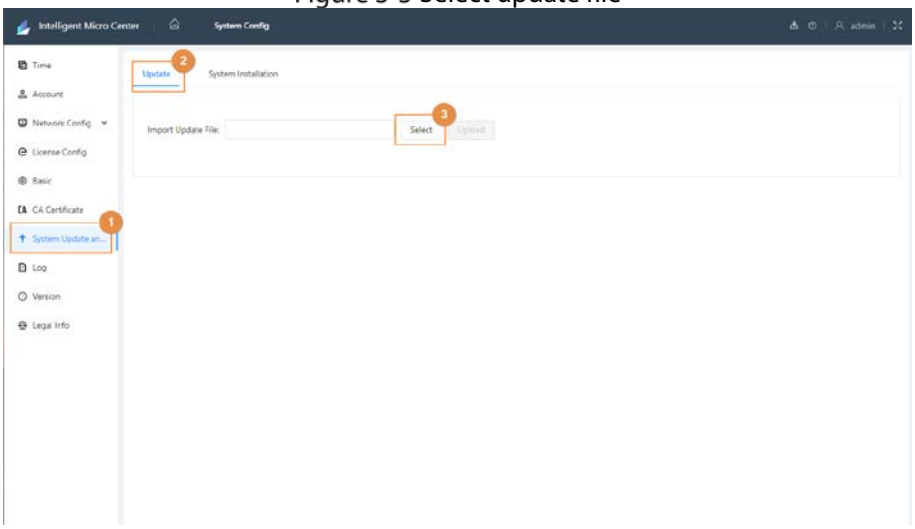


Figure 3-2 Home page



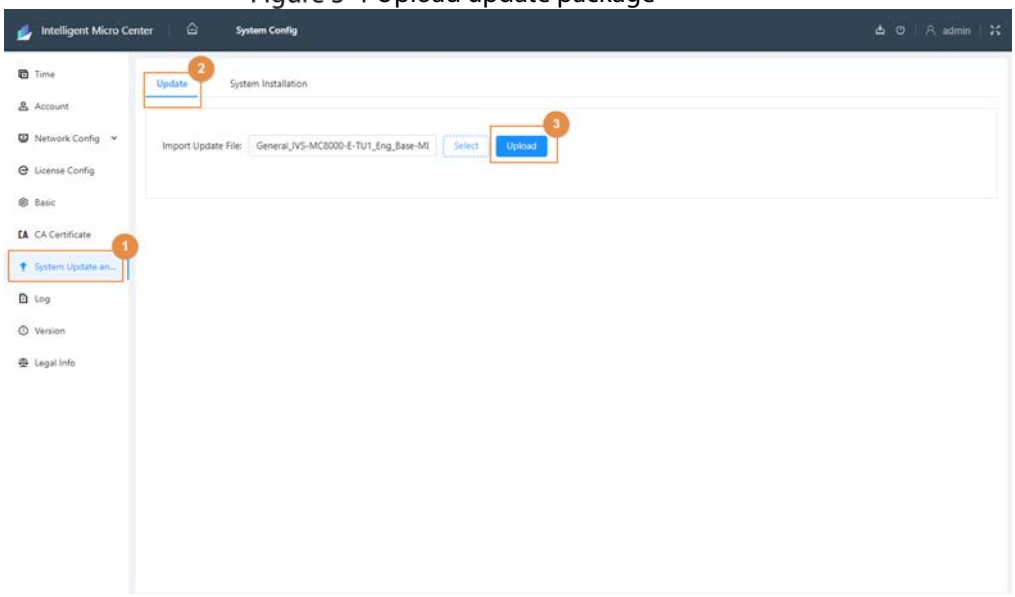
Step 2 Select **Systme Config** > **System update and installation** > **Update**, and then click **Select** to select the update file you need.

Figure 3-3 Select update file



Step 3 Click **Upload**.

Figure 3-4 Upload update package



Step 4 Enter the password, and then click **OK**. Click **OK** in the pop-up window to confirm update. When the process is 100%, the system will upload update file. The system will update automatically.

