

ConfigTool

User's Manual



V1.2.6






Foreword

General

This manual introduces the functions and operations of the ConfigTool (hereinafter referred to as "the Tool"). Read carefully before using the tool, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.2.6	<ul style="list-style-type: none">• Added Encoding Strategy.• Added Average Bit Rate (ABR).• Added the encryption and decryption function when exporting and importing configurations.• Added VTS/VTO/VTH configurations in the download template.	January 2024
V1.2.5	Added the LLDP function.	November 2023
V1.2.4	<ul style="list-style-type: none">• Added the configuration file import function.• Added configuration search function.• Updated the building configuration function.	October 2023

Version	Revision Content	Release Time
V1.2.3	<ul style="list-style-type: none"> ● Updated Modify IP page. ● Updated device configuration function. ● Updated system configuration function. ● Added file upgrade function. ● Added intranet and extranet online upgrade function. ● Updated Building Configuration page. 	January 2023
V1.2.2	<ul style="list-style-type: none"> ● Updated the installation function. ● Added online upgrade function. ● Updated password reset function. ● Updated building configuration page. ● Updated system configuration function. ● Updated tool setting function. 	July 2022
V1.2.1	Deleted online upgrade function.	April 2022
V1.2.0	<ul style="list-style-type: none"> ● Updated home page. ● Added online upgrade function. ● Updated functions in adding devices. ● Updated functions in configuring video device parameters. ● Updated functions in resetting device password. 	January 2022
V1.1.7	<ul style="list-style-type: none"> ● Added join user experience improvement program" and privacy policy. ● Updated access control devices function. ● Added alarm host devices function. ● Update pictures in building configuration. ● Updated configuring parameters function. 	May 2021
V1.1.6	Updated functions in building configuration.	February 2021
V1.1.5	Updated functions in building configuration.	January 2021
V1.1.4	<ul style="list-style-type: none"> ● Added installation and uninstallation function, VDP function, android digital function and building configuration function. ● Updated pictures in the manual. ● Updated configuring ACS parameters function and CGI protocol. 	September 2020
V1.1.3	<ul style="list-style-type: none"> ● Added batch config items. ● Updated user page. ● Added to support ACS devices. 	June 2020
V1.1.0	Added upgrade transmission speed.	March 2020
V1.0.7	<ul style="list-style-type: none"> ● Added help section. ● Deleted online upgrade function. 	September 2019
V1.0.6	Updated resetting device password function.	July 2019

Version	Revision Content	Release Time
V1.0.5	<ul style="list-style-type: none"> ● Updated configuring system settings function. ● Changed the notice box in upgrade function and online upgrade function. ● Updated the template management page, and updated configuring video device parameters function. 	March 2019
V1.0.4	<ul style="list-style-type: none"> ● Added a notice box when you click reset password in the reset password menu. ● Added a notice box when click batch download and upgrade detect in the online upgrade menu. ● 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	<ul style="list-style-type: none"> ● Added the description of uninstallation. ● Modified the basic operations section. 	November 2016
V1.0.0	First release.	February 2016

Privacy Protection Notice

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

Table of Contents

Foreword.....	1
1 Overview.....	1
2 Installation and Uninstallation.....	2
2.1 Installation.....	2
2.2 Uninstallation.....	4
3 Home Page.....	5
4 Basic Operations.....	7
4.1 Adding Devices.....	7
4.1.1 Adding One Device.....	7
4.1.2 Adding Multiple Devices.....	10
4.2 Initializing Devices.....	12
4.3 Modifying IP.....	15
4.3.1 Modifying One IP.....	15
4.3.2 Modifying IP in Batches.....	15
4.4 Upgrading Devices.....	16
4.4.1 General Upgrade.....	17
4.4.2 File Upgrade.....	18
4.5 Online Upgrade.....	19
4.5.1 Detecting Devices.....	19
4.5.2 Online Upgrading Devices.....	23
4.5.3 Exporting and Viewing the Upgrade Result.....	26
4.5.4 Intranet and Extranet Online Upgrade.....	28
4.6 Configuring Device Parameters.....	29
4.6.1 Accessing the Configuration Page.....	29
4.6.2 Configuring Video Device Parameters.....	29
4.6.3 Access Control Devices.....	36
4.6.4 VDP.....	39
4.6.5 Android Digital Signage.....	51
4.6.6 Alarm Host Devices.....	53
4.7 Configuring System Settings.....	54
4.7.1 Timing.....	54
4.7.2 Rebooting.....	56
4.7.3 Restoring.....	57
4.7.4 Changing Device Password.....	60
4.7.5 Batch Configuration.....	61
4.7.6 License.....	63
4.7.7 LLDP.....	65

4.8	Resetting Device Password.....	65
4.8.1	Resetting Password in Batches.....	66
4.8.2	Resetting Password of One Device.....	67
4.9	Building Configuration.....	68
4.9.1	Generating Configuration and Distributing.....	69
4.9.2	Importing Configuration and Distributing.....	73
4.10	CGI Protocol.....	74
4.10.1	CGI Command Configuration.....	74
4.10.2	Changing CGI Commands in batches.....	74
4.10.3	Table Configuration.....	75
5	Help.....	77
5.1	Help File.....	77
5.2	Software Version.....	77
5.3	Settings.....	77
5.3.1	Configuring Parameters.....	77
5.3.2	Login Authentication.....	79
Appendix 1	Cybersecurity Recommendations.....	82

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 the device.
- Configure video parameters, encoding parameters and profile mode; Configure access controller (card number byte revert of different channels, TCP port number, log, and more); Configure VDP (device details, physical information, and Sip server information); Configure Android digital signage (APP configuration, Android commission, and log exporting).
- Synchronize device time, restart 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.

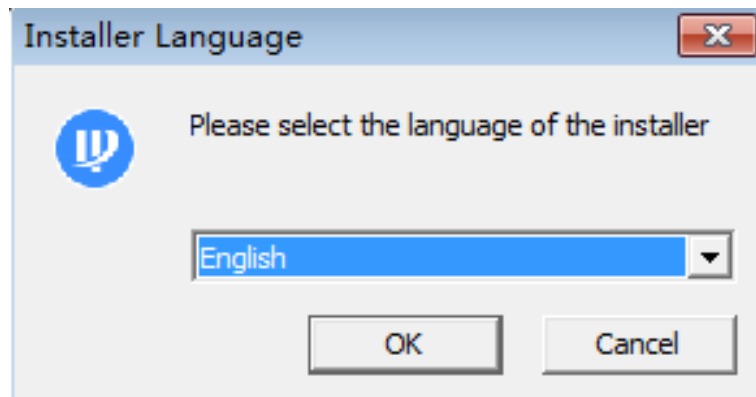
2.1 Installation

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

Procedure

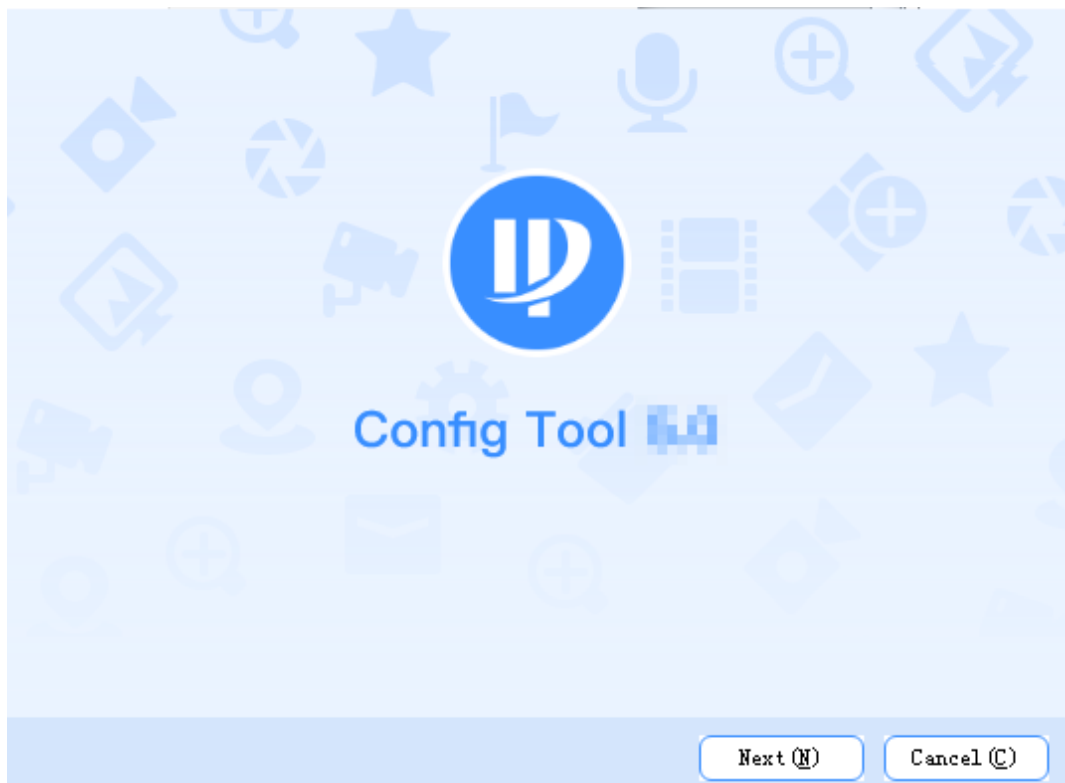
- Step 1 Double-click the installation package, and then the Tool pops up the **Installer Language** dialog box.

Figure 2-1 Install language



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

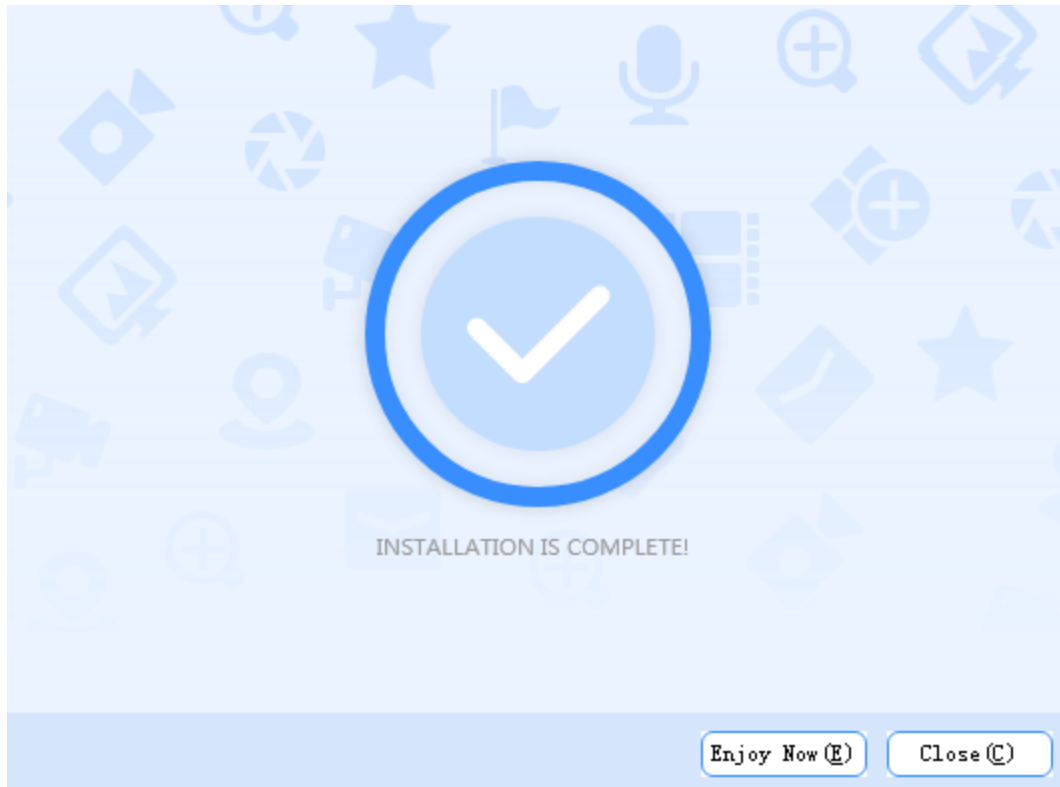
Figure 2-2 Welcome



- Step 3 Click **Next**.

- Step 4 Read the software license agreement, select **I agree**, and then click **Browse** to select save path.
- Step 5 Click **Install**.

Figure 2-3 Install

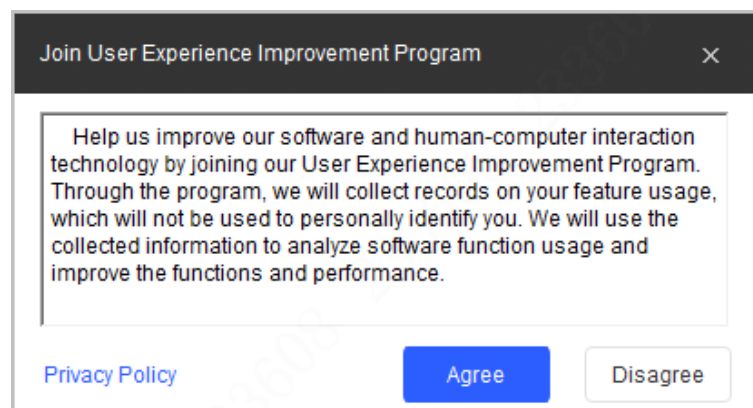


- Step 6 Click **Enjoy Now** to complete the installation and start the Tool, or click **Close** to exit.
- Step 7 Read software license agreement and Config Tool privacy policy, select **I have read and accepted**, and then click **Agree and continue**.
- Step 8 Click **Agree** to join user experience improvement program.



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

Figure 2-4 Join user experience improvement program

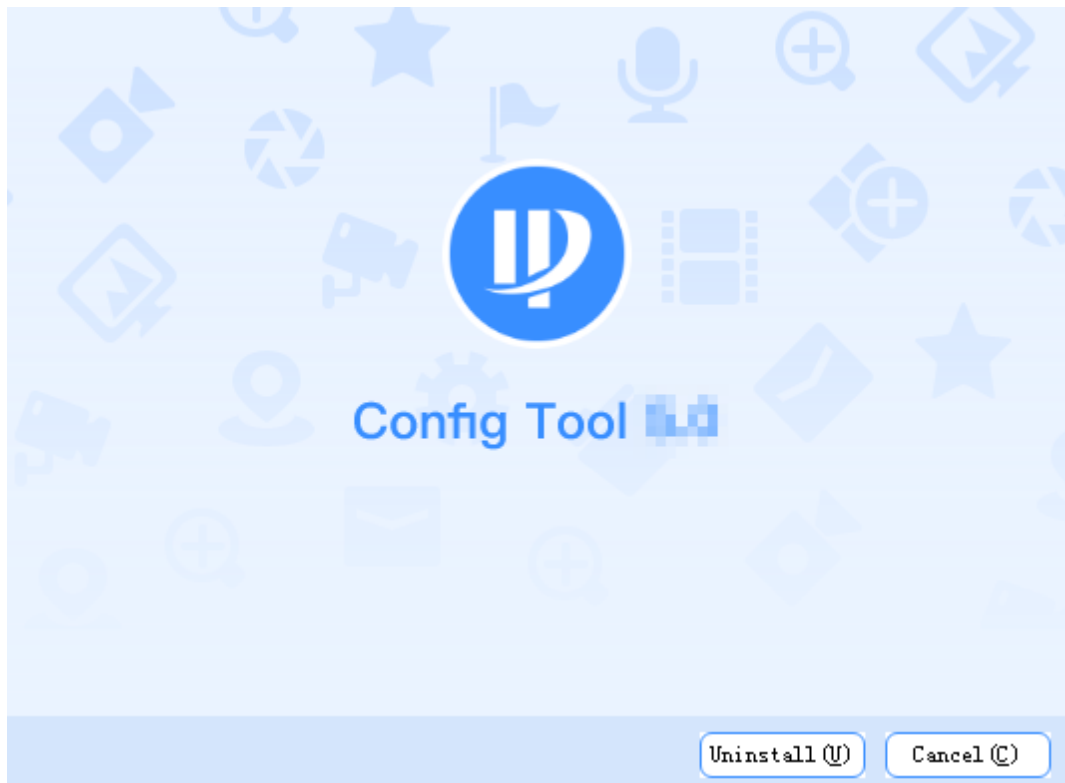


2.2 Uninstallation

Procedure

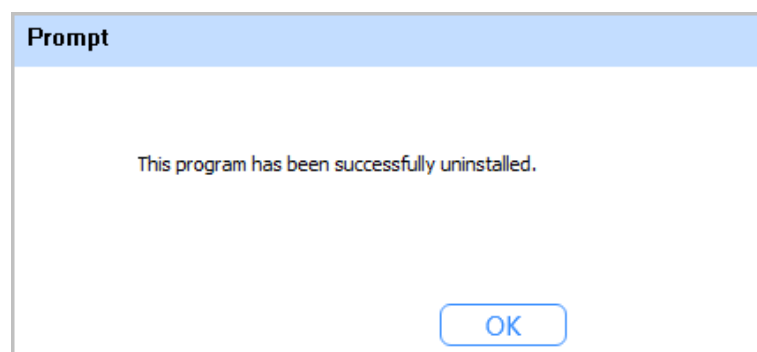
- Step 1 Click **Start > All Programs > ConfigTool > Uninstall ConfigTool** on your computer (uses Windows 7 as an example).

