General Surveillance Management Center

Quick Deployment Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V8.5.0

Foreword

General

This user's manual introduces the functions and operations of the general surveillance management center (hereinafter referred to as "the system" or "the platform").

You can get the user's manual from https://software.dahuasecurity.com/en/download.

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.

Frequently Used Functions

Icon/Parameter	Description
	View the details of an item.
	Clear all selected options.
Search...	Search for items by keywords or specified content.
or **Delete**	Delete items one by one or in batches.
, or **Edit**	Edit the parameters of an item.
, , **Enable** , or **Disable**	Enable or disable items one by one or in batches.
or **Export**	Exported the selected content to your local computer.
or **Refresh**	Refresh the content.
*	A parameter that must be configured.

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license 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.

Operation Requirements

A suitable operating environment is the foundation for the device to work properly. Confirm whether the following conditions have been met before use.

- Use the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the operating temperature and humidity of the device.
- Use the device on a stable base.
- Do not let any liquid flow into the device to avoid damage to internal components. When liquid flows into the device, immediately disconnect the power supply, unplug all cables connected to it, and contact after-sales service.
- Do not plug or unplug RS-232, RS-485 and other ports with the power on, otherwise, the ports will be easily damaged.
- Back up data in time during deployment and use, in an effort to avoid data loss caused by abnormal operation. The company is not liable for data security.
- The company is not responsible for damages to the device or other product problems caused by excessive use or other improper use.

Installation Requirements

- Make sure that the power is off when you connect the cables, install or disassemble the device.
- For devices with earthing systems, make sure they are grounded to avoid being damaged by static electricity or induced voltage, and prevent electrocution from occurring.
- All installation and operations must conform to local electrical safety regulations.
- Use accessories suggested by the manufacturer, and installed by professionals.
- Do not block the ventilator of the device, and install the device in a well-ventilated place.
- Do not expose the device to heat sources or direct sunlight, such as radiator, heater, stove or other heating equipment, which is to avoid the risk of fire.
- Do not place the device in explosive, humid, dusty, extremely hot or cold sites with corrosive gas, strong electromagnetic radiation or unstable illumination.
- Avoid heavy stress, violent vibration, and immersion during installation.

Safe and stable power supply is a prerequisite for proper operation of the device.

- Make sure that the ambient voltage is stable and meet the power supply requirements of the device.
- Prevent the power cord from being trampled or pressed, especially the plug, power socket and the junction from the device.
- For devices that can be powered by multiple supplies, do not connect them to two or more kinds of power supplies; otherwise, the device might be damaged.

- Refer to the specific user's manual for the power requirements of single device.

It is recommended to use the device with a lightning protector for better lightning-proof effect.

Transportation Requirements

- Pack the device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Avoid heavy stress, violent vibration, and immersion during transportation.
- Transport the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the transporting temperature and humidity of the device.

Storage Requirements

- Store the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the storing temperature and humidity of the device.
- Avoid heavy stress, violent vibration, and immersion during storage.

Maintenance Requirements

- Contact professionals for regular inspection and maintenance of the device. Do not disassemble or dismantle the device without a professional present.
- Use accessories suggested by the manufacturer, and maintain the device by professionals.

Table of Contents

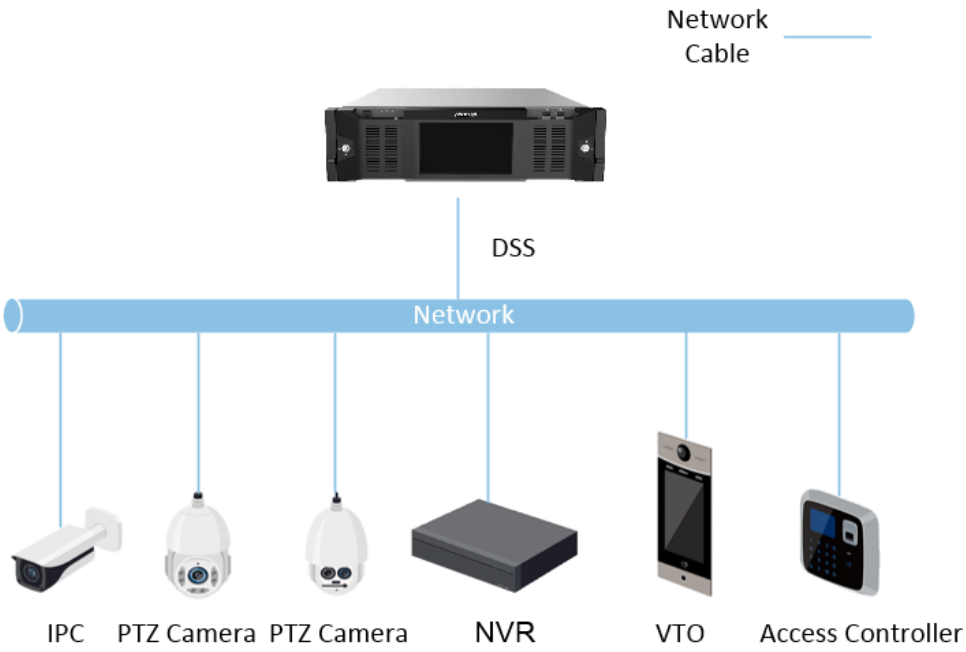
1 Overview

The system supports standalone deployment, distributed deployment, hot standby, and N+M deployment, and LAN to WAN mapping.

Standalone Deployment

For projects with a small number of devices, only one server is required.

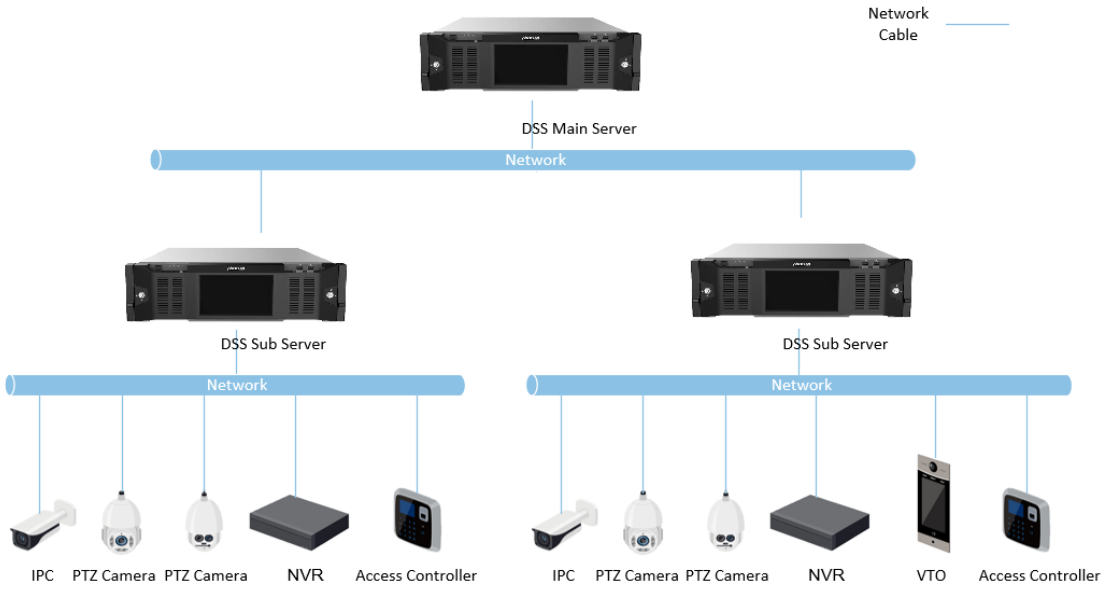
Figure 1-1 Standalone deployment



Distributed Deployment

Suitable for medium to larger projects. Sub servers are used to share system load, so that more devices can be accessed. The sub servers register to the main server, and the main server centrally manages the sub servers.