Figure 3-5 Confirm password

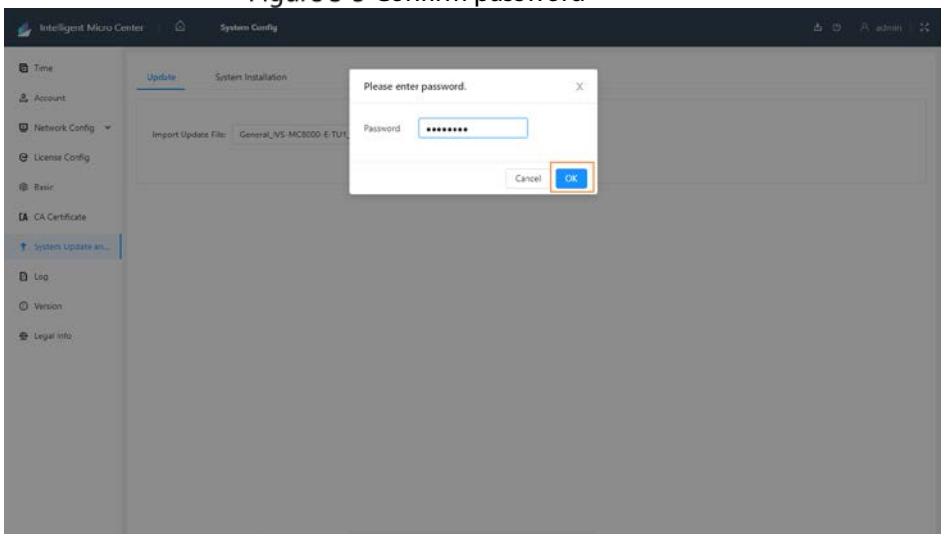


Figure 3-6 Confirm update

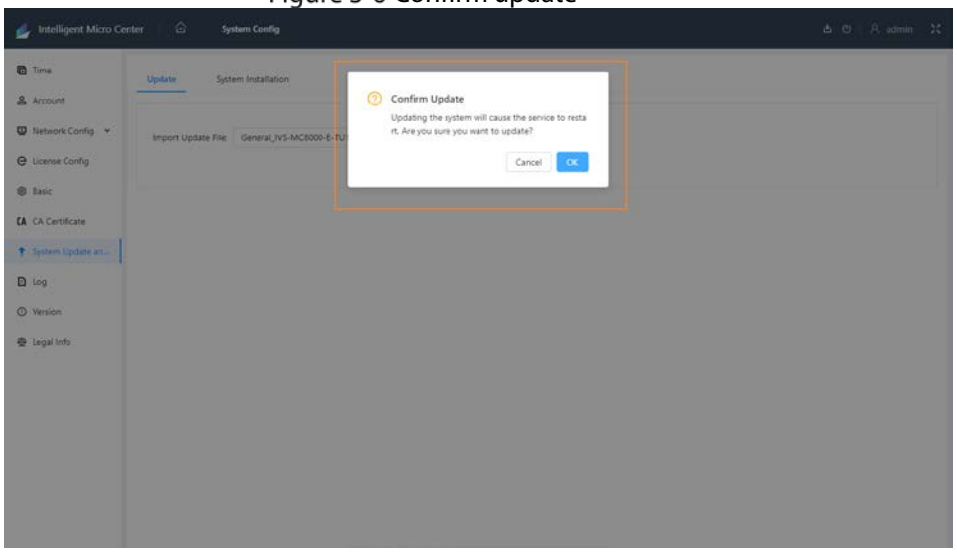


Figure 3-7 Upload update file

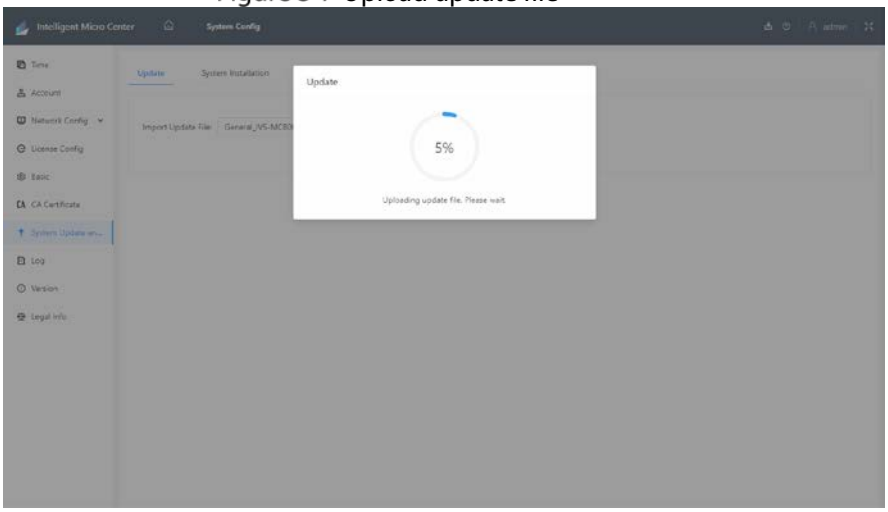
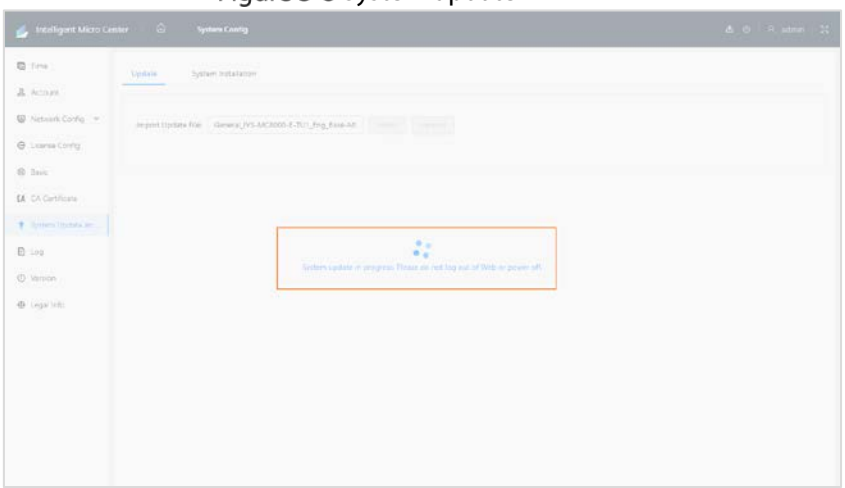
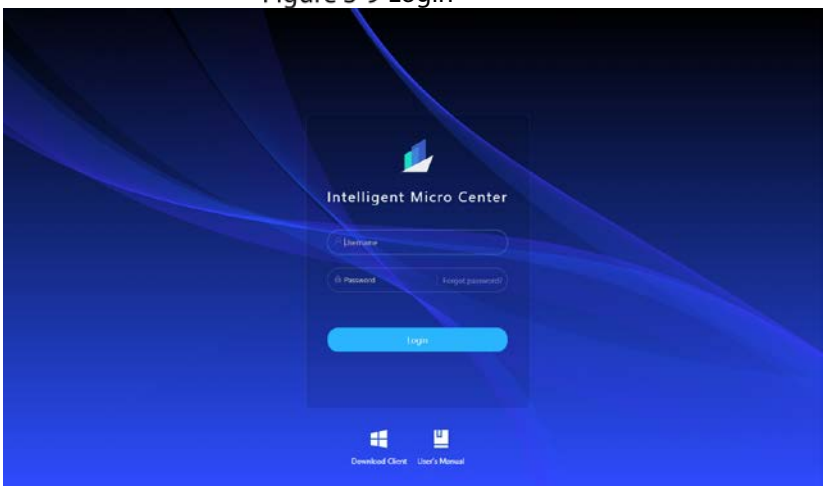


Figure 3-8 System update



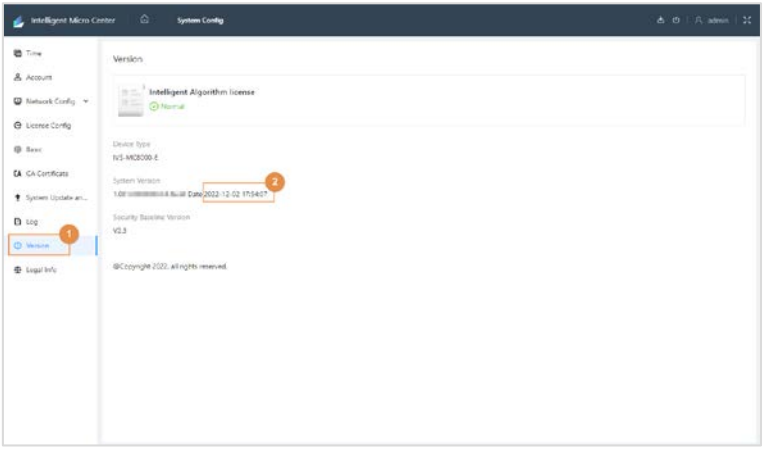
Step 5 After update, the system will restart and enter the login page automatically. Enter the username and password to login.

Figure 3-9 Login



Step 6 Select **System Config** > **Version** to check the version information.

Figure 3-10 Check the version information



4 Reinstalling Server

4.1 Before Deployment

Before deployment, you need to connect the server to the switch. If the device only connects 1 data cable, we recommend you connect the network cable to the first network port of the left. Meanwhile, prepare the devices needed and download packages from GDP.

4.1.1 Preparing Installation Package

Before deployment, you need to download the following packages from GDP.

- CentOS7.4 system one-click deployment mirror package
  CentOS-7-aarch64-Minimal-1708-Custom-v10-Base-221219.iso.
  GDP material No.: see the Release Notes.
  System disk: 1 USB flash drive (16 GB or above, 32 GB recommended).
- Basic Package
  File name:
  General_IVS-Centos-7-Aarch64-Base_7.4.1708-Atlas310-MD5-****_V1.***.*******.*.R.*****ta
  GDP material No: see the Release Notes.
- Patch package
  File name ： General_IVS-Centos-7-Aarch64-Base_7.4.1708-Atlas310-*****.***.*******.*.R.*****tagz
  GDP material No: see the Release Notes.
- Micro center program package
  File name:
  General_IVS-MC8000-E-TU1_Eng_Base-MD5-****_V1.***.*******.*.R.******.tar.gz
  GDP material No.: see the Release Notes.

Installation package name varies according to version and release date.

4.1.2 Configuration Requirements

Table 4-1 Configuration requirements

Parameter	Description
Operating System	CentOS 7.4
Kernel Version	4.18.0-147.8.1.el7.aarch64
CPU	FT-D2000
Intelligent Analysis Card	AIX3200

4.2 Installing CentOS System

Prepare a USB flash drive to install the CentOS system to the server.

4.2.1 Preparing the USB Flash Drive

Prerequisites

- Prepare 1 USB flash drive (8 GB or larger size, 16 GB recommended).
- Prepare 1 computer or laptop and the UltraISO tool has been installed in advanced.
- Prepare Centos7.4 system mirroring package.

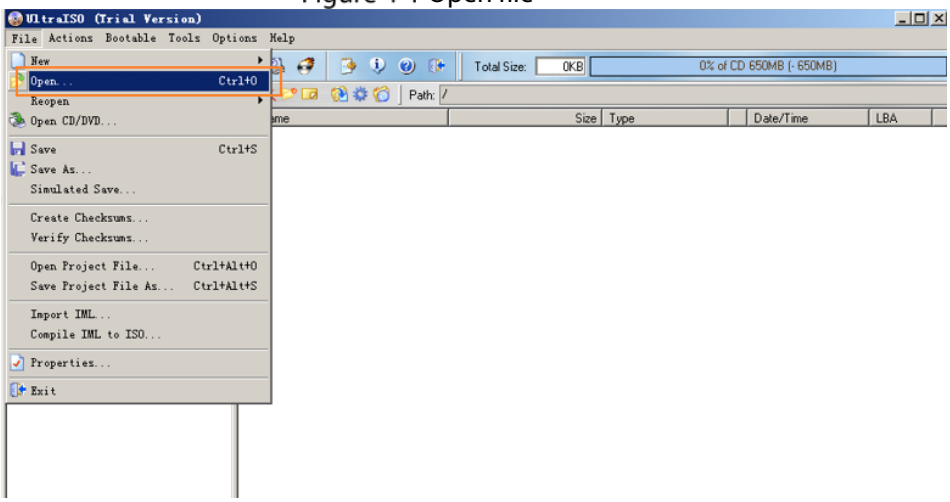
If the server has installed CentOS 7.4 system, you can skip this chapter.