Figure 2-5 Uninstall



- Step 2 Click **Uninstall** to uninstall the Tool.
After the uninstallation is completed, the **Prompt** page will be displayed.

Figure 2-6 Prompt



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

3 Home Page

After starting the Tool, the home page is displayed.



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

Figure 3-1 Home page

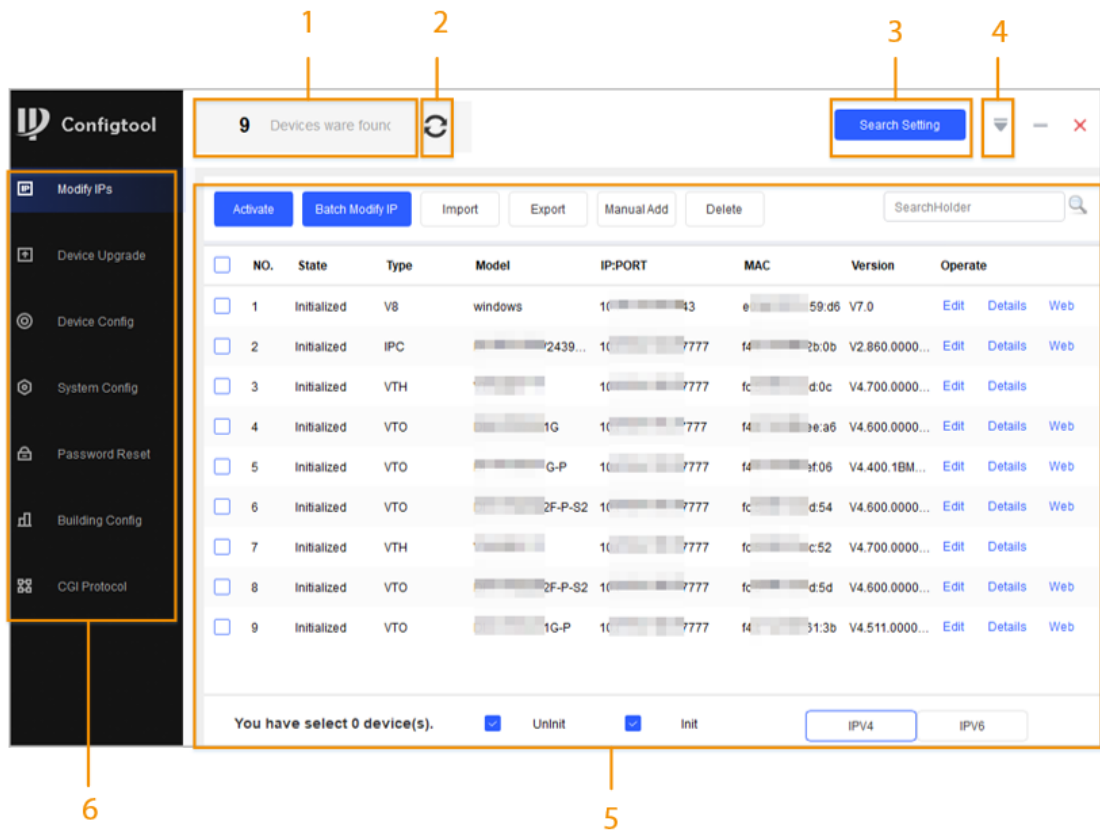



Table 3-1 Home page description

No.	Function	Description
1	-	Displays searched devices.
2	Refresh	Click to refresh the device list that is displayed in the main page. After opening the Tool, if the username or password has not been changed, every time you click , a notice box will pop up prompting you to go to Search Setting to change your username or password. Select Don't prompt again and the notice box will no longer be displayed.

No.	Function	Description
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.
5	Main page	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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.



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

4.1.1.1 Adding by IP Address

Procedure


- Step 1 Click  **Modify IP**, and then select **Manual Add > IP Address**.
- Step 2 Configure manual add parameters, and then click **OK**.

Figure 4-1 Manual add (IP address)

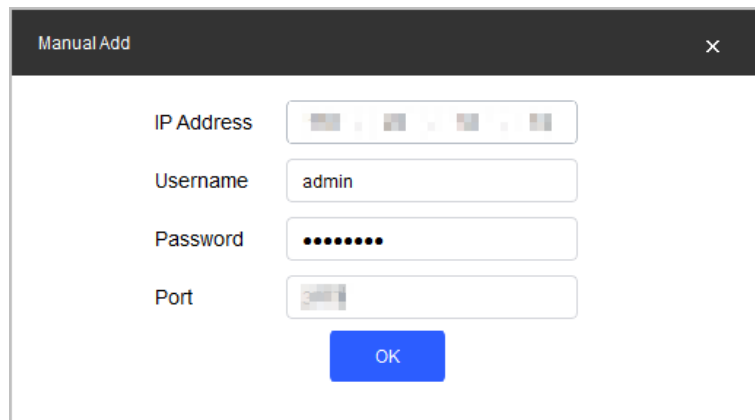


Table 4-1 Description of manual add parameters

Parameter	Description
IP Address	The IP address of the device.
Username	The username and password for device login.
Password	
Port	The device port number.


- Step 3 Click **OK**.

The newly added device is in the device list.

4.1.1.2 Adding by Registering

Under the internal and external network scenario, if ConfigTool cannot be directly connected to the device but the device can access the computer where ConfigTool is located, you can obtain and deliver device configurations through registering.

Procedure

Step 1 Click  **Modify IP**, and then select **Manual Add > Register**.


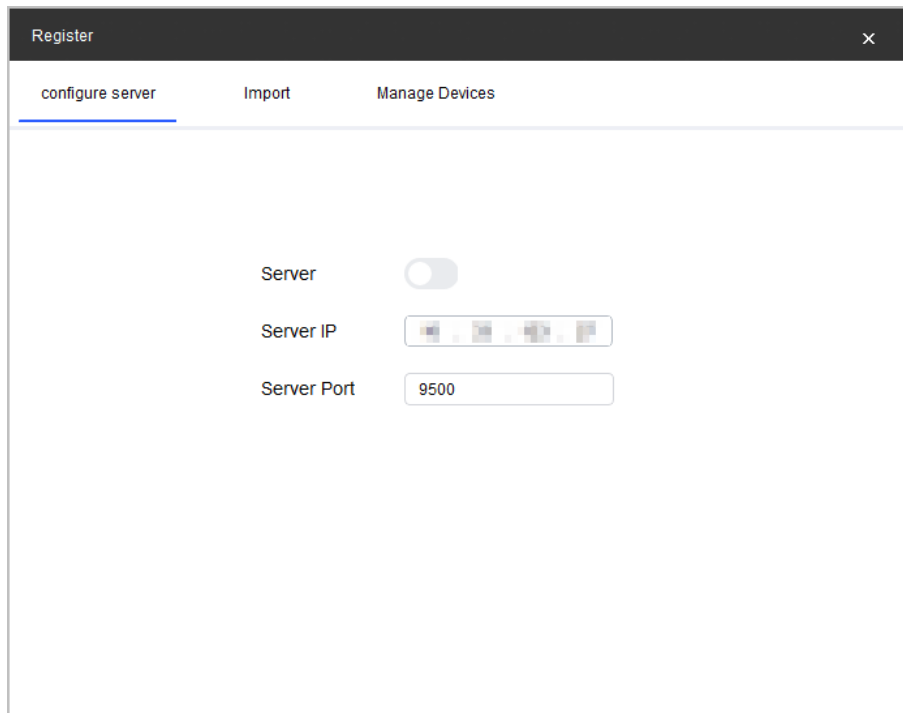
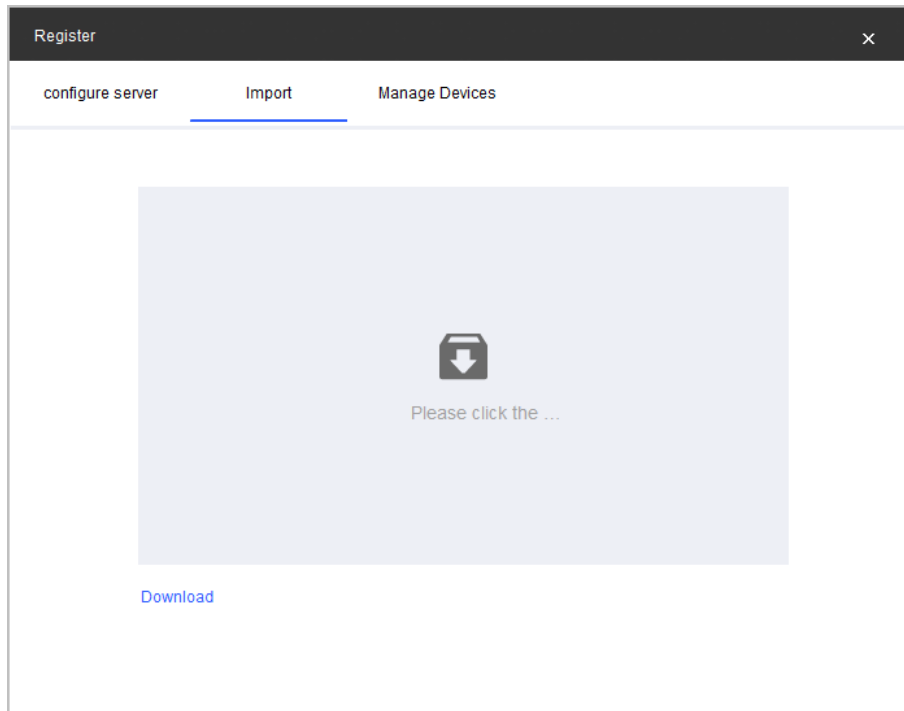
Step 2 Enter the **Server IP** and **Server Port**, and then click  next to the **Server** to enable registering function.


Figure 4-2 Configure the Server



Step 3 Click the **Import** tab, and then click **Download** to download the registering template.

Figure 4-3 Download the template



Step 4 Enter the device registration information in the downloaded excel file, and then click  to import the device.



- Supports adding multiple devices.
- The imported devices can be viewed on the **Manage Devices** page.

Step 5 Click **Manage Devices** tab to view the imported devices.



- The **IP** and **Port** columns display the IP and port numbers of the device.
- The devices whose status is **Synced** are automatically added to the device list on the **Modify IP** page.

Figure 4-4 Manage the Device

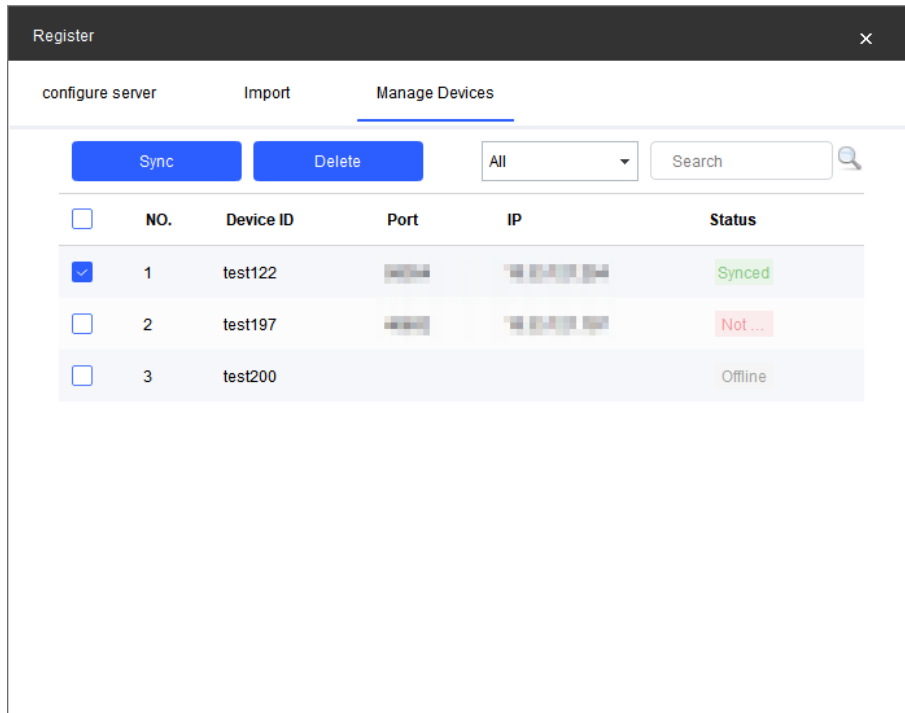


Table 4-2 Description of status parameters

Status	Whether the device is registered to the ConfigTool	Whether the device is added to the Modify IP page
Synced	Yes	Yes
Not Synced	Yes	No
Offline	No	No

Step 6 (Optional) Select the device that is not synced, and then click **Sync** to add the device to the device list on the **Modify IP** page and the status of the device switches to **Synced**.

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.

Background Information

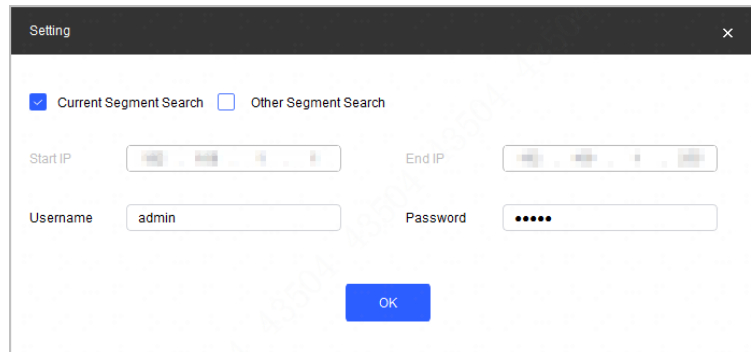


You can set filtering conditions to search specified devices quickly.

Procedure

Step 1 Click **Search Setting**.

Figure 4-5 Setting



Step 2 Select search method.

- **Current Segment Search** : Select the **Current Segment Search** checkbox. Enter the username in the **Username** box and the password in the **Password** box. The system will search devices accordingly. **Current Segment Search** is selected by default.
- **Other Segment Search** : Select the **Other Segment Search** checkbox. Enter IP address in the **Start IP** box and **End IP** box respectively. Enter username and password. The system will search the devices accordingly.




- If you select both the **Current Segment Search** checkbox and the **Other Segment Search** checkbox, 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 other operations.
- Supports searching up to 16 network segments simultaneously.