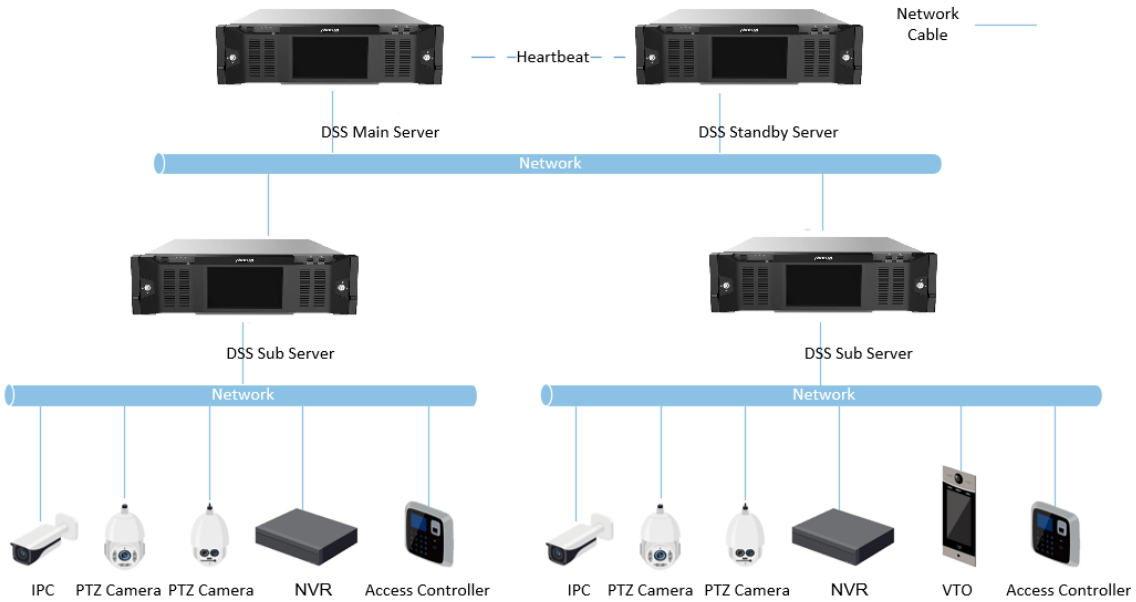
Figure 1-2 Distributed deployment



Hot Standby

Used with systems that require high stability. The standby server takes over the system when the active server malfunctions (such as with power-off and network disconnection). You can switch back to the original active server after it recovers.

Figure 1-3 Hot standby

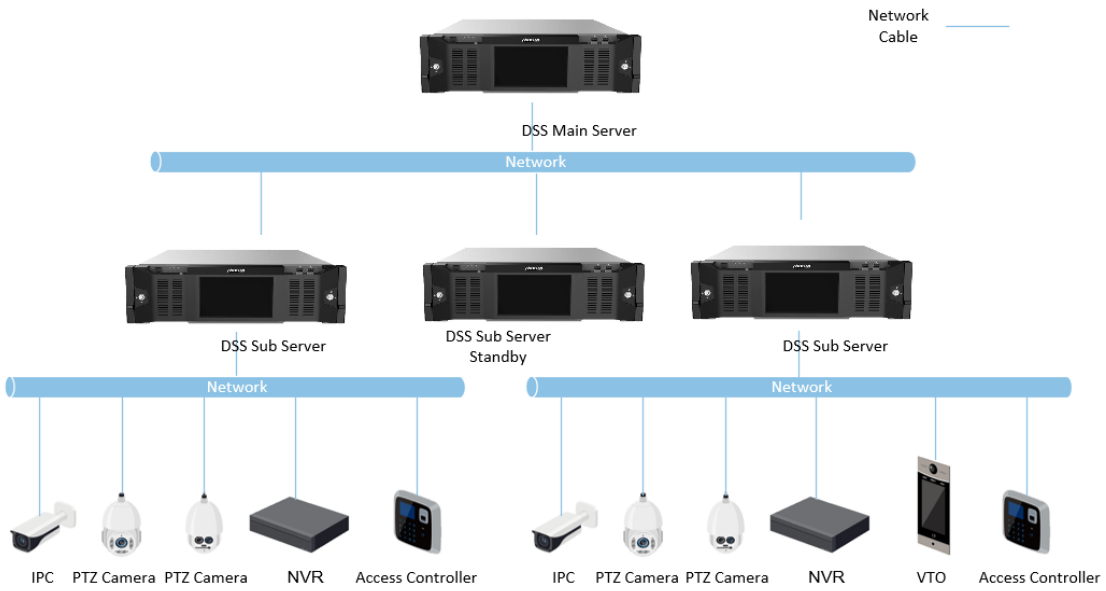


N+M

Each sub server has a standby server to maintain stability. When a sub server malfunctions, the system replaces it with an idle standby server. When the malfunctioning server normalizes, you can

manually switch back to it. If you do not manually switch them, the system will automatically make the switch if the standby server malfunctions.

Figure 1-4 N+M



LAN to WAN Mapping

Perform port mapping when:

- The server of the platform and devices are on a local area network, and the DSS client in on the internet. To make sure that the DSS client can access the platform server, you need to map the platform IP to the Internet.
- The platform is on a local area network, and the devices are on the Internet. If you want to add devices to the platform through automatic registration, you need to map the IP address and ports of the platform to the Internet. For devices on the Internet, the platform can add them by their IP addresses and ports.

The configuration system does not differentiate service LAN ports and WAN ports. Make sure that the WAN ports and LAN ports are the same.

2 Standalone Deployment

2.1 Configuring Basic Parameters

Procedure

Step 1 Turn on the platform, and then click **Network**.

Step 2 On the **Select Port** drop-down list, select the port that is connected to the network card you want to configure, and then on the **Default Port** drop-down list, select the default network card of the platform.

Step 3 Configure the IP address, subnet mask, default gateway, and DNS, and then click **OK**.

The platform will automatically restart.

Step 4 Go to https://*IP address that you configured*/config in the browser.

For first-time login, follow the on-screen instructions to set a password, security questions, and time zone.

Step 5 Configure network parameters.

1. Select **Quick Guide** > **NIC Config**, or **Network Config** > **NIC Config**.
2. Configure the parameters, and then click **Apply and Restart**.

Default network card and its parameters have been configured in step 2 and 3.

Table 2-1 Network card parameter description

Parameter	Description
Select NIC Mode	• Multi-address Multiple network card (hereinafter referred to as NIC) mode. You can configure different network parameters for different NIC to access to multiple network segments and achieve high network reliability. For example, to configure hot standby, the NIC 2 can be used to set spare server IP. This can also be used in ISCSI storage expansion solution. When setting ISCSI storage expansion, NIC 1 can be used for communication, NIC 2 is reserved and NIC 3 and NIC 4 can be used for ISCSI storage. • Load Balancing Multiple NICs share one IP and work at the same time to share the network load, providing greater network capacity than the single NIC mode. When one of them fails, the network load will be re-distributed among the rest NICs to ensure network stability. • Fault-tolerant Multiple NICs share one IP. Normally, one of them works. When the working NIC fails, another one will automatically take over the job to ensure network stability. • Link Aggregation Bind NICs so that all the bound NICs work at the same time and share network load. For example, bind two NICs and set multi-address for the other two NICs. Then the server has three IPs. The bandwidth of the two bound NICs is 2K and the other two are 2K respectively. This is applicable to stream forwarding, not storage.
Add Network Card	When the NIC mode is fault tolerance, load balance or link aggregation, you need to add network card. Select NIC to bind. You can bind 2 NICs as needed.
Network Card Config	After NIC is selected or added, its information will be displayed.
MAC Address	Displays the MAC address of the server.
IPv4	After selecting a network card, you can set its IP address, subnet mask, default gateway and DNS server address.
IPv6	Enable IPv6 and configure the parameters to connect the platform to an IPv6 network, you can add devices with IPv6 address to the platform.
Default Network Card	Select the default NIC. This NIC will be used as the default NIC to forward data package between non-consecutive network segments such as WAN or public network.