Procedure

Step 1 Double-click  to open UltraISO tool.

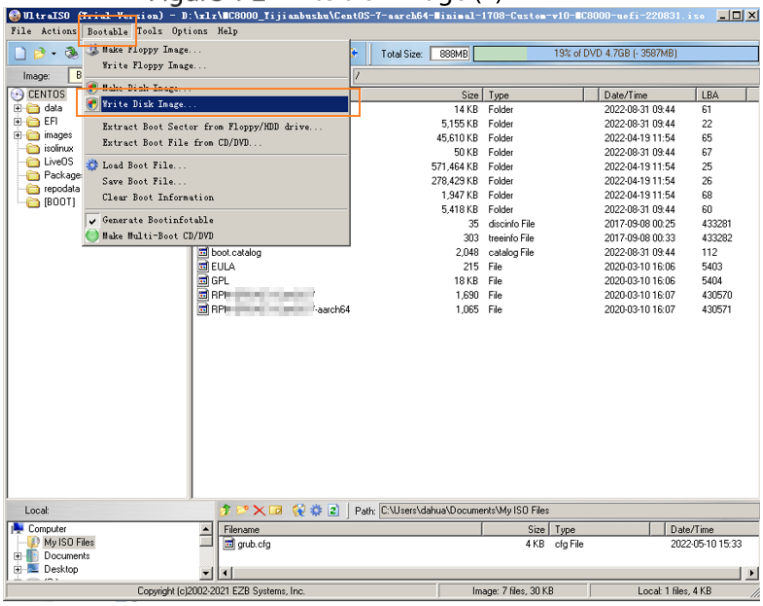
Step 2 Select **File** > **Open**, select the CentOS 7.4 installation package, and then click **Open**.

Figure 4-1 Open file



Step 3 Select **Bootable** > **Write Disk Image**.

Figure 4-2 Write disk image (1)

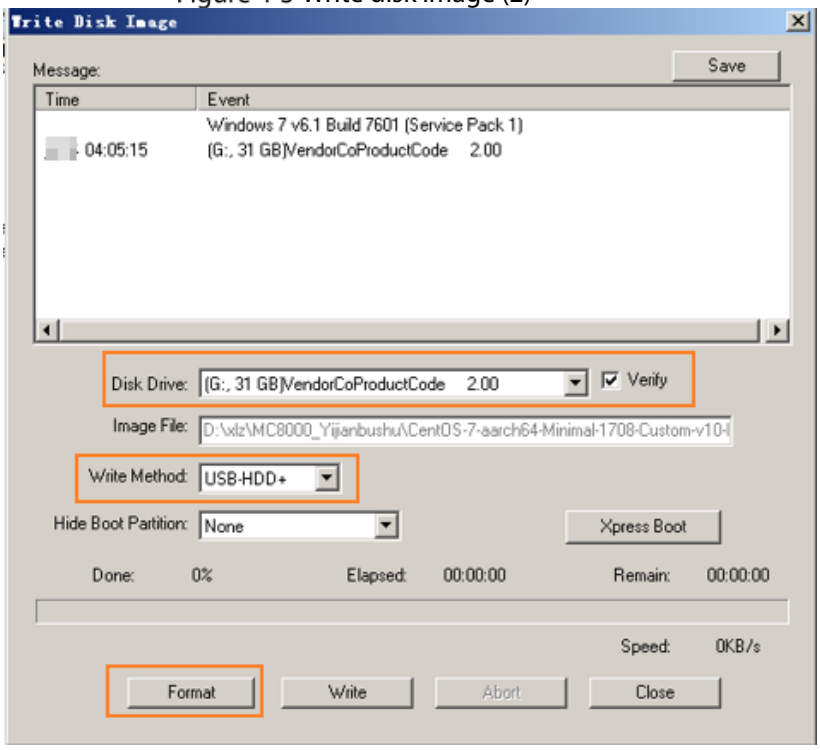


Step 4 Configure **Disk Drive** and **Write Method**, and then click **Format**.

Formatting will clear all the data in HDD. Be careful.

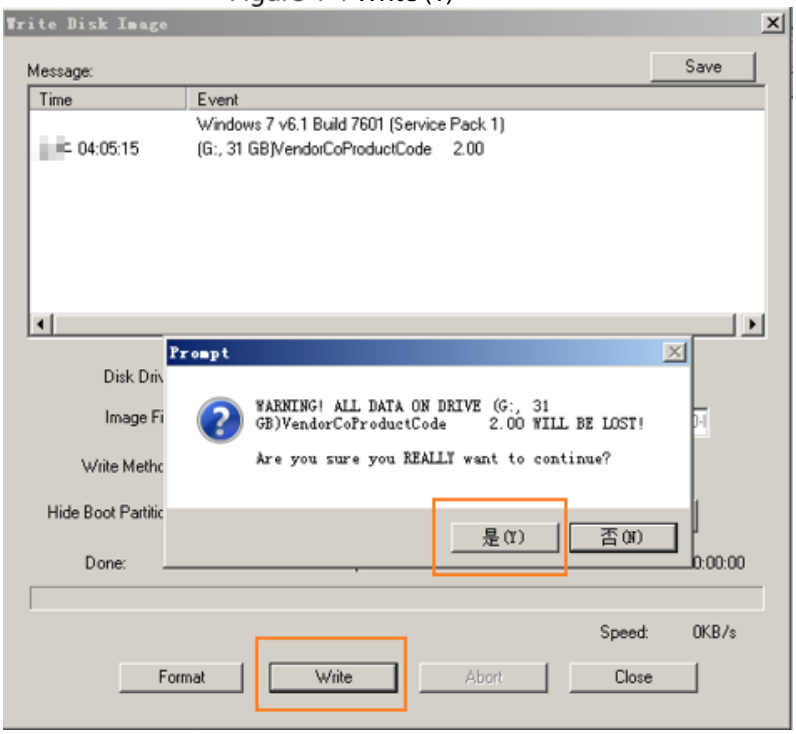
Default without modification.

Figure 4-3 Write disk image (2)



Step 5 Click **Write.**

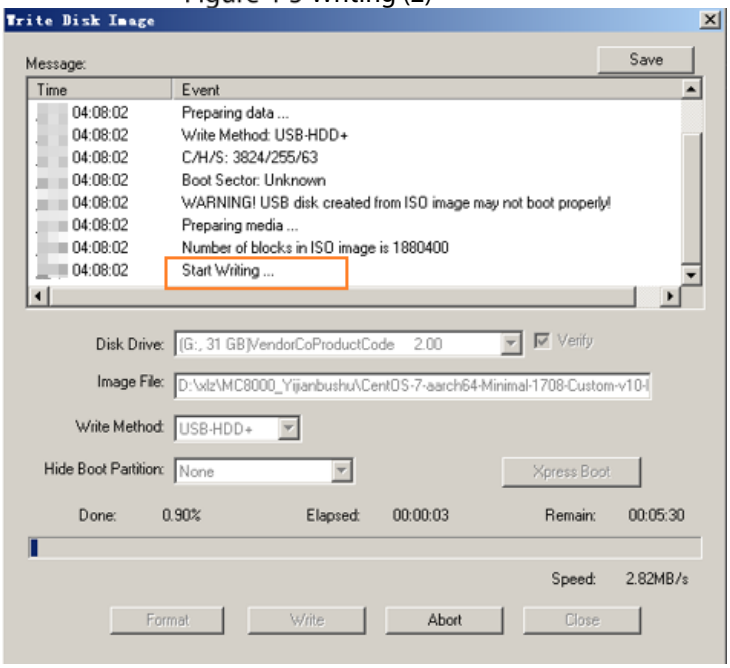
Figure 4-4 Write (1)



Step 6 In the pop-up window, click **OK**.

