ConfigTool (Windows Version)

User’s Manual

V1.1.7

Foreword

General

This manual introduces the functions and operations of the ConfigTool (hereinafter referred to as "the Tool").

Safety Instructions

The following categorized signal words with defined meaning 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, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.1.7	1. Added "Join User Experience Improvement Program" and "Privacy Policy". 2. Updated "4.5.3 Access Control Devices". 3. Added "4.5.6 Alarm Host Devices". 4. Update pictures in "4.8 Building Configuration". 5. Updated "5.3.1 Configuring Parameters".	May 2021
V1.1.6	Updated functions in building config.	February 2021
V1.1.5	Updated building configuration.	January 2021

Version	Revision Content	Release Time
V1.1.4	1. Added "2 Installation and Uninstallation", "4.5.4 VDP", "4.5.5 Android Digital Signage", and "4.8 Building Configuration". 2. Updated pictures in the manual. 3. Modified "4.5.3 Configuring ACS Parameters" and "4.9 CGI Protocol".	September 2020
V1.1.3	1. Added batch config items. 2. Optimized user interface. 3. Added to support ACS devices.	June 2020
V1.1.0	Added upgrade transmission speed.	March 2020
V1.0.7	1. Added "Help" section. 2. Deleted "Online Upgrade" section.	September 2019
V1.0.6	Updated "4.7 Resetting Device Password."	July 2019
V1.0.5	1. Updated the pictures in "4.6 Configuring System Settings." 2. Changed the notice box to the new one in "4.4 Upgrad", and "3.9 Online Upgrade." 3. Updated the template management interface, and add the description of profile management in "4.5.2 Configuring Video Device Parameters."	March 2019
V1.0.4	1. Added a notice box when you click reset password in the reset password menu. 2. Added a notice box when click batch download and upgrade detect in the online upgrade menu. 3. Added the function to get back video password in the system settings menu.	April 2018
V1.0.3	Added cybersecurity recommendations and online upgrade section.	September 2017
V1.0.2	Modified the basic operations section.	March 2017
V1.0.1	1. Added the description of uninstallation. 2. Modifed the basic operations section.	November 2016
V1.0.0	First release.	February 2016

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.

- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Table of Contents

1 Overview

The Tool provides the following functions to configure and maintain devices such as IPC, NVR, Access Controller and Video Intercom:

- Initialize the device.
- Change device IP.
- Upgrade device.
- Configure video and encoding parameters and profile mode; Configure access controller (card No. byte revert of different channels, TCP port No., log, and more); Configure VDP (device details, physical information. Sip server information); Configure Android digital signage (APP Configuration, Android commission, and log exporting).
- Synchronize device time, reboot device, restore system default, modify device password, reset password and perform batch configuration.
- Configure VTO and VTH information.
- Configure device information in batches through CGI commands or tables.

Do not use the Tool with Device Diagnostic Tool, SmartPSS (Smart Professional Surveillance System) or DSS (Digital Surveillance System) at the same time; otherwise it might cause device search exceptions.

2 Installation and Uninstallation

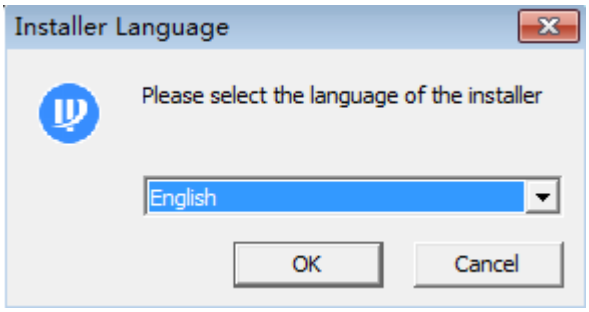
This chapter introduces how to install and uninstall the Tool.

2.1 Installation

Make sure that you have the Tool installation package; if not, contact customer service.

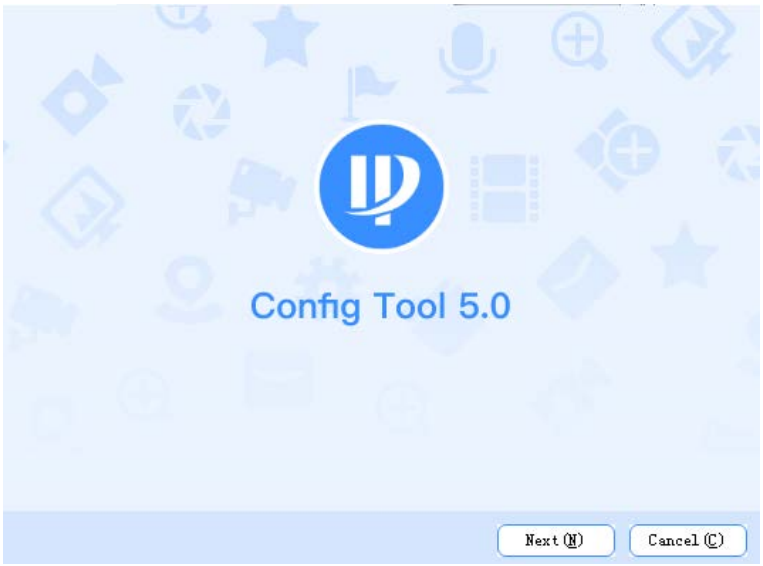
Step 1 Double-click the installation package.

Figure 2-1 Installer language



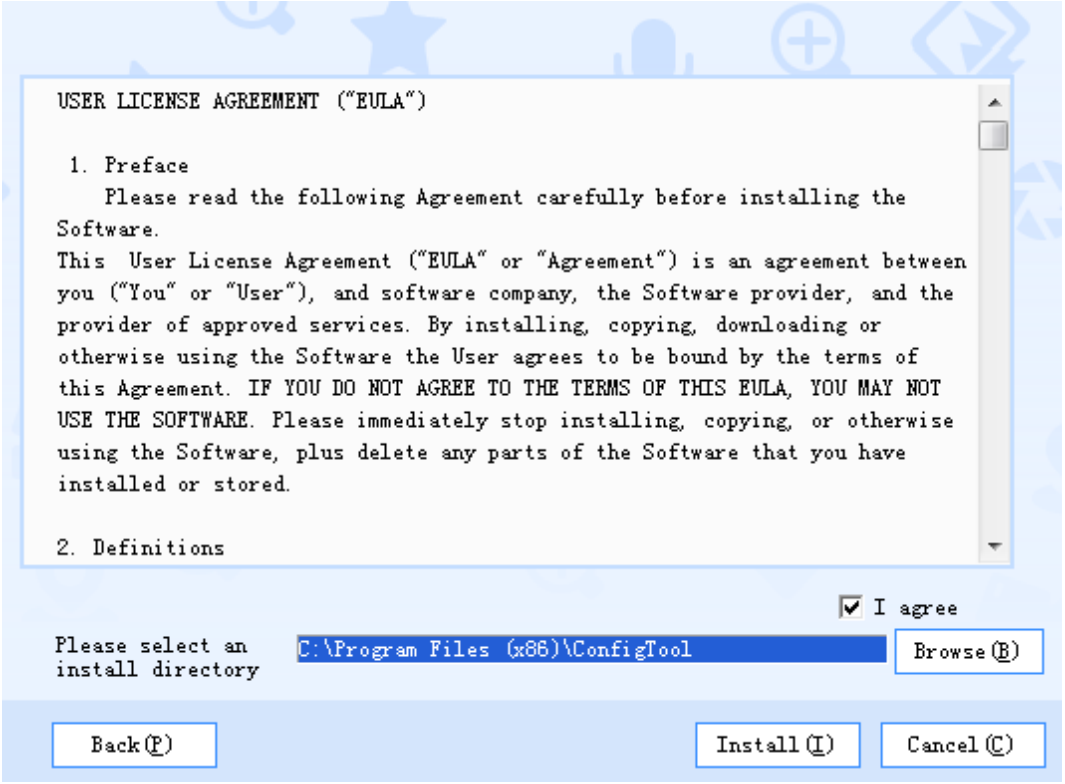
Step 2 Select **English** as the installer language, and then click **OK**.

Figure 2-2 Welcome



Step 3 Click **Next**.

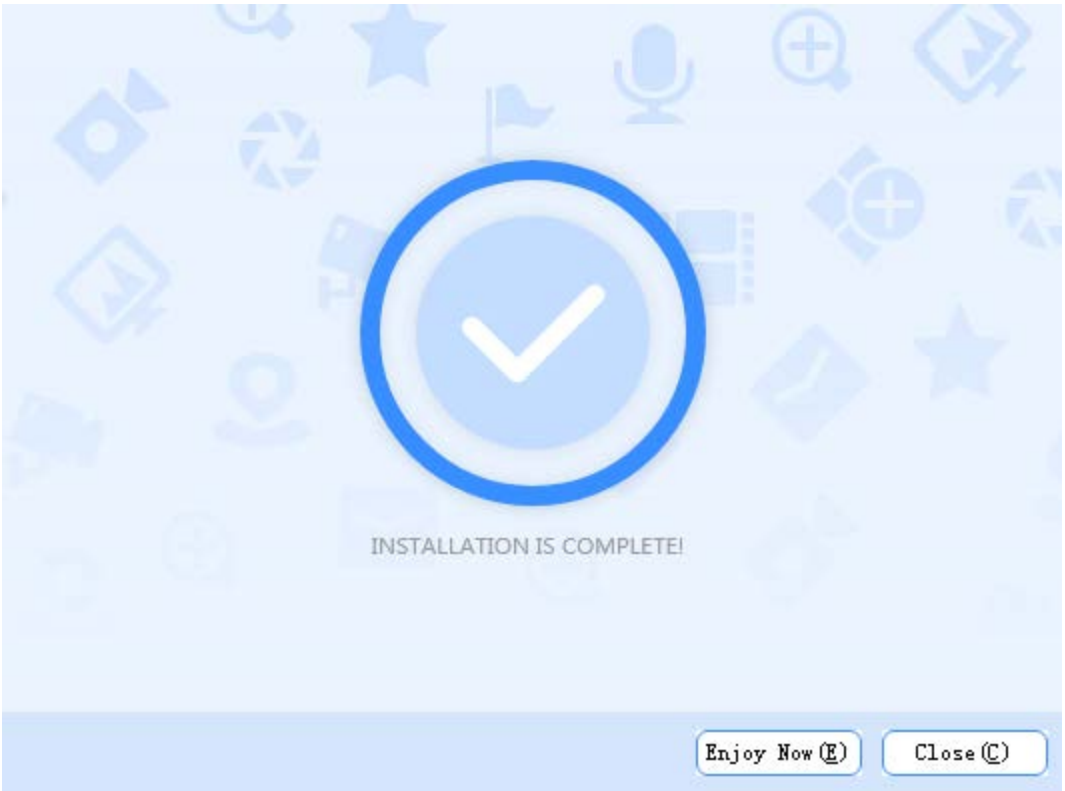
Figure 2-3 Selecting an install directory



Step 4 Read the *User License Agreement*, select **I agree**, and then click **Browse** to select the save path.

Step 5 Click **Install**.

Figure 2-4 Install

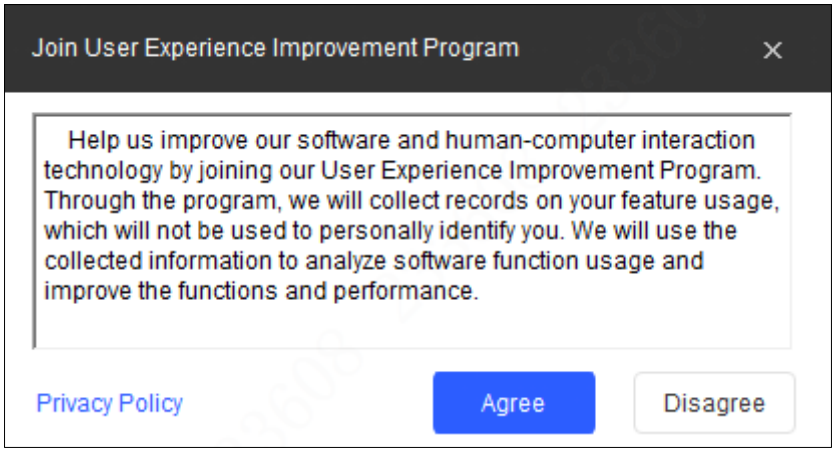


Step 6 Click **Enjoy Now** to complete the installation and start the Tool, or click **Close** to exit.

Step 7 Click **Agree** to join user experience improvement program.

Click **Privacy Policy** to view the specific content.

Figure 2-5 Join user experience improvement program

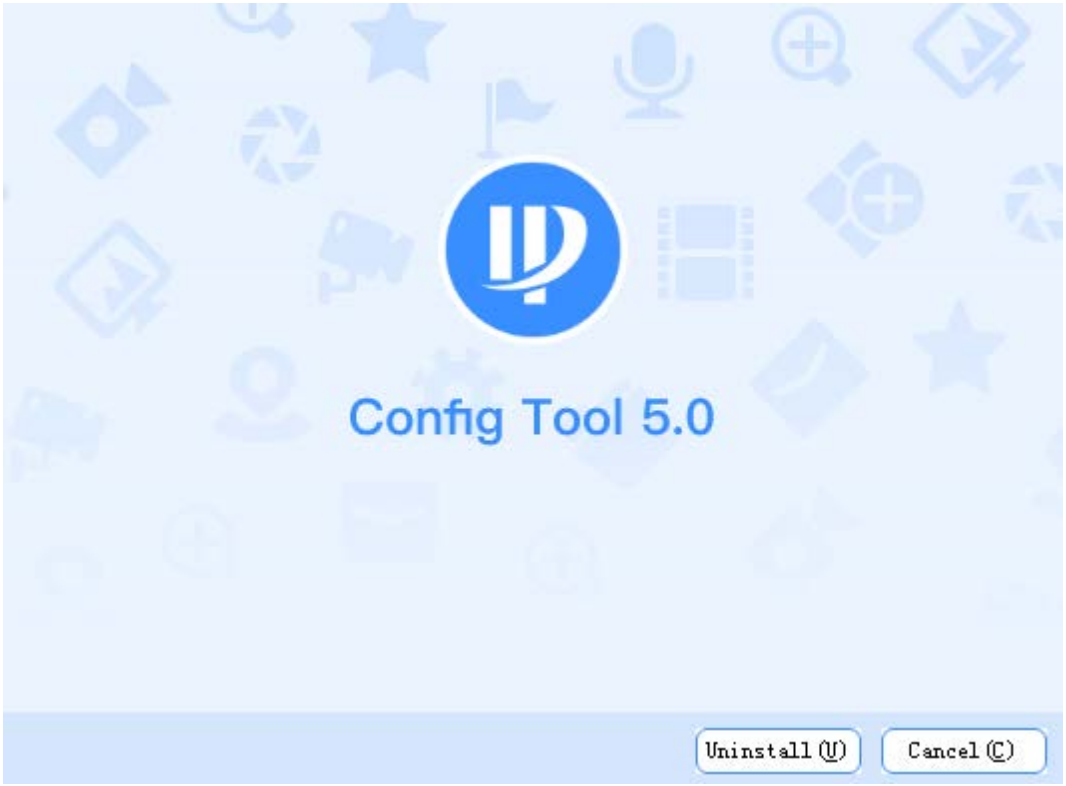


Step 8 (Optional) or click **Close** to complete the installation and close the Tool.

2.2 Uninstallation

Step 1 On your computer (take Windows 7 as an example), click **Start > All Programs > ConfigTool > Uninstall ConfigTool**.

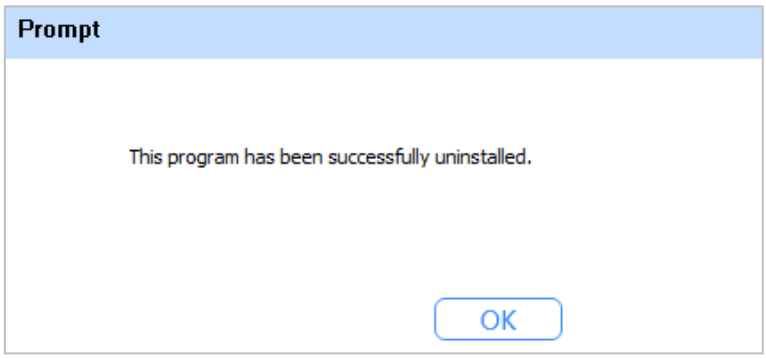
Figure 2-6 Uninstall



Step 2 Click **Uninstall** to uninstall the Tool.

After the uninstallation is completed, the **Notice** interface will be displayed**.**

Figure 2-7 Notice



Step 3 Click **OK** to complete the uninstallation.

3 Main Interface

After starting the Tool, the main interface is displayed.

- After start, the Tool searches devices according to the network segments set in **Search setting**.
- **Current Segment Search** check box is selected by default.

Figure 3-1 Main interface

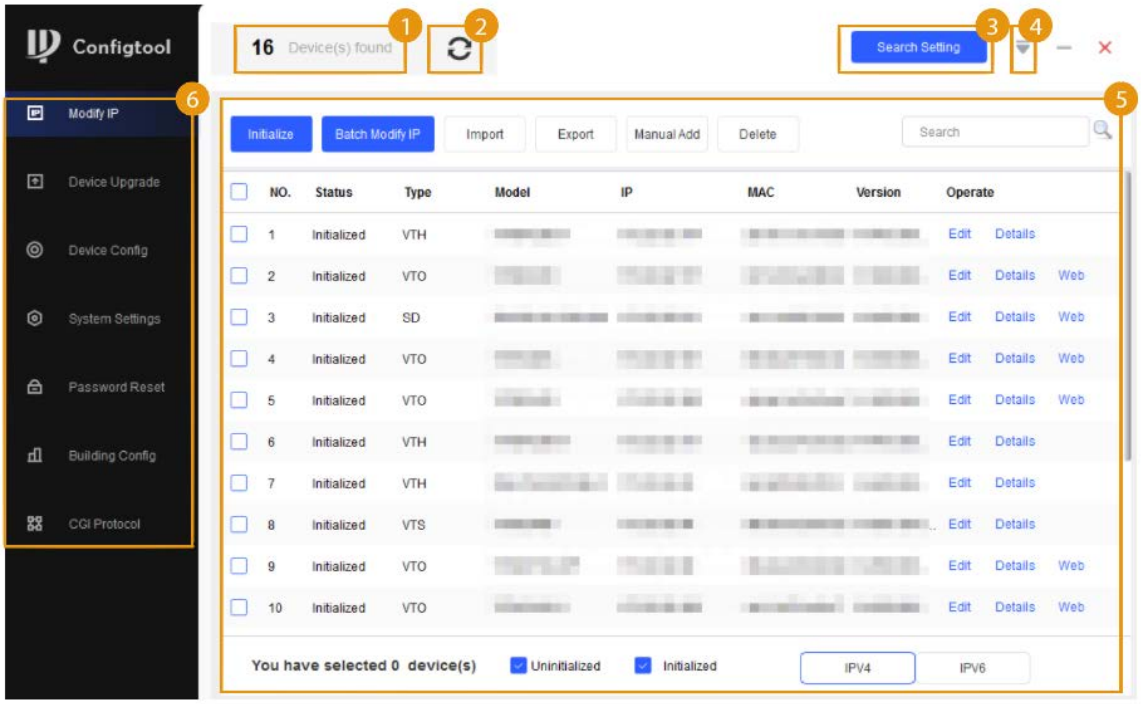


Table 3-1 Main interface description

No.	Function	Description
1	—	Displays searched devices.
2	Refresh	Click to refresh the device list that is displayed in the main interface.
3	Search Setting	You can search the devices within the current network segment or other network segments.
4	Help	Click to check the **Help** file, software license, software version and related parameters.

No.	Function	Description
5	Main interface	• **Initialize**: Select one or multiple devices to start initializing them. • **Batch Modify IP**: Select multiple devices to modify their IP addresses. • **Import**: Import one or multiple devices through template. • **Export**: Select one or multiple devices to export device details. • **Manual Add**: Add a device by entering device details such as IP address, type, username, password and port. • **Delete**: Select one or multiple devices to remove from the list.
6	Functions	• **Modify IP**: Modify IP address of one device or multiple devices. • **Device Upgrade**: Upgrade device versions. • **Device Config**: Configure encoding, image, and profile management. • **System Settings**: Set device system time, restart device, restore device, modify password and reset password. • **Password Reset**: Reset password through the QR code and XML file. • **Building Config**: Add building organization nodes, link building devices and synchronize configurations. • **CGI Protocol**: Configure device information in batches through CGI commands or tables.

4 Basic Operations

4.1 Adding Devices

You can add one or more devices as needed.

⚠

Make sure that the device is in the same network segment with the PC installed with the Tool; otherwise the Tool cannot find the device.

4.1.1 Adding One Device

Step 1 Click Modify IP.

Step 2 Click Manual Add.

Step 3 Select IP Address or Device SN from **Add Type** list.