Step 6 Set server time zone and time.

1. After restart completes, log in to the configuration system again, and then select **Basic Config** > **Time Config**.
2. Configure the parameters, and then click **Application**.

Table 2-2 Parameters description

Parameter	Description
Time Zone	Select time zone of the server.
Date/Time	Click the box to select the date and time.
Sync PC	Click **Sync PC** to synchronize the time of the server with the computer that you are using.

Step 7 Configure the work mode.

1. After restart completes, log in to the configuration system again, and then select **Quick Guide** > **Service Mode**, or select **Mode Config** > **Service Mode**.
2. Select **Main Server** or **Sub Server**.
   - For single-server deployment and hot standby deployment, set the work mode to **Main Server**.
   - For distributed deployment and N+M deployment, set the work mode of the main server to **Main Server** , and that of the spare servers to **Sub Server**.

     If the server is set to **Sub Server**, you need to enter main server IP address and HTTPS port number.
3. Click **Apply and Restart**.

2.2 Configuring Dual Network Cards

2 network cards are usually used for network segmentation. For example, the platform and devices are on 2 different network segments. You can log in to the platform through the IP address of the default network card, and the platform can access devices through another network card.

Prerequisites

Set the network card mode to multi-address mode, and then configure the parameters of each network card. For details, see "2.1 Configuring Basic Parameters".

Background Information

Currently, only 2 network cards can be used in dual network card mode, and DSS Client needs to connect only to default network card.

Procedure

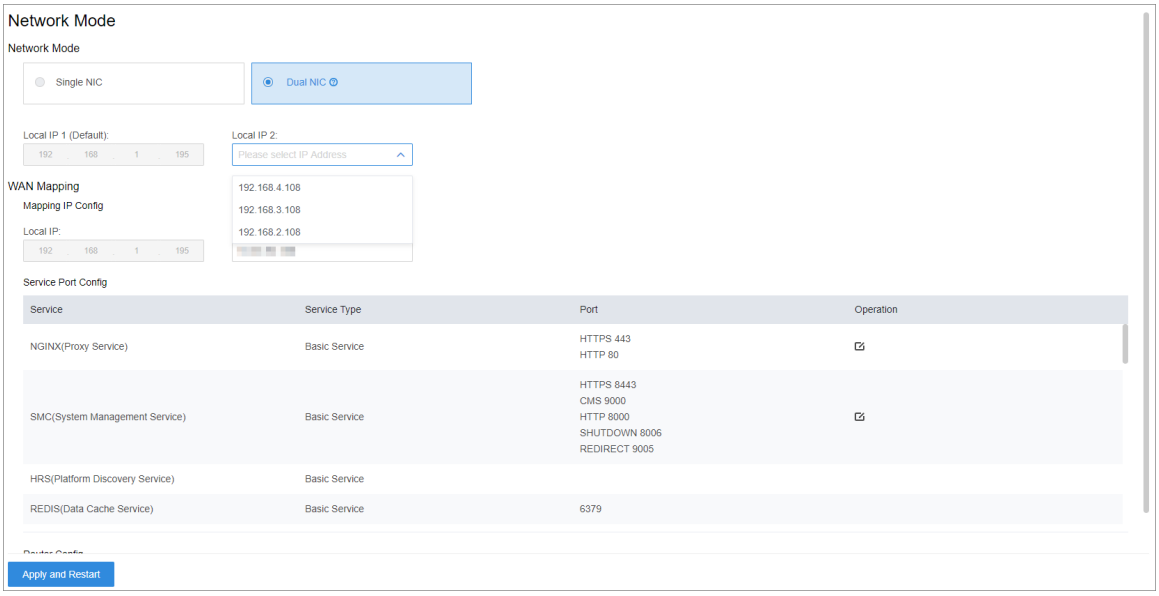
Step 1 Go to https://*platform IP address*/config in the browser.

Step 2 Enter the username and password, and then click **Login**.

Step 3 Select **Network Config** > **Network Mode**, and then select **Dual NIC**.

Step 4 On the **Local IP 2** drop-down box, select the IP address of the other network card, and then click **Apply and Restart**.

Figure 2-1 Dual network cards mode



Related Operations

In dual network cards mode, you can configure LAN and WAN mapping for the default network card. For details, see the corresponding chapter.

2.3 Installing DSS Client

Procedure

Step 1 Go to https://*IP address of the platform* in the browser.

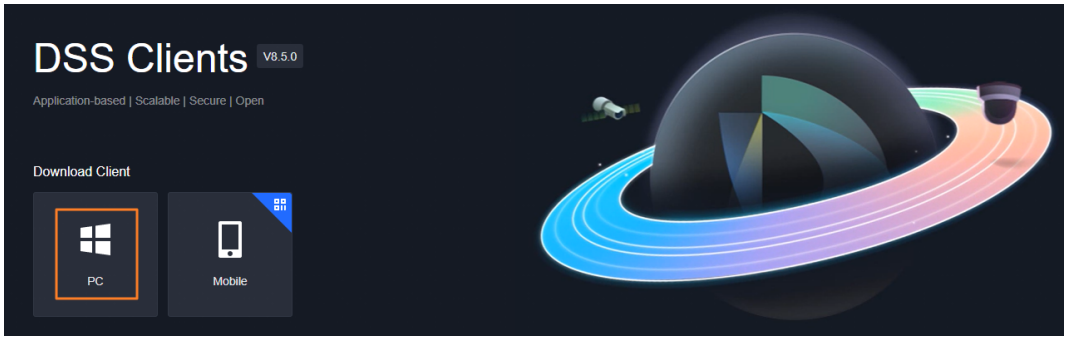
Step 2 Click **PC** , and then **Download**.

The platform also supports installation by MSI package. Visit https://software.dahuasecurity.com/en/download/ and download the MSI package of the platform version you need. Please be advised that you cannot overwrite the PC client installed with an exe package, and vice versa. Also, the PC client installed with an MSI package does not support automatic update. You must download the package of the new version an install it manually.

If you save the program, go to Step 3.

If you run the program, go to Step 4.

Figure 2-2 Download DSS Client



Step 3 Double-click the DSS Client program.

Step 4 Select the checkbox of **I have read and agree to the DSS agreement** and then click **Next**.

Step 5 Select a path for installation, and then click **Install**.

The installation progress is displayed. It takes about 5 minutes to complete.

2.4 Installing Mobile Client

Procedure

Step 1 Enter IP address of the DSS in the browser and then press Enter.

Step 2 Click **Mobile**, and then scan the QR code to download the App.

3 Distributed Deployment

3.1 Configuring Main Server

Most of the parameters you need to configure for the main server are the same as single-server deployment. Among them, you must select the service mode to **Main Server**. For details, see the previous chapter.

3.2 Configuring and Enabling Sub Servers

Prerequisites

- Prepare two servers and configure the basic parameters for them. For details, see the previous chapter.
- One server works as the main server, and set its service mode to **Main Server** . The other one works as the sub server, and set its service mode to **Sub Server**.