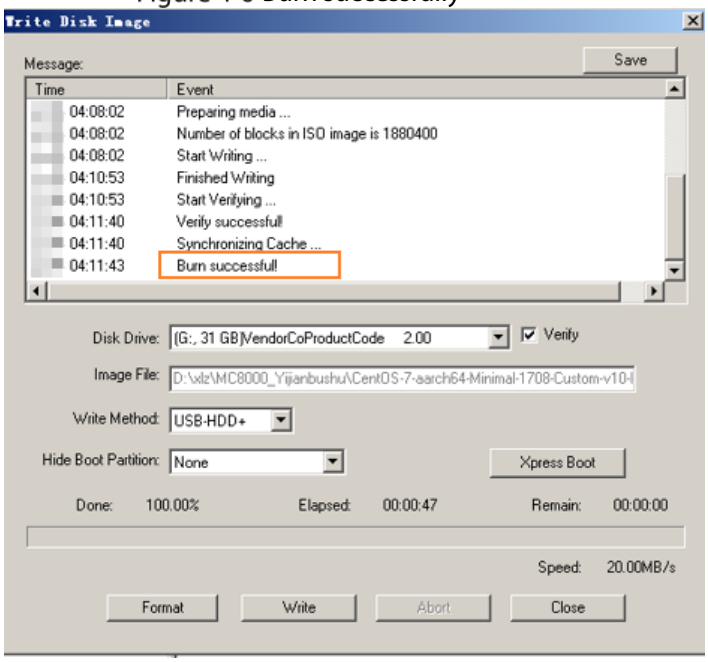
The system starts writing data, and the progress bar is displayed.

Figure 4-5 Writing (2)



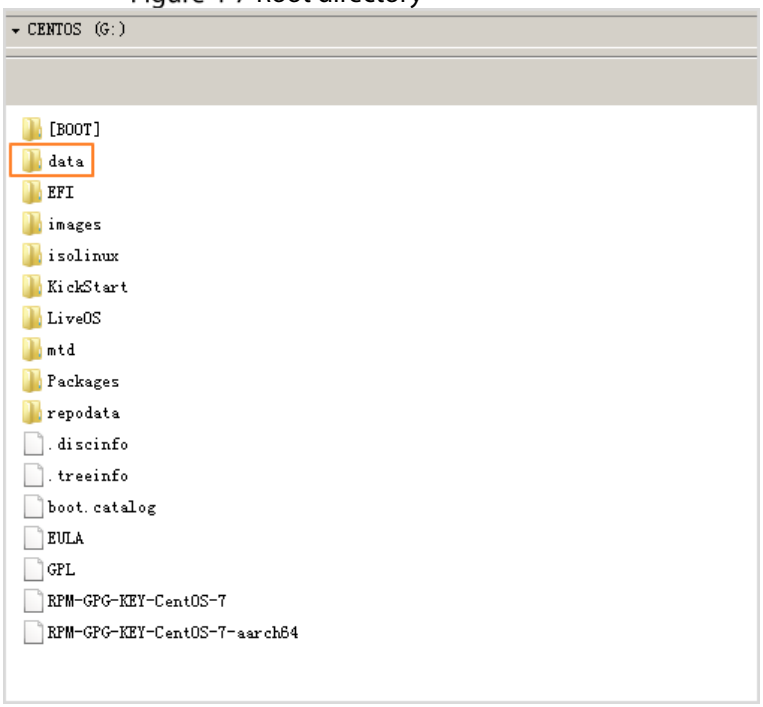
Step 7 After you successfully burn the USB flash drive, click **Close**.

Figure 4-6 Burn successfully



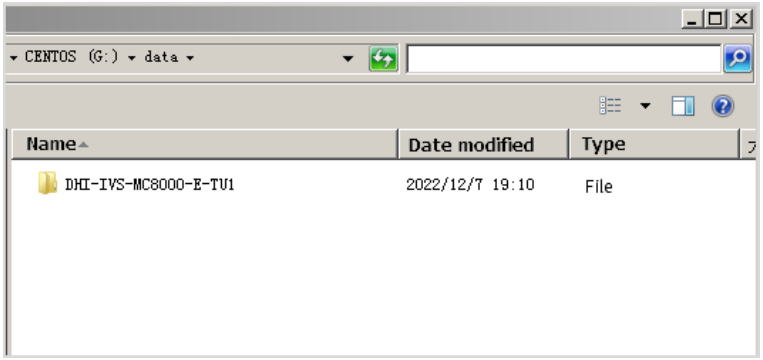
Step 8 Enter the USB flash drive root directory, and then click it to enter the data directory.

Figure 4-7 Root directory



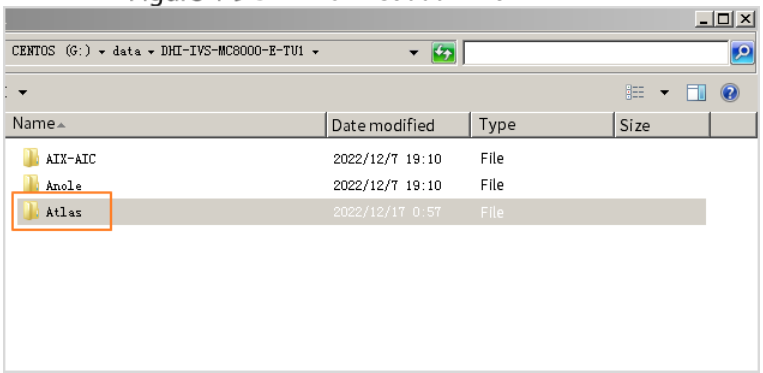
Step 9 Click **DHI-IVS-MC8000-E** to enter the directory.

Figure 4-8 Data



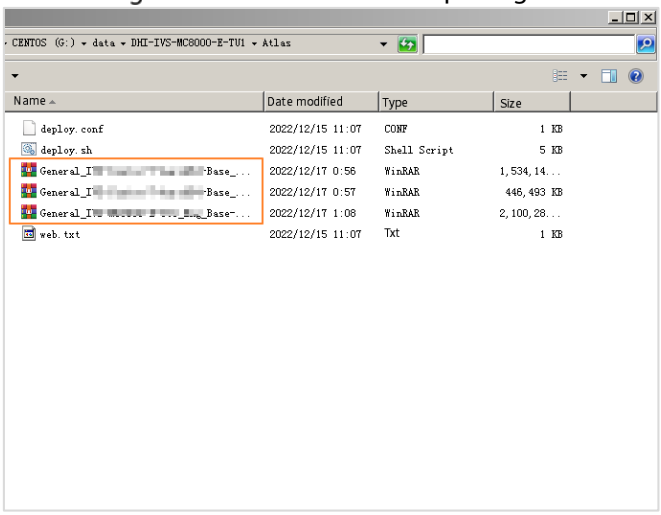
Step 10 Click **Atlas** to enter the directory.

Figure 4-9 DHI-IVS-MC8000-E-TU1



Step 11 Save the basic package, driver package, patch package, and installation package to F:\data\Atlas.