Step 3 Click **OK**.

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



- 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.

Background Information



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

Procedure

- 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 then click **Open**.

The system imports the device details. After the import completes, a success prompt will be 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.

Background Information

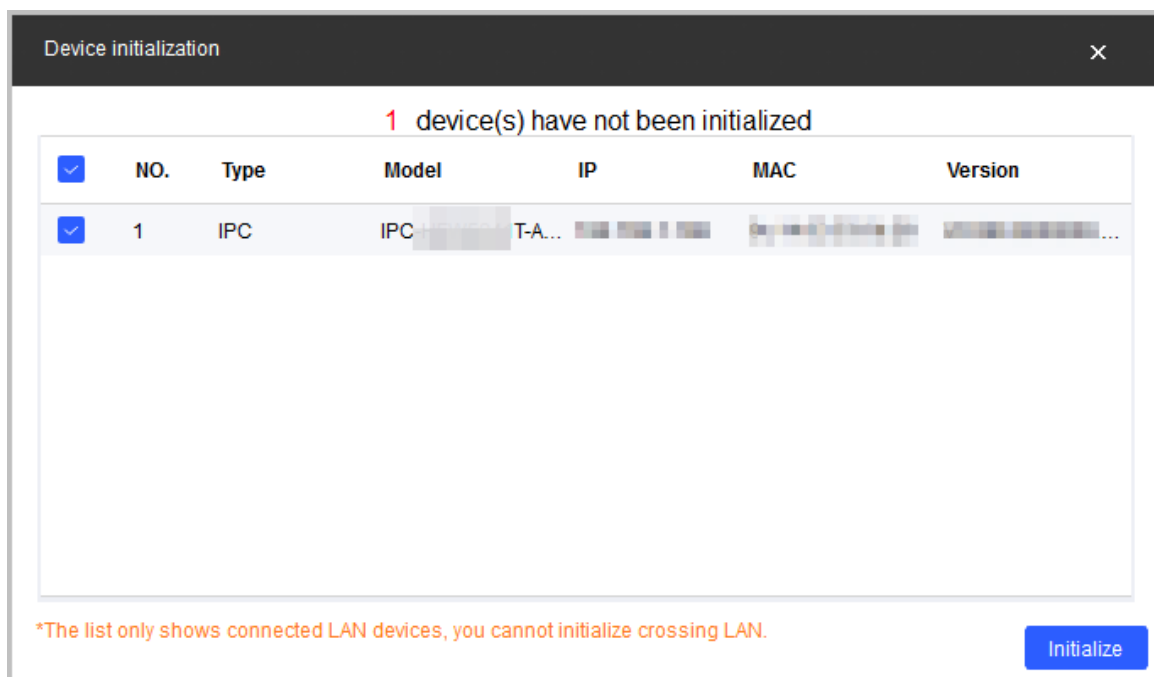
- This function is available on select models.
- The initializing operation can only be performed to the devices within the local area network.
- Any operation cannot be performed on uninitialized devices.

Procedure

Step 1 Click  **Modify IP**.

Step 2 Select devices to be initialized, and then click **Initialize**.

Figure 4-6 Device initialization (1)



Step 3 Configure initialization parameters, and then click **Next**.

Figure 4-7 Device initialization (2)

Device initialization
×

1 device(s) have not been initialized

Username

New Password

Weak
Medium
Strong

Confirm Password

Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them. (excluding Single quote('), double quote("), colon(:), semicolon(;), connection symbol(&))

Email Address (for password reset)

Select P/N

*After you have set new password, please set password again in "Search Setting".



- If you do not provide the email address 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.

Table 4-3 Initialization parameters

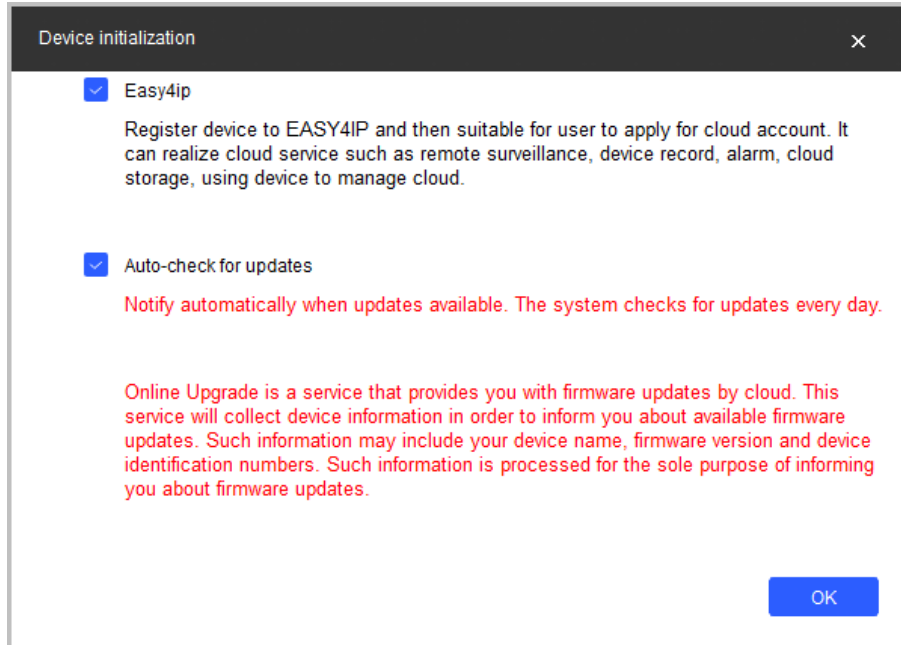
Parameter	Description
Username	The user name is admin by default.
New Password	Enter your new password. A prompt appears to inform you the strength of your new password. <div style="background-color: #d3d3d3; padding: 2px 5px; margin-top: 5px; font-size: 10px;">The password strength might vary depending on the devices.</div>
Confirm Password	Confirm the new password.
Email Address	It is selected by default. The email address is used for password reset.

Step 4 Select **Easy4ip** or select **Auto-check for updates**, and then click **OK**. If neither is needed, leave them unselected.



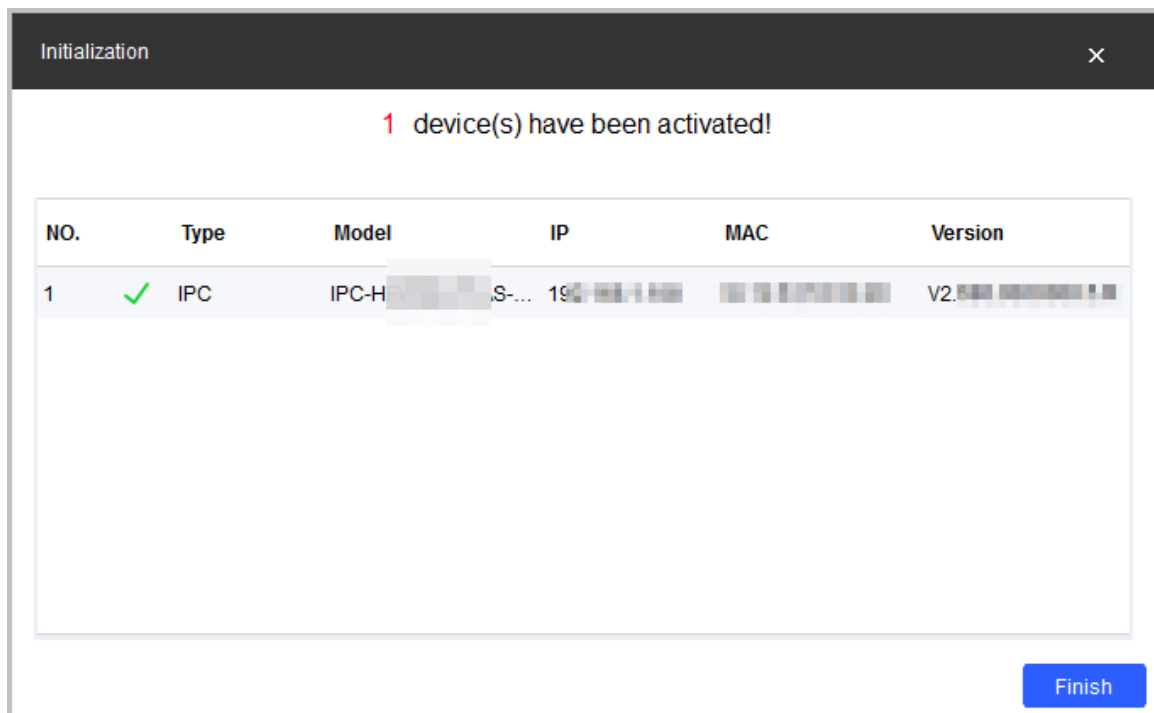
Some devices do not support automatic detection and Easy4ip.

Figure 4-8 Device initialization (3)



Step 5 Click the success icon (✓) or click the failure icon (⚠) for details.

Figure 4-9 Initialization



Step 6 Click **Finish**.

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

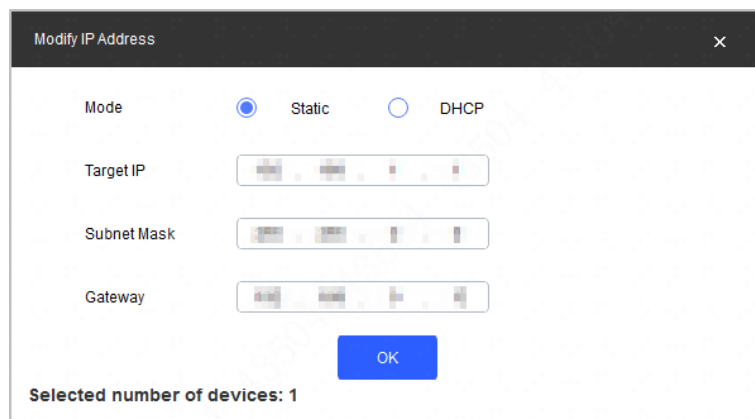
Procedure

- 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 4-10 Modify IP address




- Step 3 Configure IP address.
- **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

Procedure

- 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 4-11 Modify IP address (3)

Modify IP Address

Mode Static

Start IP Same IP

Subnet Mask

Gateway

OK

Selected number of devices: 2

Step 4 Configure IP address.

- **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** checkbox, the IP address of the devices will be set to the same one.

Step 5 Click **OK**.

4.4 Upgrading Devices

Supports upgrading device separately or in batches, and upgrading through files.

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 \geq 200 MB, the Tool loads the package at 16 KB every time. The speed cannot be modified.
- If $100 \text{ MB} \leq$ package size < 2 GB, 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 Settings".



If the device disconnects during update, the device might restart 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.

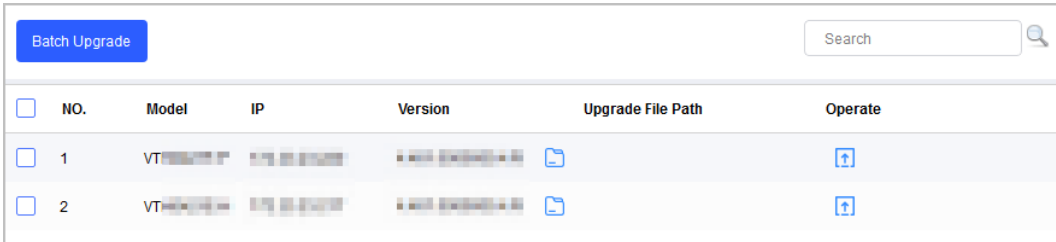
4.4.1 General Upgrade





4.4.1.1 Upgrading One Device


Procedure

Step 1 Click  Device Upgrade.

Figure 4-12 Upgrade




<input type="checkbox"/>	NO.	Model	IP	Version	Upgrade File Path	Operate
<input type="checkbox"/>	1	VT...		
<input type="checkbox"/>	2	VT...		

Step 2 Click  next to the device that you want to upgrade. Select the specific file that needs to be upgraded, and then 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 **Prompt** dialog box will be displayed indicating the device will be restarted, and then the device restarts automatically.

4.4.1.2 Upgrading Devices in Batches

You can upgrade multiple devices in the same software version.

Procedure

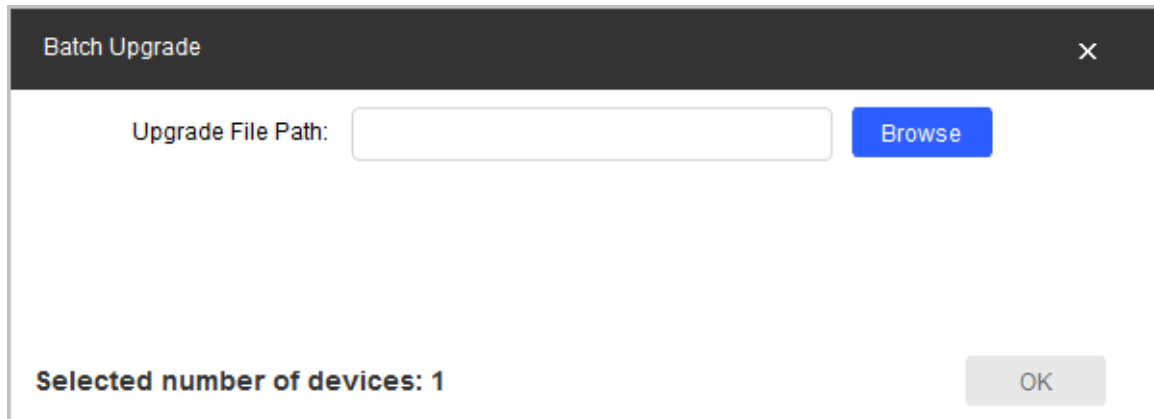
Step 1 Click  Device Upgrade.

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 all selected devices can receive the same software update.

Figure 4-13 Batch upgrade



Step 3 Click **Batch Upgrade**.


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

Step 5 Click **OK**.

4.4.2 File Upgrade

Procedure

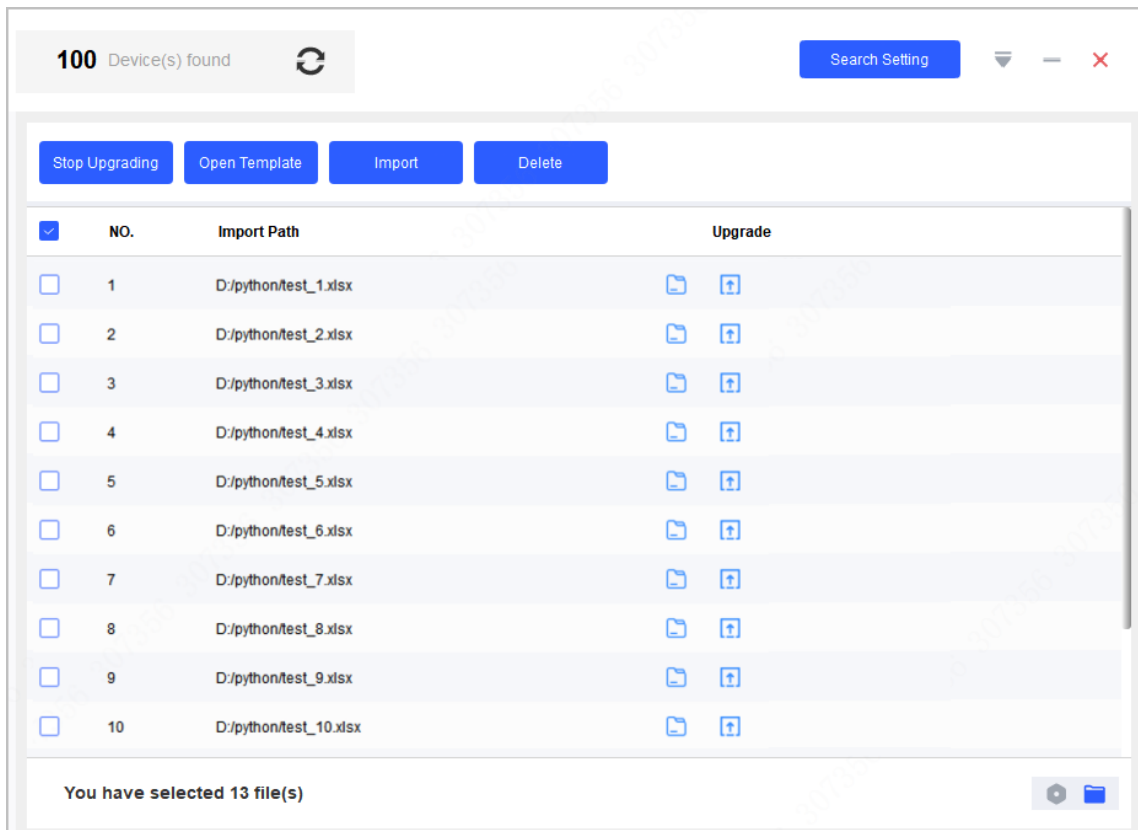
Step 1 Click  **Device Upgrade**.