Figure 4-1 Manual add (IP address)

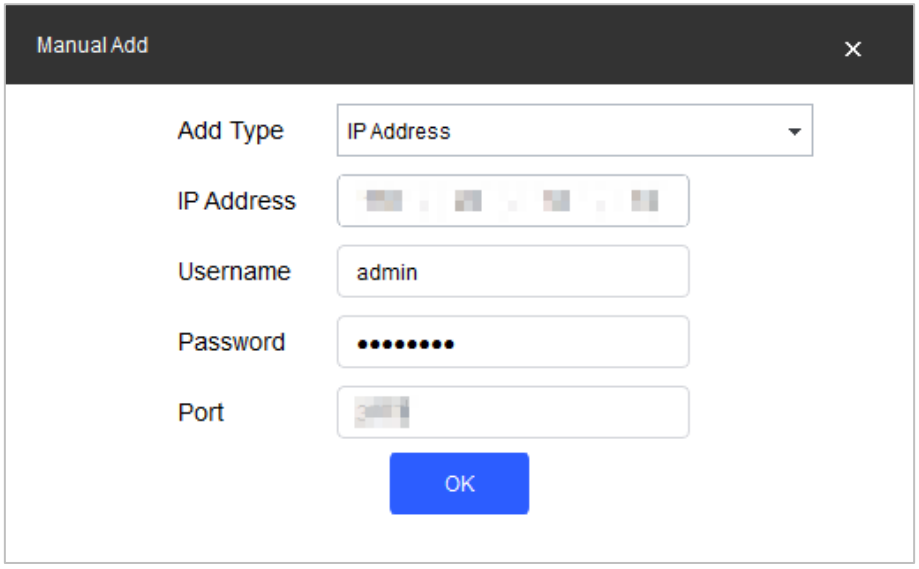
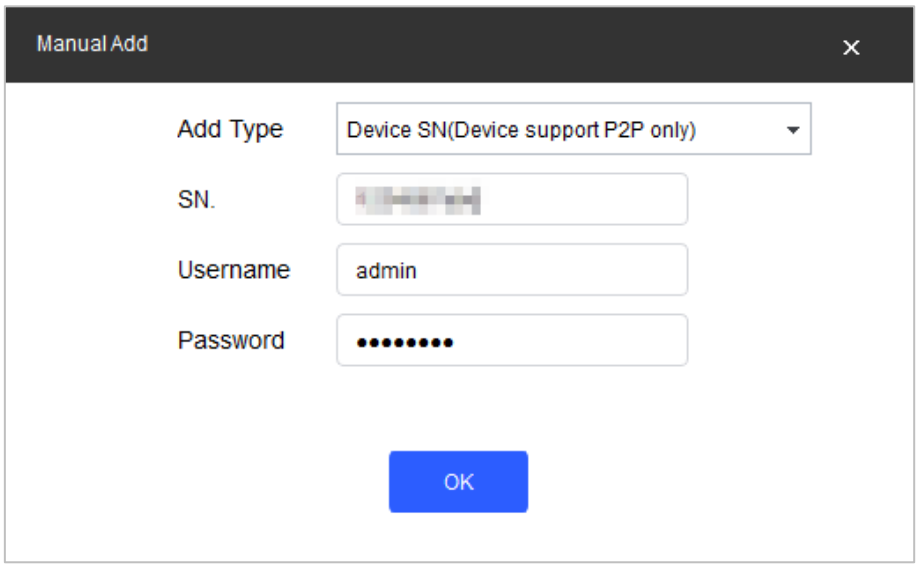


Figure 4-2 Manual add (Device SN)



Step 4 Configure parameters.

Table 4-1 Manual add parameters

Add Method	Parameter	Description
IP Address	IP Address	The IP address of the device.
	Username	The user name and password for device login.
	Password	
	Port	The device port number.
Device SN (Device support P2P only)	SN	The serial number of the device.
	Username	The user name and password for device login.
	Password	

Step 5 Click **OK**.

The newly added device appears in the device list.

4.1.2 Adding Multiple Devices

You can add multiple devices through searching devices or importing the template.

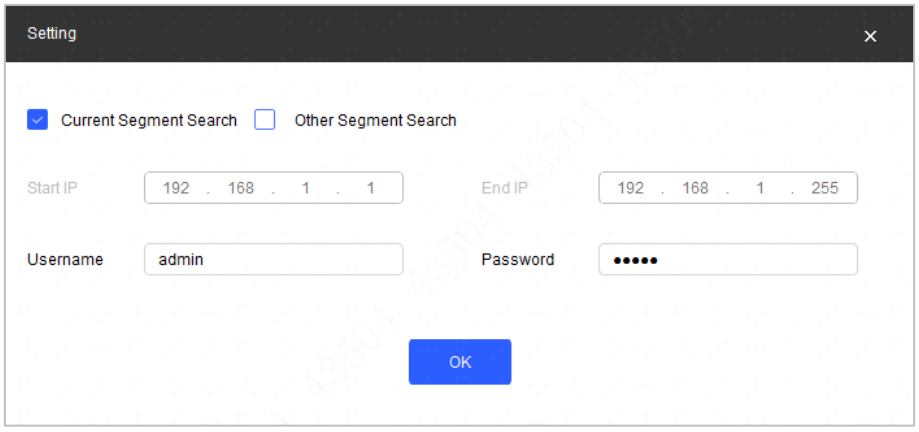
4.1.2.1 Adding by Searching

You can add multiple devices by searching in the current segment or other segment.

You can set filtering conditions to search specified devices quickly.

Step 1 Click Search Setting.

Figure 4-3 Setting



Step 2 Select search method. **Current Segment Search** is selected by default.

- Current Segment Search
  Select the **Current Segment Search** check box. Enter the user name in the **Username** box and the password in the **Password** box. The system will search devices accordingly.
- Other Segment Search
  Select the **Other Segment Search** check box. Enter IP address in the **Start IP** box and **End IP** box respectively. Enter user name and password. The system will search the devices accordingly.

- If you select both the **Current Segment Search** check box and the **Other Segment Search** check box, the system searches devices under both conditions.
- Use the login username and password when you want to modify IP, configure the system, update the device, restart the device, and more.

Step 3 Click **OK**.

Results will appear in the device list on the main user interface.

- Click to refresh the device list.
- The system saves the search conditions when exiting the software and reuses the same conditions when the software is launched again.

4.1.2.2 Adding by Importing Device Template

You can add devices by filling in and importing an Excel template. You can import 1000 devices at most.

Close the template file before importing devices; otherwise the import will fail.

Step 1 Click Modify IP, select one device, click **Export**, and then follow the on-screen guide to save template file locally.

Step 2 Open the template file, and then fill in the information of devices to be added.

Step 3 Click **Import**, select the template and click **Open**.

The system imports the device details. After the import completes, a success notice is displayed.

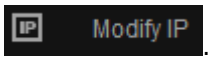
Step 4 Click **OK**.

The newly imported devices appear in the device list.

4.2 Initializing Devices

You can initialize one or multiple devices as needed.

- This function is available on select models.
- The initializing operation can only be performed to the devices within the local area network.
- Operations cannot be performed on uninitialized devices, and they do not appear on other interfaces of the Tool.

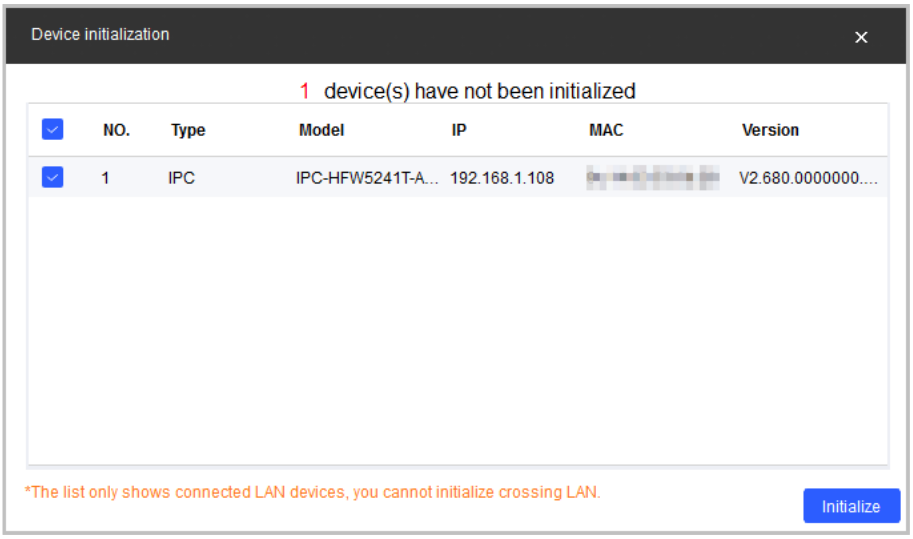
Step 1 Click 

.

Step 2 Select one or several uninitialized devices.

Step 3 Click Initialize.

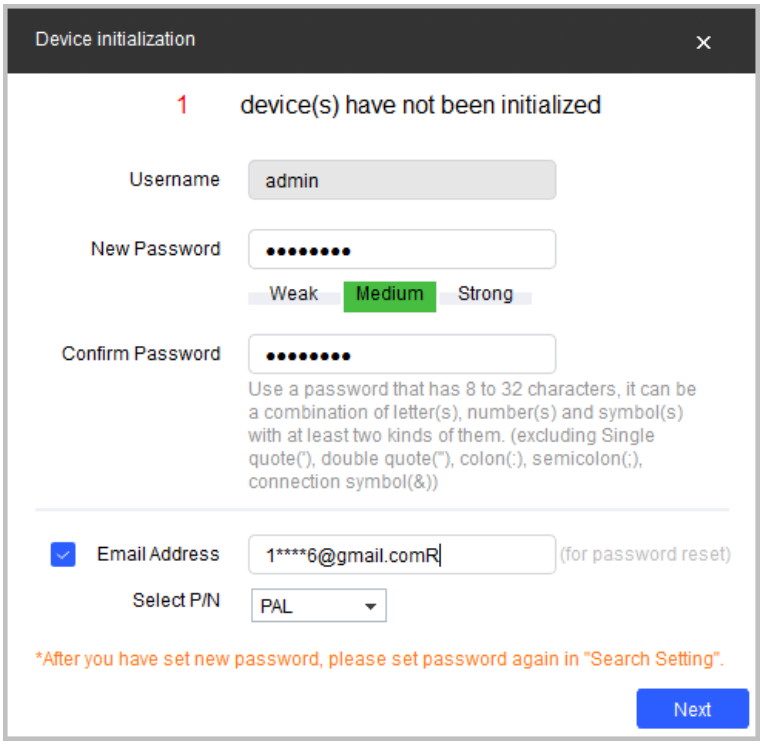
Figure 4-4 Device initialization (1)



Step 4 Select devices to be initialized, and then click **Initialize**.

- If you do not provide the reserved information for password reset, you can only reset the password through XML file.
- When initializing multiple devices, the Tool initializes all devices based on the password reset mode of the first selected device.

Figure 4-5 Device initialization (2)



Step 5 Configure the initialization parameters for the device.

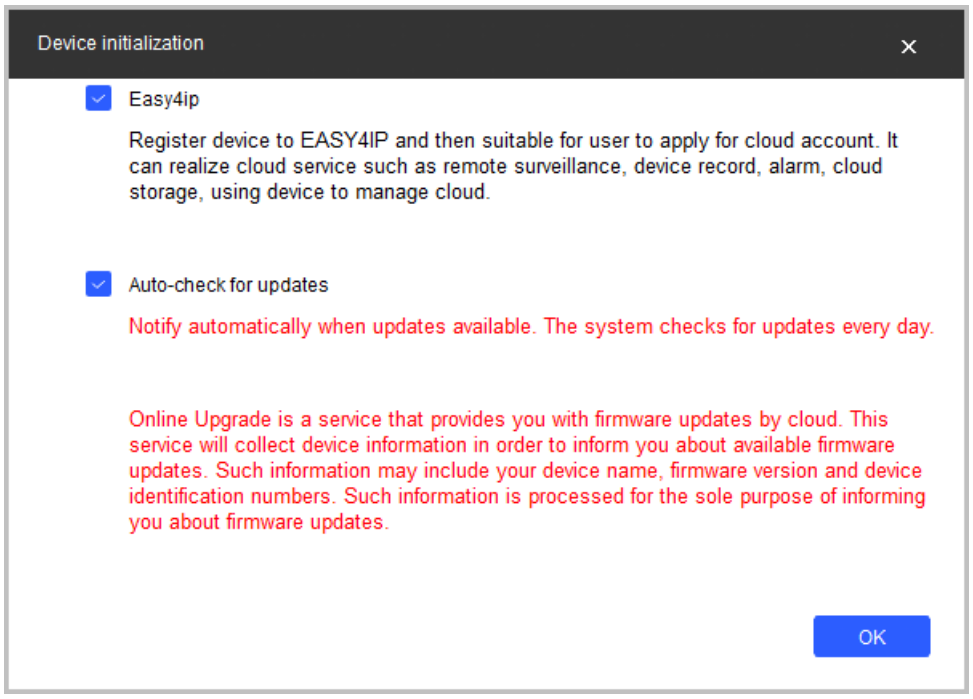
Table 4-2 Initialization parameters

Parameter	Description
Username	The user name is **admin** by default.
New Password	Enter your new password. A notice appears informing you of the strength of your new password. The password might vary depending on the devices, the actual password shall prevail.
Confirm Password	Confirm the new password.
Email Address	Selected by default. The email address will be used for password reset.

Some devices do not support automatic detection and Easy4ip.

Step 6 Click **Next**.

Figure 4-6 Device initialization (3)

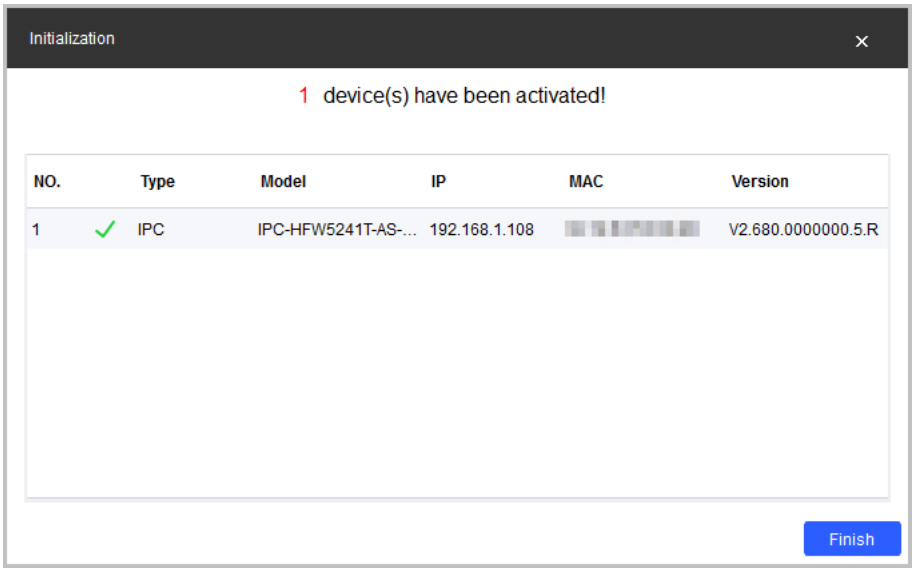


Step 7 Select **Easy4ip** or select **Auto-check for updates** as needed. If neither is needed, leave them unselected.

Step 8 Click **OK**.

Click the success icon (✓) or click the failure icon (⚠) for details.

Figure 4-7 Initialization



Step 9 Click **Finish**.

After initialization is completed, the status of the devices shows as **Initialized** on the main interface of the Tool. The devices also appear on other interfaces of the Tool.

4.3 Modifying IP

You can modify IP for one or more devices at a time.

You can modify IP in batches only if the login passwords for all the devices are the same; otherwise you can only modify one IP at a time.

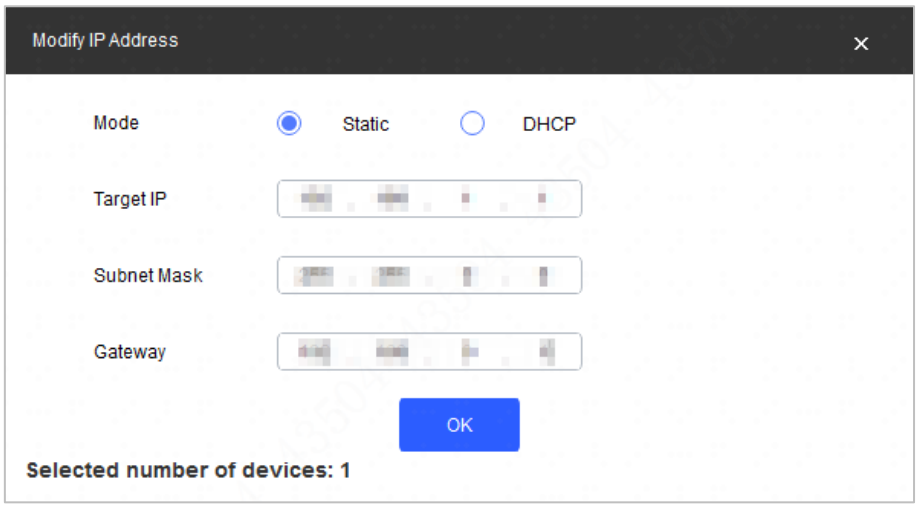
4.3.1 Modifying One IP

Step 1 Click Modify IP.

Step 2 Select the device for which you want to modify IP, and then click **Edit**.

If the device is not in the device list, perform search again. For details, see "4.1 Adding Devices."

Figure 4-8 Modify IP address



Step 3 Configuring the IP address as needed.

- DHCP mode: If the DHCP server is available in the network, when you select **DHCP**, the device will automatically obtain the IP address from the DHCP server.
- Static mode: When you select **Static**, you need to enter **Target IP**, **Subnet Mask**, and **Gateway**. The IP address of the device will be changed to the one you set.

Step 4 Click **OK**.

4.3.2 Modifying IP in Batches

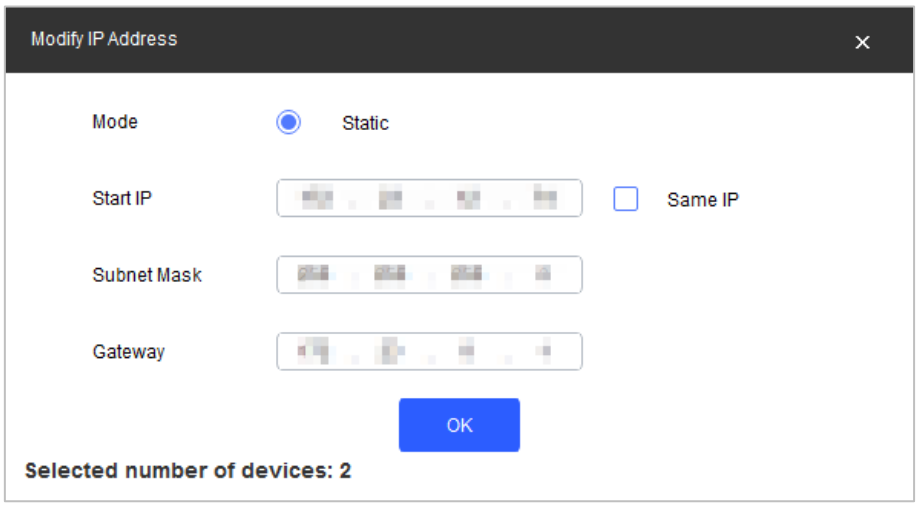
Step 1 Click Modify IP.

Step 2 Select the devices for which you want to modify IP.

If the device is not in the device list, perform search again. For details, see "4.1 Adding Devices."

Step 3 Click Batch Modify IP.

Figure 4-9 Modify IP address (3)



Step 4 Configuring the IP address as needed.

- DHCP mode: If the DHCP server is available in the network, when you select **DHCP**, the device will automatically obtain the IP address from the DHCP server.
- Static mode: When you select **Static**, you need to enter **Start IP**, **Subnet Mask**, and **Gateway**. The IP addresses of the devices will be modified successively starting from the first IP entered.

If you select the **Same IP** check box, the IP address of the devices will be set to the same one.

Step 5 Click **OK**.

4.4 Upgrading Devices

You can upgrade one or more devices on the PC where the Tool is located.

Upgrade speed varies depending on the package size.

- If package < 100 MB, the Tool loads the package 1 KB every time. The speed cannot be modified.
- If package size ≥ 200 MB, the Tool loads the package at 16 KB every time. The speed cannot be modified.
- If 100 MB≤ package size < 2 G, the Tool loads the package 1 KB every time. To speed up the process, you can set the speed to 16 KB every time. For details, see "5.3 Setting."