Figure 4-10 Save installation packages



4.2.2 Selecting USB Flash Drive

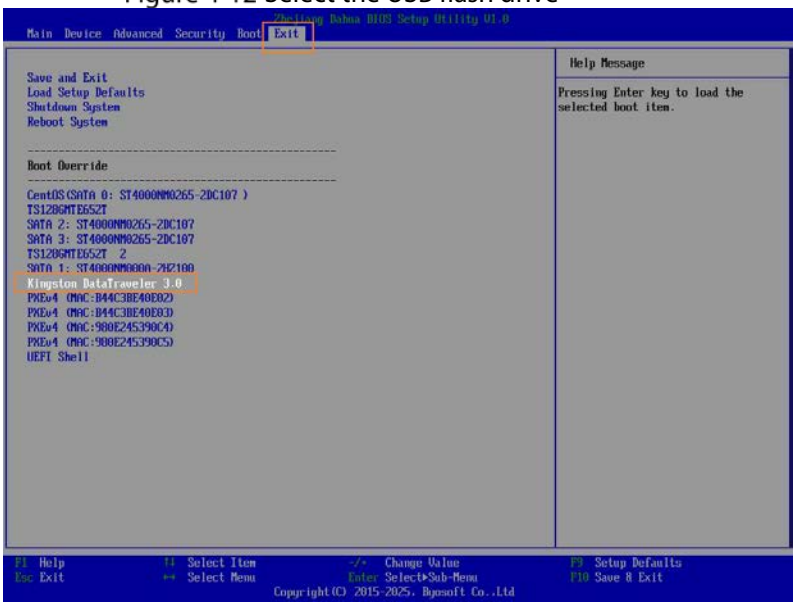
Connect the display and keyboard to the Server, and then insert USB drive to boot up.

Step 1 When the logo is displayed, press Delete to enter **BIOS Setup Utility** page.

Figure 4-11 Logo

Step 2 Enter the **Exit** page, and then select the USB flash drive you insert before. Press Enter to boot installation system.

Figure 4-12 Select the USB flash drive

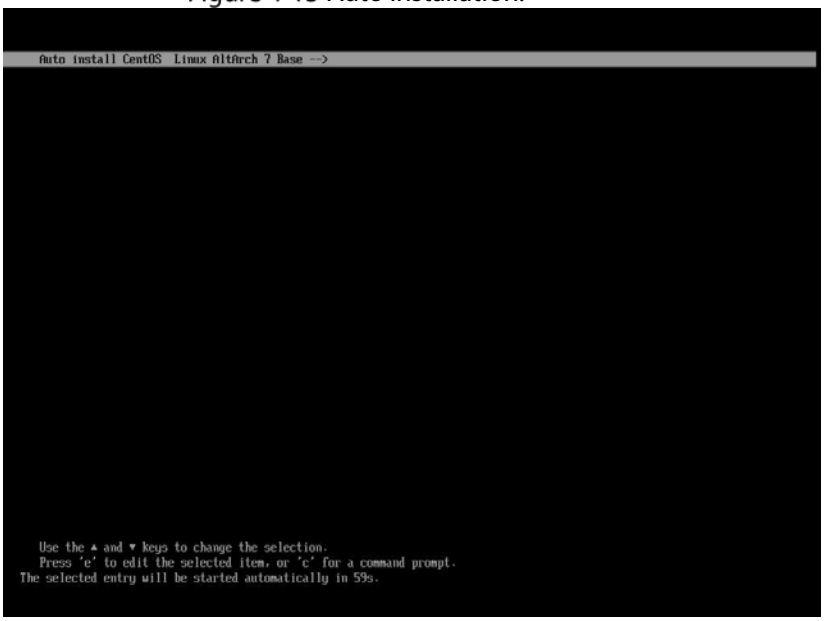


Operations might differ depending on different servers.

4.2.3 Selecting Operating System

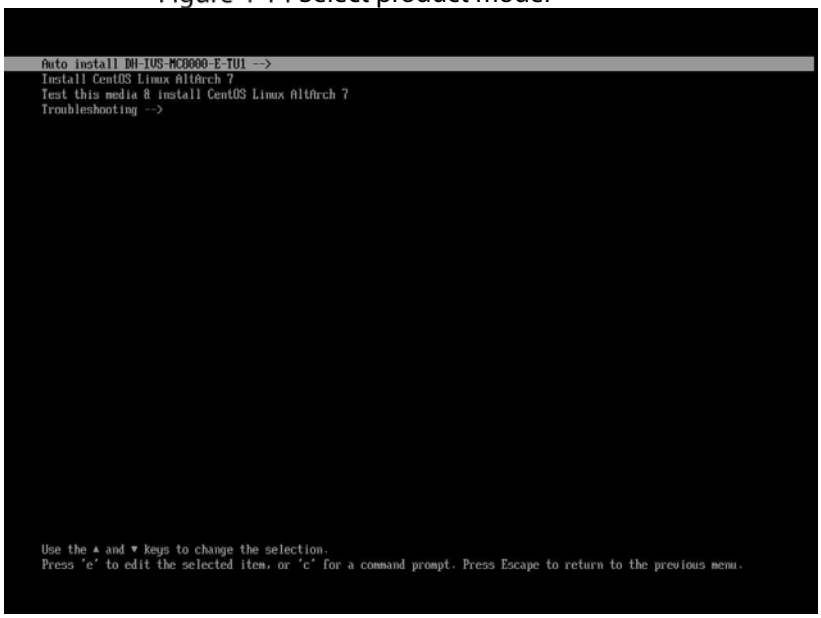
Step 1 Select **Auto install CentOS Linux AltArch 7 Base** and then press Enter to select product type.

Figure 4-13 Auto installation.



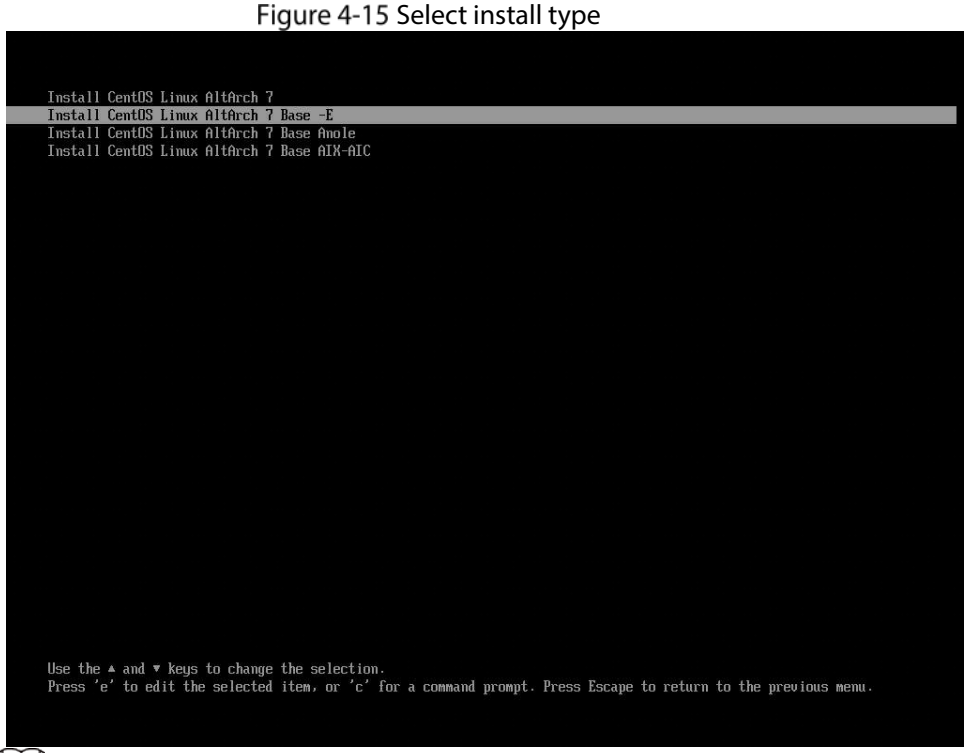
Step 2 Select **Auto install DHI-IVS-MC8000-E-TU1**, and then press Enter to select installation type.

Figure 4-14 Select product model



Step 3 Select **Install CentOS Linux AltArch 7 Base -E**, and then press Enter to install.

Figure 4-15 Select install type



The installation process takes about 70 minutes and the system will automatically restart twice.