Procedure

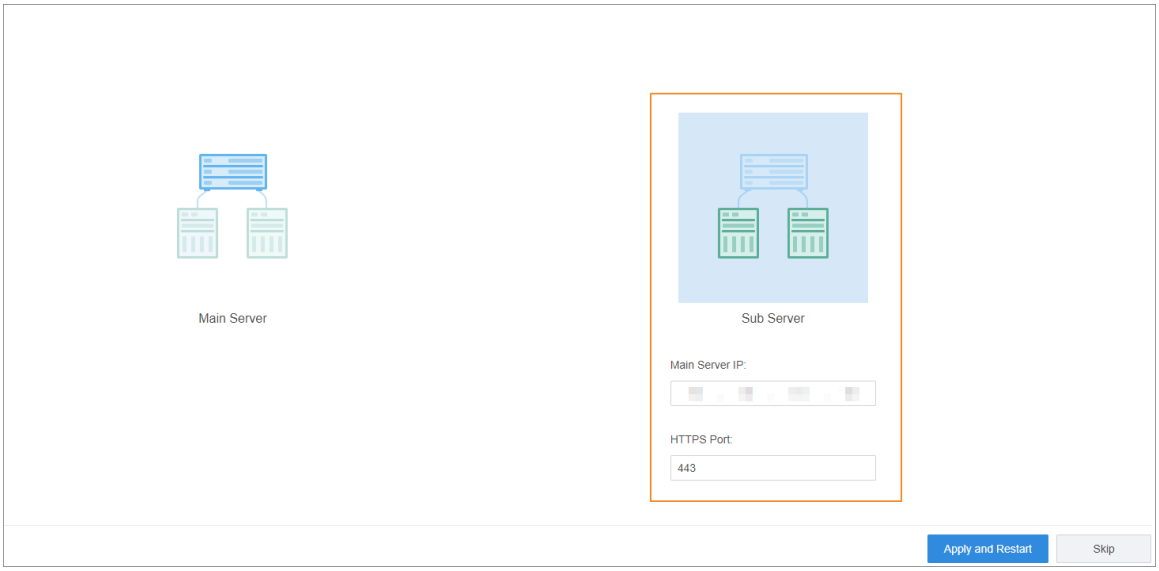
Step 1 Go to https://*sub server IP address*/config in the browser.

Step 2 Enter the username and password, and then click **Login**.

Step 3 Select **Quick Guide** > **Service Mode**, or **Mode Config** > **Service Mode**, and then select **Sub Server**.

Step 4 Enter the IP address and HTTPS port of the main server, and then click **Apply and Restart**.

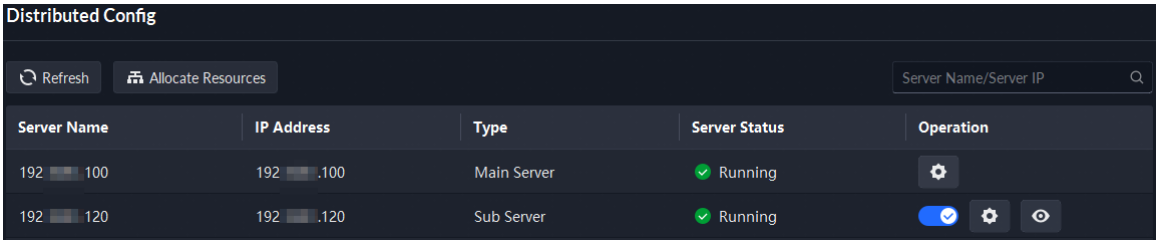
Figure 3-1 Configure the sub server



Step 5 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Deployment**.

Step 6 Click of the sub server to enable it.

Figure 3-2 Enable the sub server



4 Hot Standby

Configure hot standby server so that when the main server fails, the spare server can take over the job and ensure system stability.

Prerequisites

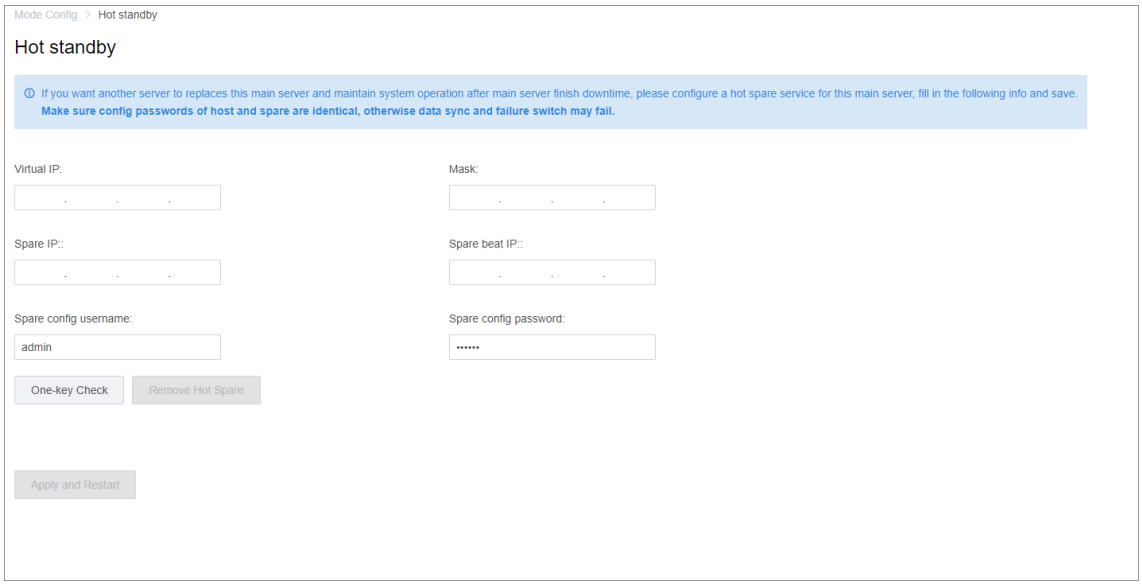
- Connect network cables.
  - Use network port 1 as business network port, and then configure an IP address on the business network segment for the network port 1. Connect network port 1 to the same LAN via switch, and the virtual IP address and the one of network port 1 need to be in the same segment.
  - Take network port 2 as heartbeat network port, which is used to keep data from both servers in synchronization. Configure an IP address for network port 2 that is on another network segment than network port 1, but the IP address of network port 2 of both servers need to be in the same network segment. You can check and configure the IP address of network port 2 on the config system.
- The network mode is set to multi-IP mode. For details, see #unique_11/unique_11_Connect_42_title_zpt_hrk_c5b.
- NTP time synchronization has been enabled on both servers. For details, see the user's manual.
- Prepare an IP address that is not used in the business network segment. After the configuration is complete, you can access this IP address to access the platform.
- Hot standby is the synchronization of the databases of the two servers. If you need to change any configuration that does not involve the databases, such as a port number, you must make sure this port number is the same on both servers.

Procedure

Step 1 Log in to the Config system.

Step 2 Select **Mode Config** > **Hot standby**.

Figure 4-1 Hot standby



Step 3 Configure the parameters.

The NIC mode must be **Multi-address** for hot spare to work normally. For details, see #unique_11/unique_11_Connect_42_title_zpt_hrk_c5b.

Table 4-1 Hot standby parameter description

Parameter	Description
Virtual IP	After setting virtual IP, it can have access to platform via the virtual IP.
Mask	It is in accordance with the mask of network port 1.
Spare IP	IP address of spare server network port 1.
Spare beat IP	IP address of spare server network port 2.
Spare config username	The login username and password of spare server Config system.  • The login password to Config system of the main and spare servers must be the same. • The password cannot be changed after hot standby is configured.
Spare config password	
One-key Check	Click **One-key Check** to confirm username and password.
Remove Hot Spare	After clicking **One-key Check** and the platform indicates everything is OK, you can click this button to remove the hot spare configuration. If you need to completely remove the hot spare configuration, you need to click this button on the spare server first, and then on the main server.  For this operation, you must access the IP addresses of the servers, and not the virtual IP address.

Step 4 Click **Apply and Restart**.

5 N+M

On the main server, enable the sub server, and then create the sub-standby relationship.