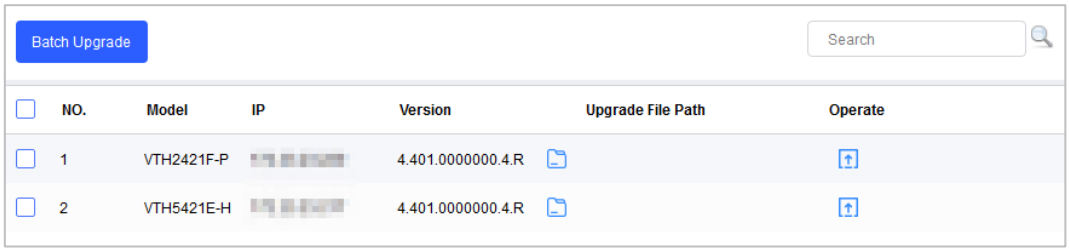
If the device disconnects during update, the device might reboot and automatically tries to update again.

- If the system notices **Upgraded successfully,** search the devices again and the devices with upgraded versions show up.
- If the system notices **Wait for retry**, wait for 1–2 minutes and then retry.
- If the system notices **Upgrade overtime** or **Failed to upgrade**, search the device and upgrade again.

4.4.1 Upgrading One Device

Step 1 Click Device Upgrade.

Figure 4-10 Upgrade



Step 2 Click to the device that you want to upgrade, and then select the specific file that needs to be upgraded and click **Open**.

If the device is not in the device list, perform search again. For details, see "4.1 Adding Devices."

Step 3 Click to start upgrading.

After upgrade is complete a **Notice** dialog box will be displayed indicating the device will be rebooted. Then the device reboots automatically.

4.4.2 Upgrading Devices in Batches

You can upgrade multiple devices to the same software version.

Step 1 Click Device Upgrade

Step 2 Select the devices that need to be upgraded.

- If the device is not in the device list, perform search again. For details, see "4.1 Adding Devices."
- Make sure selected devices are all able to receive the same software update.

Step 3 Click Batch Upgrade.

Figure 4-11 Batch Upgrade

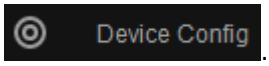
Step 4 Click **Browse** to select the files that need to be upgraded.

Step 5 Click **OK**.

4.5 Configuring Device Parameters

Configure device parameters such as encoding, video, and profile.

4.5.1 Accessing the Configuration Interface

Step 1 Click 

.

Step 2 Select the device in the device list, and then click **Get Device Info** or double-click the device.

If the device is not in the device list, perform search again. For details, see "4.1 Adding Devices."

Step 3 (Optional) Select the device in the device list, and then click **Get Device Info** or double-click the device.

Step 4 (Optional) If the login dialog box is displayed, enter your username and password, and then Click **OK**.

- For an encoder, the **Encode** interface is displayed.
- For an ACS device, the **ACS Config** interface is displayed.

4.5.2 Configuring Video Device Parameters

You can configure device parameters such as the encoding, video, and profile.

The interface and parameters might vary depending on the device type and model, and the actual interface shall prevail.

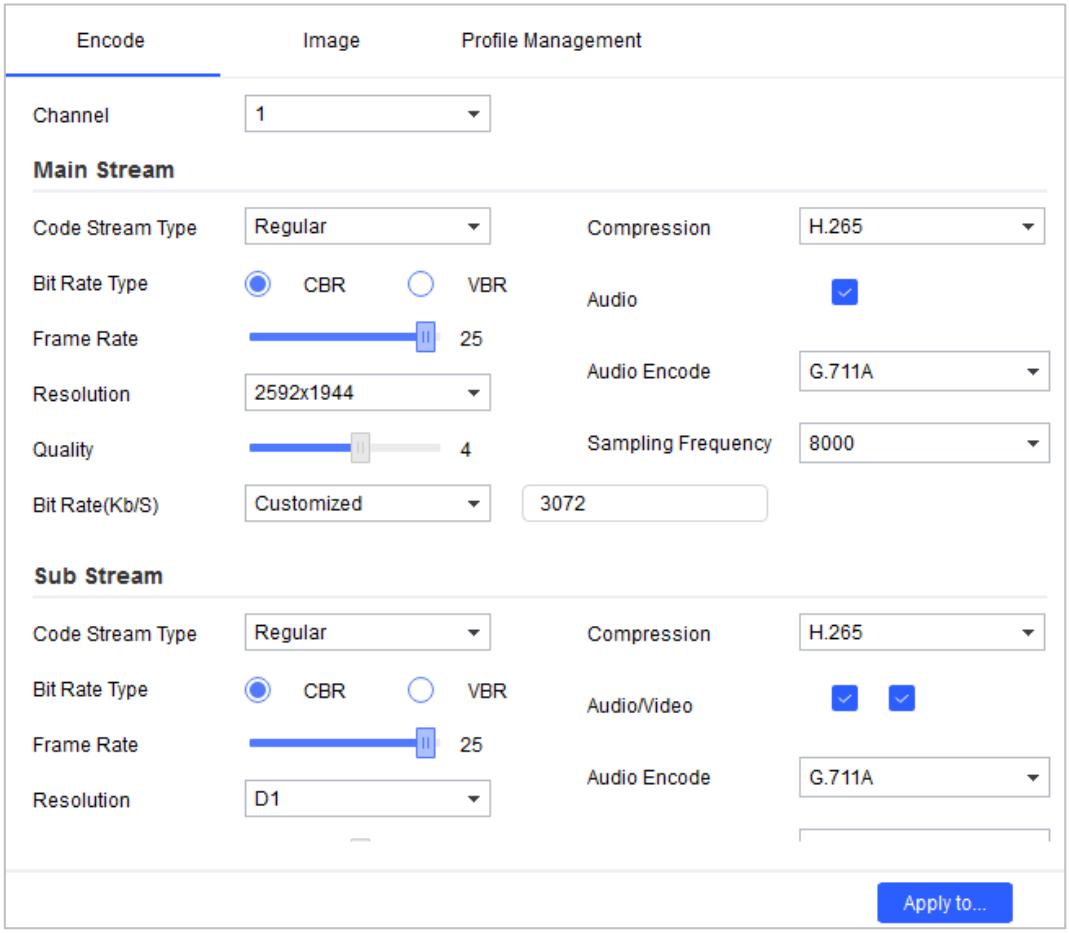
4.5.2.1 Configuring Encoding Parameters

You can configure parameters such as code stream type, compression and resolution of the device.

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 On the **Encode** interface, set the parameters for main stream and sub stream.

Figure 4-12 Encode



The encoding parameters might vary with different models, and the actual product shall prevail.

Table 4-3 Encode parameters

Parameter	Description
Channel	Select channel number.
Code Stream Type	Includes **Regular**, **Motion**, and **Alarm**. The sub stream only supports **Regular** type.
Compression	Includes the following video encoding modes: ● H.264: Main profile encoding. ● H.264B: Baseline profile encoding. ● H.264H: High profile encoding. ● H.265: Main profile encoding. ● MJPG: Under this mode, the video image requires a higher bit rate to ensure video quality. It is recommended to use the maximum bit rate value to get the best results. ● SVAC2.0: SVAC2.0 encoding

Parameter	Description
Bit Rate Type	Includes the following two types of bit rates: ● Constant Bit Rate (CBR): The bit rate is fluctuating around the set value without changing significantly. ● Variable Bit Rate (VBR): The bit rate changes along with the monitored environment. When the compression is set as **MJPG**, the bit rate can only be **CBR**.
Frame Rate	Total frames per second. The higher the frame rate, the more clear and smooth the image will become.
Resolution	Video resolution. The maximum video resolution might be different depending on your device model.
Quality	Video image quality level. You can configure this parameter when the bit rate type is set as **VBR**.
Bit Rate (Kb/S)	Select a suitable value as needed. You can configure this parameter when the bit rate type is set as CBR.
Audio/Video	● To enable the audio function, select the **Audio** check box. ● To monitor with the sub stream, select the **Video** check box. For the sub stream, you can enable the audio function only after the video function is already enabled. In the **Sub Stream** section, the two check boxes next to **Audio/Video** stand for Audio and Video respectively. To enable audio, select the first check box; for video, select the second one.
Audio Encode	Audio encoding modes includes G.711A, G.711Mu, G.726, and AAC. The setting of audio encoding mode will apply to both audio and voice intercom.
Sampling Frequency	The sampling frequency of the audio.

Step 3 Click **OK** to complete settings.

Step 4 (Optional) Apply the configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

4.5.2.2 Configuring Video Parameters

You can check the live video and set video effects.

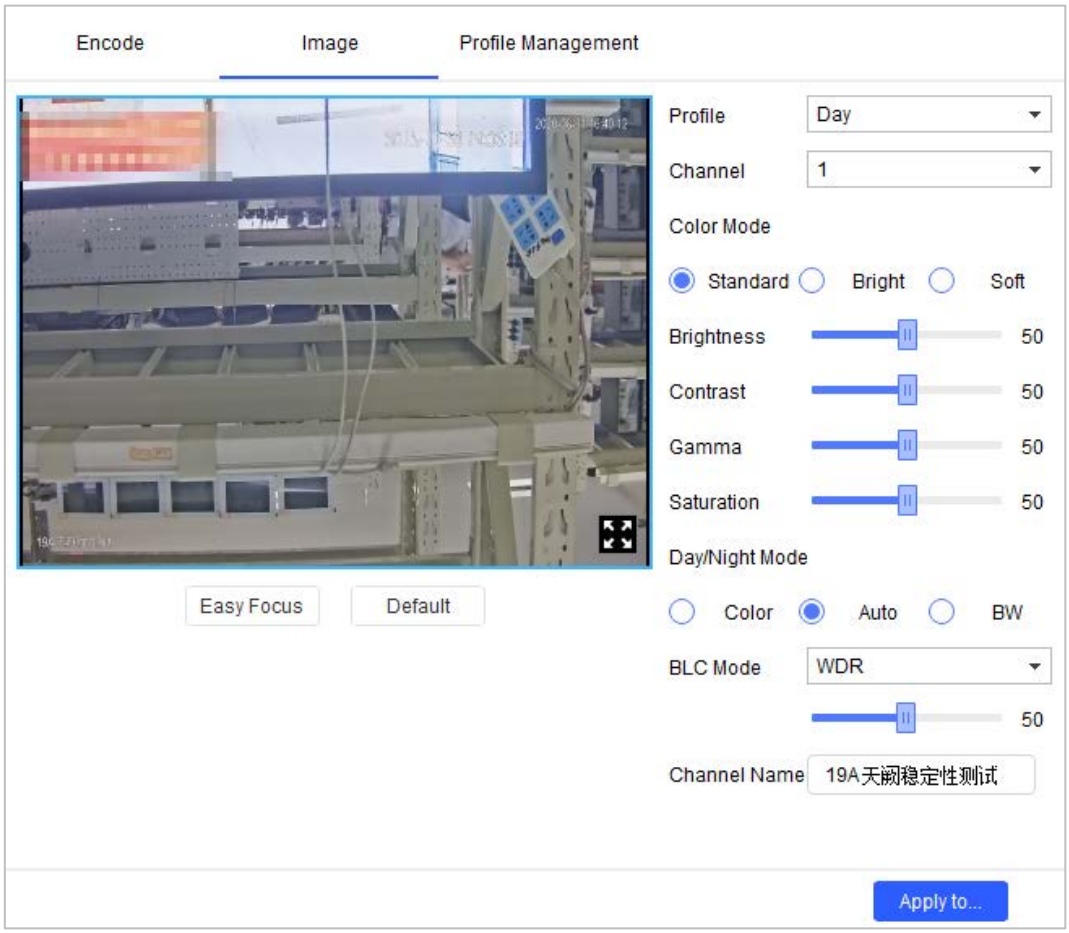
Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Click the **Image** tab.

- Click **Default** to restore the default parameters settings.

- Roll mouse wheel on the image to zoom in or zoom out. Right-click on the image to return to default size.
- On the image, click to display in full screen, and click on full screen to restore the default.

Figure 4-13 Image



Step 3 Configure the video parameters.

Table 4-4 Video parameters

Parameter	Description
Profile	Select the device profile from **Day**, **Night**, and **Normal**.
Channel	Select channel number.
Color Mode	Select image color mode from **Standard**, **Bright**, and **Soft**.
Brightness	Adjust image brightness. The bigger the value, the brighter the image.
Contrast	Adjust image contrast. The bigger the value, the more obvious the contrast between the light and dark areas.
Gamma	Adjust image brightness in a non-linear way to improve the dynamic display range. The bigger the value, the brighter the image.
Saturation	Adjust color. The bigger the value, the lighter the color. This value does not affect the general image lightness.

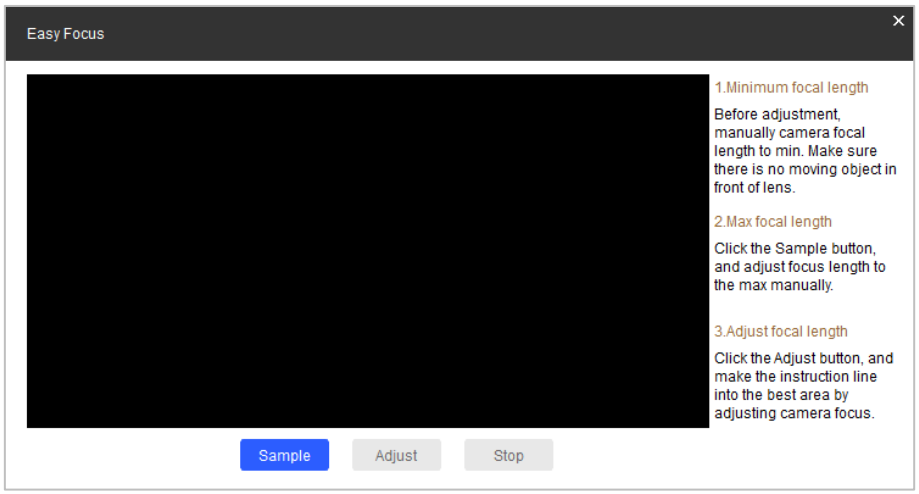
Parameter	Description
Day/Night Mode	Includes the following three options: ● Color: Select this option to set image color. ● Auto: Select this option to automatically set the image to be one of the other two options according to the environment. ● BW: Black and white. Select this option to set image to be black and white.
BLC Mode	● OFF: Turn off the backlight compensation mode. ● BLC: Backlight compensation. In environments with strong backlighting, the compensation function can reduce the appearance of dark silhouettes in a picture. ● WDR: Wide Dynamic Range. For locations that are strongly lit, this function reduces brightness levels by adding a dark contrast, making the image clearer. ● HLC: Highlight Compensation. This function can reduce brightness to help balance lighting in the picture.
Channel Name	Set device channel name. Cannot input null characters.

Step 4 (Optional) Set the **Easy Focus** function.

Complete this step when you need to make fine adjustments to the focal distance.

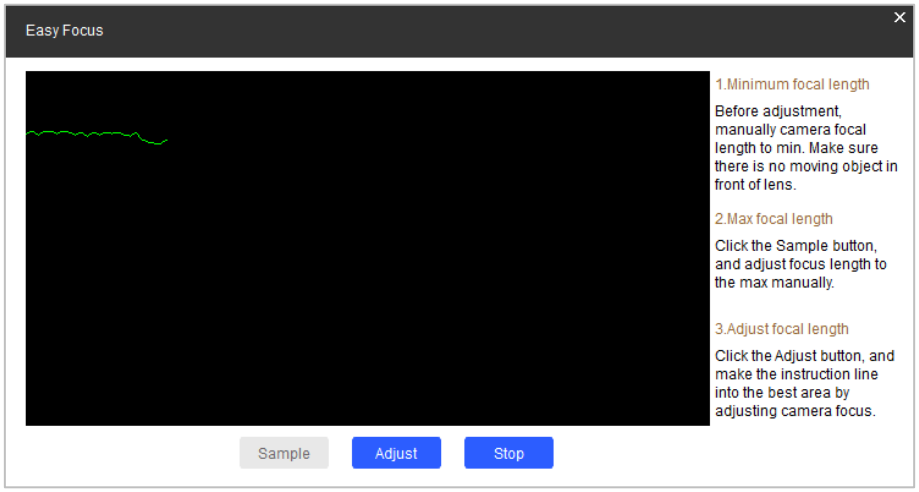
1) Click **Easy Focus**.

Figure 4-14 Easy focus



2) Manually adjust the device focal length to the minimum value, and then click **Sampling**. Meanwhile, manually adjust the device focal length to the maximum value.

Figure 4-15 Sampling

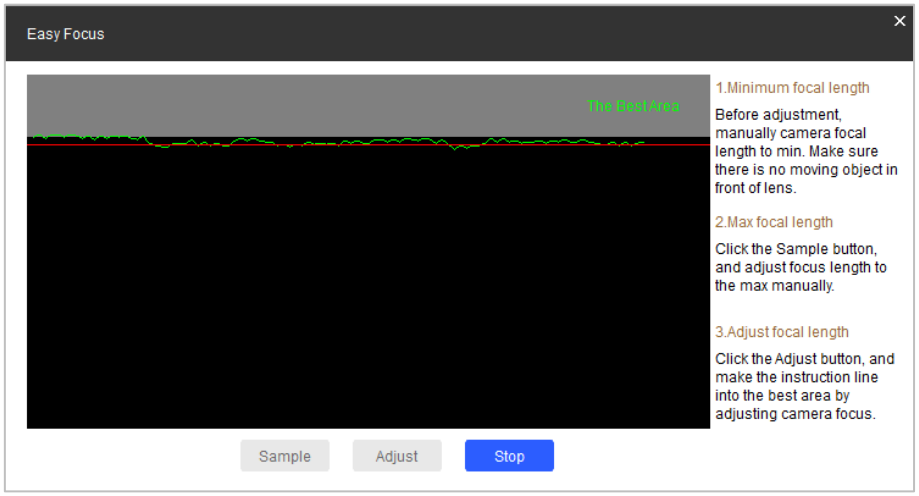


3) Click **Adjust**.

The Best Area interface is displayed. Manually adjust the focus until the focal length indicating line is in the best area.

- The red line indicates the image definition value, and the green line indicates the definition value when the focal length changes from minimum to maximum.
- Click **Stop** to stop making fine adjustments to the focal distance.

Figure 4-16 Final result



4.5.2.3 Configuring Profile Parameters

To let device switch profiles automatically while working, you can set the switch methods.

This function corresponds to the Profile Management function of cameras. For more details, see the user's manual of the camera.

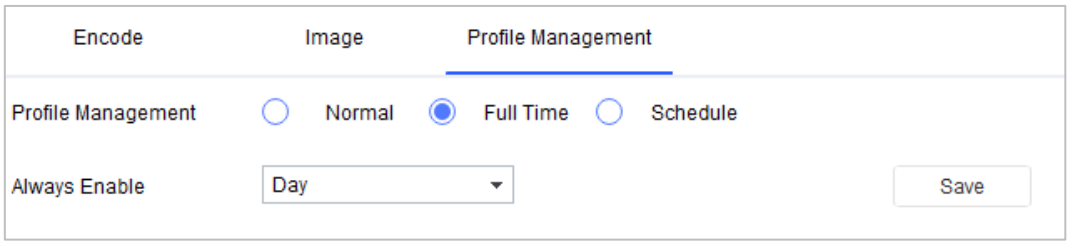
Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Click the Profile Management tab.

Step 3 Configure parameters.

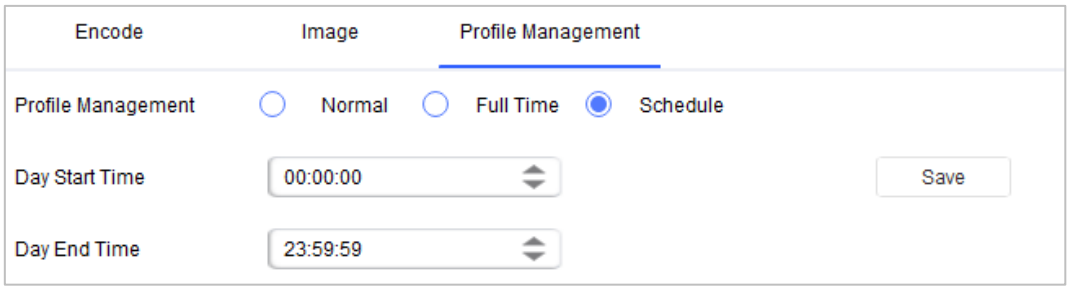
- Select **Normal**. The device works according to the Normal profile.
- Select **Full Time**, and then select **Day** or **Night**. The device works according to the Day or Night profile.

Figure 4-17 Full time



- Select **Schedule**, and then type **Day Start Time** and **Day End time**. The rest time is night. For example, if you set 8:00–17:00 as day, 0:00–8:00 and 18:00–24:00 are night, and the device switches profiles according to the schedule.

Figure 4-18 Schedule



Step 4 Click **Save** to complete settings.

Step 5 (Optional) Apply configuration to other devices.

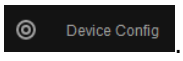
1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

4.5.3 Access Control Devices

For access control devices, you can configure the parameters on the **Device Config** interface, such as device channel number, card number, TCP port, CommPort, and bit rate, get system logs, and enable OSDP (Open Supervised Device Protocol).

4.5.3.1 Configuring Access Control Parameters

The interface and parameters are for reference only, and might differ from the actual device type and model.