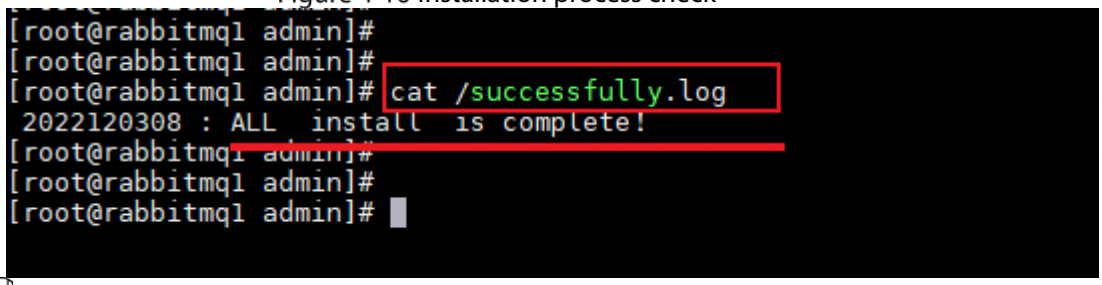
4.2.4 Installation Process Checking

Check whether the system has been installed.

Step 1 Use Xshell to remotely log in to the server.

Step 2 Run **cat /successfully.log** command to check the output. If **ALL install is complete!** appears, it means the installation has been completed.

Figure 4-16 Installation process check



After installation, see "1 Initialization" for follow up operations.

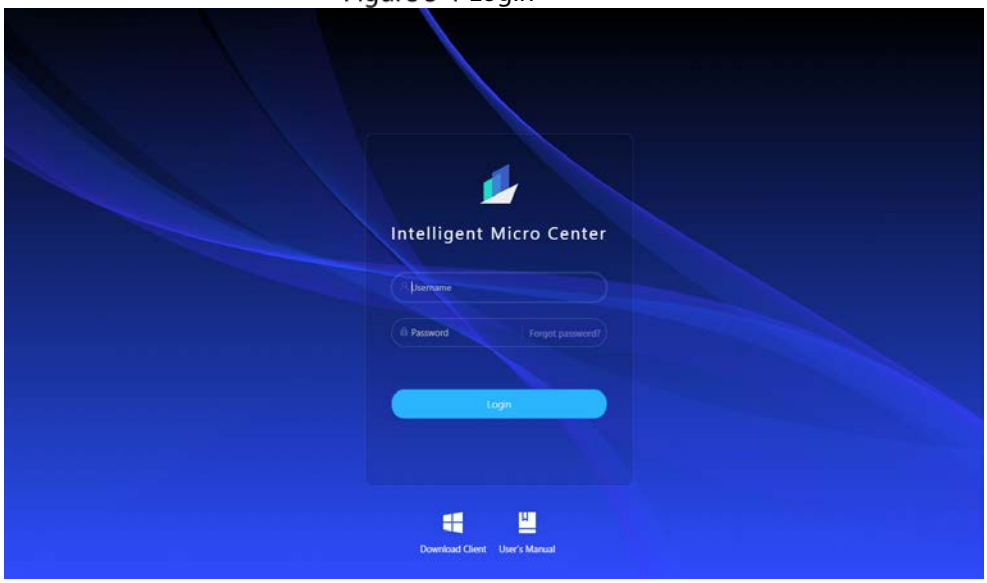
5 Applying for Encryption

- For baseline server, you need to insert the permanent dongle to the USB port.
- MC8000 supports two encryption methods: hardware-based encryption and software-based encryption.

5.1 Software-based Encryption

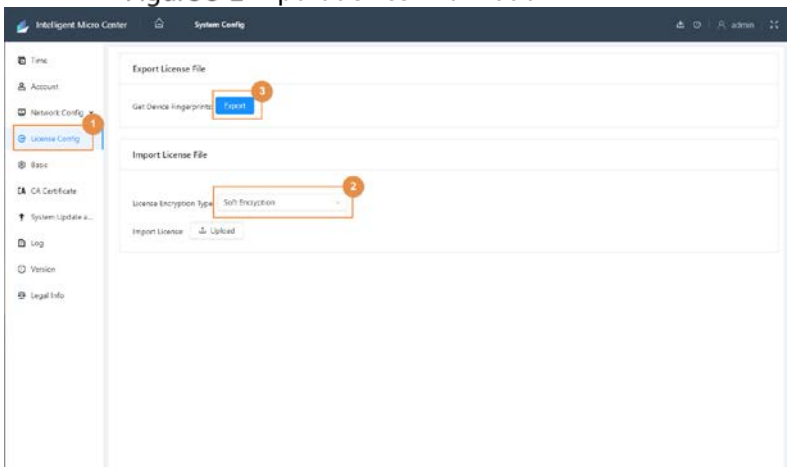
Step 1 Open the Chrome browser, enter the real IP address of the server (http://192.168.1.108), and then press the Enter. Enter the username and password, and then click **Login**.

Figure 5-1 Login



Step 2 Select **System Config** > **License Config**, and then select **Soft Encryption** as the license encryption type. Click **Export** to export device information files to local computer.

Figure 5-2 Export device information

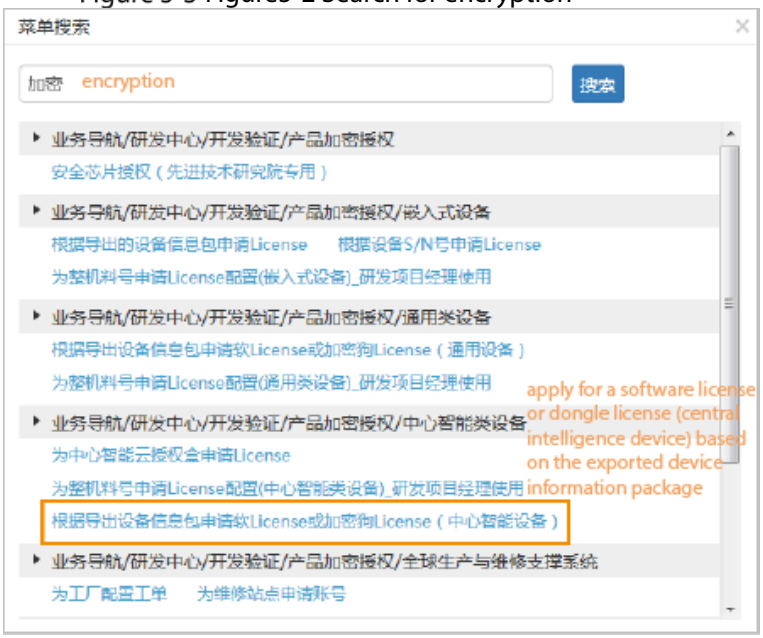


The format of the file is xxxxx_server.dat, and the actual format depending on actual files.

Step 3 Apply for software-based encryption on Dahua portal.

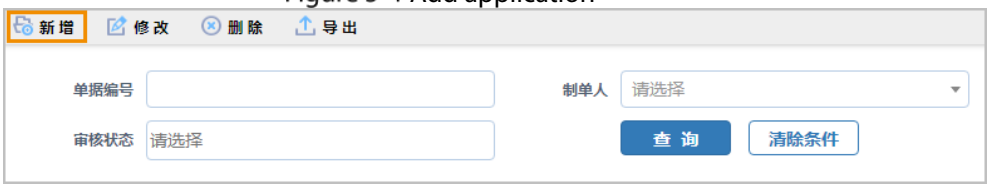
1) In the portal menu navigation bar, enter 加密 (encryption), select 根据导出设备信息包申请软 **License** 或加密狗 **License**（中心智能设备）(apply for a software license or dongle license (central intelligence device) based on the exported device information package).

Figure 5-3 Figure5-2 Search for encryption



2) Click 新增 (**add**) to add a software-based encryption application.

Figure 5-4 Add application



3) Enter the application information.

If you apply for permanent encryption, enter the project name, business opportunity No., and corresponding technical support in the reason field, and then attach the contract.