Prerequisites

- The relevant servers have been well deployed.
- The DSS client has been installed. For details, see #unique_13/unique_13_Connect_42_title_fsv_v2l_jyb.

Procedure

Step 1 Log in to the DSS client of the main server. On the **Home** page, click > **System Deployment**.

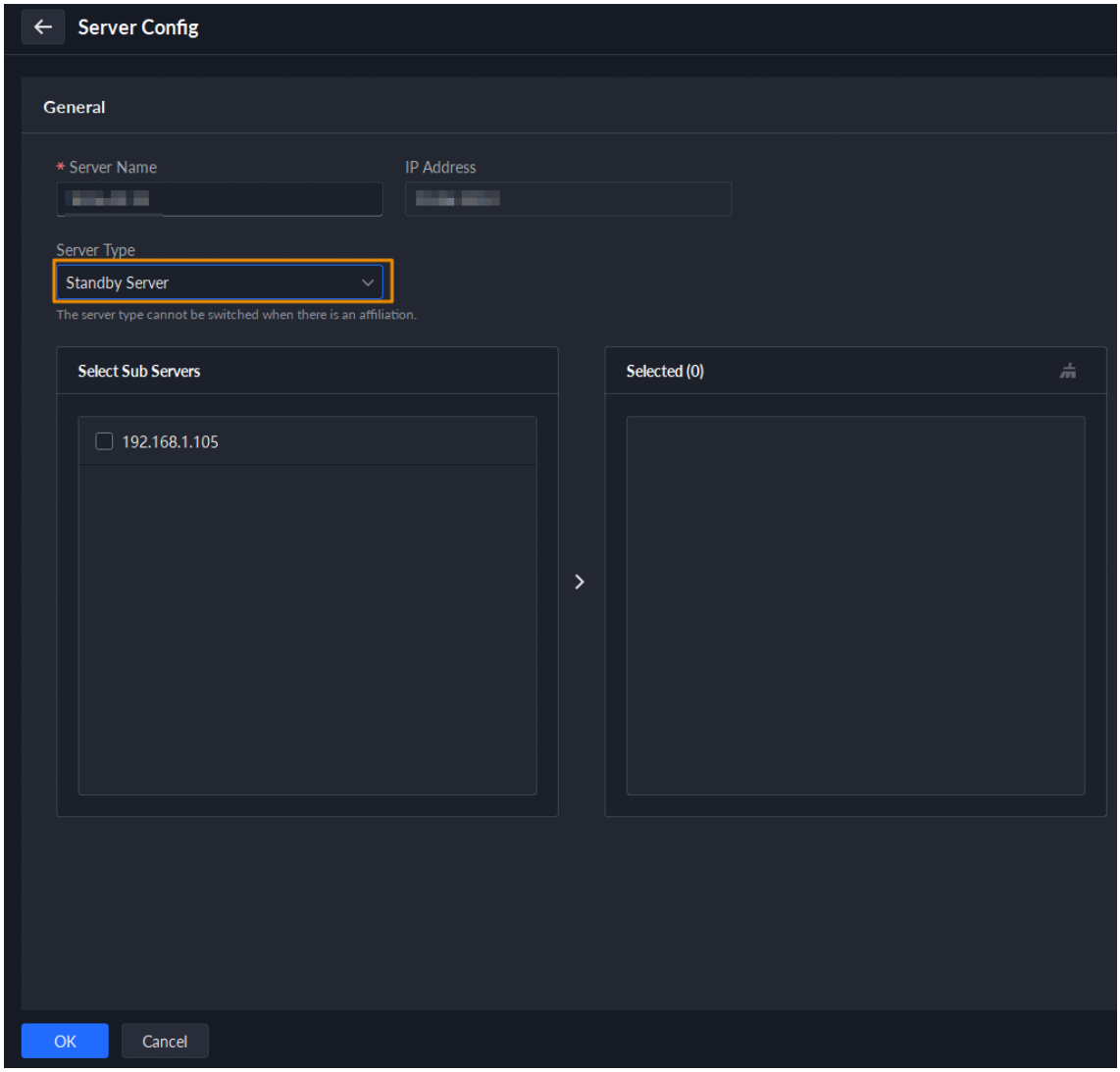
Step 2 Click .

Step 3 Click to enable the sub servers.

Step 4 Configure a standby server.

1. Click of a sub server.
2. Select **Standby Server** for **Server Type**, and then click **OK**.

Figure 5-1 Configure a standby server

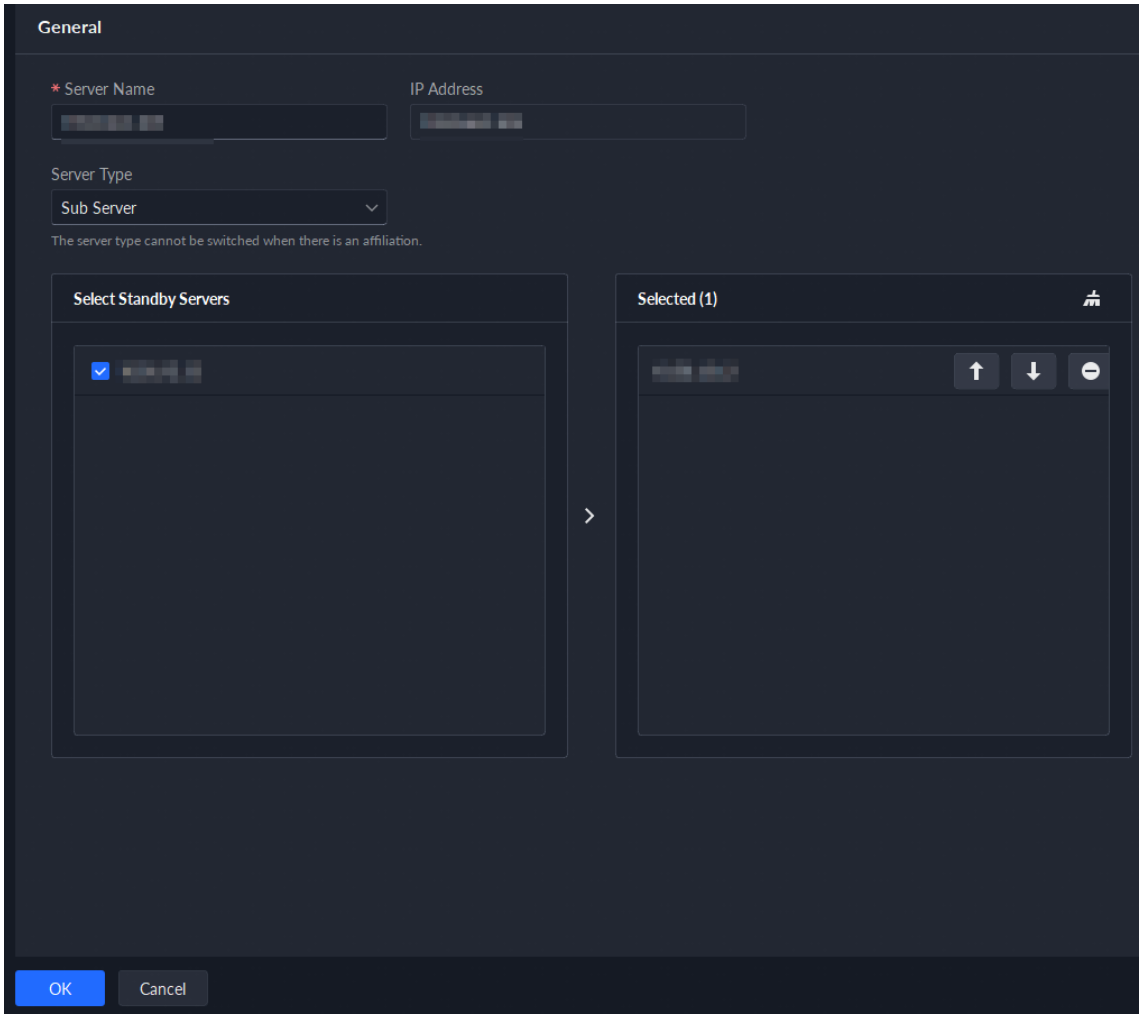


Step 5 Configure the sub-standby relationship in either of the following ways.