Step 1 Open the Tool and select 

.

Step 2 Select an access control device in the device list, and then click **Get Device Info**, or double-click the device.

Step 3 (Optional) If the login dialog box is displayed, enter the username and password for the device, and click **OK**.

Step 4 Configure parameters.

Figure 4-19 Access control config

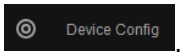
Table 4-5 Access control parameters description

Parameter	Description
Channel	Select channel to set the parameters.
Card No.	• **Byte Revert**: When ACS controller works with third-party readers (except HID), and the card reading result does not match the sent card number. For example, the card reading result is hexadecimal 0x12345678 (decimal 305419896) while the sent card number is hexadecimal 0x78563412 (decimal 2018915346), you can select **Byte Revert** to match them. • **HIDpro** Convert: When the ACS controller works with HID readers, and the card reading result does not match the sent card number, for example, the card reading result is hexadecimal 0x12345678 (decimal 305419896) while the sent card number. is hexadecimal 0x78563412 (decimal 2018915346), you can select **HIDpro Revert** to match them. • **No Convert**: If the system fails to match card reading result with the sent card No. by operating **Byte Revert** or **HIDpro Convert**, you can select **No Convert** to restore.
SysLog	To get device log, click **Get**.
Reader Serial No.	Select the reader to set bitrate.
Bitrate	If card reading is slow, you can increase bitrate. It is 9600 by default.
OSDPEnable	When ACS controller works with third-party readers through ODSP protocol, enable ODSP.

Step 5 (Optional) Apply the configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

4.5.3.2 Configure Network Parameters

Step 1 Open the Tool and select 

.

Step 2 Select an access control device in the device list, and then click **Get Device Info**, or double-click the device.

Step 3 (Optional) If the login dialog box is displayed, enter your username and password, and click **OK**.

Step 4 Configure parameters.

Figure 4-20 Network parameters configuration

Table 4-6 Network parameters description

Parameter	Description
TCP Port	Change TCP port number and click **Save**. When adding the device to the platform, enter this new port number.
Host IP	Host IP address configured for auto registration.
Host Port	Host Port configured for auto registration.
Device ID	Device ID configured for auto registration.
Enable Auto Registration	After enabling auto registration, when the device automatically registers to a server, it will report its current network location to the designated server for the client software to access the device.

Step 5 After the configuration, click **Save** to send the auto registration parameters to the device.

Step 6 (Optional) Apply the configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**.
   The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

4.5.4 VDP

4.5.4.1 VTO

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Configure VTO parameters.

Figure 4-21 VTO configuration

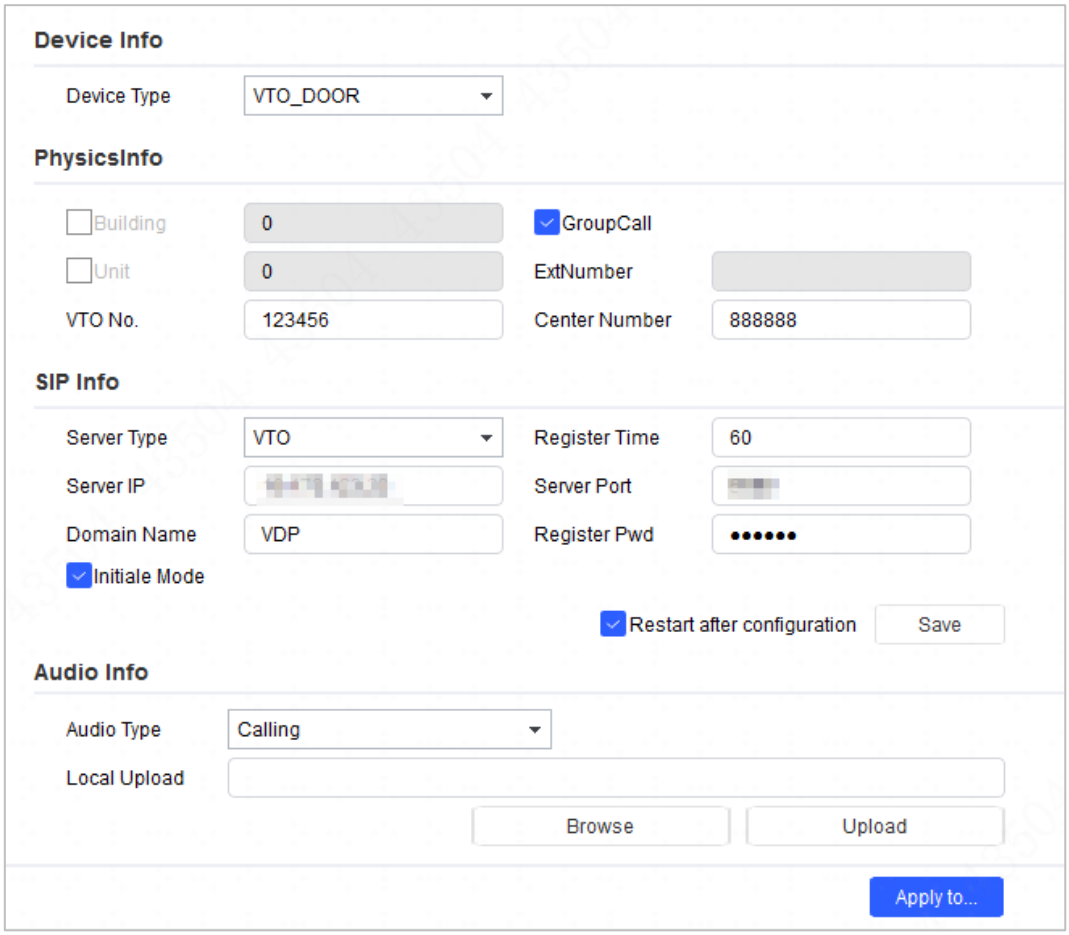


Table 4-7 VTO parameters

Parameter		Description
Device Type		Select the **Device Type** from VTO_DOOR and VTO_WALL.
PhysicsInfo	Building	Enter the number of the building where the VTO is installed.
	Unit	Enter the number of the unit where the VTO is installed.
	VTO No.	VTO number.
	GroupCall	When the device acts as a server, enable or disable group call function.
	ExtNumber	Extension number of the VTO.
	Center Number	Center call number.

Parameter		Description
SIP Info	Server Type	Select the server type.
	Server IP	The IP address of the SIP server.
	Domain Name	Domain name of the SIP server.
	Register Time	Register time of the SIP server.
	Server Port	Port number of the SIP server.
	Register PWD	Registration password of the SIP server.
	Initiale Mode	Select the check box to enable the server.
	Restart after configuration	Select the check box, and the dveice will restart after configuration.

Step 3 Click **Save**.

Step 4 Select the audio type according to the actual situation.

Step 5 Click **Browse** to upload the audio file, and then click Upload to upload selected file.

Only files in .mp3 format are supported.

Step 6 (Optional) Apply the configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Save**. The success icon ( ) will be displayed if the application is successful; otherwise the failure icon ( ) will be displayed.
2) Click **Return** to return to the configuration interface.

4.5.4.2 VTH

4.5.4.2.1 Network Config

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Click the **Network Config** tab, and configure the parameters.

Figure 4-22 Network configuration

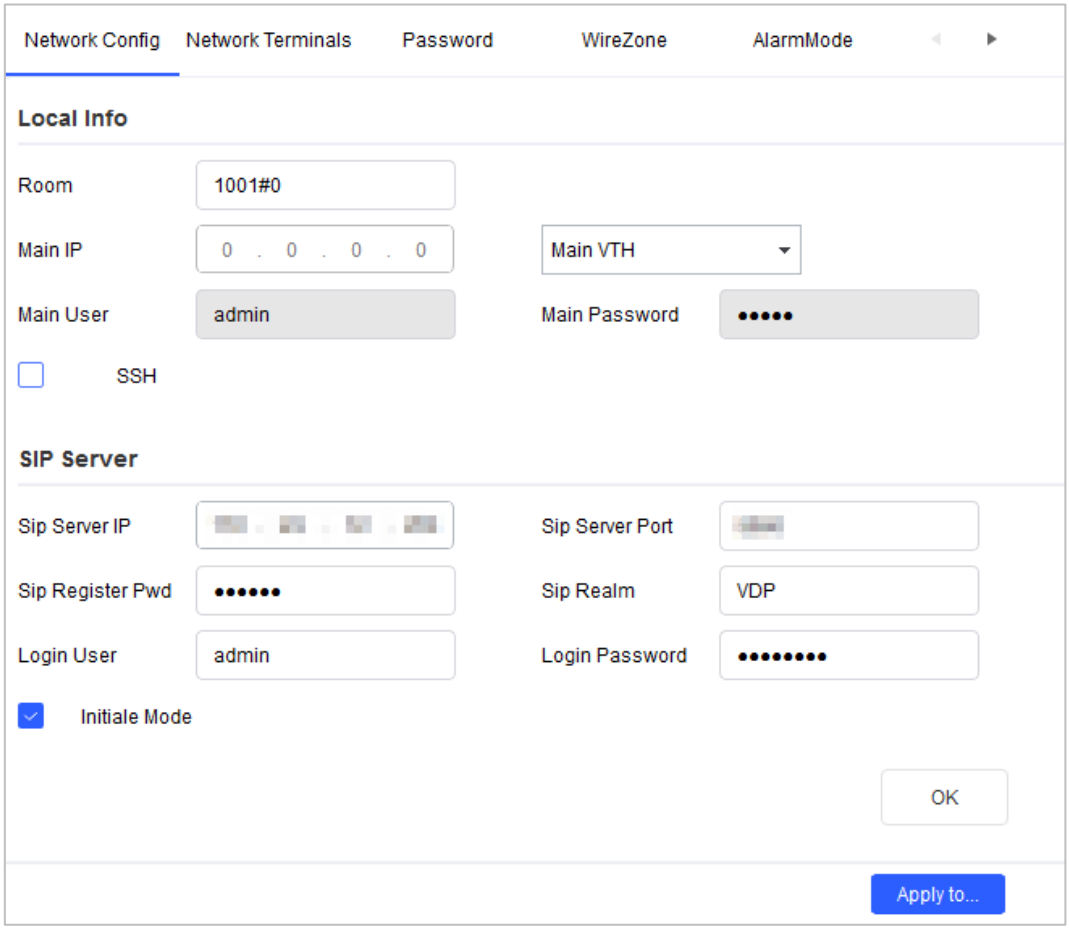


Table 4-8 Network configuration parameters

Parameter		Description
Local Info	Room	Enter the room number.
	Main IP	Enter the IP address of the host. ● When selecting **Main VTH**, you do not need to enter the main IP, main user, and main password. ● When selecting **Sub VTH**, you need to enter the main IP, main user, and main password.
	Main User	Enter the username of the host.
	Main Password	Enter the login password of the host.
	SSH	Select the check box to enable SSH authentication to perform safety management.
SIP Server	Sip Server IP	Enter the IP address of the server.
	Sip Server Port	Enter the port number of the SIP server.
	Sip Register Pwd	Enter registration password of the SIP server.
	Sip Realm	Enter the domain name of the SIP server.
	Login User	The port username of the SIP server.

Parameter		Description
	Login Pwd	The login password of the SIP server.
	Initiale Mode	Select the check box to enable the server.

Step 3 Click **OK**.

Step 4 (Optional) Apply configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

4.5.4.2.2 Network Terminals

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Click the Network Terminals tab, select the master VTO, and then configure parameters.

Figure 4-23 Network Terminals

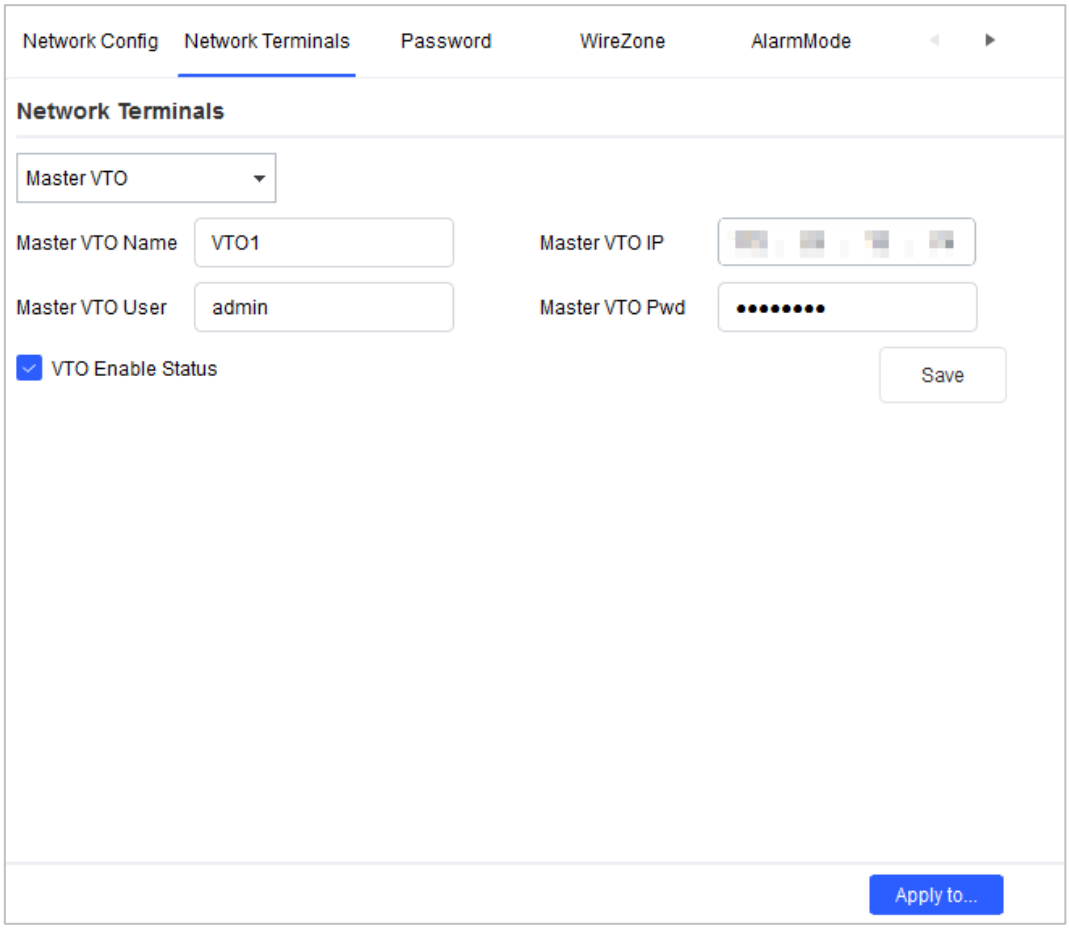


Table 4-9 Network terminal parameters

Parameter	Description
MasterVTO Name	Enter the name of the master VTO.
MasterVTO IP	Enter the IP address of the master VTO.
MasterVTO User	Enter the username of the master VTO.

Parameter	Description
Master VTO Pwd	Enter the password of the master VTO.
VTO Enable Status	Select the check box to enable the master VTO.

Step 3 Click **Save**.

Step 4 (Optional) Apply the configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

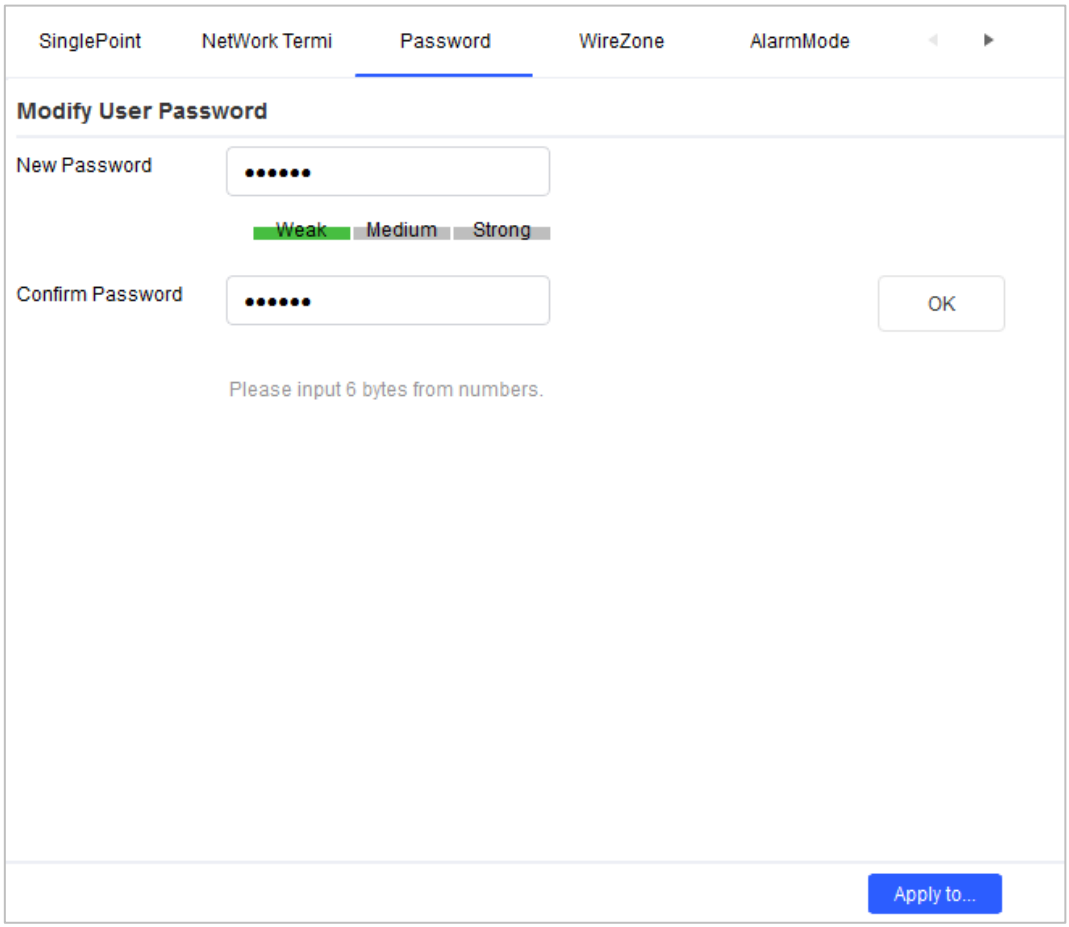
4.5.4.2.3 Password

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Click the **Password** tab, and then enter the new password and confirm password.

The password contains 6 numbers.

Figure 4-24 Password



Step 3 Click **OK**.

Step 4 (Optional) Apply configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

4.5.4.2.4 Wire Zone

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Click the **WireZone** tab, and configure parameters.

Figure 4-25 4.5.4.2.2 WireZone

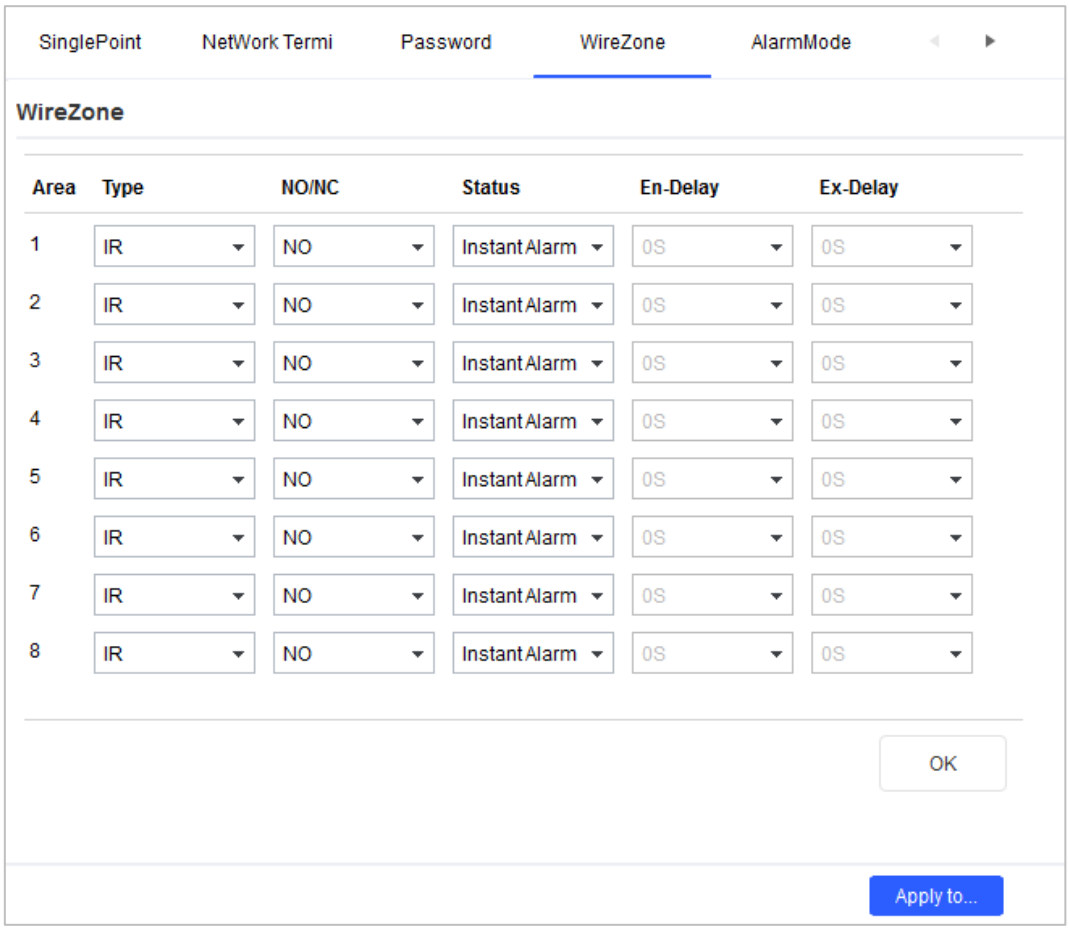


Table 4-10 WireZone parameters

Parameter	Description
Area	The number of the area.
Type	You can select the alarm type from IR, Gas Sensor, Smoke Sensor, Urgency Btn, Door Sensor, Stolen Alarm, Perimeter, and Doorbell.
NO/NC	Select **NO** or **NC** as needed.
Status	You can select the alarm status from **Instant Alarm**, **Delay Alarm**, **Bypass**, **Remove**, and **24-hour**.
En-Delay	When setting the alarm status to **Delay Alarm**, you need to set the entry delay time.
Ex-Delay	When setting the alarm status to **Delay Alarm**, you need to set the existing delay time.