Step 2 Click  on the lower-right corner of the page to switch to file upgrade mode.

Step 3 Click **Open Template**, and then enter the IP address, port, username, password and upgrade file path of the device.

Step 4 Click **Import** to import the filled template.

Figure 4-14 File upgrade



Step 5 Upgrade the device.

The upgrading steps of the file upgrade mode is consistent with the general mode. For details, see "4.4.1 General Upgrade".

4.5 Online Upgrade

4.5.1 Detecting Devices

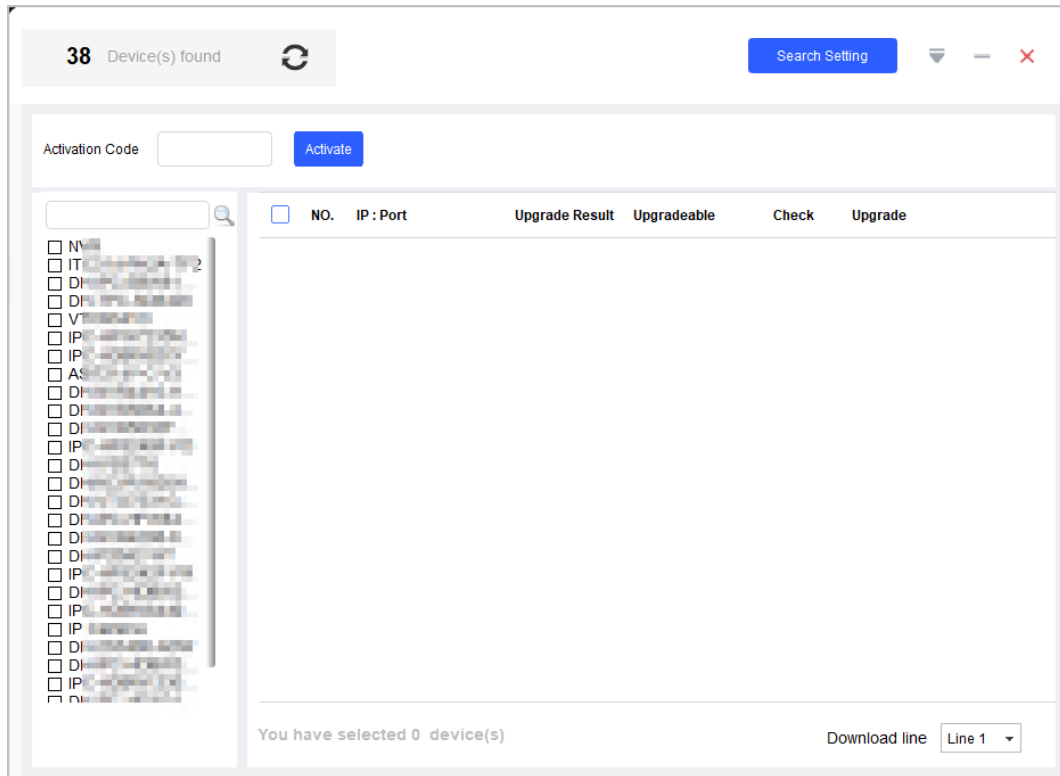
Prerequisites

Make sure that the PC where ConfigTool is installed is connected to the Internet.

Procedure

Step 1 Click Online Upgrade.

Figure 4-15 Online upgrade page

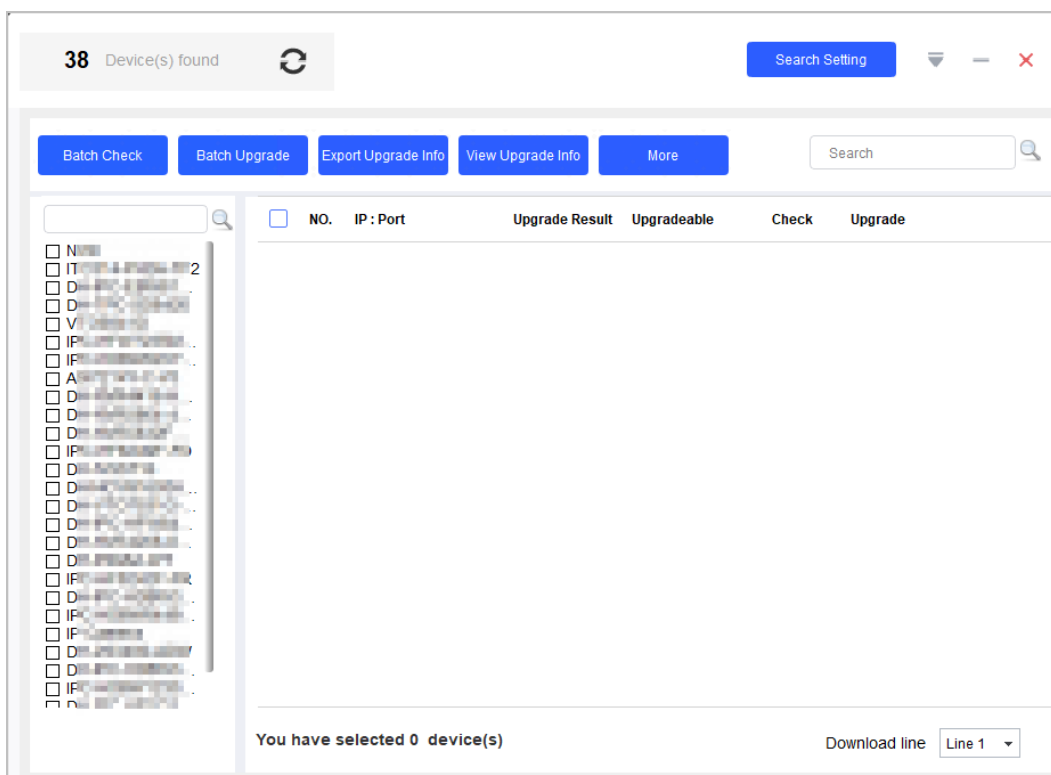


Step 2 Enter the **Activation Code** , and then click **Activate**.



Inactive users cannot perform online upgrade operations. The activation code needs to be applied for from the service provider.

Figure 4-16 Online upgrade page after activation

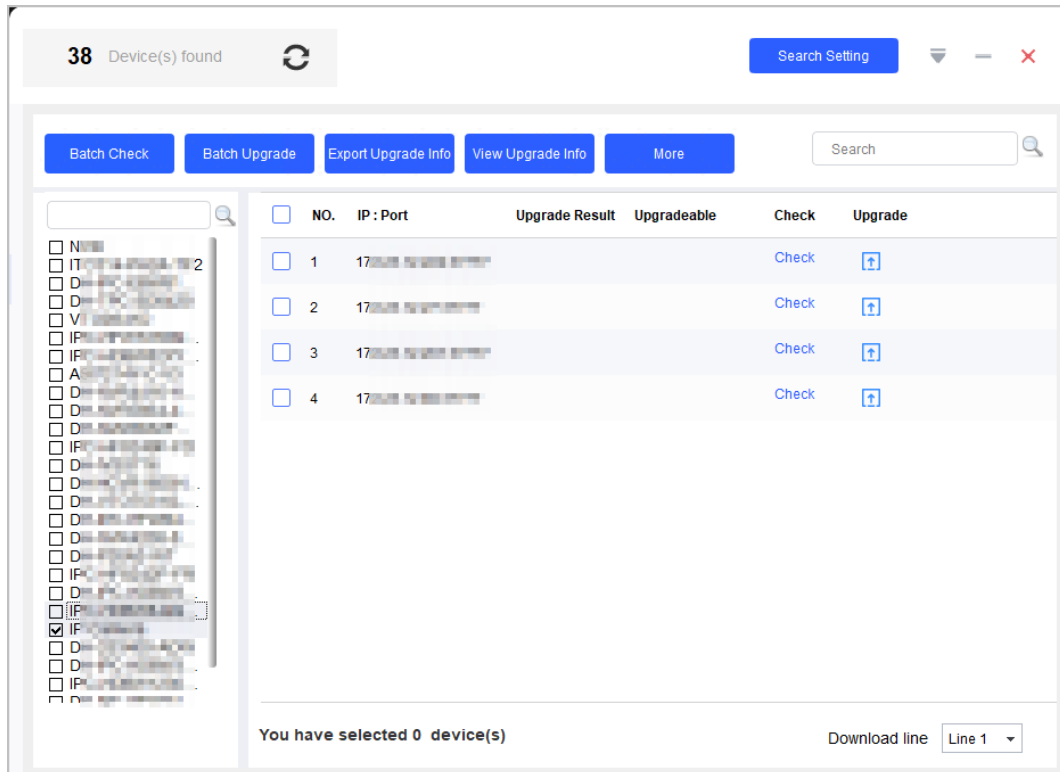


Step 3 Select the model to be operated on the left side of the page, and then the corresponding device information will be displayed in the device list.



Multiple devices of the different models can be upgraded in batches at one time.

Figure 4-17 Select online upgrade devices




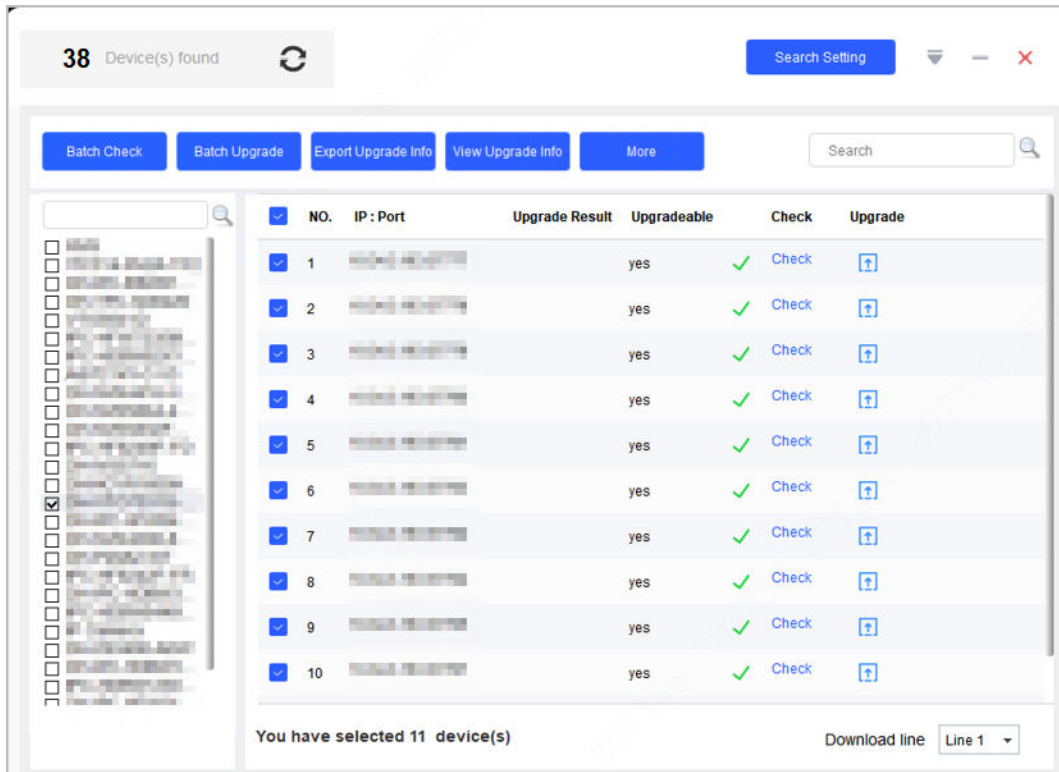
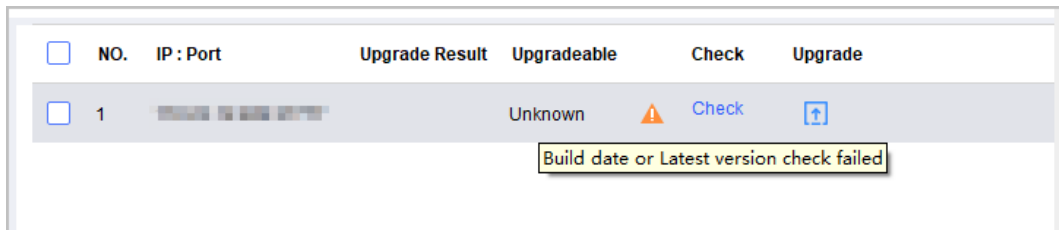
- Step 4** Click **Check** corresponding to the device or select the devices to be checked, and then click **Batch Check** to check whether there is a new upgrade program.
- If the device is upgradable, the **Upgradeable** column displays **yes** and the **Upgrade Result** column is empty.
 - If the device is not upgradable, the **Upgradeable** column displays **no**.
 - If the check fails, click  to view the failure reason.

Figure 4-18 Check upgrade status



Step 5 (Optional) When the device checks multiple upgradeable programs at the same time, if the detection is successful, the upgradeable column displays **Unknown**. Point to **Unknown** to display specific prompts.

Figure 4-19 Check multiple upgradeable programs




4.5.2 Online Upgrading Devices

Prerequisites

- The online upgrade function has been activated. For details, see "4.5.1 Detecting Devices".
- All devices that need to be upgraded have successfully completed the checking, and those that have not been checked or failed to be checked will not be added to the upgrade queue.

Procedure

Step 1 Click  corresponding to the device, or select the devices to be upgraded, and then click **Batch Upgrade**.