- Go to the **Server Configuration** page of the sub server to select a standby server.

  1. Click of a sub server.
  2. On the **Select Standby Server(s)** page, select one or more standby servers.

Figure 5-2 Select a standby server



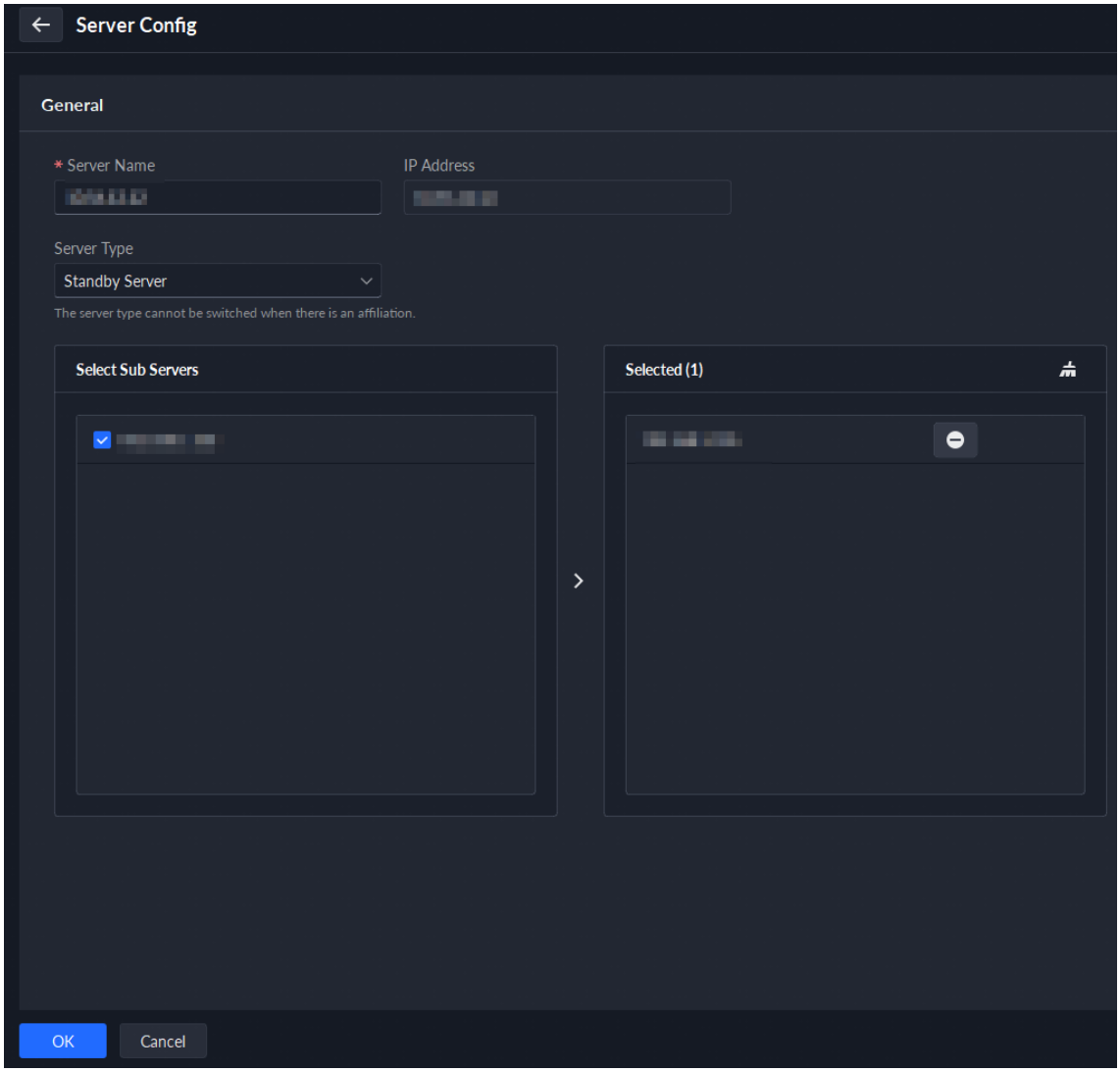
3. Click **OK**.

- Go to the **Server Configuration** page of the standby server to select a sub server.

1. Click of a standby server.
2. On the **Select Sub Server(s)** page, select one or more sub servers.

   You can click to adjust the priority.

Figure 5-3 Select a sub server



3. Click **OK**.

6 Configuring LAN or WAN

6.1 Configuring Router

If the platform is in a local network, you can visit it from the public network by performing DMZ mapping. For the list of the ports to be mapped, see the table below.

Table 6-1 Port matrix (Main platform)

Network Deployment	Service	Platform Listening Port	Application Protocol
PC/mobile client and platform are not on the same network segment.	PC Client Login	443 (NGINX Service)	The HTTPS port that the PC client uses to log in to the platform.
		61616 (MQ Service)	The MQ-openwire port that the PC client uses to receive the platform notifications (TCP).
	Mobile Client Login	443 (NGINX Service)	The HTTPS port that the mobile client uses to log in to the platform.
		1883 (MQ Service)	The MQ-mqtt protocol port that the mobile client uses to receive the platform notifications (TCP).
	VDP App Login	443 (NGINX Service)	The HTTPS port that the VDP app uses to log in to the platform.
	Live View	9100 (MTS Service)	The RTSP port used to watch live video streams (TCP).
		9102 (MTS Service)	The RTSP over TLS port used to perform encrypted transmission of video streams during live view (TCP) .
	Video Playback	9320 (SS Service)	The RTSP port used to play back videos (TCP).
		9322 (SS Service)	The RTSP over TLS port used to perform encrypted transmission of video streams during video playback (TCP).
	View Passed Vehicles Records	40000–49999 (PTS Service)	The port segment used to forward ANPR image streams (TCP).

Network Deployment	Service	Platform Listening Port	Application Protocol
	Video Intercom	5080 (DA_SCS Service)	The registration port that the device/mobile client/PC client uses to register to the platform through SIP (UDP).
		20000–22000 (DA_SCS Service)	The port segment used to forward audio streams of video intercom (UDP).
		9100 (MTS Service)	The RTSP port for video intercom audio/video streams (TCP).
		9102 (MTS Service)	The RTSP over TLS port used to perform encrypted transmission of video intercom audio/video streams (TCP).
Device and platform are not on the same network segment.	Video Intercom	5080 (DA_SCS Service)	The registration port that the device/mobile client/PC client uses to register to the platform through SIP (UDP).
		20000–22000 (DA_SCS Service)	The port segment used to forward audio streams of video intercom (UDP).
		9100 (MTS Service)	The RTSP port for video intercom audio/video streams (TCP).
		9102 (MTS Service)	The RTSP over TLS port used to perform encrypted transmission of video intercom audio/video streams (TCP).
	Video on Wall (stream pulling of platform)	9090 (MGW Service)	The RTSP port that decoders use to pull the stream from the platform to play video on the wall (TCP).
	The device automatically registers to the platform and opens the webpage of the auto registered device.	9005 (SMC Service)	The redirection port that devices use to automatically register to the platform (TCP).
		9500 (ARS Service)	The port used by devices to automatically register to the platform (TCP).
		9399 (BSID Service)	The port used by devices to register sublinks to the platform (TCP).