Step 3 Click **OK**.

Step 4 (Optional) Apply the configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

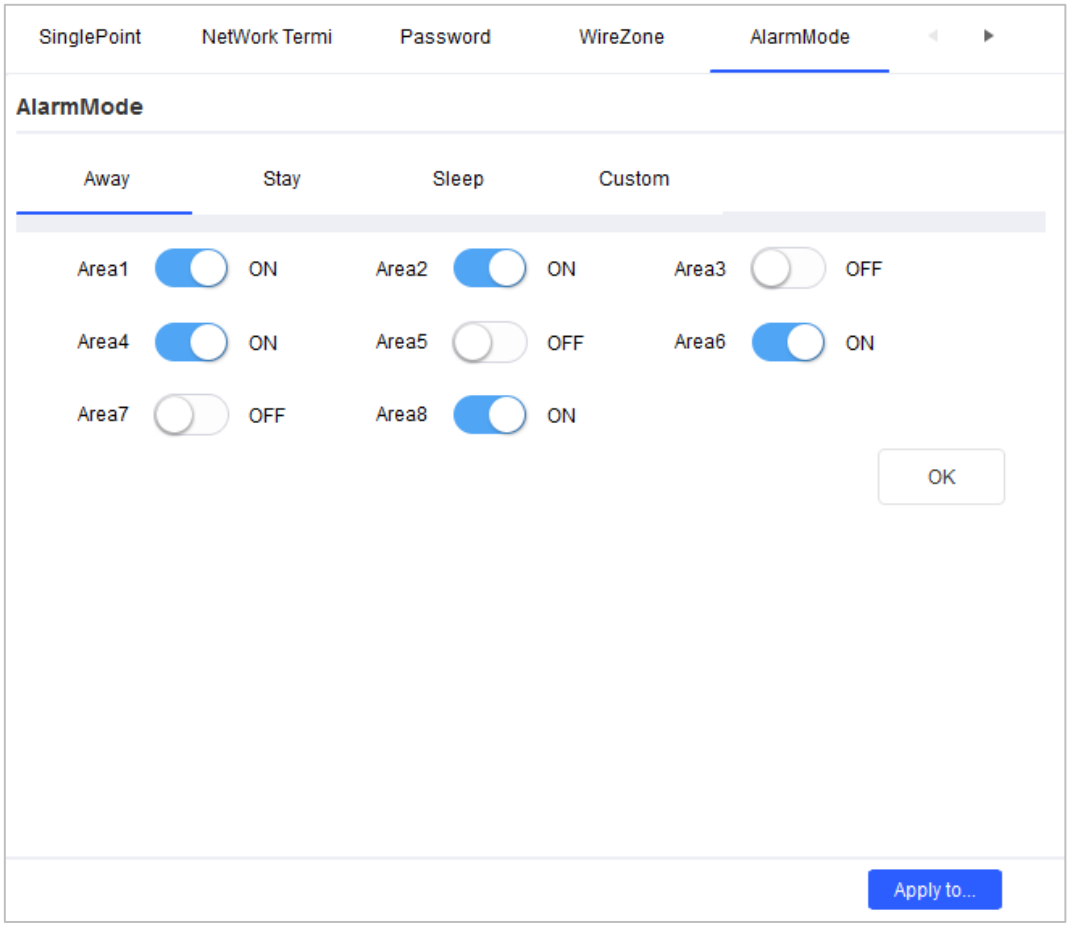
4.5.4.2.5 Alarm Mode

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Click the **AlarmMode** tab, and configure the parameters.

Enable or disable areas in different modes as needed.

Figure 4-26 AlarmMode



Step 3 Click **OK**.

Step 4 (Optional) Apply the configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

4.5.4.2.6 Arm

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Click the **Arm** tab, and configure parameters.

Figure 4-27 Arming

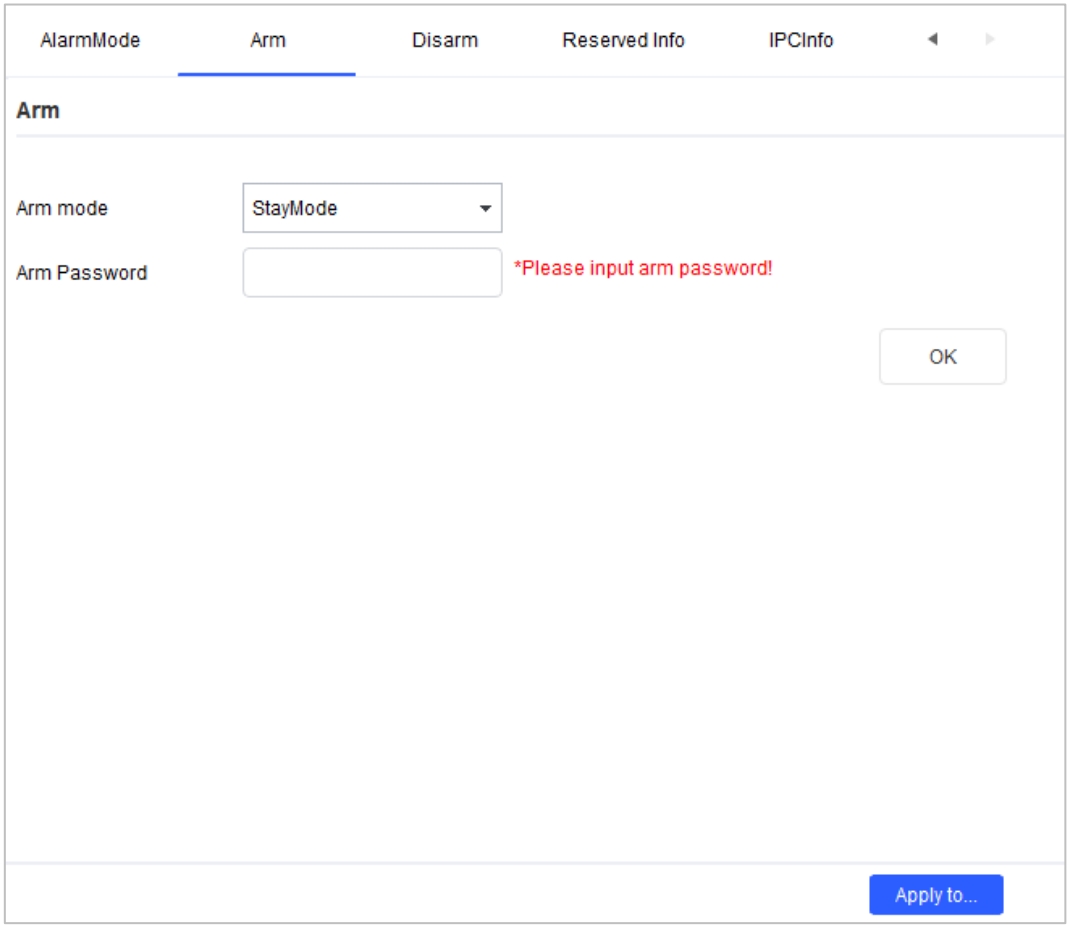


Figure 4-28 WireZone parameters

Parameter	Description
Alarmed Mode	Select the alarm mode from **StayMode**, **Away Mode**, **SleepMode**, and **CustomMode**.
Alarmed Password	Enter the arming password. The password contains 6 numbers.

Step 3 Click **OK**.

Step 4 (Optional) Apply configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

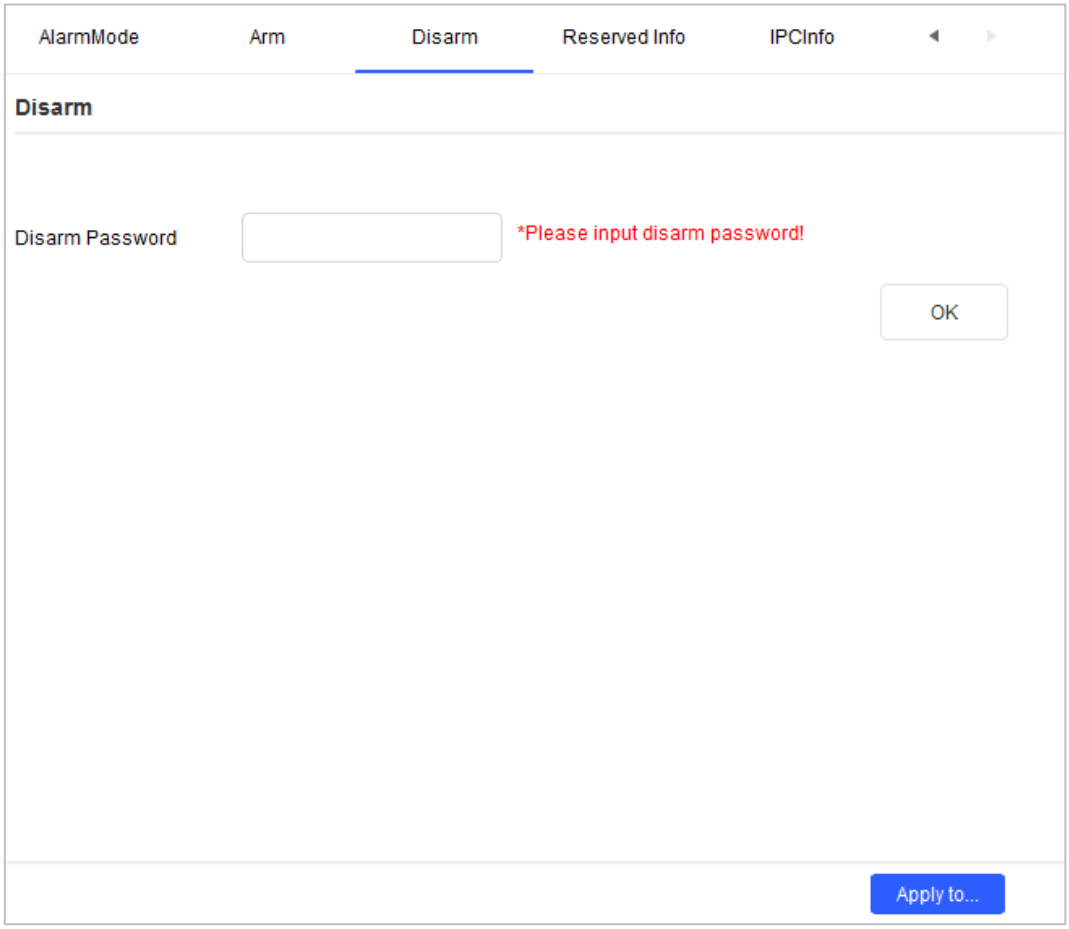
4.5.4.2.7 Disarm

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Click the **Disarmed** tab, and enter the disarming password.

The password contains 6 numbers.

Figure 4-29 Disarm



Step 3 Click **OK**.

Step 4 (Optional) Apply the configuration to other devices.

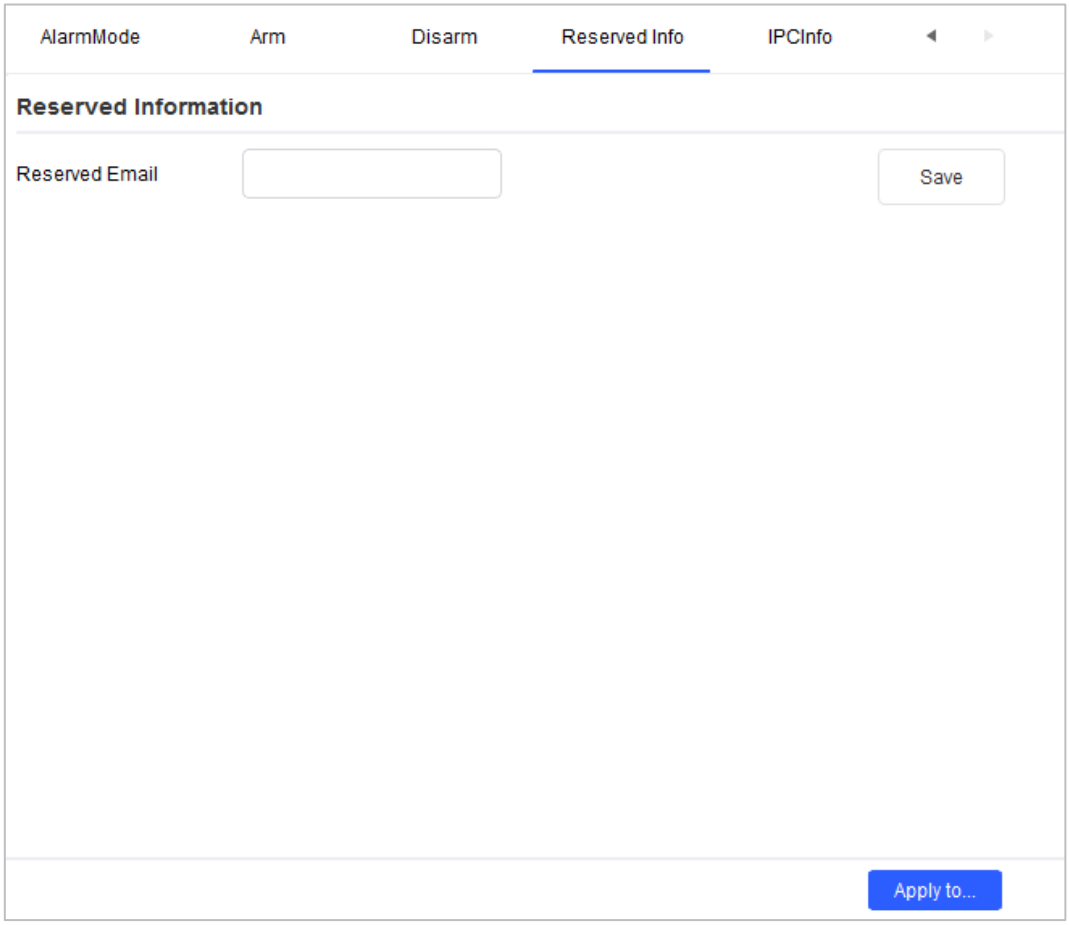
1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

4.5.4.2.8 Reserved Info

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Click the **Reserved Info** tab, and enter the reserved email address.

Figure 4-30 Reserved information



Step 3 Click **Save**.

Step 4 (Optional) Apply the configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

4.5.4.2.9 IPC Info

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Click the **IPCInfo** tab, select the IPC that you want to configure, and then configure other parameters.

Figure 4-31 IPCInfo

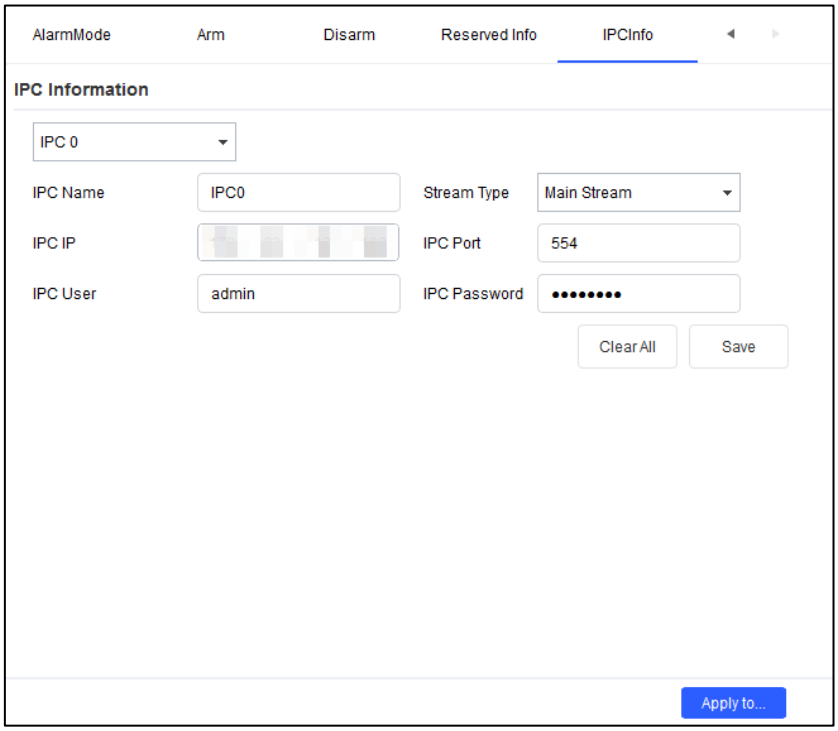


Table 4-11 IPC Parameters

Parameter	Description
IPC Name	Enter the name of the IPC.
Stream Type	Select the stream type from **Main Stream** and **Sub Stream** according to the actual situation.
IPC IP	Enter the IP address of the IPC.
IPC Port	Enter the Port number of the IPC.
IPC User	Enter the username of the IPC.
IPC Password	Enter the login password of the IPC.

Step 3 Click **Save**.

Step 4 (Optional) Apply configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon ( ) will be displayed if the application is successful; otherwise the failure icon ( ) will be displayed.
2) Click **Return** to return to the configuration interface.

4.5.4.3 VTS

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Configure VTS parameters.

Figure 4-32 VTS configuration

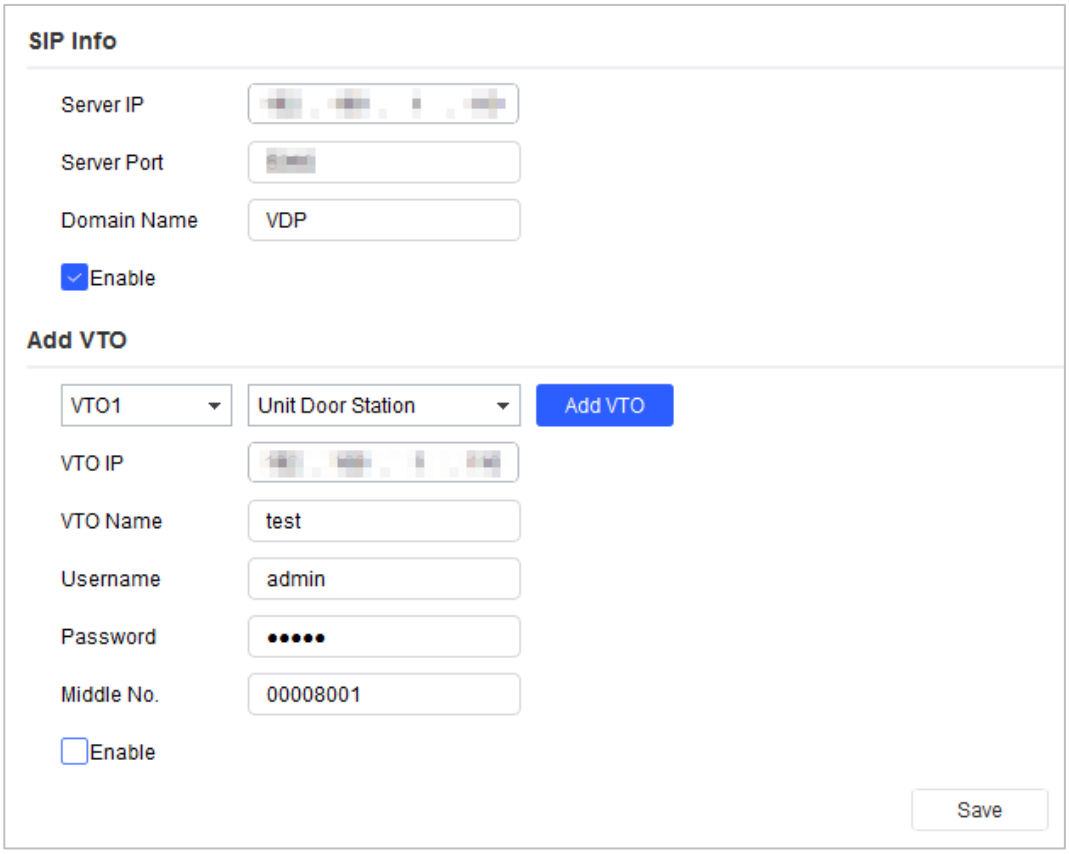


Table 4-12 VTO parameters

Parameter		Description
SIP Info	Server Type	Select the server type.
	Server IP	The IP address of the SIP server.
	Domain Name	The domain name of the SIP server.
	Register Time	The register time of the SIP server.
	Server Port	The port number of the SIP server.
Add VTO	Add VTO	Click **Add VTO** to add a new VTO.
	VTO No.	The added VTO number.
	VTO Type	Select Unit Door Station or Fence Station.
	VTO IP	Enter the IP address of VTO.
	VTO Name	Enter the name of VTO.
	User name	Enter the web login username.
	Password	Enter the web login password.
	Middle No.	Enter the number in the following format: Building number # Unit number # VTO number
	Enable	Select the check box to enable the server.