Figure 5-5 Enter the software-based information application

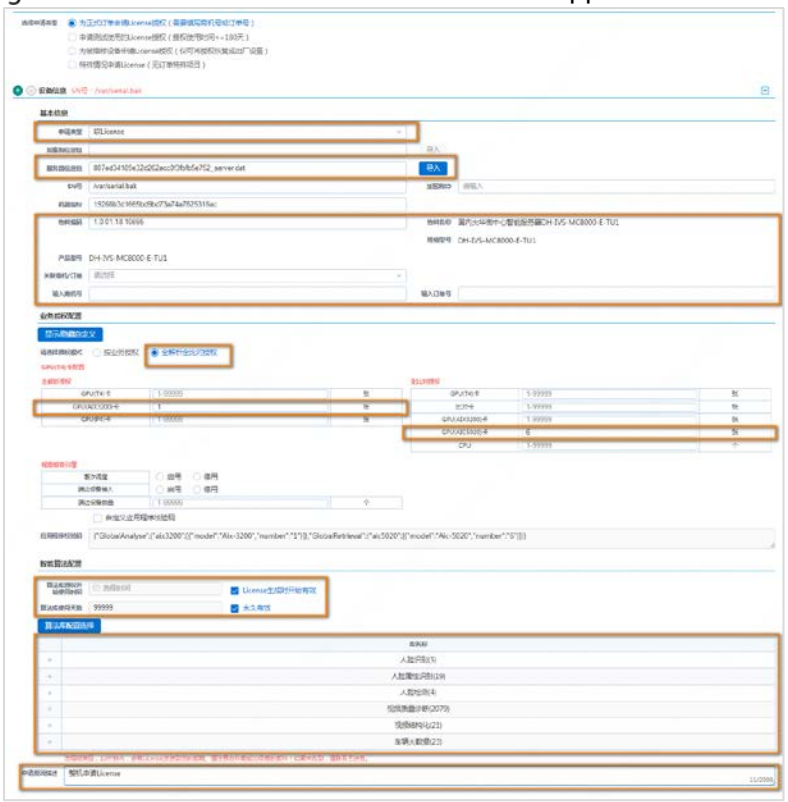


Table 5-1 Parameter description

Parameter	Description
Type	Select the application type. Supports dongle and software license. ● For hardware-based encryption, select 加密狗 (dongle). ● For software-based encryption, select 软 **License** (software License).
Material No.	Click the text box, and then enter the material No. of the server. For server material No, see Table 5-2.
Algorithm Database Usage Days	Select 永久有效 (**permanently effective**).
Algorithm Database Config	Select face recognition(5), Face attributes recognition(19), face detection(4), video quality diagnostics(2079) and video metadata(21) and vehicle big data(23).
Description of reason for application	Enter the application reason.

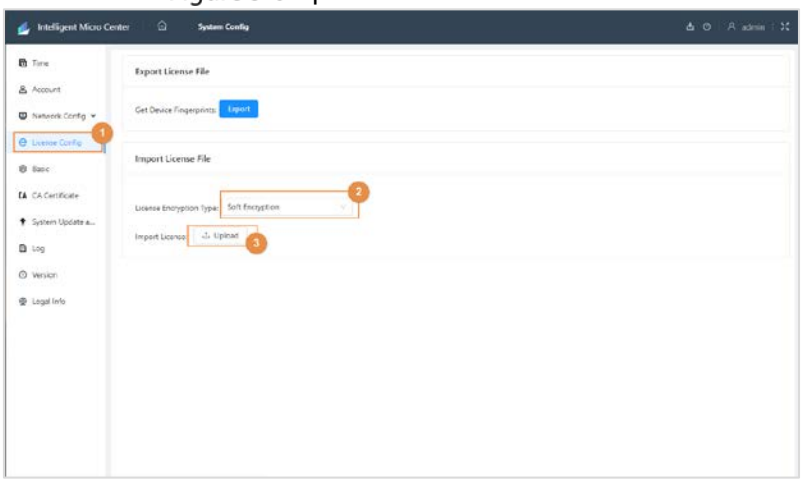
Table 5-2 Server material No.

Server Name and Model	Material No.
Domestic Dahua Micro Center Intelligent ServerDHI-IVS-MC8000-E-TU1	1.0.01.18.10729
Domestic Dahua Micro Center Intelligent Server DHI-IVS-MC8000-2E-TU1	1.0.01.18.10730

4) Click **Save** on the upper Left Corner, and then click **Submit**.
After the process is approved, you will receive an email from the portal. Click the link in the email to download the software-based encryption certificate. Click a zip file named after the application date.

Step 4 Go back to **Micro Intelligent Center** page, and then click **License Config** on the **System Config** page. Select **Hard Encryption** as the license encryption type. Click **Upload** to import software-based encryption license to the system.

Figure 5-6 Upload soft license.



Step 5 After importing license, wait for 5 minutes, and then view version. If the **Intelligent Algorithm License** displays **Normal**, the authorization has taken effect. For follow up operations, see"2 Service Status Verification".

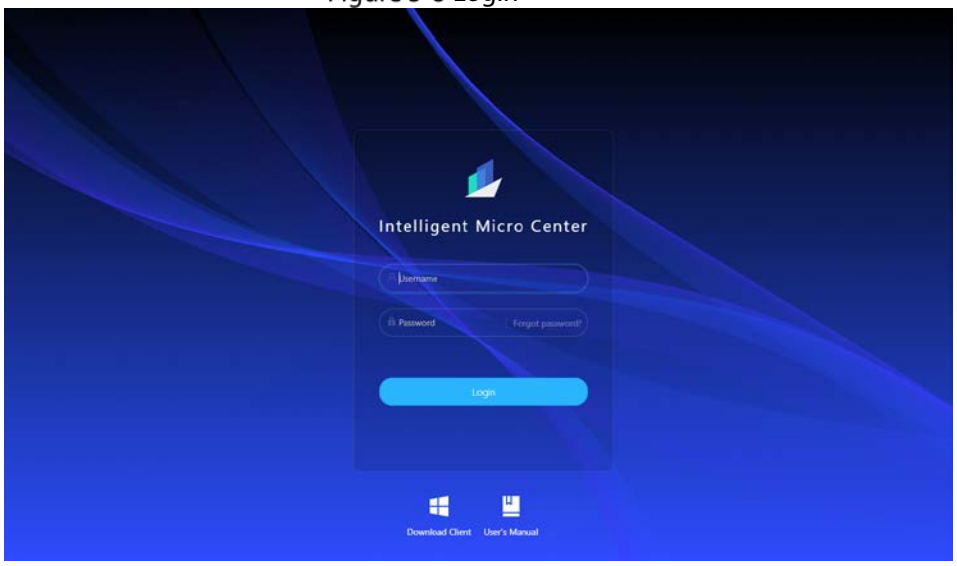
Figure 5-7 Authorization verification

5.2 Hardware-based Encryption

Step 1 Insert the dongle to the USB port

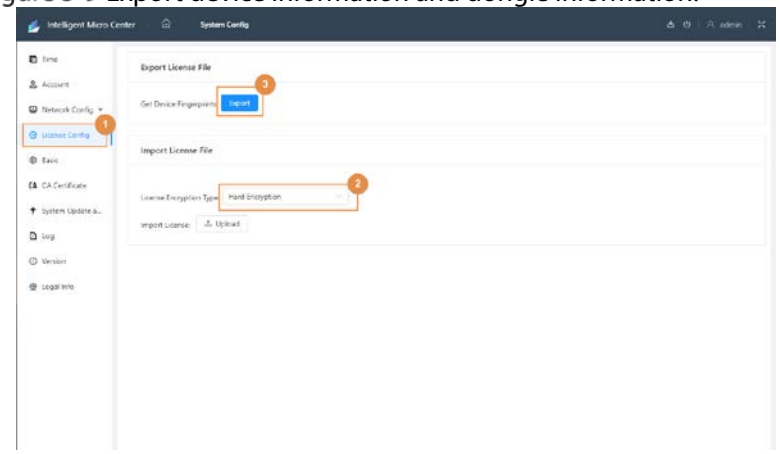
Step 2 Open the Chrome browser, enter the real IP address of the server (http://192.168.1.108), and then press the Enter. Enter the username and password, and then click **Login**.

Figure 5-8 Login



Step 3 Select **System Config** > **License Config,** and then set **License Encryption Type** as **Hard Encryption**. Click **Export** to export device information and dongle information to local computer.

Figure 5-9 Export device information and dongle information.



The name of device information file is “xxxxx_server.dat” and the name of the dongle information file is “xxxxx_dog.dat”.