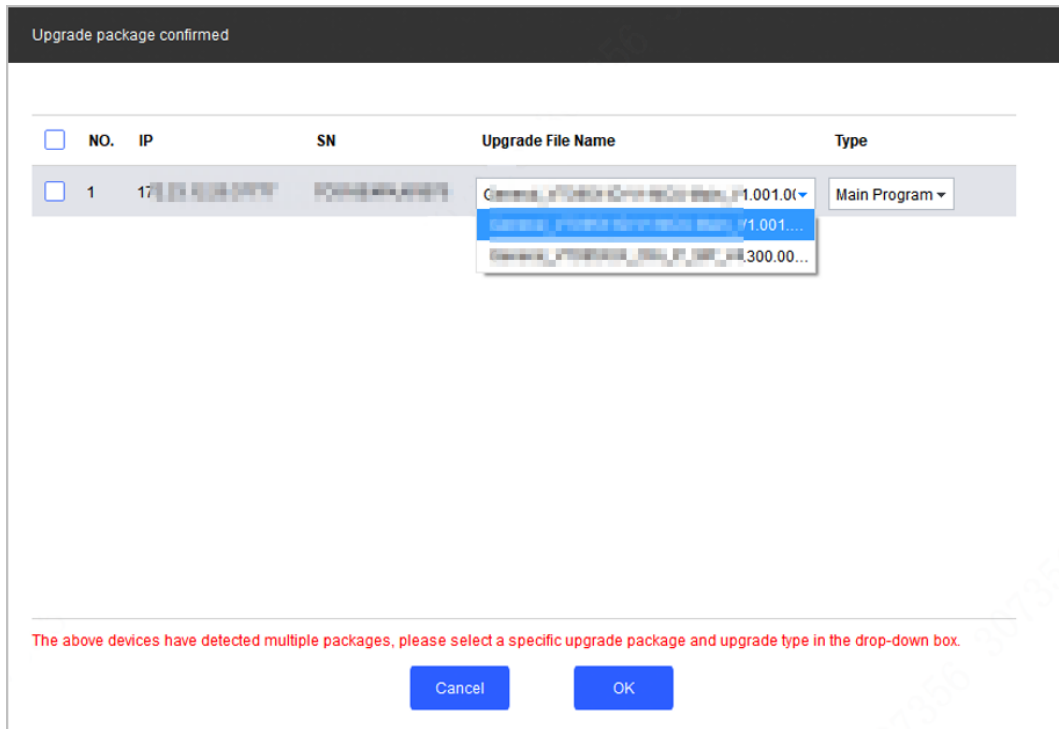


The upgrade result displays only the latest upgrade result. If the upgrade succeeds, the **Upgrade Result** displays as **Success**; if the upgrade fails, the **Upgrade Result** displays as

Fail. If there is no upgrade record or the last upgrade is more than 3 months old, nothing is displayed.

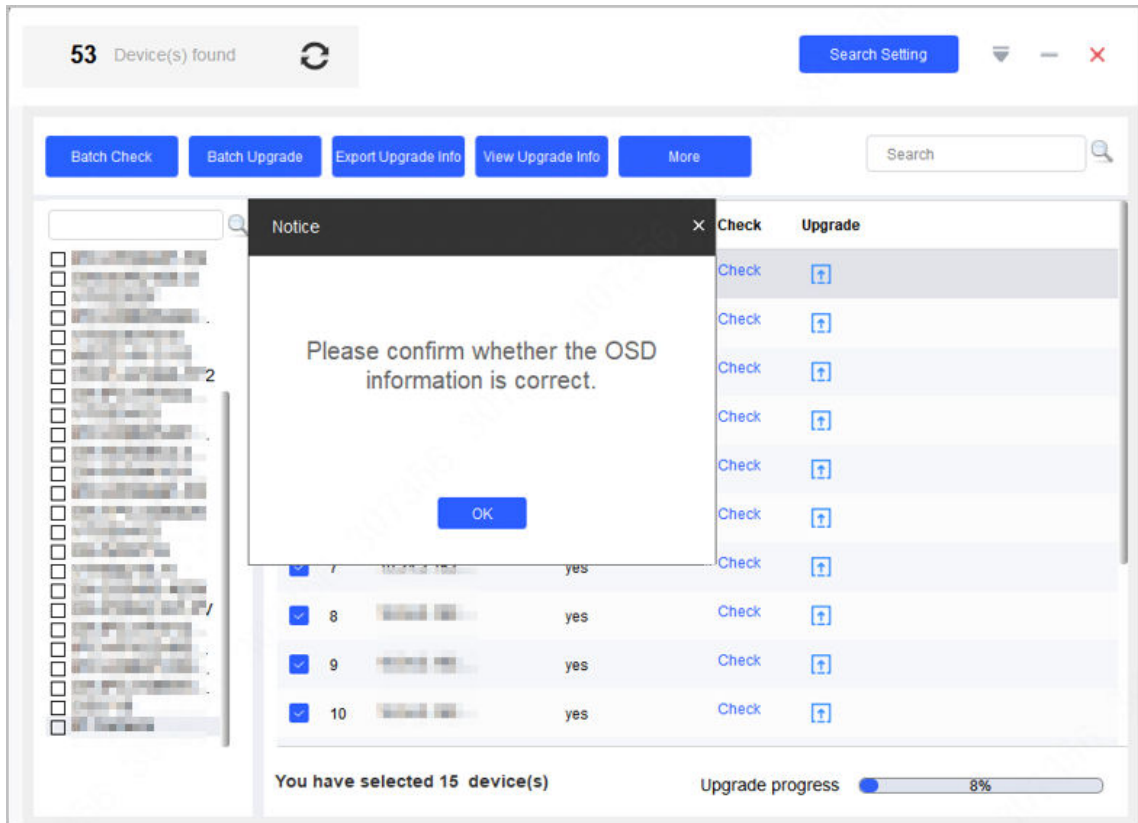
Step 2 (Optional) If the device detects multiple upgradeable programs at the same time, select the **Upgrade File Name** and **Type**, and then click **OK**.

Figure 4-20 Select upgrade package



Step 3 After clicking **Batch Upgrade**, you need to confirm whether key information such as the device OSD and third-party access configuration is lost before the upgrade of the first device. After confirmation, click **OK**.

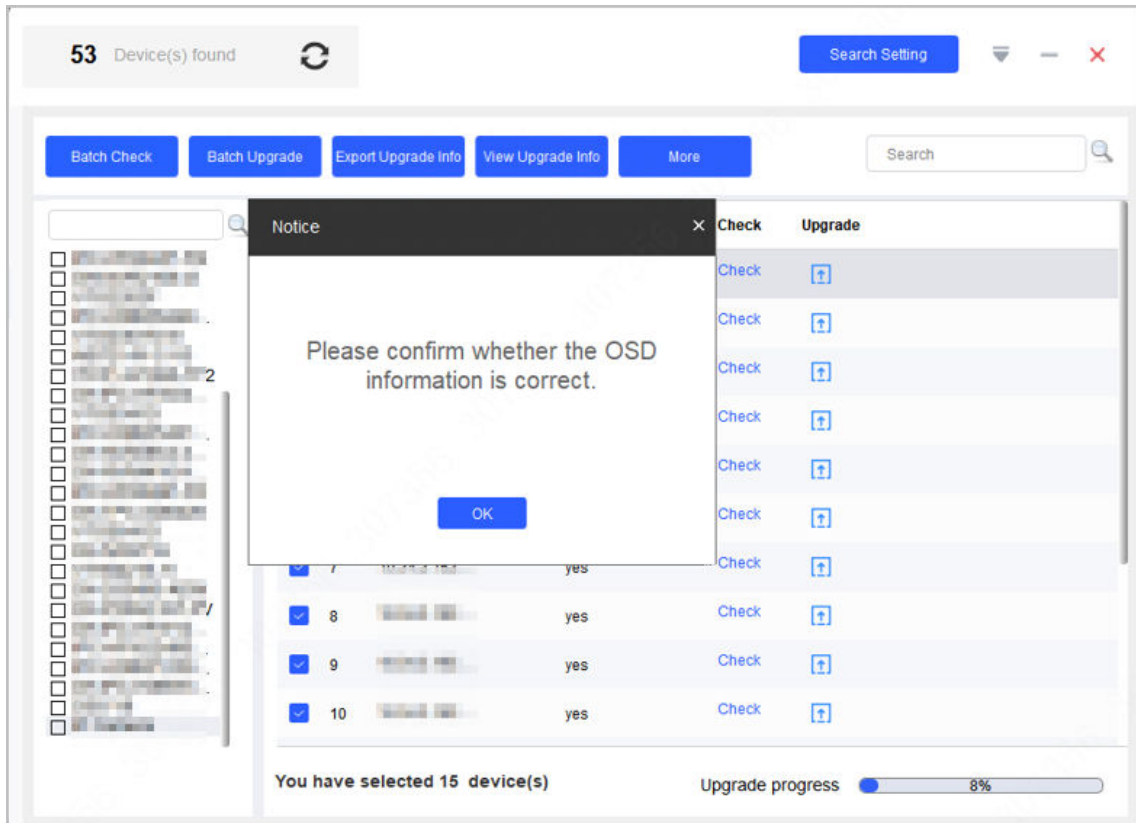
Figure 4-21 Confirm ODS information



Step 4 After the OSD information is confirmed, the Tool collects online rates for all devices in the remaining task queue.

The Tool first upgrades 20% of the remaining devices, waits for 3 minutes when the last device of the 20% is upgraded, and then checks whether the 20% of the devices can log in normally. If the online rate exceeds 90%, the remaining 80% of the devices will be upgraded directly. If the online rate is lower than 90%, a pop-up dialog will prompt that the remaining 80% of devices cannot start normally. Click **OK** to continue upgrading the remaining devices, otherwise all the subsequent upgrades will be cancelled.

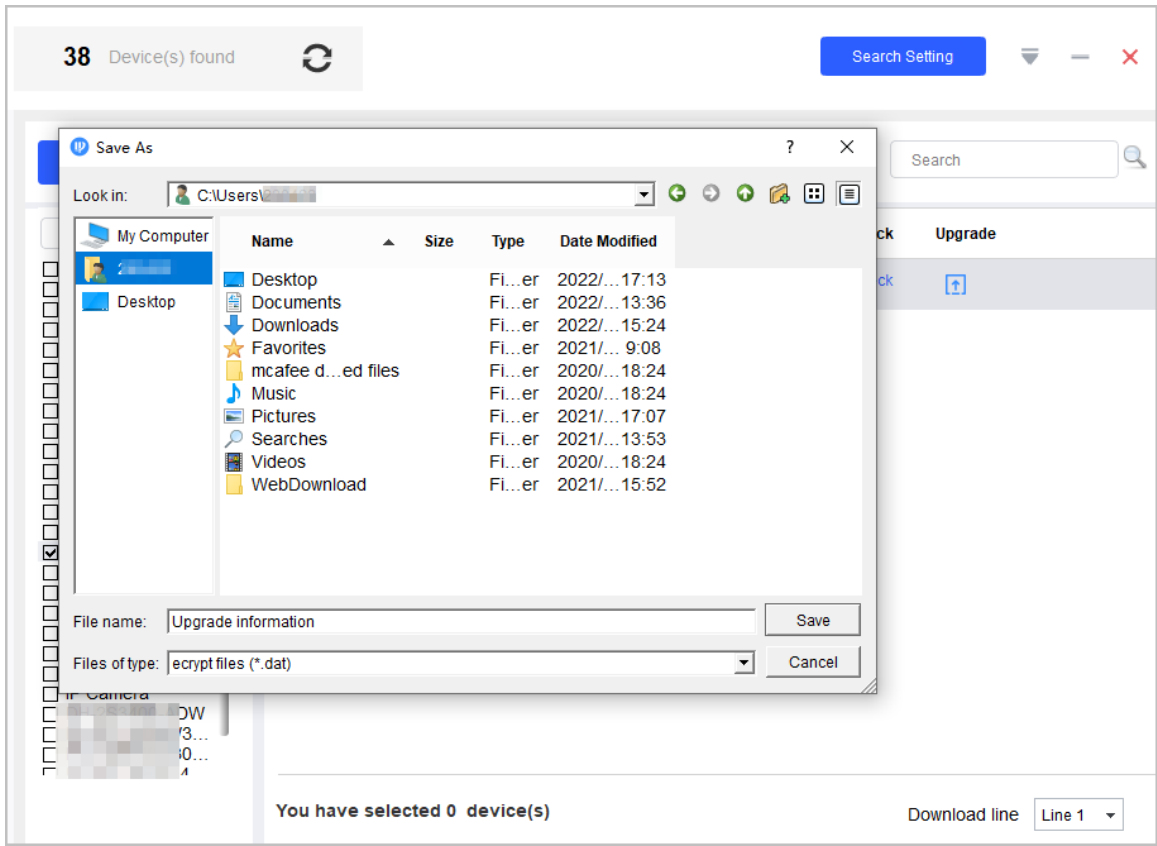
Figure 4-22 Collect online rate



4.5.3 Exporting and Viewing the Upgrade Result

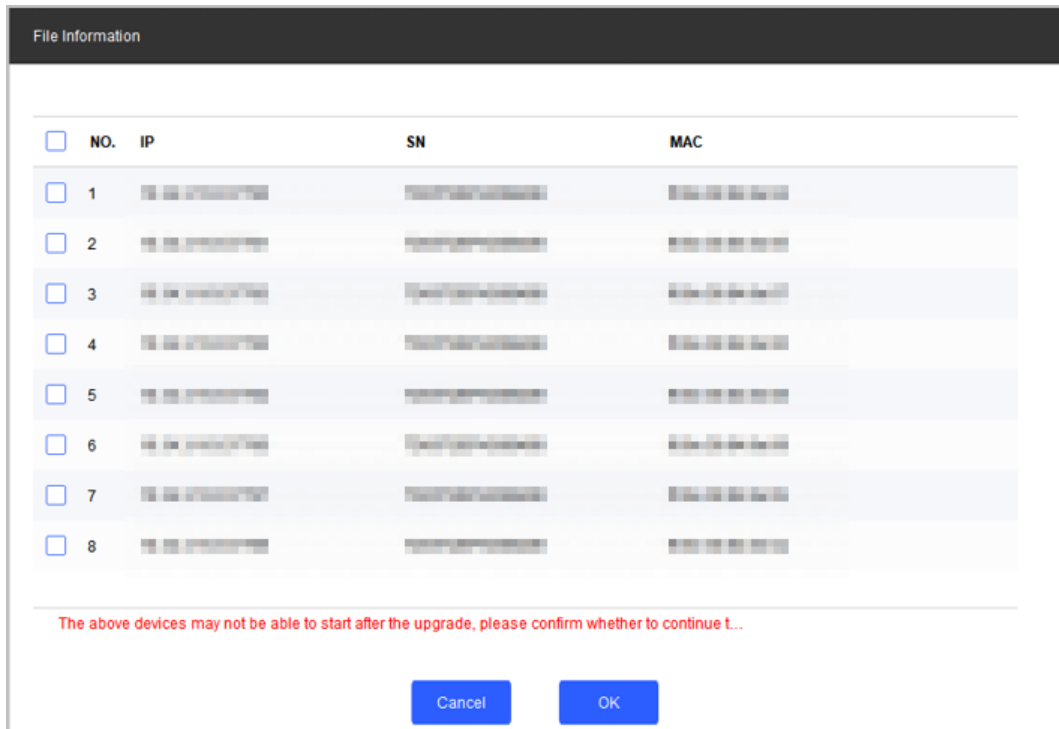
- Click **Export Info** to export the upgrade result to the computer.

Figure 4-23 Export upgrade result



- Click **View Info** to view the exported .dat file.