Step 3 Click **Save**.

4.5.5 Android Digital Signage

You can configure apps in batches, debug Android, and export logs.

4.5.5.1 Configuring APP

You can change the IP address of APP registration in batches.

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Click the **App Config** tab.

Step 3 Enter the IP address in **APP IP Config**.

Step 4 Click **Modify**.

Figure 4-33 Modify app configuration

Step 5 (Optional) Apply the configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

4.5.5.2 Enabling Android Commission

Enable or disable the Android Commission function.

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

Step 2 Click the **Android Debug** tab.

Step 3 Select **On** in **ADB Enable**.

Step 4 Click **OK**.

Figure 4-34 App Commission

Step 5 (Optional) Apply the configuration to other devices.

1) Click **Apply to**, select the devices that you need to sync the configured parameters to, and then click **Config**. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
2) Click **Return** to return to the configuration interface.

4.5.5.3 Exporting Log

You can export the logs of Android digital signage.

Step 1 Complete Step 1 to Step 4 in "4.5.1 Accessing the Configuration Interface."

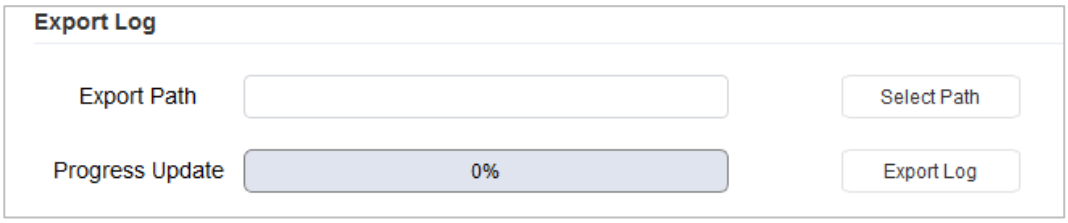
Step 2 Click the **Export Log** tab.

Step 3 Click **Select Path** to select the export path.

Step 4 Click Export Log.

The exporting progress is displayed.

Figure 4-35 Modify app configuration



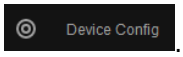
4.5.6 Alarm Host Devices

4.5.6.1 Device Information

You can view the device information on this interface.

Figure 4-36 Device information

4.5.6.2 Configure Network Parameters

Step 1 Open the Tool and select 

.

Step 2 Select an alarm host device in the device list, and then click **Get Device Info**, or double-click the device.

Step 3 (Optional) If the login dialog box is displayed, enter your username and password, and then click **OK**.

Step 4 Configure parameters.

Figure 4-37 Network parameters configuration

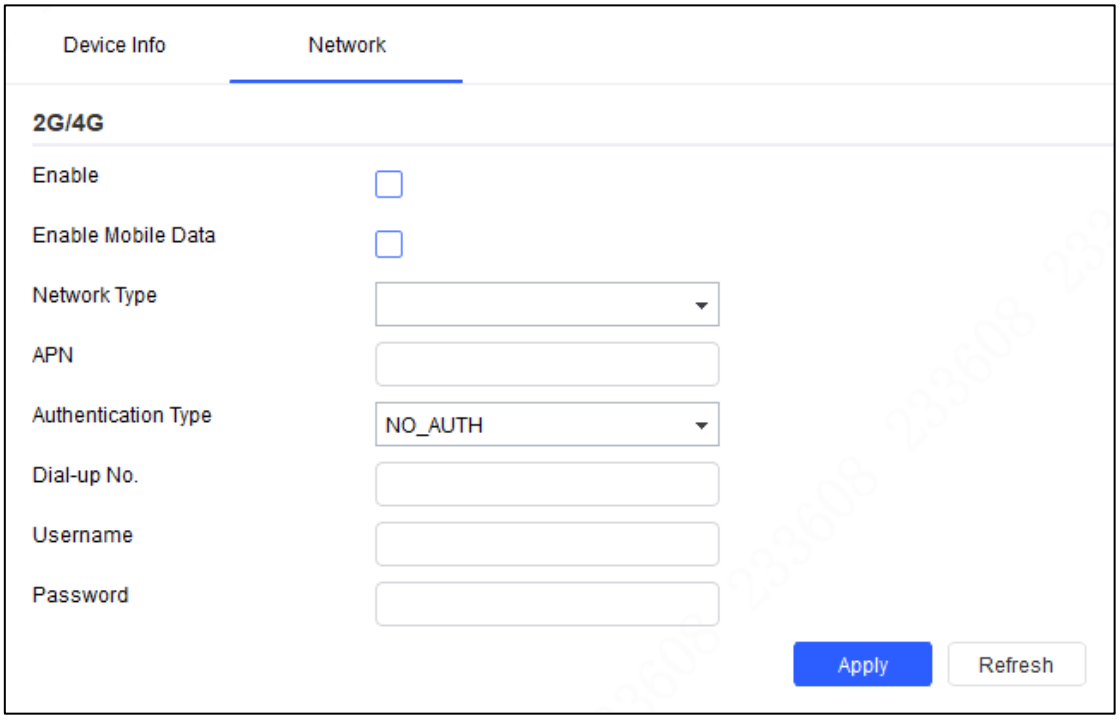


Table 4-13 Network parameters description

Parameter	Description
Enable	Select the check box to enable 2G/4G network.
Enable Mobile Data	Select the check box to enable cellular data network.
Network Type	Select the network type supported by the device.
APN	Set the access point name for dial-up Internet access.
Authentication Type	Select the authentication type for dial-up Internet access.
Dial-up No.	Select the dial-up number for dial-up Internet access.
Username	Select the username for dial-up Internet access.
Password	Select the password for dial-up Internet access.

Step 5 Click **Apply** to apply the parameters to the device.

4.6 Configuring System Settings

You can configure the settings for system time, reboot, restore, device password and video password.

4.6.1 Timing

You can calibrate the device time.

Step 1 Click System Settings.

Figure 4-38 Timing

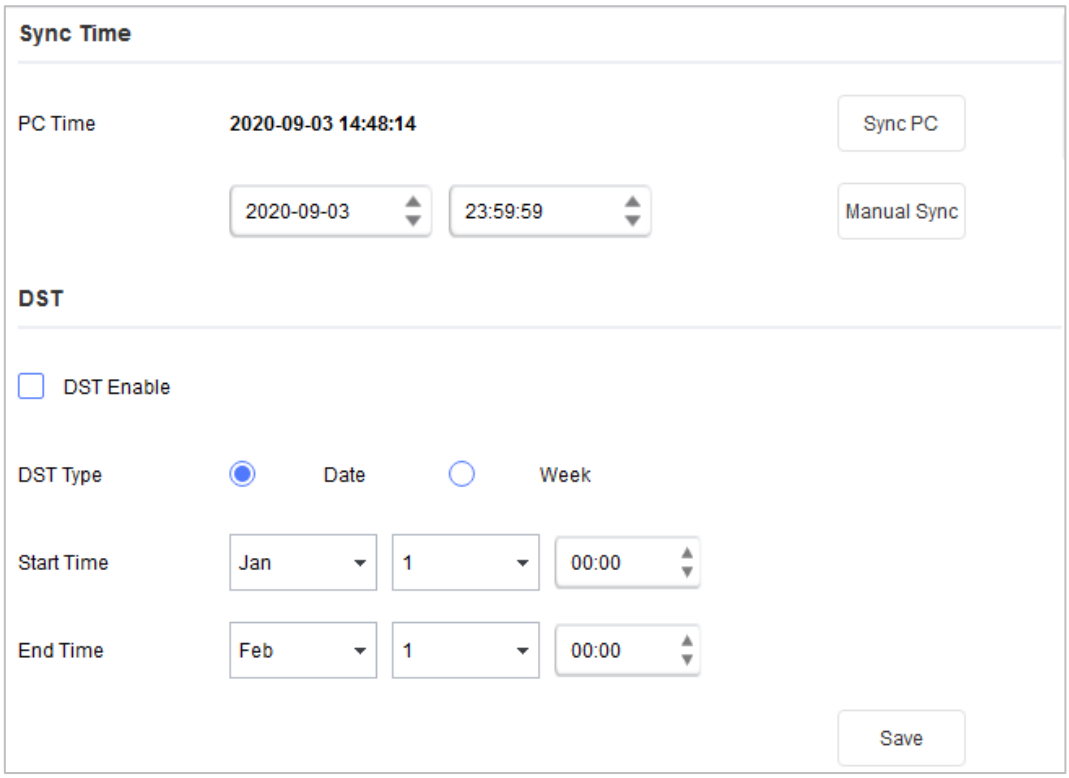
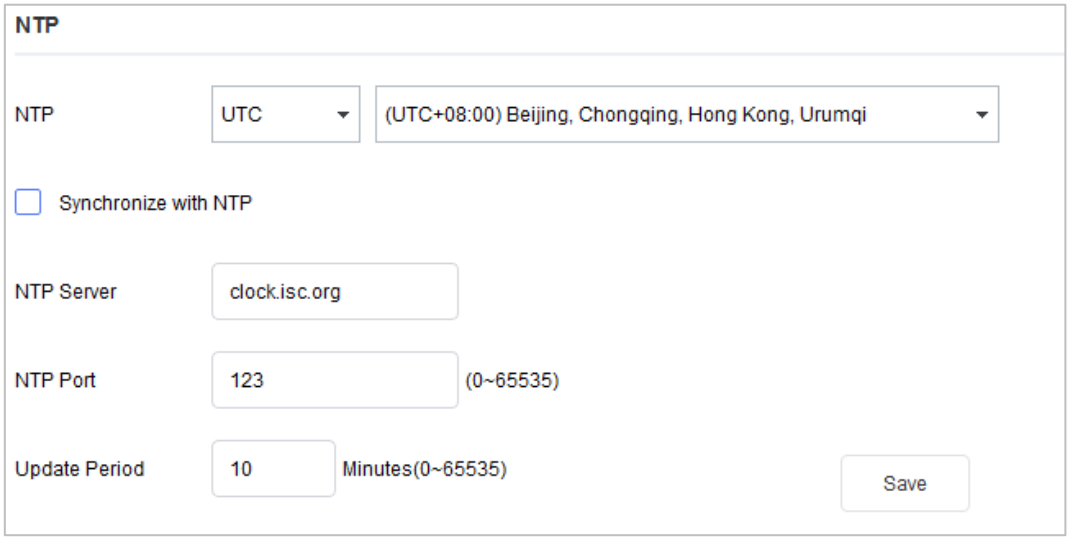


Figure 4-39 Timing



Step 2 Click ▸ next to the device type, and then select one or multiple devices.

If the device is not in the device list, perform search again. For details, see "4.1 Adding Devices."

Step 3 Select the time sync method for the device.

- Manual sync: Specify the time and select the time zone, and then click **Manual Sync**. The device time will sync with the setting.

- PC sync: Click **Sync PC**. The device time will sync with the PC time.
- NTP sync: Select the **Synchronize with NTP** check box and set the parameters.

Table 4-14 NTP Parameters

Parameter	Description
NTP	Select UTC or GMT, and then select a time zone from the drop-down list on the right.
NTP Sever	Enter the IP address or domain name of the corresponding NTP server.
NTP Port	Enter the port number of corresponding NTP server.
Update Period	Enter the time interval of when the device synchronizes with NTP.

Step 4 (Optional) Select **DST Enable** (Daylight Saving Time) check box and set the parameters.

Implement this step when you use the device in the countries or regions where DST is used.

Table 4-15 DST Parameters

Parameter	Description
DST Type	Select **Date** or **Week** according to the actual needs.
Start Time	Set the DST start time and end time.
End Time	

Step 5 Click **Save** to complete settings.

4.6.2 Rebooting

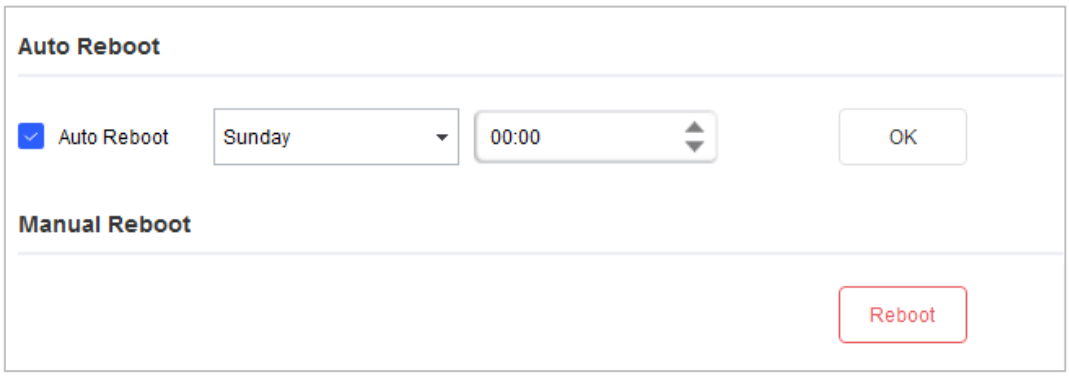
You can manually or automatically reboot the device.

Reboot will interrupt operations, so reboot the device when it is idle.

Step 1 Click System Settings.

Step 2 Click the **Reboot** tab.

Figure 4-40 Reboot



Step 3 Click ▸ next to the device type, and then select one or more devices.

If the device is not in the device list, perform search again. For details, see "4.1 Adding Devices."

Step 4 Select the reboot type for the device as needed.

- Auto reboot: Under **Auto Reboot**, select the **Auto Reboot** check box and set a day of a week and the specific time, and then click **OK**.
  The device will reboot at the set time.
- Manual reboot: Under **Manual Reboot**, click **Reboot**.
  The device reboots immediately.

4.6.3 Restoring

4.6.3.1 Restoring Default Configurations of Device

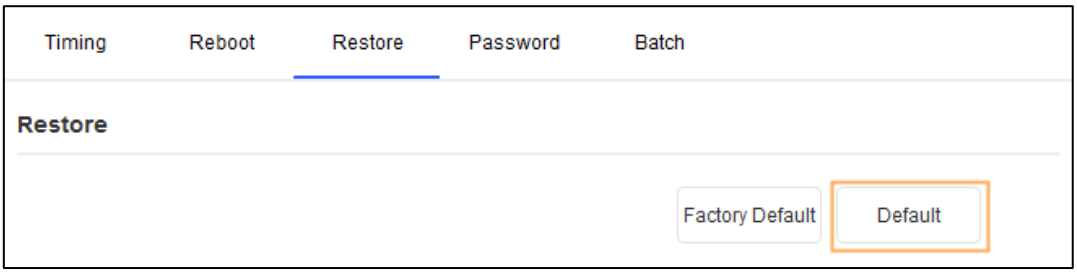
Restore settings except:

- Network settings such as IP address
- User information

Step 1 Click System Settings.

Step 2 Click the **Restore** tab.

Figure 4-41 Restore default configurations



Step 3 Click next to the device type, and then select one or multiple devices.

If the device is not in the device list, perform search again. For details, see "4.1 Adding Devices."

Step 4 Click **Default** and click **OK** to restore default configurations.

The results are displayed next to the device after restoring is completed. Icon (✓) means success; icon (⚠) means failure and you can click icon to view the details.

4.6.3.2 Restoring Factory Configurations of Device

You can restore the factory default configurations..

Step 1 Click System Settings.

Step 2 Click the **Restore** tab.

Figure 4-42 Restore default configurations

Step 3 Click ▸ next to the device type, and then select one or more devices.

If the device is not in the device list, perform search again. For details, see "4.1 Adding Devices."

Step 4 Click **Factory Default** and click **OK** to restore factory configurations.

The results are displayed next to the device after restoring is completed. Icon (✓) means success; icon (⚠) means failure and you can click icon to view the details.

4.6.3.3 Export Configurations

Step 1 Click System Settings.

Step 2 Click the **Restore** tab.

Figure 4-43 Restore default configurations

Step 3 Click ▸ next to the device type, and then select one or multiple devices.

If the device is not in the device list, perform search again. For details, see "4.1 Adding Devices."

Step 4 Click **Export** under the **Export File** tab, select saving path and enter the file name. Then click **OK**.

The results are displayed next to the device after restoring is completed. Icon (✓) means success; icon (⚠) means failure and you can click icon to view the details.

4.6.3.4 Import Configurations

The first 4 steps are the same as **Export**.

Step 5 Click **Import** and then click **OK** to apply the imported configurations to all devices of same type, same model and same version. Then select the saving path and the imported file.

The results are displayed next to the device after restoring is completed. Icon (✓) means success; icon (⚠) means failure and you can click icon to view the details.

Figure 4-44 Restore default configurations

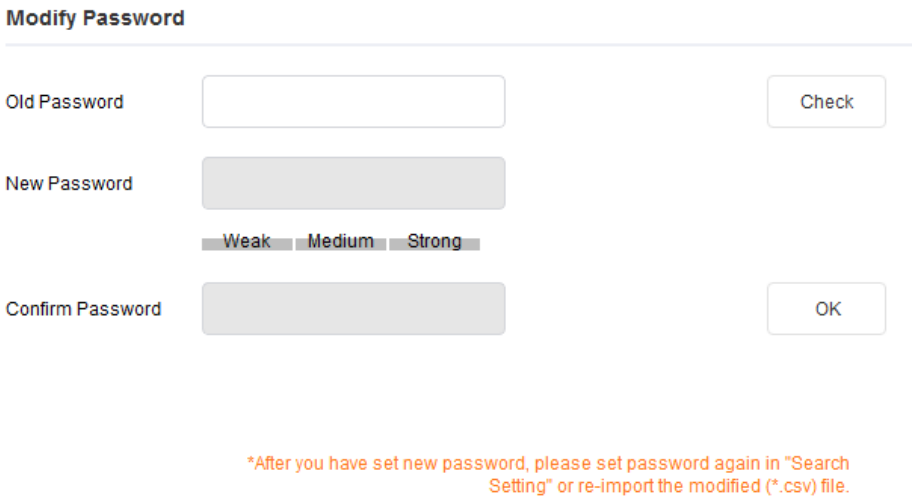
4.6.4 Modifying Device Password

You can modify the device login password.

Step 1 Click System Settings.

Step 2 Click the **Device Password** tab.

Figure 4-45 Device password



Step 3 Click next to the device type, and then select one or multiple devices.

If you select multiple devices, the login passwords must be the same.

Step 4 Set the password.

Follow the password security level hint to set a new password.

Table 4-16 Password parameters

Parameter	Description
Old Password	Enter the device old password. To make sure that the old password is entered correctly, you can click **Check** to verify.
New Password	Enter the new password for the device. A notice appears informing you of the strength of your password. The password might vary depending on the devices, the actual password shall prevail.
Confirm Password	Confirm the new password.

Step 5 Click **OK** to complete modification.

4.6.5 Batch Config

4.6.5.1 Video Standard

There are two video standards, PAL and NTSC. Select as needed.

Step 1 Click System Settings.

Step 2 Click the **Batch** tab.

Figure 4-46 Table configuration

Step 3 Click ▶ next to the device type, and then select one or multiple devices.

- If the device is not in the device list, perform search again. For details, see "4.1 Adding Devices."
- If you do not know which device the video file is exporting you can select multiple devices so that the system will go through each one until successful.

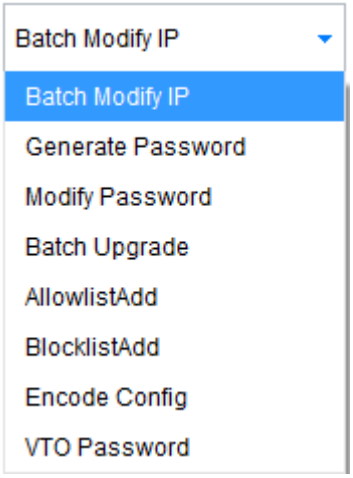
Step 4 Select **PAL** or **NTSC** from the **Video Standard** drop-down list as needed, and then click **Save**.