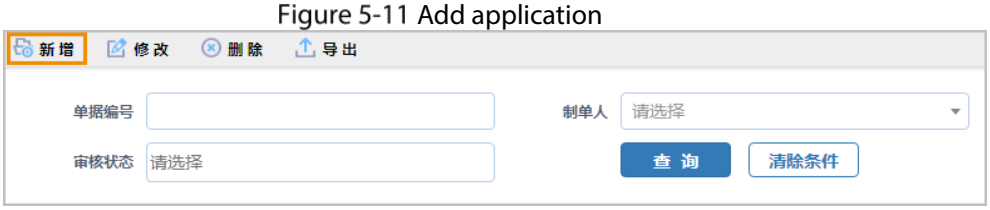
Step 4 Apply for software-based encryption on Dahua portal.

1) In the portal menu navigation bar, enter 加密 (encryption), select 根据导出设备信息包申请软 **License** 或加密狗 **License**（中心智能设备）(apply for a software license or dongle license (central intelligence device) based on the exported device information package).

Figure 5-10 Search for encryption

2) Click 新增 (add) to add a software-based encryption application.

Figure 5-11 Add application



3) Enter the application information.

If you apply for permanent encryption, enter the project name, business opportunity No., and corresponding technical support in the reason field, and then attach the contract.

Figure 5-12 Enter the application information

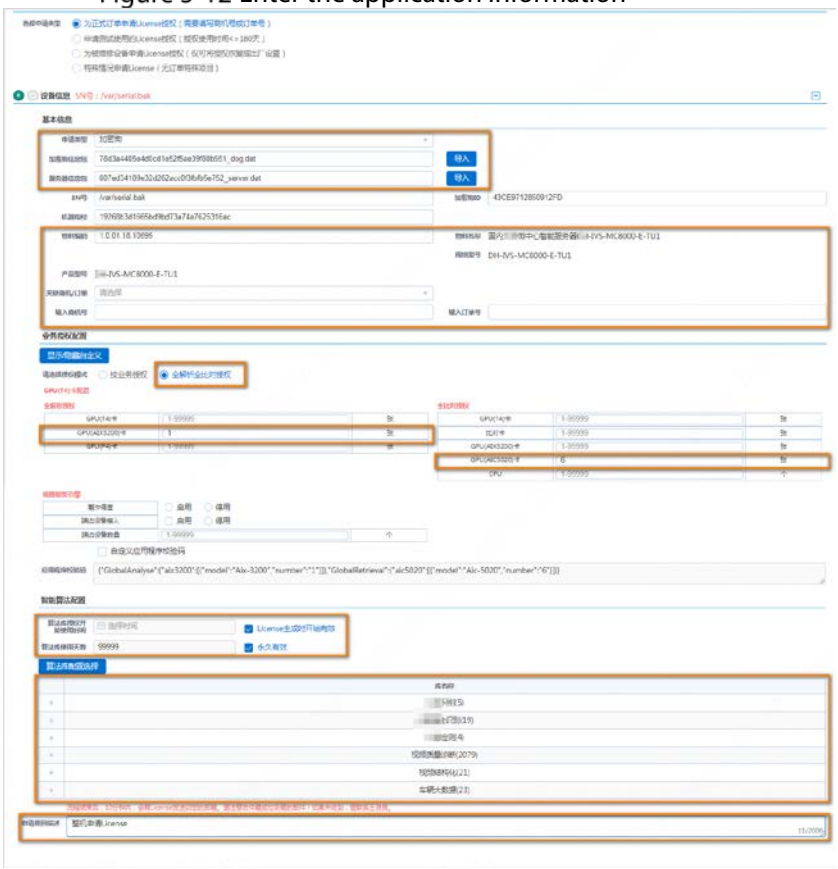


Table 5-3 Parameter description

Parameter	Description
Type of application	Select the application type. Supports dongle and software license. ● For hardware-based encryption, select 加密狗 (dongle). ● For software-based encryption, select 软 License (software License).
Material No.	Click the text box, and then enter the material No. of the server. Material No. see Table 5-4.
Algorithm Database Usage Days	Select 永久有效 (permanently effective) ☑ means selected, and ☐ means not selected.
Algorithm Database Config	Select face recognition(5), Face attributes recognition(19), face detection(4), video quality diagnostics(2079) and video metadata(21) and vehicle big data(23)
Description of reason for application	Enter the application reason.

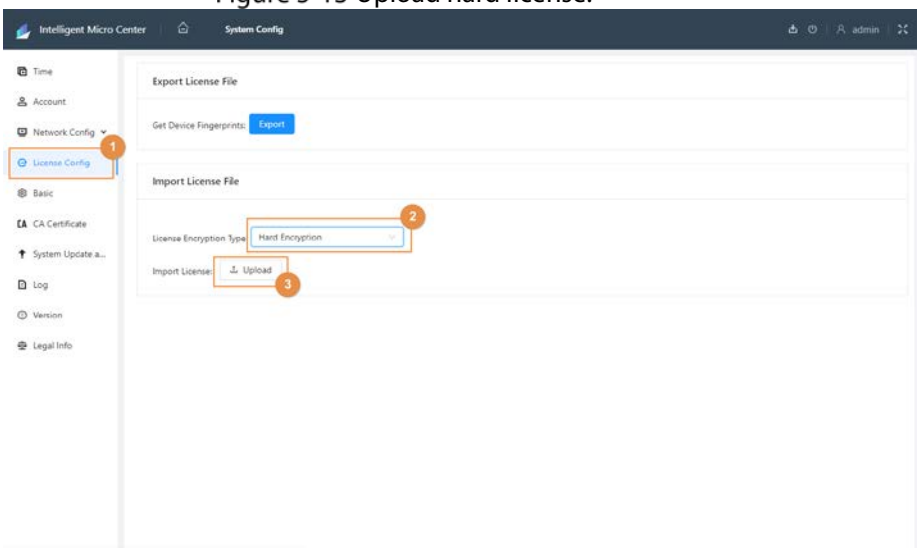
Table 5-4 Server material No.

Server Name and Model	Material No.
Domestic DahuaMicro Center Intelligent ServerDHI-IVS-MC8000-E-TU1	1.0.01.18.10729
Domestic Dahua Micro Center Intelligent Server DHI-IVS-MC8000-2E-TU1	1.0.01.18.10730

4) Click **Save** on the upper left corner, and then click **Submit**.
After the process is approved, you will receive an email from the portal. Click the link in the email to download the software-based encryption certificate, which is a zip file named after the application date.

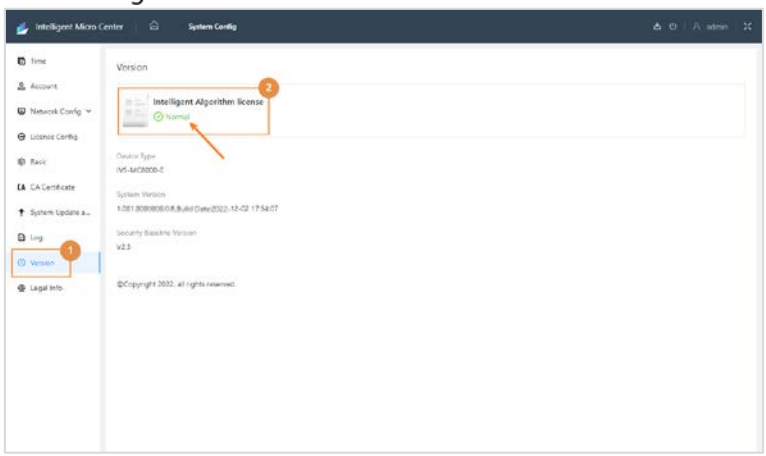
Step 5 Go back to **Micro Intelligent Center** page, and then click **Licnese Config** on the **System Config** page. Configure **License Encryption Type** as **Hard Encryption**. Click **Upload** to import hardware-based encryption license to the system.

Figure 5-13 Upload hard license.



Step 6 After importing license, wait for 5 minutes, and then view version. If the Intelligent Algorithm License displays Normal, the authorization has taken effect. For follow up operations, see"2 Service Status Verification".

Figure 5-14 Authorization verification



Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords.

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between

1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188