Figure 4-24 View upgrade result



4.5.4 Intranet and Extranet Online Upgrade

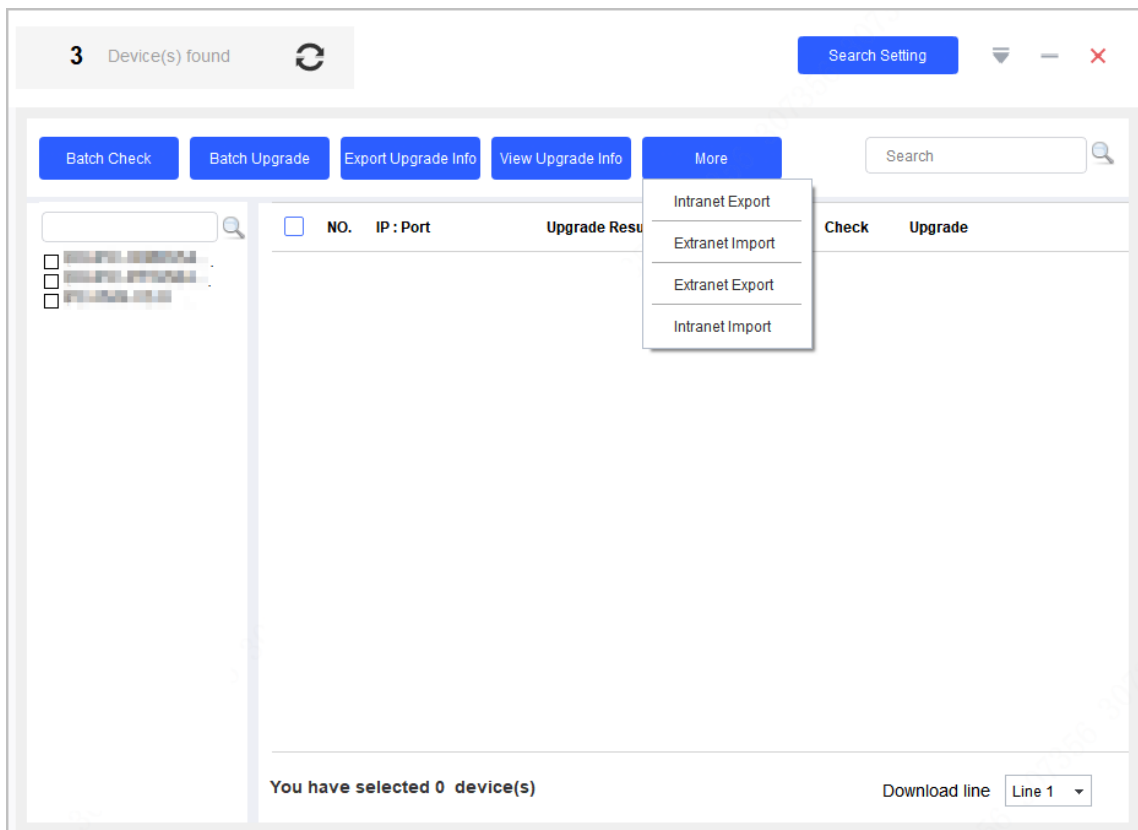
Procedure

Step 1 Click **Intranet Export** to export device information.




- After clicking **Intranet Export**, all devices in the device list will be exported. If there are any devices that do not need to be upgraded, you can delete them on the **Modify IP** page.
- Make sure the account password is correct.

Figure 4-25 Intranet and extranet online upgrade



Step 2 Copy the exported file to the computer that can be connected to the Internet, click **Extranet Import**, and then select the file.



After the import is successful, the Tool automatically starts to detect and download the upgrade package, and the download directory of the upgrade package can be selected and viewed through  > **Setting** on the upper right corner of the Tool.

Step 3 Click **Extranet Export** to copy the exported dat file and the upgrade package to the intranet computer.



The upgrade package must be stored in the default download path of the Intranet computer. Otherwise, the upgrade will fail.

Step 4 Click **Intranet Import** on the intranet computer, select the exported dat file and the device to be upgraded, and then click **Upgrade** or **Batch Upgrade**.

4.6 Configuring Device Parameters

Configure device parameters such as encoding, video and profile.

4.6.1 Accessing the Configuration Page

Procedure

Step 1 Click  **Device Config**.

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

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

4.6.2 Configuring Video Device Parameters

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



The page and parameters might vary depending on the device type and model.

4.6.2.1 Configuring Encoding Parameters

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

Procedure

Step 1 Complete Step 1 to Step 3 in "4.6.1 Accessing the Configuration Page".

Step 2 On the **Encode** page, configure the parameters for main stream and sub stream.

Figure 4-26 Encode

Channel 1

Main Stream

Code Stream Type Regular	Compression H.264H
Encoding Strategy Regular	Audio <input checked="" type="checkbox"/>
Bit Rate Type CBR	Audio Encode G.711A
Frame Rate 25	Sampling Frequency 8000
Resolution QFHD	
Quality 4	
Bit Rate(Kb/S) Customized	3328

Sub Stream

Code Stream Type Regular	Compression H.264H
Bit Rate Type CBR	Audio/Video <input type="checkbox"/> <input checked="" type="checkbox"/>




[Apply to...](#)



The encoding parameters might vary with different models.

Table 4-4 Encode parameters

Parameter	Description
Channel	Select channel number.
Code Stream Type	Includes Regular , Motion , and Alarm . The sub stream only supports Regular type.
Encoding Strategy	Includes Regular , Smart Codec , and AI Codec . Only the main stream can configure this parameter.
Compression	<p>Includes the following video encoding modes:</p> <ul style="list-style-type: none"> ● 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. We recommend you use the maximum bit rate value to get the best results. ● SVAC2.0: SVAC2.0 encoding.

Parameter	Description
Bit Rate Type	<p>Includes the two types of bit rates:</p> <ul style="list-style-type: none"> ● 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. ● Average Bit Rate (ABR) : The bit rate is controlled to save bandwidth and improve image quality.  <p>When the compression is set as MJPG , the bit rate can only be CBR.</p>
Frame Rate	<p>Total frames per second.</p> <p>The higher the frame rate, the more clear and smooth the image.</p>
Resolution	<p>Video resolution.</p> <p>The maximum video resolution might be different depending on your device model.</p>
Quality	<p>Video image quality level.</p> <p>You can configure this parameter when the bit rate type is set as VBR.</p>
Bit Rate (Kb/S)	<p>Select a suitable value.</p>  <p>You can configure this parameter when the bit rate type is set as CBR.</p>
Audio/Video	<ul style="list-style-type: none"> ● Select the Audio checkbox to enable audio function. ● Select the Video checkbox to monitor with sub stream. <p>For the sub stream, you can enable the audio function only after the video function is already enabled.</p>  <p>In the Sub Stream section, the two checkboxes next to Audio/Video stand for audio and video respectively. To enable audio, select the first checkbox; for video, select the second one.</p>
Audio Encode	<p>Audio encoding modes includes G.711A, G.711Mu, G.726 and AAC.</p> <p>The setting of audio encoding mode will apply to both audio and voice intercom.</p>
Sampling Frequency	<p>The sampling frequency of the audio.</p>

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 page.

4.6.2.2 Configuring Video Parameters

You can check the live video and set video effects.

Procedure

Step 1 Complete **Step 1** to **Step 3** in "4.6.1 Accessing the Configuration Page".

Step 2 Click the **Image** tab.





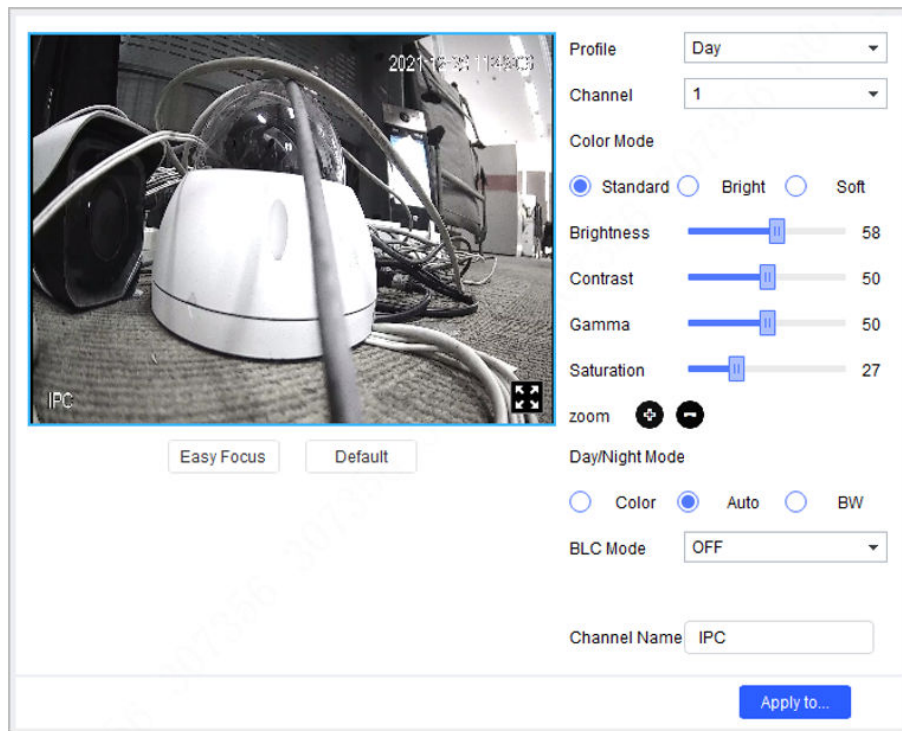
- Click **Default** to restore the default parameters settings.
- Roll mouse wheel on the image to zoom in or zoom out. Right-click on the image to return to default size.
- On the image, click  to display in full screen, and then click  on full screen to restore the default.




Figure 4-27 Image



Step 3 Configure the video parameters.

Table 4-5 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.

Parameter	Description
Saturation	Adjust color. The bigger the value, the lighter the color. This value does not affect the general image lightness.
Zoom	Click  or  to adjust the zoom speed.  This function is available on select models.
Day/Night Mode	Includes the following three options: <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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. Channel name cannot input null characters.

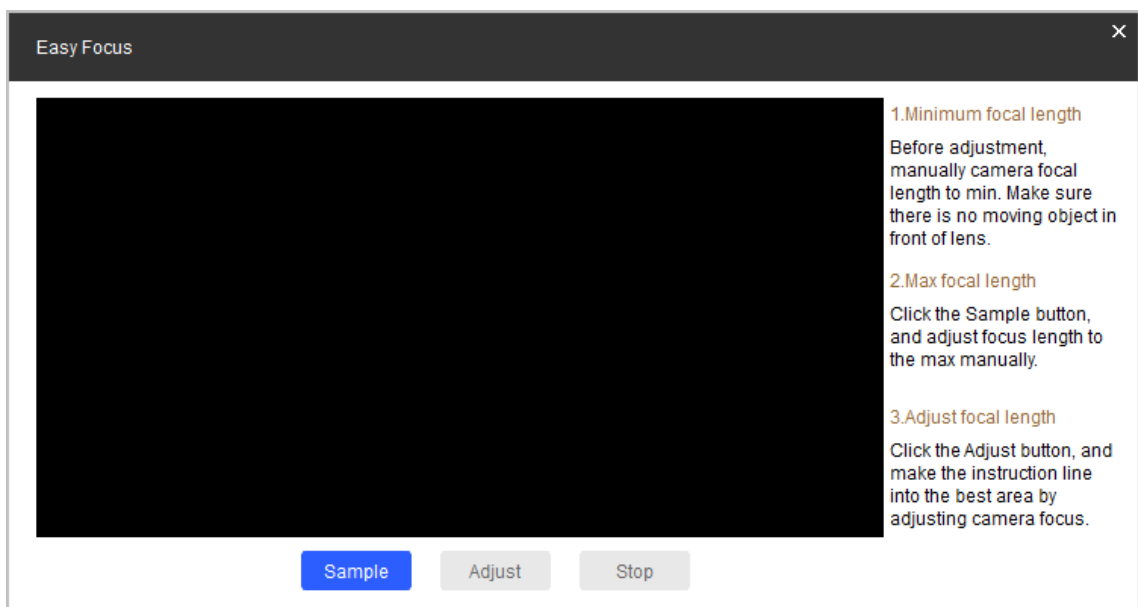
Step 4 (Optional) Configure the **Easy Focus** function.



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

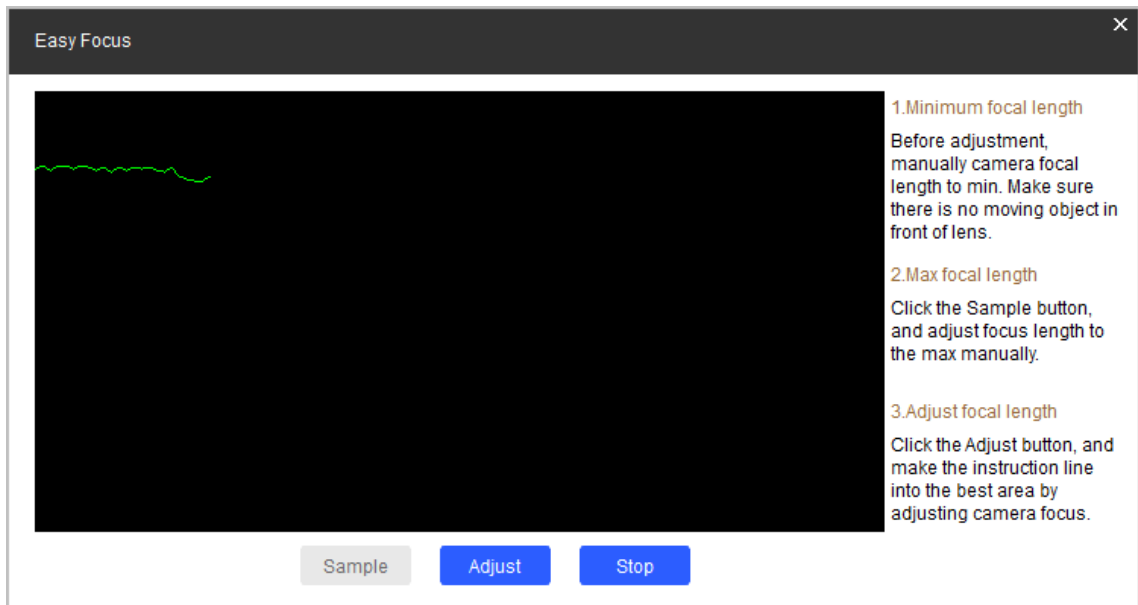
1. Click **Easy Focus**.

Figure 4-28 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 4-29 Sampling



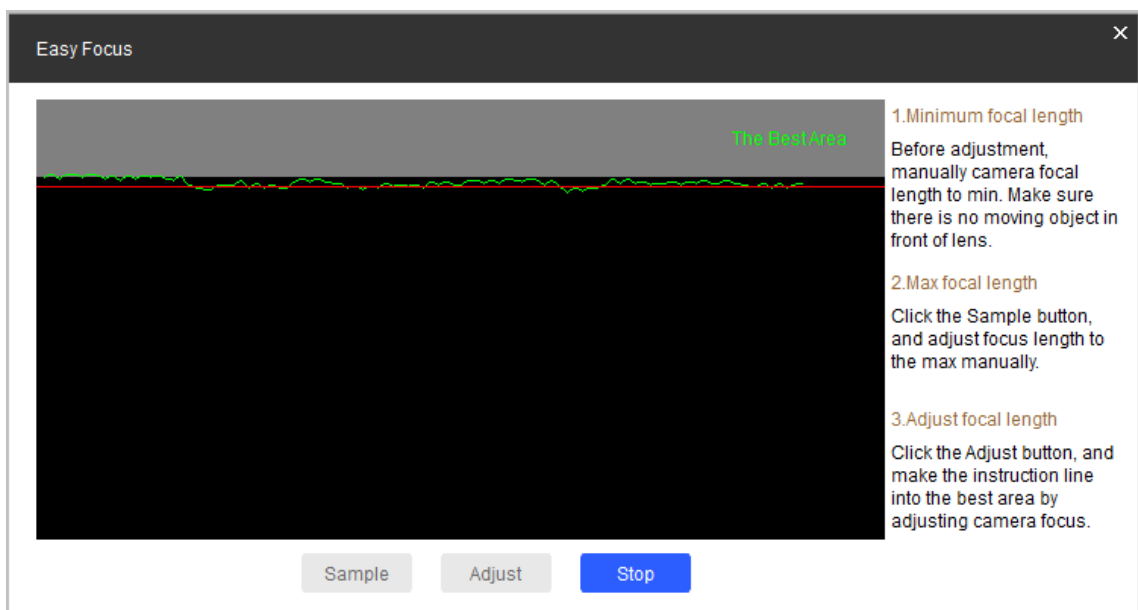
3. Click **Adjust**.