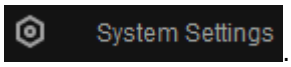
The results are displayed next to the device after restoring is completed. Icon (✓) means success; icon (⚠) means failure and you can click icon to view the details.

4.6.5.2 Table Config

The Table Config function enables you to perform some device configurations in batches. This is useful when you have a lot of devices to configure. Configurations include modifying IP, creating and modifying password, upgrading devices, adding allowlist and blocklist, and setting encoding parameters.

Figure 4-47 Table Config items



Step 1 Click 

.

Step 2 Click the **Batch Config** tab.

Figure 4-48 Table config

- If the device is not in the device list, perform search again. For details, see "4.1 Adding Devices."
- If you do not know which device the video file is exporting from, you can select multiple devices so that the system will go through each one until successful..

Step 3 In the **Table Config** section, click **Open** to open the template, fill in the sheet(s) as required, and then save the template locally.

The **Result** column of the template displays whether the configuration is successful. No need to enter.

Step 4 Select a config type from the **Operation Type** drop-down list, click **Config**, select the template you saved, and then click **Open**.

Figure 4-49 Import template

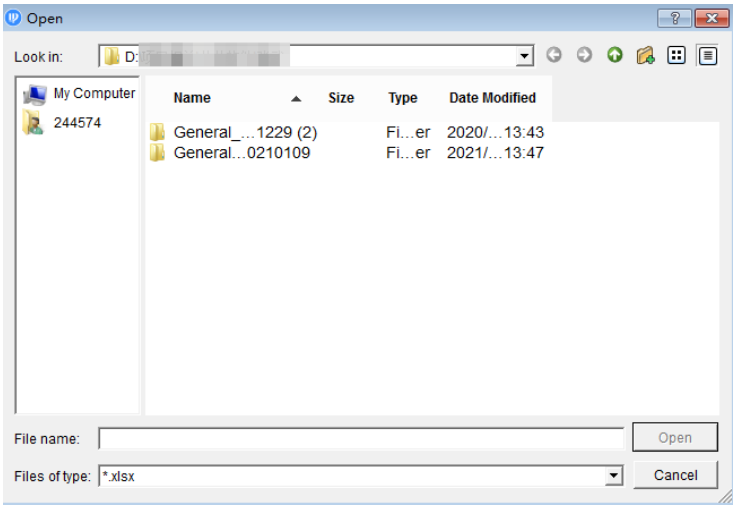


Table 4-17 Description of the operation type

Operation Type	Description
Batch Modify IP	Change passwords in the table in batches.
Generate Password	Generate password in batches.
Modify Password	Change login password in batches.
Batch Upgrade	Update devices in batches.
AllowlistAdd	Configure IP addresses in Allowlist in batches.
BlocklistAdd	Configure IP addresses in Blocklist in batches.
Encode Config	Configure encoding parameters in batches.

	Only supports H264 or H265, stream and enabling or disabling intelligent encoding.
VTO Password	Change the VTO password of engineering, duress, unlock and issuing card in batches.

Step 5 To confirm the result, open the template, and then view the **Result** column.

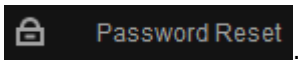
4.7 Resetting Device Password

You can reset device password.

- The password resetting operation can only be performed to the devices in the same network segment with the ConfigTool PC. To reset other password on the device, you need to log in with the admin account.
- You can only reset the password of initialized devices.
- Some devices do not support the password reset function.

4.7.1 Resetting Password in Batches

Reset password of two or more devices in batches. You can only use the XML method to reset passwords in batches.

Step 1 Click 

.

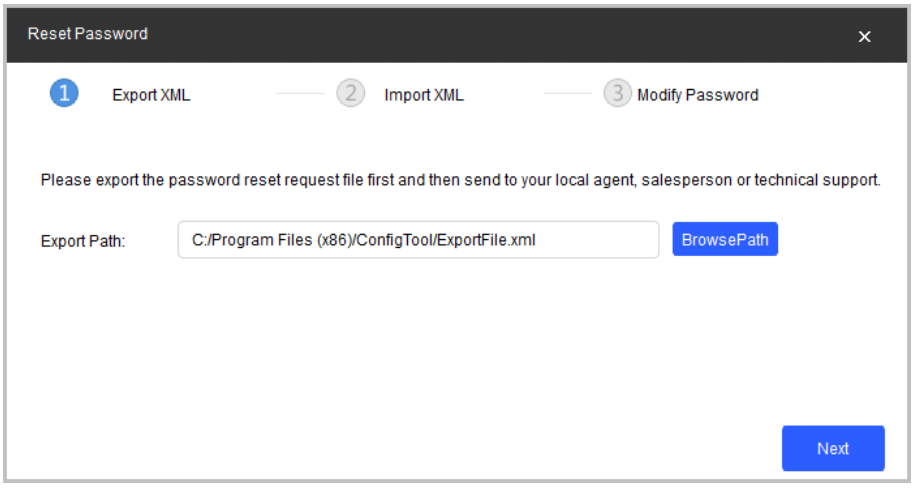
Step 2 Select the devices that need to reset password, click **Batch Reset**, click **Agree** and then **OK**.

Step 3 Export XML.

3) Click **BrowsePath** to select the save path for the exported XML file.
4) Click **Next** to export the file.

Step 4 Use the enterprise email that is officially certified by device manufacturer to send the ExportFile.xml file to the local technical support, and then get the result.xml file from the technical support.

Figure 4-50 Reset ExportFile.xml

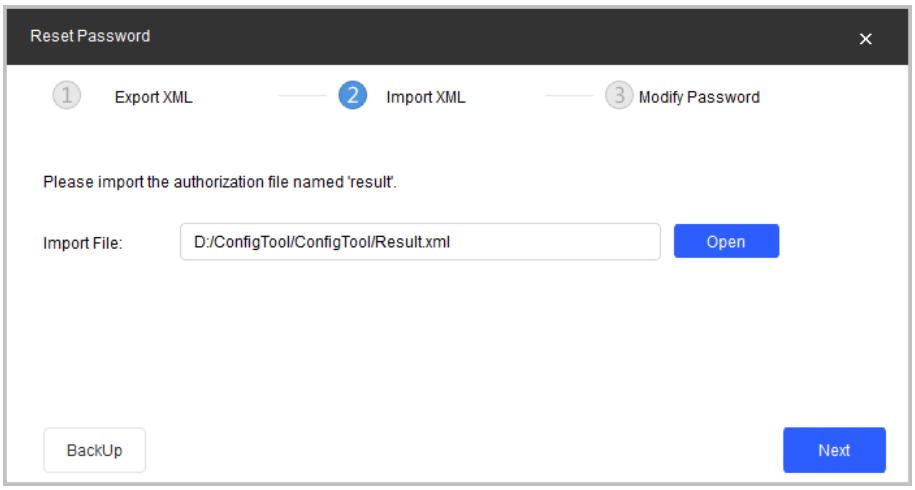


Step 5 Import XML.

If the **Reset Password-Import XML** interface is closed, click **Import Result.xml** on the **Reset Password** interface, and then import the result.xml file from the dialogue box displayed.

1) Click **Open** to import the **result.xml** file from the save path.

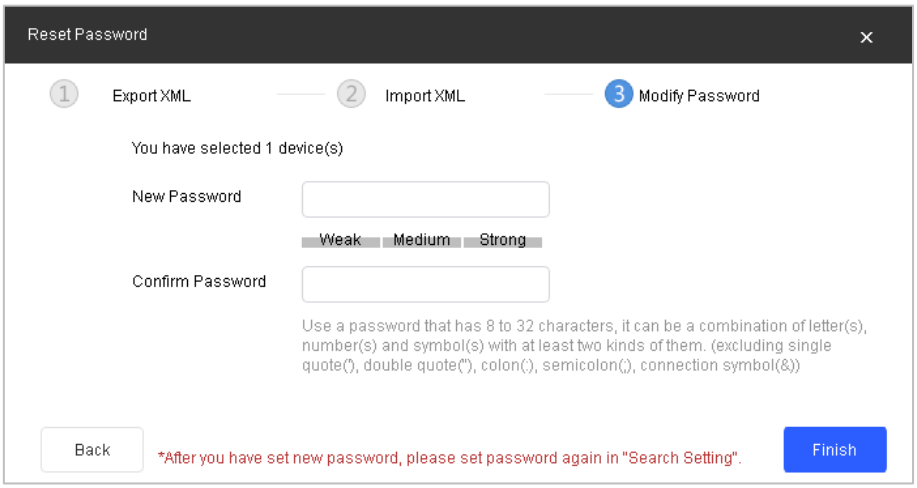
Figure 4-51 Reset password



2) Click **Next** to start importing.

After exporting the XML, the **Reset Password-Modify Password** interface is displayed.

Figure 4-52 Reset password-modify password



Step 6 Modify password.

1) Enter the new password and confirm password.

The password might vary depending on the devices, the actual password shall prevail.

Step 7 Click **Finish** to start resetting the password.

The result is displayed next to the device after operation is completed. Click the success icon (✓) or click the failure icon (⚠) for the details.

4.7.2 Resetting Password of One Device

This procedure is only applicable to a single device.

The interface might vary depending on the device type and model, and the actual interface shall prevail.

Step 1 Click Password Reset.

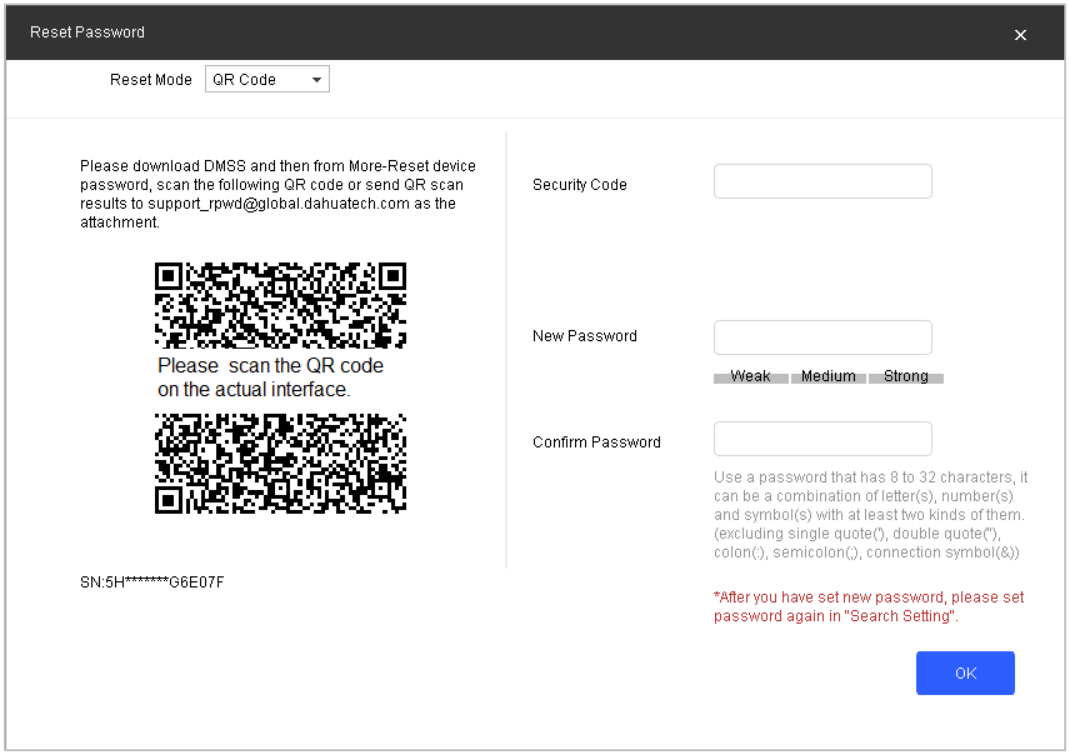
Step 2 Select the device that needs to reset the password, and then click **Reset**.

Step 3 Reset password.

- Reset by scanning QR code

1) Select **QR Code** from the **Reset Mode** drop-down list.
2) Perform operations according to the instructions on the interface to obtain the security code.
3) Enter old password, new password, and confirm password.

Reset by sending XML file. For details, see "4.7.1 Resetting Password in Batches."



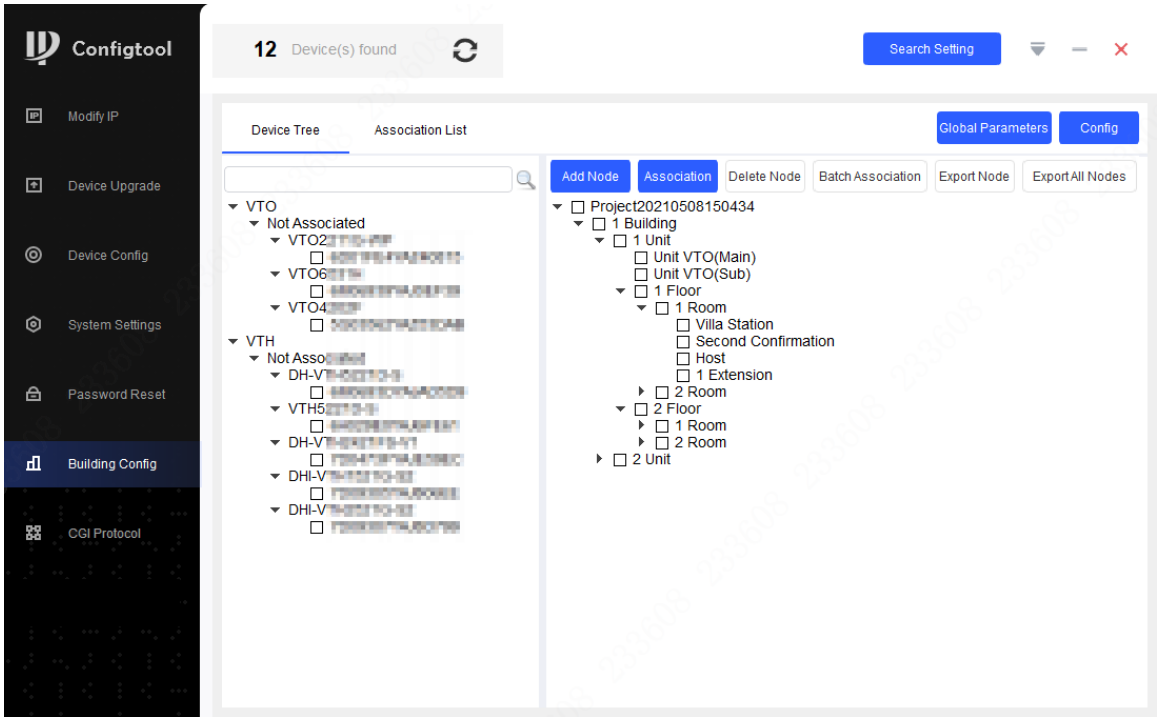
Step 4 Click **OK** to start resetting the password.

The result is displayed next to the device after restoring is completed. Click the success icon (✓) or click the failure icon (⚠) for the details.

4.8 Building Configuration

You can link building devices with organization nodes and send configurations to the actual VTO or VTH as needed.

Figure 4-51 Building configuration interface



4.8.1 Configuring Global Parameters

Configure the information of the server, VTO and VTH devices.

Step 1 Select Building Config > Global Parameters.

Step 2 Configure device information.

Figure 4-53 Global parameters

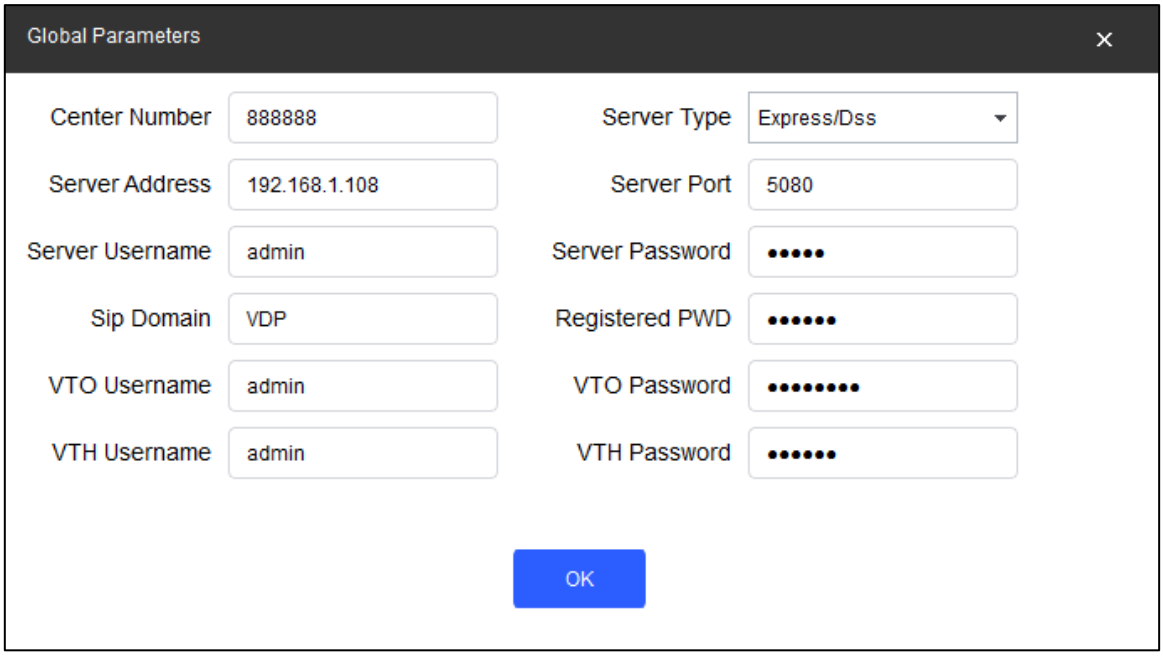


Table 4-18 Global parameter description

Parameters	Description
Center Number	Enter the center number. It is 888888 by default.

Server Type	Select server type. It is **Express/DSS** by default.
Server Address	Enter server address. The default address is 192.168.1.108.
Server Username, Password	Enter server username and password. By default, the user is admin.
SIP Domain	Enter the SIP domain and registration password. They are VDP and 123456 by default.
VTO/VTH Username and Password	• The username and password are **admin** and **admin123** for VTO. • The username and password are **admin** and **123456** for VTH. The username and password for all VTO and VTH need to be the same. Otherwise the configuration might fail.

Step 3 Click **Save**.

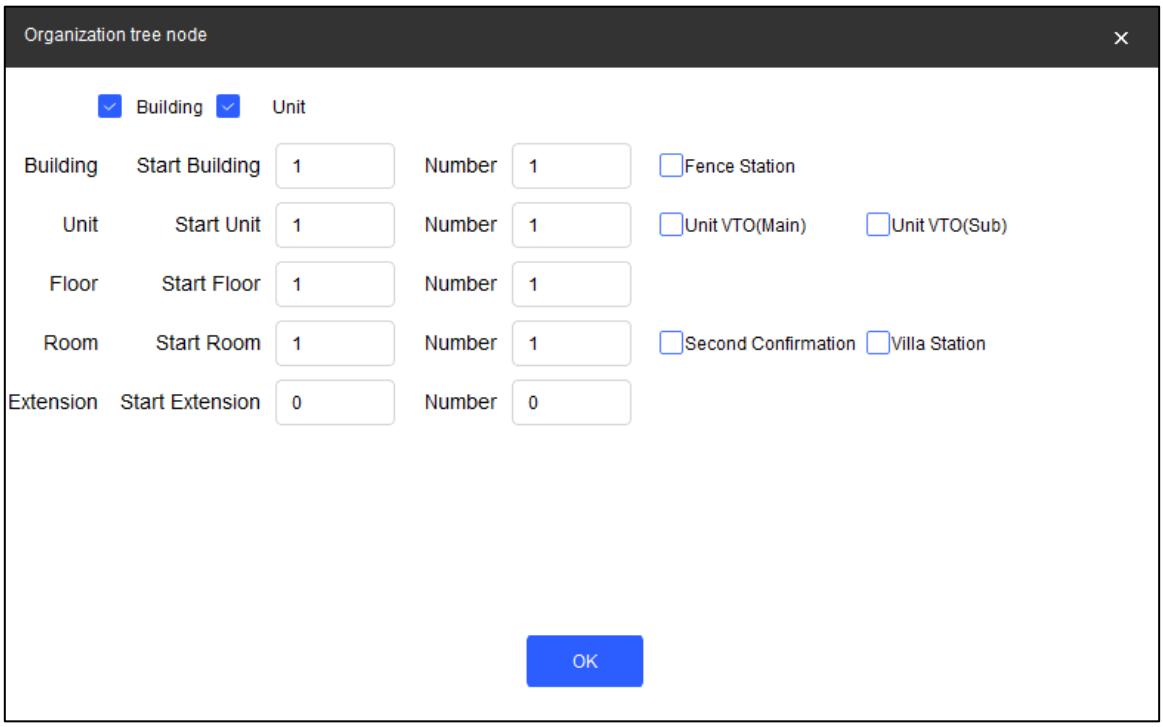
4.8.2 Adding Organization Node

You can add organization nodes as needed.