Network Deployment	Service	Platform Listening Port	Application Protocol
		39550–39649 (BSID Service)	The platform proxy port segment used to open the automatically registered device webpage (TCP).
	Download Device Files/ Access 4G Devices	9399 (BSID Service）	The port used by devices to register sublinks to the platform (TCP).
	Receive ONVIF Device Alarms	8686 (PCPS Service)	The port used by ONVIF devices to push notifications to the platform (TCP).
	Alarm	18800 (SMC Service)	TCP
		18800 (SMC Service)	UDP
		18801 (SMC Service)	HTTP
		18443 (SMC Service)	HTTPS

Table 6-2 Port matrix (Sub platform)

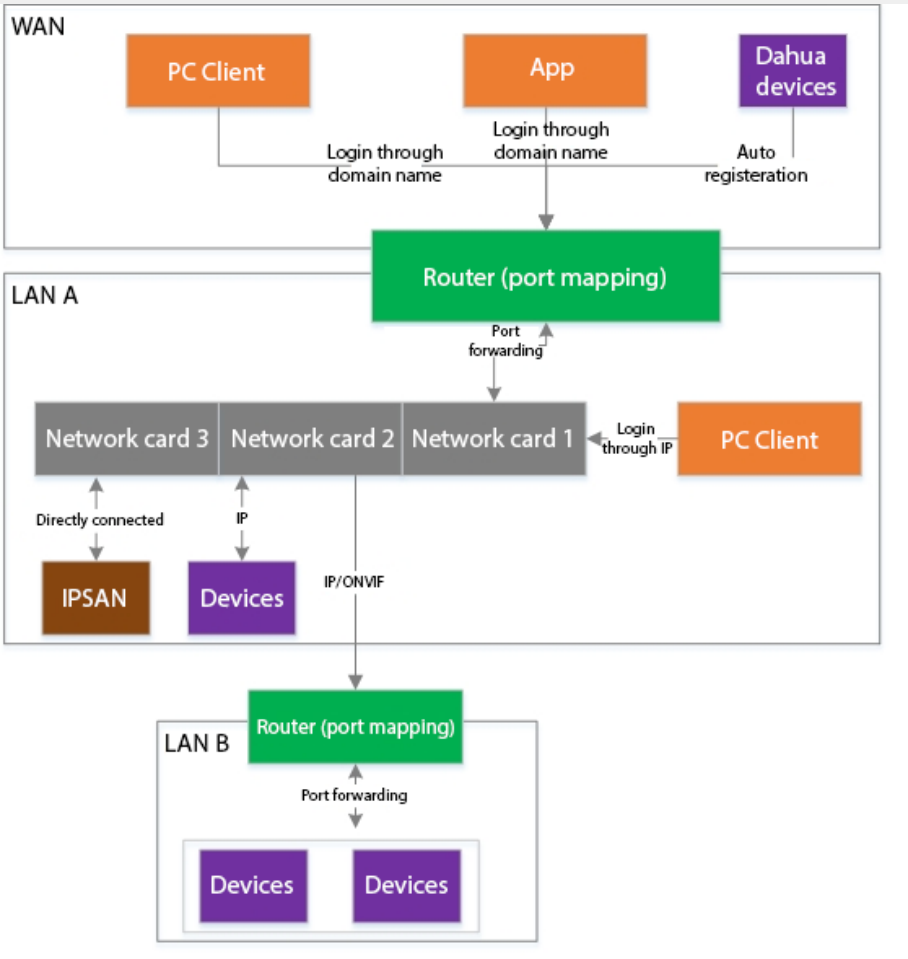
Network Deployment	Service	Listening Port	Application Protocol
PC/mobile client and platform are not on the same network segment.	Live View	9100 (MTS Service)	The RTSP port used to watch live video streams (TCP).
		9102 (MTS Service)	The RTSP over TLS port used to perform encrypted transmission of video streams during live view (TCP) .
	Video Playback	9320 (SS Service)	The RTSP port used to play back videos (TCP).
		9322 (SS Service)	The RTSP over TLS port used to perform encrypted transmission of video streams during video playback (TCP).
	View Passed Vehicles Records	40000–49999 (PTS Service)	The port segment used to forward ANPR image streams (UDP).

Network Deployment	Service	Listening Port	Application Protocol
	Video Intercom	5080 (DA_SCS Service)	The registration port that the device/mobile client/PC client uses to register to the platform through SIP (UDP).
		20000–22000 (DA_SCS Service)	The port segment used to forward audio streams of video intercom (UDP).
		9100 (MTS Service)	The RTSP port for video intercom audio/ video streams (TCP).
		9102 (MTS Service)	The RTSP over TLS port used to perform encrypted transmission of video intercom audio/video streams (TCP).
Device and platform are not on the same network segment.	The device automatically registers to the platform and opens the webpage of the auto registered device.	9500 (ARS Service)	The port used by devices to automatically register to the platform (TCP).
		9399 (BSID Service）	The port used by devices to register sublinks to the platform (TCP).
	Download Device Files/Access 4G Devices	9399 (BSID Service）	The port used by devices to register sublinks to the platform (TCP).
	Receive ONVIF Device Alarms	8686 (PCPS Service)	The port used by ONVIF devices to push notifications to the platform (TCP).
	Video Intercom	5080 (DA_SCS Service)	The registration port that the device/mobile client/PC client uses to register to the platform through SIP (UDP).
		20000–22000 (DA_SCS Service)	The port segment used to forward audio streams of video intercom (UDP).
		9100 (MTS Service)	The RTSP port for video intercom audio/ video streams (TCP).

Network Deployment	Service	Listening Port	Application Protocol
		9102 (MTS Service)	The RTSP over TLS port used to perform encrypted transmission of video intercom audio/video streams (TCP).

- Make sure that the number of the WAN ports is consistent with that of the LAN ports.
- You can configure LAN and WAN mapping and dual network cards mode at the same time. For how to configure dual network cards, see "2.2 Configuring Dual Network Cards".

Figure 6-1 Topology of deploying LAN and WAN mapping and dual networks cards



6.2 Mapping IP or Domain Name

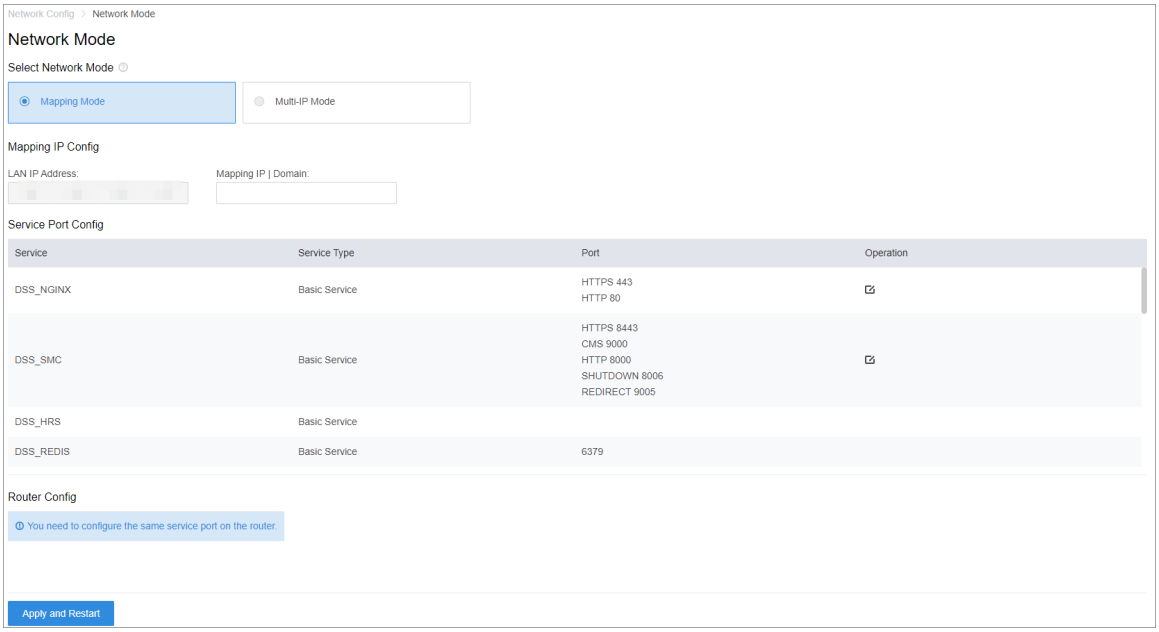
If the platform is deployed in a local network, you can map the IP address of the server to a fixed WAN IP or a domain name, and then log in to the server using the WAN IP or domain name.