The **Best Area** page 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 4-30 Final result



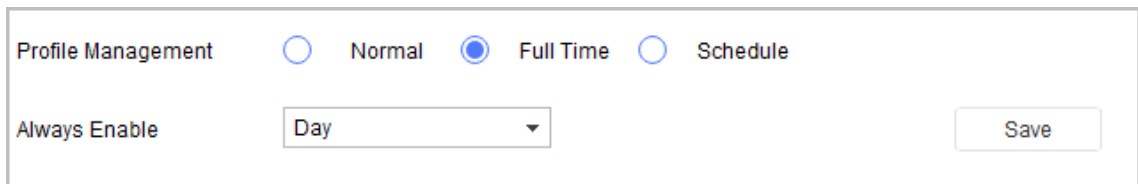
4.6.2.3 Configuring Profile Parameters

You can set the switch methods to let the device switch profiles automatically while working. This function corresponds to the profile management function of cameras. For more details, see the user's manual of the camera.

Procedure

- Step 1 Complete Step 1 to Step 3 in "4.6.1 Accessing the Configuration Page".
- 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.

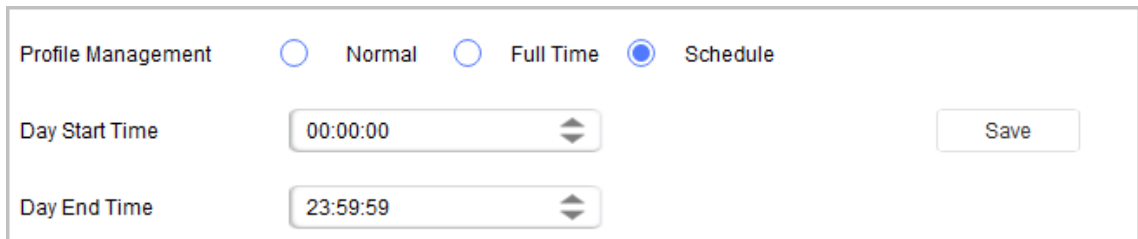
Figure 4-31 Full time



The screenshot shows the 'Profile Management' section with three radio buttons: 'Normal', 'Full Time' (selected), and 'Schedule'. Below the radio buttons, there is a label 'Always Enable' and a dropdown menu currently set to 'Day'. A 'Save' button is located to the right of the dropdown menu.

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

Figure 4-32 Schedule



The screenshot shows the 'Profile Management' section with three radio buttons: 'Normal', 'Full Time', and 'Schedule' (selected). Below the radio buttons, there are two time input fields: 'Day Start Time' with the value '00:00:00' and 'Day End Time' with the value '23:59:59'. A 'Save' button is located to the right of the 'Day Start Time' field.

- 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 page.

4.6.2.4 Configuring Alarm Tone

Supports uploading alarm tones separately or in batches to video devices.

Background Information



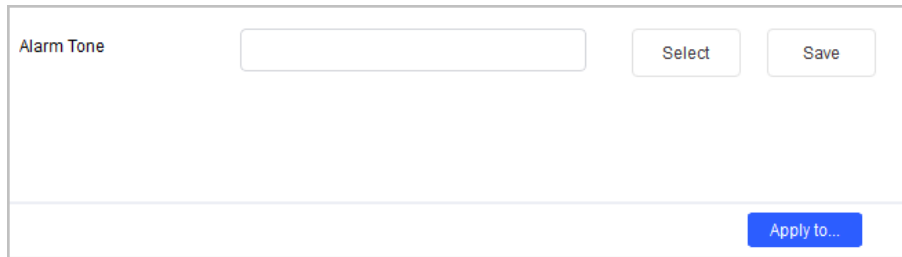
Only devices with alarm tone function can display this tab.

Procedure

- Step 1 Complete Step 1 to Step 3 in "4.6.1 Accessing the Configuration Page".

- Step 2 Click the **Alarm Tone** tab.
- Step 3 Click **Select** to select the alarm tone from the computer.

Figure 4-33 Select alarm tone



- 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 page.

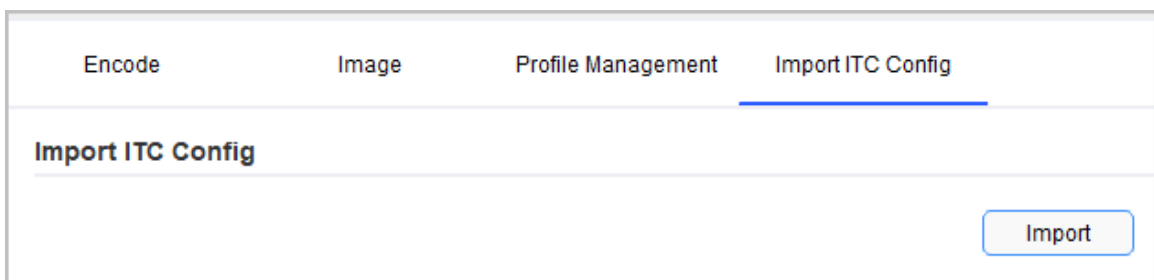
4.6.2.5 Importing ITC Configuration Files

You can import configuration files to ITC devices. This function is only available on ITC devices.

Procedure

- Step 1 Double-click a ITC device on the device tree, and then enter the username and password of the device to log in to the device.
- Step 2 Click **Import ITC Config**, and then click **Import**.

Figure 4-34 Import configuration file



- Step 3 Select the configuration file and then import it to the system.
- Step 4 (Optional) Apply the configurations to other ITC devices.
 1. Click **Apply to**, and then select ITC devices.
 2. Click **Configuration**.

The configurations will be applied to the selected devices. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.

4.6.3 Access Control Devices

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

4.6.3.1 Configuring Access Control Parameters

Procedure

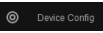
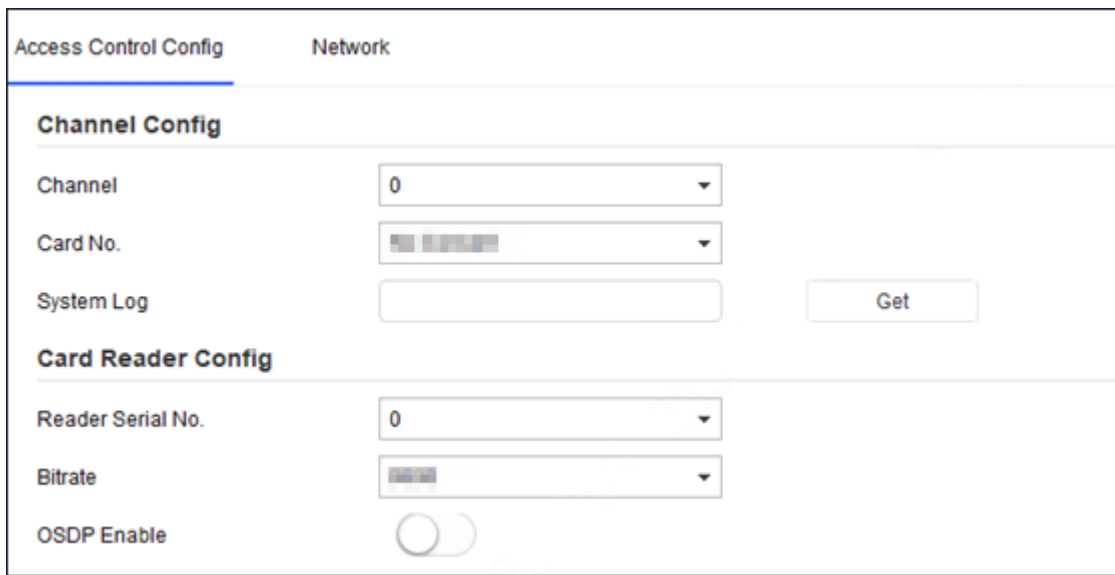
- Step 1** Open the Tool, and then select .
- Step 2** Select an access control device in the device list, and then click **Get Device Info**, or double-click the device.
- Step 3** (Optional) If the login dialog box is displayed, enter the username and password for the device, and click **OK**.
- Step 4** Configure access control parameters.

Figure 4-35 Access control config




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

Table 4-6 Access control parameters description

Parameter	Description
Channel	Select channel to set the parameters.

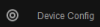
Parameter	Description
Card No.	<ul style="list-style-type: none"> ● Byte Revert : When ACS controller works with third-party readers (except HID), and the card reading result does not match the sent card number. For example, the card reading result is hexadecimal 0 x 12345678 (decimal 305419896) while the sent card number is hexadecimal 0 x 78563412 (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 0 x 12345678 (decimal 305419896) while the sent card number. is hexadecimal 0 x 78563412 (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	Click Get to get device log.
Reader Serial No.	Select the reader to set bit rate.
Bitrate	If card reading is slow, you can increase bit rate. It is 9600 by default.
OSDP Enable	When ACS controller works with third-party readers through OSDP protocol, you can enable OSDP function.

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 page.

4.6.3.2 Configure Network Parameters

Procedure

Step 1 Open the Tool, and then 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 4-36 Network parameters configuration

Table 4-7 Network parameters description

Parameter	Description
TCP Port	Change TCP port number, and then 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**.
2. The success icon (✓) will be displayed if the application is successful; otherwise the failure icon (⚠) will be displayed.
3. Click **Return** to return to the configuration page.

4.6.4 VDP

4.6.4.1 VTO

Procedure

Step 1 Complete **Step 1** to **Step 3** in "4.6.1 Accessing the Configuration Page".

Step 2 Configure VTO parameters.

Figure 4-37 VTO configuration

The screenshot shows a web-based configuration interface for a VTO device. It is organized into four main sections:

- Device Info:** Contains a 'Device Type' dropdown menu set to 'VTO_DOOR'.
- PhysicsInfo:** Includes checkboxes for 'Building' and 'Unit' (both unchecked), a 'VTO No.' text field with '123456', a 'GroupCall' checkbox (checked), an 'ExtNumber' text field, and a 'Center Number' text field with '888888'.
- SIP Info:** Features a 'Server Type' dropdown (set to 'VTO'), 'Server IP' and 'Server Port' text fields (blurred), a 'Domain Name' text field (set to 'VDP'), a 'Register Time' text field (set to '60'), and a 'Register Pwd' text field (masked with dots). There are also checkboxes for 'Initiale Mode' (checked) and 'Restart after configuration' (checked), along with a 'Save' button.
- Audio Info:** Contains an 'Audio Type' dropdown (set to 'Calling') and a 'Local Upload' text field. Below the text field are 'Browse' and 'Upload' buttons.

At the bottom right of the interface is a blue 'Apply to...' button.

Table 4-8 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.
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.

Parameter		Description
	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 checkbox to enable the server.
	Restart after configuration	Select the checkbox, and then the device will restart after configuration.

Step 3 Click **Save**.

Step 4 Select the audio type.

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 page.

4.6.4.2 VTH

4.6.4.2.1 Network Configuration


Procedure

Step 1 Complete Step 1 to Step 3 in "4.6.1 Accessing the Configuration Page".

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

Figure 4-38 Network configuration

Table 4-9 Network configuration parameters

Parameter		Description
Local Info	Room	Enter the room number.
	Main IP	Enter the IP address of the host.  <ul style="list-style-type: none"> 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 checkbox 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.

Parameter	Description
Sip Realm	Enter the domain name of the SIP server.
Login User	The port username of the SIP server.
Login Password	The login password of the SIP server.
Initiale Mode	Select the checkbox 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.

4.6.4.2.2 Network Terminals

Procedure

Step 1 Complete **Step 1** to **Step 3** in "4.6.1 Accessing the Configuration Page".

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

Figure 4-39 Network Terminals

Table 4-10 Network terminal parameters

Parameter	Description
Main VTO Name	Enter the name of the main VTO.
Main VTO IP	Enter the IP address of the main VTO.
Main VTO User	Enter the username of the main VTO.

Parameter	Description
Main VTO Pwd	Enter the password of the main VTO.
VTO Enable Status	Select the check box to enable the main 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 page.

4.6.4.2.3 Password

Procedure

Step 1 Complete **Step 1** to **Step 3** in "4.6.1 Accessing the Configuration Page".

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



The password contains 6 numbers.

Figure 4-40 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 page.

4.6.4.2.4 Wire Zone

Procedure

Step 1 Complete Step 1 to Step 3 in "4.6.1 Accessing the Configuration Page".

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

Figure 4-41 Wire Zone

Area	Type	NO/NC	Status	En-Delay	Ex-Delay
1	IR	NO	Instant Alarm	0S	0S
2	IR	NO	Instant Alarm	0S	0S
3	IR	NO	Instant Alarm	0S	0S
4	IR	NO	Instant Alarm	0S	0S
5	IR	NO	Instant Alarm	0S	0S
6	IR	NO	Instant Alarm	0S	0S
7	IR	NO	Instant Alarm	0S	0S
8	IR	NO	Instant Alarm	0S	0S

Table 4-11 Wire zone 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 .
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.

4.6.4.2.5 Alarm Mode

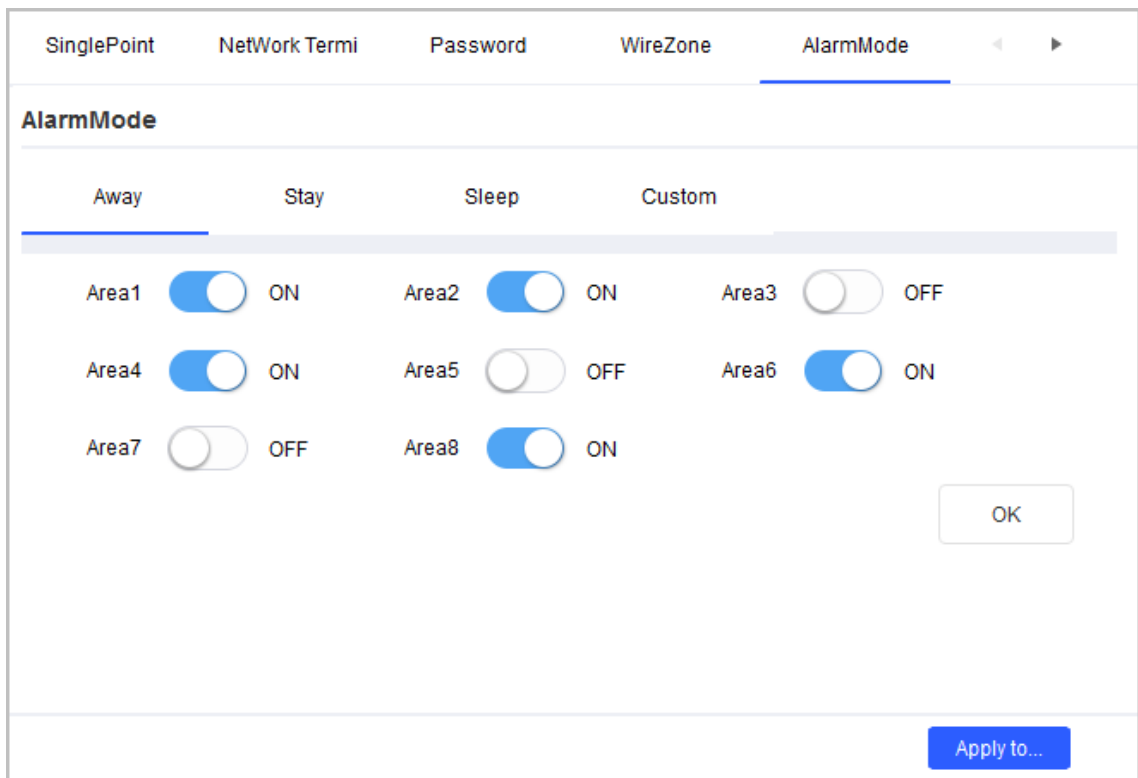
Procedure

Step 1 Complete Step 1 to Step 3 in "4.6.1 Accessing the Configuration Page".

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

Enable or disable areas in different modes.

Figure 4-42 Alarm mode



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 page.

4.6.4.2.6 Arm


Procedure

Step 1 Complete Step 1 to Step 3 in "4.6.1 Accessing the Configuration Page".

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

Figure 4-43 Arming

Table 4-12 Arm parameters

Parameter	Description
Arm mode	Select the alarm mode from StayMode , Away Mode , SleepMode , and CustomMode .
Arm 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 page.