Step 1 Select Building Config > Device Tree.

Step 2 Click **Add Node** to add building organization node as needed.

Figure 4-54 Add nodes



Enable **Building** and **Unit** when you need to select them.

- When selecting Fence Station, there will be a node under the Project.
- When selecting Unit VTO(main) or Unit VTO(sub), there will be a main or sub unit VTO.
- When the unit is disabled, the VTO will be added under the building. If the building is disabled, the VTO will be added under the project.

Step 3 Click **OK**.

4.8.3 Configuring Linkage

Link the devices with organization nodes, and then you can check the linkage information sending status.

Step 1 Click Building Config > Device Tree.

Step 2 Select a device from the device tree and a node from the organization nodes tree, and then click **Association**.

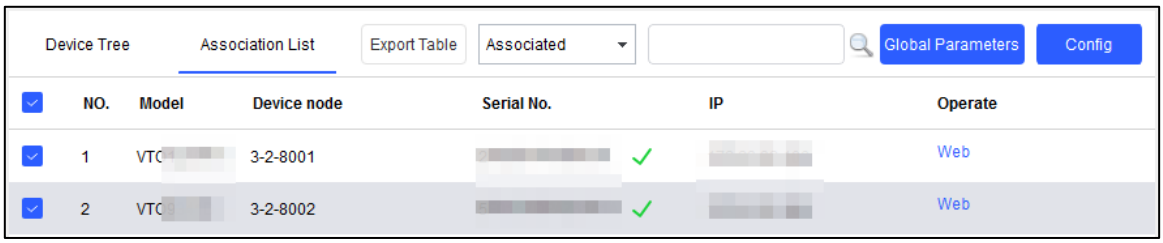
You can only associate one device with one node to an operation.

Step 3 Click **Association List,** select devices to be sent and click **Config**.

The icon next to the device serial number shows the sending status.

- ✓ means that the linkage sent successfully.
- ⚠ means that the linkage sent failed. You can click ⚠ to check for the reasons.

Figure 4-55 Association list



4.8.4 Linking Devices in Batches

You can link the devices with organization nodes in batches through the template.

Step 1 Click Building Config > Device Tree.

Step 2 Select the nodes to be linked, and then click **Export Node**.

Step 3 Select the exported table destination path, and click **Save**.

Step 4 Open the table and enter the serial number of each device linking with each node and save the file.

- The entered SN must belong to devices existing under the device tree. Otherwise the linkage might fail.
- VTH can only link with VTH devices.

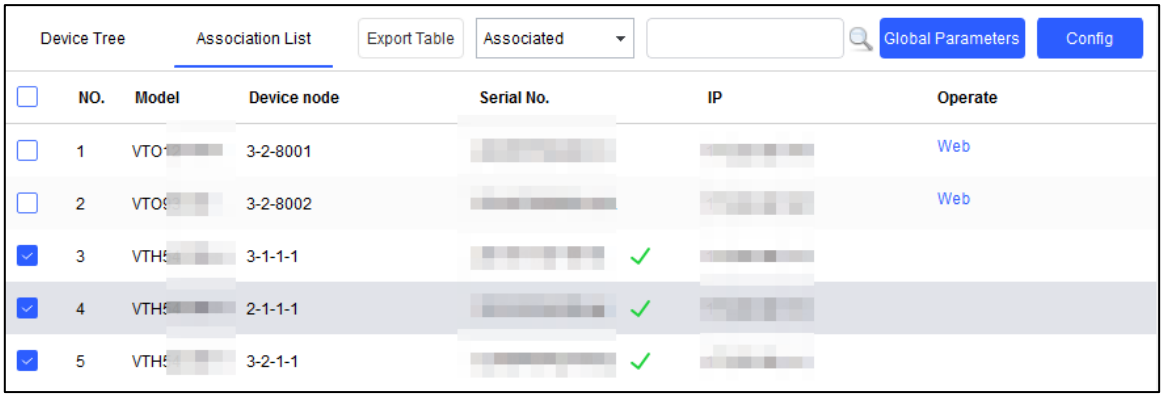
Step 5 Click **Batch Association** and select the finished table.

Step 6 Click **Association List,** select devices to be sent and click **Config**.

The icon next to the device serial number shows the sending status.

- ✓ means that the linkage sent successfully.
- ⚠ means that the linkage sent failed. You can click ⚠ to check for the reasons.

Figure 4-56 Association list



4.8.5 Exporting Related Information

You can export related information table to your PC.

Step 1 Click Building Config > Association List.

Step 2 Select devices to be exported and click **Export Table**.

Step 3 Select storage path, and click **Save**.

Step 4 Open the table on local, and you can view the related linkage information.

4.9 CGI Protocol

You can modify device password or other parameters through CGI commands and table. Make sure that you have the corresponding commands from technical support in advance.

Use https protocol when configuring information; otherwise the notice **Operation via http is not safe** will appear.

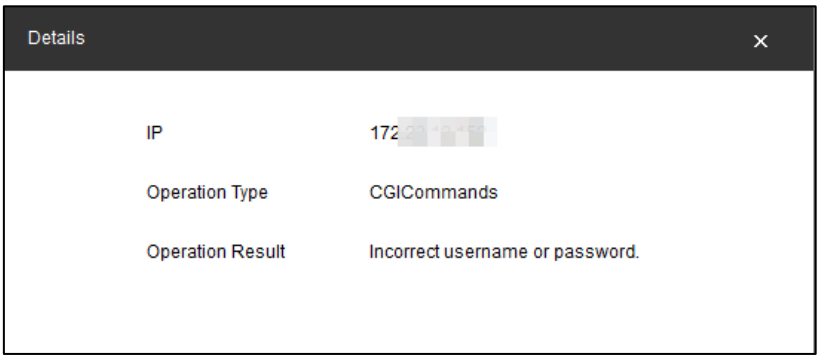
4.9.1 CGI Command Configuration

Step 1 Click CGI Protocol.

Step 2 Enter the Url path, and click **Config**.

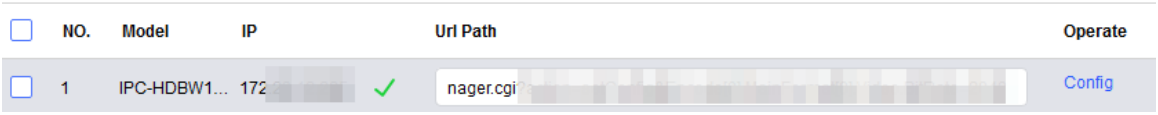
1) If shows next to the device IP, it means that the configuration failed. You can click the icon to see details.

Figure 4-57 Error message



2) **Incorrect username or password** means that the username and password you have entered in **Search Settings** are different from that of the device.
3) Change in **Search Settings** to the username and password of the device, and then configure CGI commands again.
4) When succeeding, ✓ shows next to the device IP.

Figure 4-58 CGI command success



4.9.2 Batch CGI Commands

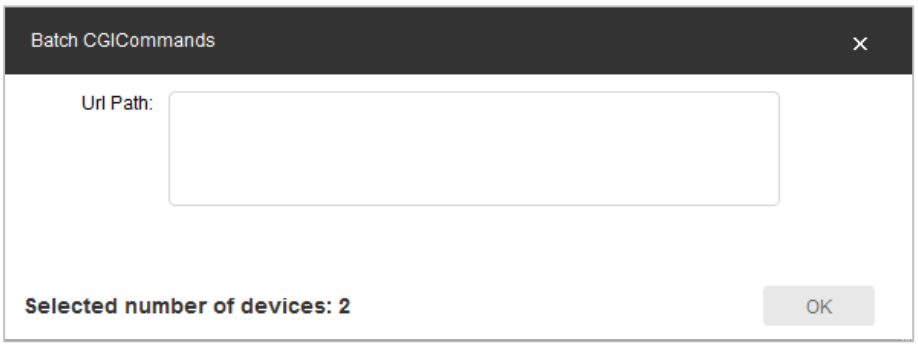
Step 1 Click CGI Protocol.

Step 2 Select the device that you want to configure in batches, click **Batch CGI Commands**, and then enter the Url path.

Step 3 Click **OK**.

Make sure that the Url paths of selected devices are the same.

Figure 4-59 Batch CGI commands



4.9.3 Table Config

Step 1 Click CGI Protocol.

Step 2 Click **Open Template**, enter IP address, port No., username, password, and CGI commands content, and then save the template and close it.

Figure 4-60 Template

Table 4-19 Parameter description of the template

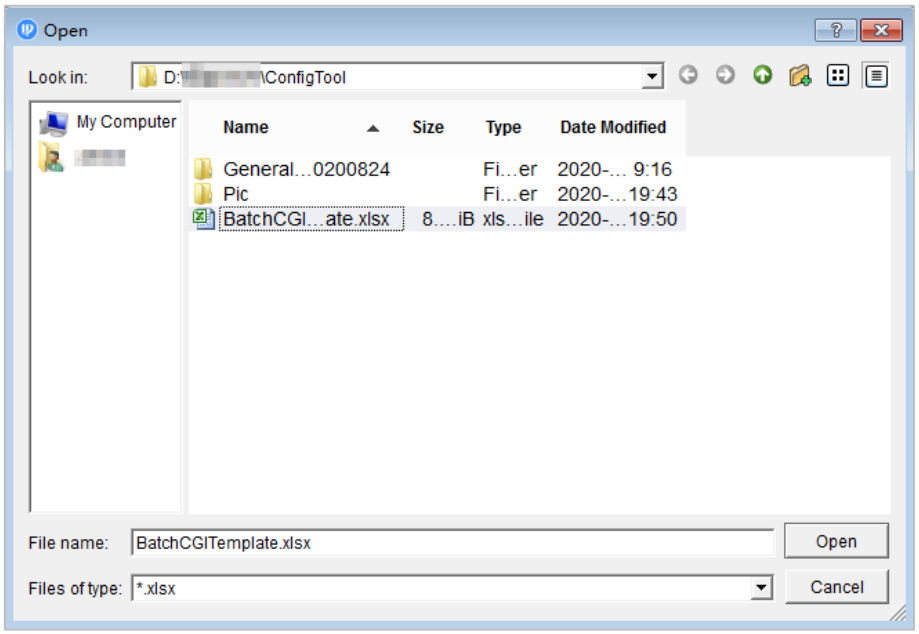
Parameter	Description
IP Address	Enter the device IP, port, login username and password.
Port	
Username	
Password	
CGI Commands Content	The command path of the device CGI configuration. Sending configuration through non-default port is available.
Protocol (0-http，1-https)	Http and https are available.
Result	The result of the CGI command execution.

Step 3 Return to CGI protocol interface, and click **Table Config**.

Step 4 Select the completed template, and click **Open** to import the template. The devices in the template will be configured as the template.

After the configuration is completed, the success notice is displayed. And you can check the result in the template.

Figure 4-61 Select a template



5 Help

This chapter introduces how to view the help file, QA file and software version, how to set network parameters and upgrade parameters.

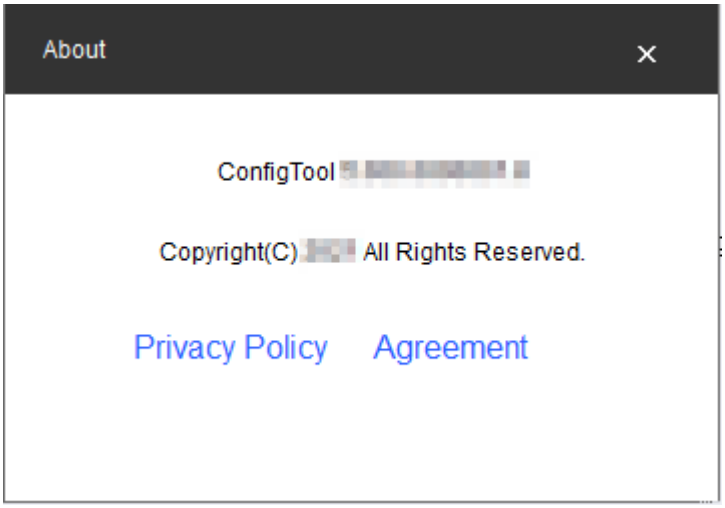
5.1 Help File

- Click at the upper-right corner, and then select **Help** to view the user's manual.
- Click and then select **QA** to view the file on frequently asked questions and the answers.

5.2 Software Version

- Click and then select **About** to view software version.
- Click and then select **About** to view privacy policy.

Figure 5-1 About



5.3 Settings

5.3.1 Configuring Parameters

Configure the mode when logging into the device and the parameters related to upgrading the device, such as upgrade timeout, update timeout interval, network timeout interval and upgrade speed.

Step 5 Click on the upper right corner of the interface, and click **Setting**.

Step 6 Configure the mode when logging into the device and the parameters related to upgrading the device

Step 7 Click **OK**.

Figure 5-2 Setting

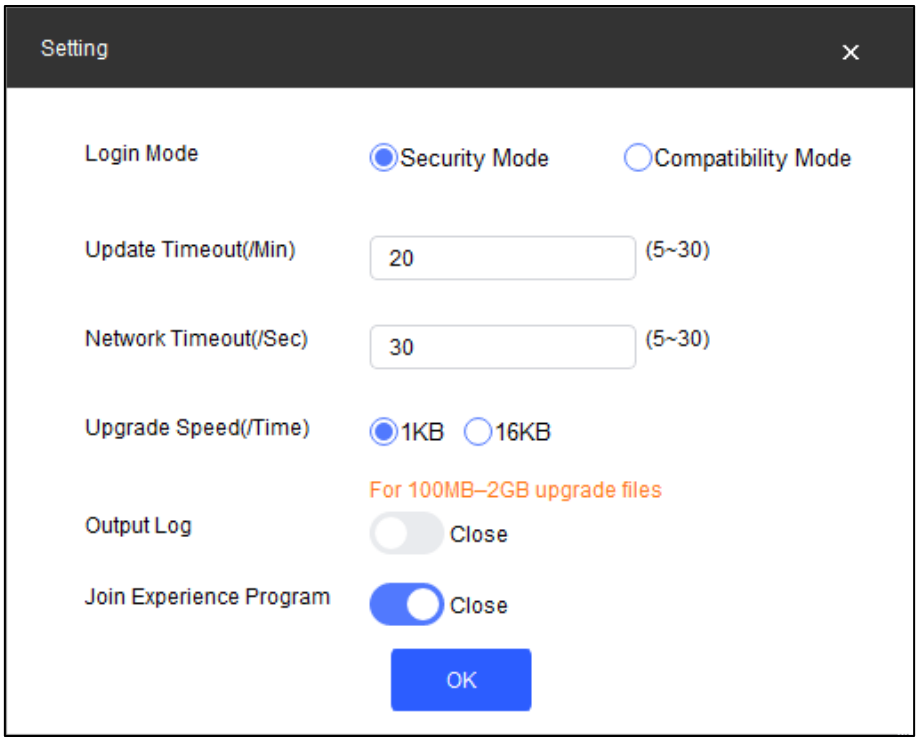


Table 5-1 Setting Parameters

Parameter	Description
Login Mode	• **Security Mode** (default): Log in only with secure authentication method. • **Compatibility Mode**: Try to log in with secure or insecure authentication method. It has potential risks and is not recommended to be used. ⚠ Compatibility mode has potential security risks. It is recommended to log in with security mode.
Update Timeout (/Min)	The maximum upgrade time for a single device when the device is upgraded. When the device upgrade time is longer than the set value, the system notices that the upgrade failed.
Network Timeout (/Sec)	The maximum timeout for network connection when the device is upgraded. When the network timeout is longer than the set value, the system stops upgrading.

Parameter	Description
Upgrade Speed (/Time)	Select the loading speed when upgrading. ● If package < 100 MB, the Tool loads the package 1 KB every time. The speed cannot be modified. ● If package size ≥ 200 MB, the Tool loads the package 16 KB every time. The speed cannot be modified. ● If 100 MB ≤ package size < 2 G, the Tool loads the package 1 KB every time. To speed up the process, you can set the speed to 16 KB every time. For details, see "5.3 Setting."
Output Log	Click to enable the function, and click to disable the function.
Join Experience Program	Click to enable the function, and click to disable the function.

5.3.2 Login Authentication

Device program version is low. Please upgrade the device or enable [ConfigTool] Compatibility Mode.

In security mode, there is a **Login Failed** dialog box displayed if the added device does not support logging in with security mode.

Operate according to the instructions and add the device again, when this hint appears. There are two methods and you can select from.

- We recommended upgrading the device bin which is available to log in by Security Mode. It can ensure the security of system.
- Click , and select **Setting**, and then switch login mode to Compatibility Mode.

Devices searched by network segment can all be successfully searched, regardless of if the devices support logging in with security mode.

Device searching does not trigger device login, and the login authentication is not performed. The device list is displayed normally.

Login failed. Device program version is low. Please upgrade the device or enable [ConfigTool] Compatibility Mode.

In security mode, if the operated device does not support logging in with security mode but has to be upgraded, rebooted and so on.

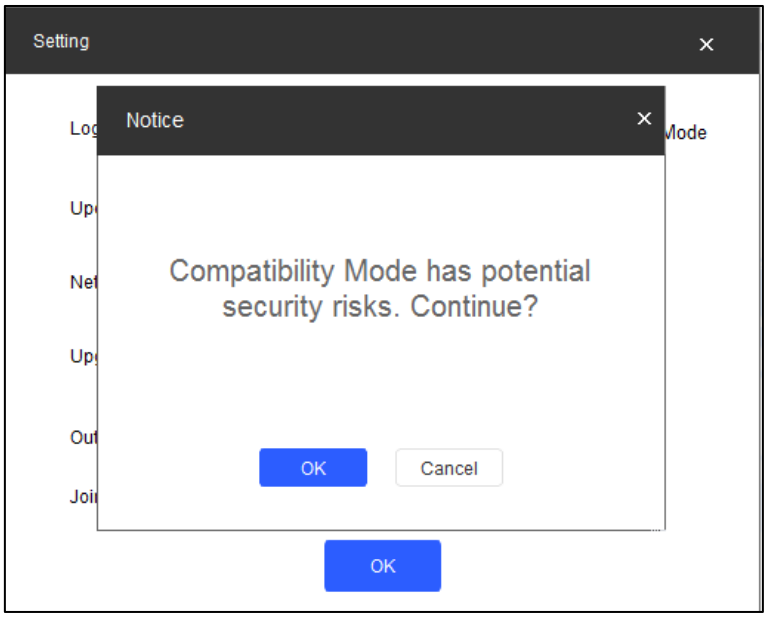
Operate according to the instructions and then repeat the failed operations when this hint appears. There are two methods. You can select one of them.

- It is recommended to upgrade the device bin which is available to log in by Security Mode. It can ensure the security of system.
- Click , and select **Setting**, and then switch login mode to **Compatibility Mode**.

Compatibility Mode has potential security risks. Continue?

Click , then select **Setting**, and switch login mode to **Compatibility Mode**.

Figure 5-3 Switch to compatibility mode (1)

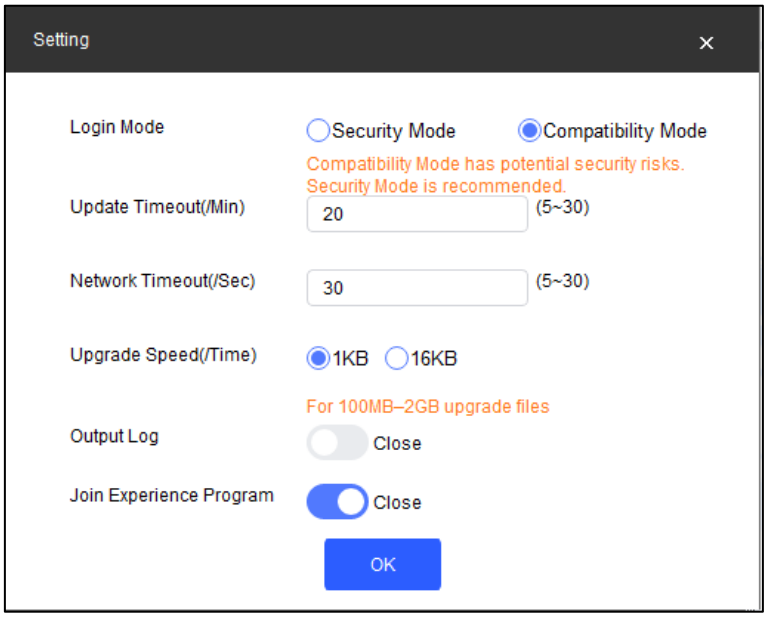


Compatibility Mode has potential security risks. Security Mode is recommended.

Switch login mode to **Compatibility Mode**, and click **OK** to confirm.

Compatibility mode has potential security risks. Think twice before operating.

Figure 5-4 Switch to compatibility mode (2)



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 on how to create a more secured security system.

Mandatory actions to be taken for basic equipment 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 equipment (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 equipment 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 equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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 equipment, 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 equipment 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 equipment, 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 equipment 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.