Procedure

Step 1 Log in to the Config system.

Step 2 Select **Network Config** > **Network Mode**.

Figure 6-2 Network mode



Step 3 Enter a fixed WAN IP address or a domain name in the **Mapping IP | Domain** box, and then click **OK**.

- If you want to use a domain name, you need to make related configurations on the domain name server.
- The DNS information of the network card must be the same as the domain name server.

Step 4 Click **OK** and then the services will restart.

Appendix 1 Service Module Introduction

Service Name		Function Description
NGINX Proxy Service	NGINX	Provides access to the platform.
System Management Service	SMC	Manages services and provides access to various functions.
Redis Data Cache Service	REDIS	Stores data that is frequently accessed.
MySQL Database Service	MySQL	Stores data for a long time.
System Config Service	CFGS	Monitors system resources and synchronizes configurations across the distributed environment.
MQ Push Notifications Service	MQ	Pushes messages among clients and platforms.
Media Gateway Service	MGW	Acquires video streams for video walls.
Protocol Conversion Proxy Service	PCPS	Accesses third-party video devices.
Device Management Service	DMS	Accesses video devices.
Alarm Distribution Service	ADS	Filters and distributes alarms from devices.
Device Auto Registration Service	ARS	Accesses devices added through automatic registration.
Image Transmission Service	PTS	Accesses ANPR devices and transfers images between the devices and the platform.
Alarm Controller Access Service	MCD	Accesses alarm controllers.
Device Search Service	SOSO	Searches for and obtains configurations from devices in local networks.
Video Intercom Service	SCS	Manages audio talks among PC clients and app, and video intercom devices.
DA Management Service	DAMS	Manages DA_BSID.
Link Management Service	DA_BSID	Downloads files from devices, manages the sleep and wake status of low-power consumption cameras that uses 4G network, and redirects to the webpage of devices added through automatic registration.

Service Name		Function Description
Access Control Management Service	ACDG	Manages MCDDOOR.
Access Control Connection Service	MCDDOOR	Accesses access control devices.
Video Storage Service	SS	Stores and forwards recorded videos on the platform.
Video Decoding to Wall Service	VMS	Accesses decoders outputs videos to video walls.
Object Storage Service	OSS	Stores files of the platform.
Media Forwarding Service	MTS	Forwards real-time video streams.

Appendix 2 RAID

RAID is an abbreviation for Redundant Array of Independent Disks. It is to combine several independent HDDs (physical HDD) to form a HDD group (logic HDD).

Comparing with one HDD, RAID provides more storage capacity and data redundancy. The different redundant arrays have different RAID level. Each RAID level has its own data protection, data availability and performance degree.

RAID Level

RAID Level	Description	Min. HDD Needed
RAID 0	RAID 0 is called striping. RAID 0 is to save the continued data fragmentation on several HDDs. It can process the read and write at the same time, so its read/write speed is N (N refers to the HDD amount of the RAID 0) times as many as one HDD. RAID 0 does not have data redundant, so one HDD damage might result in data loss that cannot be restored.	2
RAID 1	It is also called mirror or mirroring. RAID 1 data is written to two HDDs equally, which guarantee the system reliability and can be repaired. RAID 1 read speed is almost close to the total volume of all HDDs. The write speed is limited by the slowest HDD. At the same time, the RAID 1 has the lowest HDD usage rate. It is only 50%.	
RAID 5	RAID 5 is to save the data and the corresponding odd/even verification information to each HDD of the RAID 5 group and save the verification information and corresponding data to different HDDs. When one HDD of the RAID 5 is damaged, system can use the rest data and corresponding verification information to restore the damaged data. It does not affect data integrity.	3
RAID 6	Based on the RAID 5, RAID 6 adds one odd/even verification HDD. The two independent odd/even systems adopt different algorithms to ensure high data reliability. Even when two HDDs are broken at the same time, there is no data loss risk. Comparing to RAID 5, the RAID 6 needs to allocate larger HDD space for odd/even verification information, so its read/write is even worse.	4
RAID 10	RAID 10 is a combination of the RAID 1 and RAID 0. It uses the extra high speed efficient of the RAID 0 and high data protection and restoring capability of the RAID 1. It has high read/write performance and security. However, the RAID 10 HDD usage efficiency is as low as RAID 1.	

RAID Capacity

See the sheet for RAID space information.

Capacity N refers to the mini HDD amount to create the corresponding RAID.

RAID Level	Total Space of the N HDD
RAID 0	N × minN
RAID 1	minN
RAID 5	(N-1) × minN
RAID 6	(N-2) minN
RAID 10	(N/2) × minN

Appendix 3 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") places great emphasis on cybersecurity and privacy protection. We continuously allocate special funds to enhance employees' awareness and capabilities in security, and ensure sufficient security protection for our products. Dahua has established a professional security team to provide comprehensive security empowerment and control throughout the entire product lifecycle, including design, development, testing, production, delivery, and maintenance. Dahua products adhere to the principle of minimum necessary data collection, service minimization, strict prohibition of backdoors, and the disabling of unnecessary and insecure services (such as Telnet). We continuously introduce innovative security technologies to bolster the security capabilities of our products. Additionally, we go above and beyond by providing global users with security alarm and 24/7 security emergency response services. This approach ensures that we are better safeguarding their security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report potential risks or vulnerabilities to the Dahua PSIRT. They can do so by visiting the cybersecurity section on the Dahua website.

The security of software platforms not only relies on the continuous attention and efforts from manufacturers throughout R & D, production, and delivery, but also requires active participation from users. Users should remain attentive to the environment and methods to ensure its secure operation. To this end, we suggest users to safely use the software platform, including but not limited to:

Account Management

1. **Use Strong 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. **Change Password Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.
3. **Assign Accounts and Permissions Reasonably**

   According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.
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. **Set and Update Passwords Reset Information Timely**

   The platform supports password reset function. To reduce the risk of being attacked, please set up related information for password reset in time. 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.
6. **Enable Account Binding IP/MAC**

It is recommended to enable the account binding IP/MAC mechanism to further improve access security.

Service Configuration

1. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.
2. **Disable Unnecessary Services and Choose Secure Modes**

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

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

   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.

Network Configuration

1. **Enable Firewall Allowlist**

   We suggest you to enable allowlist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the allowlist.
2. **Network Isolation**

   The network should be isolated by partitioning the video monitoring network and the office network on the switch and router to different VLANs. This prevents attackers from using the office network to launch Pivoting attacks on the video monitoring network.

Security Auditing

1. **Check Online Users**

   It is recommended to check online users irregularly to identify whether there are illegal users logging in.
2. **View the Platform Log**

   By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

Physical Protection

We suggest that you perform physical protection to the device that has installed the platform. 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.

Perimeter Security

We suggest that you deploy perimeter security products and take necessary measures such as authorized access, access control, and intrusion prevention to protect the software platform security.

ENABLING A SMARTER SOCIETY AND BETTER 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