4.6.4.2.7 Disarm

Procedure

Step 1 Complete Step 1 to Step 3 in "4.6.1 Accessing the Configuration Page".

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



The password contains 6 numbers.

Figure 4-44 Disarm

AlarmMode Arm **Disarm** Reserved Info IPCInfo

Disarm

Disarm Password *Please input disarm password!

OK

Apply to...

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 page.

4.6.4.2.8 Reserved Information

Procedure

Step 1 Complete **Step 1** to **Step 3** in "4.6.1 Accessing the Configuration Page".

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

Figure 4-45 Reserved information

AlarmMode Arm Disarm **Reserved Info** IPCInfo

Reserved Information

Reserved Email Save

Apply to...

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 page.

4.6.4.2.9 IPC Information

Procedure

Step 1 Complete Step 1 to Step 3 in "4.6.1 Accessing the Configuration Page".

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

Figure 4-46 IPCI information

The screenshot shows a web interface for configuring IPC information. At the top, there are navigation tabs: AlarmMode, Arm, Disarm, Reserved Info, and IPCInfo. The IPCInfo tab is selected. Below the tabs, the page title is "IPC Information". There is a dropdown menu for selecting an IPC, currently showing "IPC 0". Below this are several input fields: "IPC Name" with the value "IPC0", "Stream Type" with a dropdown menu showing "Main Stream", "IPC IP" with a masked IP address, "IPC Port" with the value "554", "IPC User" with the value "admin", and "IPC Password" with a masked password. At the bottom right of the form area are two buttons: "Clear All" and "Save". At the very bottom right of the page is a blue button labeled "Apply to...".

Table 4-13 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.

Parameter	Description
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 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 page.

4.6.4.3 VTS

Procedure

Step 1 Complete **Step 1** to **Step 3** in "4.6.1 Accessing the Configuration Page".

Step 2 Configure VTS parameters.

Figure 4-47 VTS configuration

SIP Info

Server IP

Server Port

Domain Name

Enable

Add VTO

VTO1

VTO IP

VTO Name

Username

Password

Middle No.

Enable

Table 4-14 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.
	Username	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 checkbox to enable the server.

Step 3 Click **Save**.

4.6.5 Android Digital Signage

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

4.6.5.1 Configuring APP

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

Procedure

- Step 1 Complete Step 1 to Step 3 in "4.6.1 Accessing the Configuration Page".
- Step 2 Click the **App Config** tab.
- Step 3 Enter the IP address in **APP IP Config**.
- Step 4 Click **Modify**.

Figure 4-48 Modify app configuration

- Step 5 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 page.

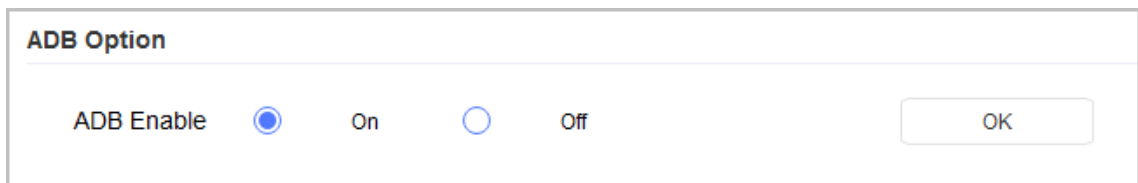
4.6.5.2 Enabling Android Commission

Enable or disable the Android commission function.

Procedure

- Step 1 Complete Step 1 to Step 3 in "4.6.1 Accessing the Configuration Page".
- Step 2 Click the **Android Debug** tab.
- Step 3 Select **On** in **ADB Enable**.
- Step 4 Click **OK**.

Figure 4-49 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 page.

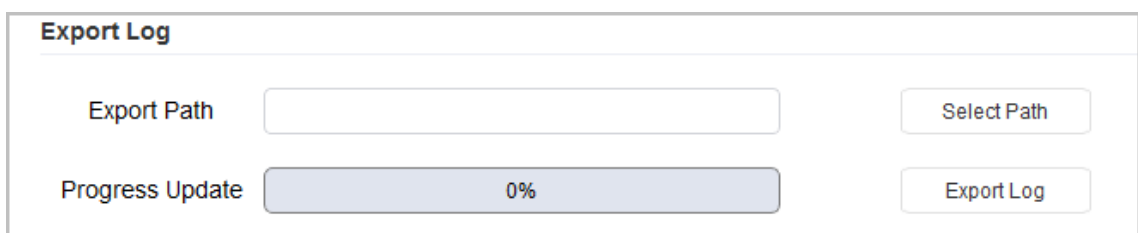
4.6.5.3 Exporting Log

You can export the logs of Android digital signage.

Procedure

- Step 1 Complete Step 1 to Step 3 in "4.6.1 Accessing the Configuration Page".
- Step 2 Click the **Export Log** tab.
- Step 3 Click **Select Path** to select the export path.
- Step 4 Click **Export Log**, and then the exporting progress is displayed.

Figure 4-50 Modify app configuration



4.6.6 Alarm Host Devices

4.6.6.1 Device Information

You can view the device information on this page.

Figure 4-51 Device information

Device Info	Network
Features	
Number of Alarm Inputs	↗
Number of Alarm Outputs	↘
Version	
Hardware Version	↗
SCM Version	↗
Web Version	↗
Security Baseline Version	↗

4.6.6.2 Configuring Network Parameters

Procedure

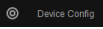
- Step 1 Open the Tool, and then select .
- Step 2 Select an alarm host device in the device list, and then click **Get Device Info**, or double-click the device.
- Step 3 (Optional) If the login dialog box is displayed, enter your username and password, and then click **OK**.
- Step 4 Configure parameters.

Figure 4-52 Network parameters configuration

Table 4-15 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.

4.7 Configuring System Settings

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

4.7.1 Timing

You can calibrate the device time on the **Time** page.

Procedure

Step 1 Click **System Setting**.

Figure 4-53 Timing (1)

Sync Time

PC Time **2020-09-03 14:48:14**

DST

DST Enable

DST Type Date Week

Start Time

End Time

Figure 4-54 Timing (2)

NTP


NTP

Synchronize with NTP

NTP Server

NTP Port (0~65535)

Update Period Minutes(0~65535)

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 operation again. For details, see "4.1 Adding Devices".

Step 3 Select the time sync method for the device.

- Manual sync: Specify the time, 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** checkbox, and then set the parameters.

Table 4-16 NTP Parameters

Parameter	Description
NTP	Select UTC, 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. The default NTP server is time.windows.com.
NTP Port	Enter the port number of corresponding NTP server.
Update Period	Enter the time interval at which the device synchronizes time with the NTP server.

Step 4 (Optional) Select the **DST Enable** (Daylight Saving Time) checkbox, and then set the parameters.



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

Table 4-17 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.

4.7.2 Rebooting

You can manually or automatically restart the device.

Background Information



Restart will interrupt operations, restart the device when it is idle.

Procedure

Step 1 Click **System Settings**.

Step 2 Click the **Reboot** tab.

Figure 4-55 Restart

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 restart type for the device.

- **Config Search:** Search for the configuration information of the device. The success icon (✓) will be displayed if the search is successful; otherwise the failure icon (⚠) will be displayed.

- **Auto reboot :** Under **Auto Reboot** type, select the **Auto Reboot** checkbox, set the specific day and time, and then click **OK**.

The device will restart at the set time.

- **Manual reboot :** Under **Manual Reboot** type, click **Reboot**.

The device restarts immediately.

4.7.3 Restoring

4.7.3.1 Restoring Default Configurations of Device

Background Information

You can restore settings except:

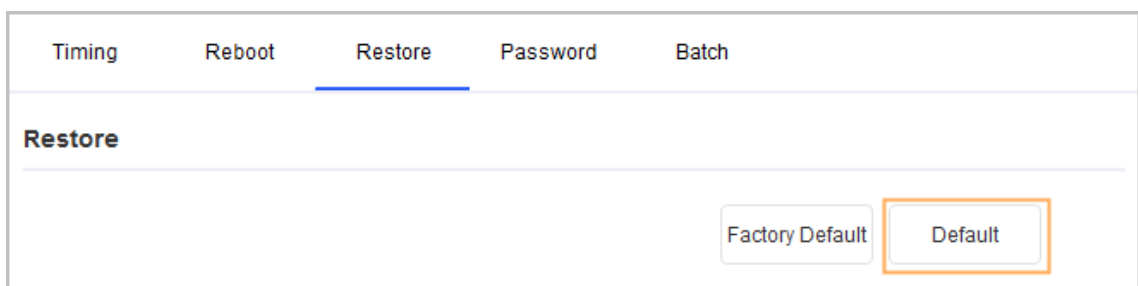
- Network settings such as IP address
- User information

Procedure

Step 1 Click  **System Settings**.

Step 2 Click the **Restore** tab.

Figure 4-56 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.

4.7.3.2 Restoring Factory Configurations of Device

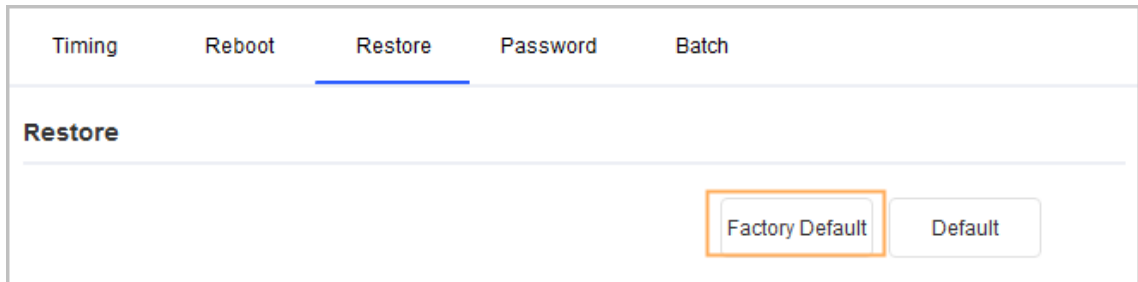
You can restore the factory default configurations.

Procedure

Step 1 Click  System Settings.

Step 2 Click the **Restore** tab.

Figure 4-57 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 then 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.

4.7.3.3 Exporting Configurations

Procedure

Step 1 Click  System Settings.

Step 2 Click the **Restore** tab.

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 (Optional) Set **Encrypt and Export Config File** under the **Config File** tab.

- If you select it, enter the password of the file you want to export. The password is customized and must be 8 to 32 characters. Fill in this password when importing, or you will fail to import. Click **Export**, select saving path, enter the file name, and then click **OK**. If the device can encrypt and export, the configurations can be exported normally.
- If you do not select it, Click **Export**, select saving path, enter the file name, and 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.

Figure 4-58 Encrypt and export config file

The screenshot shows a web interface titled "Config File". On the left, there is a button labeled "Export". To its right, the checkbox "Encrypt and Export Config File." is checked with a blue checkmark. Below these, there are two input fields: "Password" and "Confirm Password", both of which are currently empty.

4.7.3.4 Importing Configurations

Procedure

Step 1 Click  System Settings.

Step 2 Click the **Restore** tab.

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 (Optional) Set **Decrypt and Import Config File.** under the **Config File** tab.

- If you select it, enter the password of the file you want to import. The file must be encrypted and exported before. The password is the same as the exporting one. Click **Import**, click **OK** on the **Notice** page, select saving path, enter the file name, and then click **OK** to apply the imported configurations to all devices of the same type, same model and same version.
- If you do not select it, click **Import**, click **OK** on the **Notice** page, select saving path, enter the file name, and then click **OK** to apply the imported configurations to all devices of the same type, same model and same version.

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

Figure 4-59 Decrypt and import config file

The screenshot shows a web interface titled "Config File". On the left, there are two buttons: "Export" and "Import". To the right of the "Export" button, the checkbox "Encrypt and Export Config File." is unchecked. To the right of the "Import" button, the checkbox "Decrypt and Import Config File." is checked with a blue checkmark. Below these, there is one input field labeled "Password", which is currently empty.

4.7.4 Changing Device Password

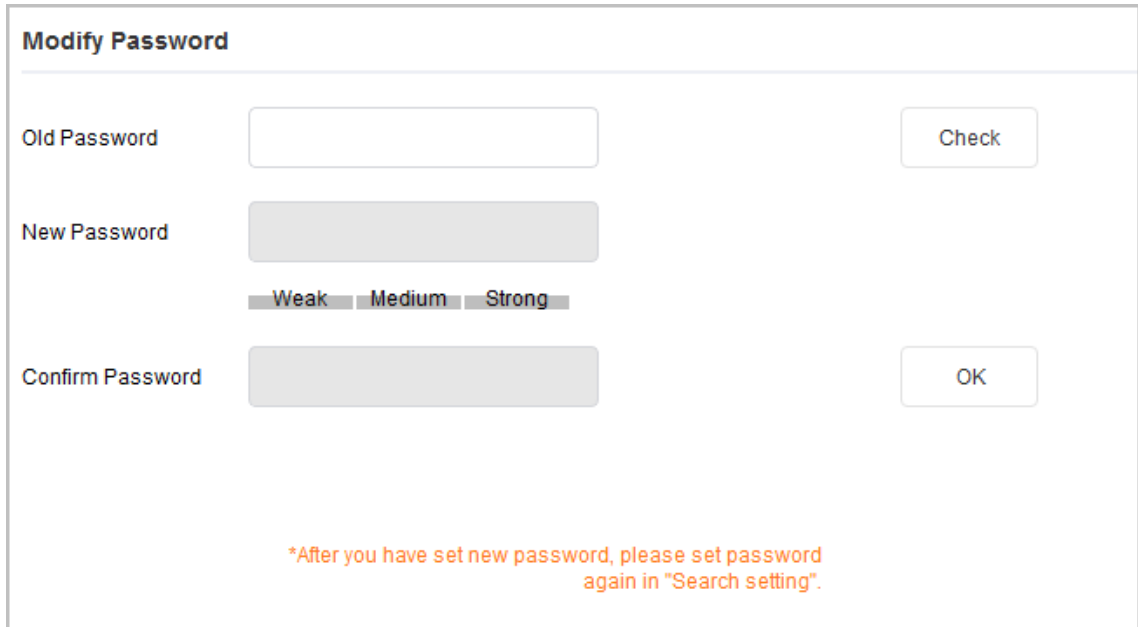
You can change the device login password.

Procedure

Step 1 Click  System Settings.

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

Figure 4-60 Device password



Modify Password


Old Password

New Password

Weak Medium Strong

Confirm Password

*After you have set new password, please set password again in "Search setting".

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 4-18 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	Set password according to the password strength prompt.
Confirm Password	Confirm the new password.

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

4.7.5 Batch Configuration

4.7.5.1 Video Standard

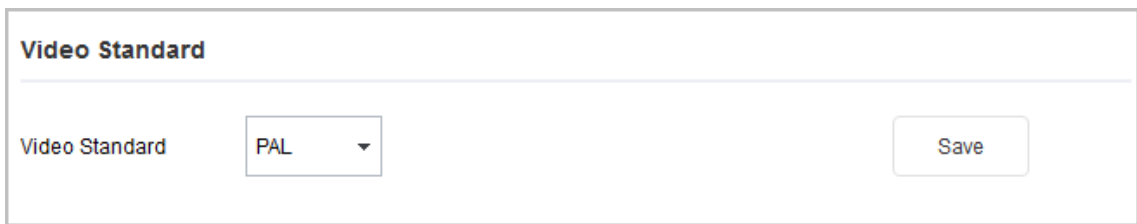
There are two video standards, PAL and NTSC.

Procedure


Step 1 Click  System Settings.

Step 2 Click the **Batch** tab.

Figure 4-61 Table configuration



The screenshot shows a configuration window titled "Video Standard". On the left, there is a label "Video Standard". To its right is a dropdown menu with "PAL" selected. Further to the right is a "Save" button.

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, and then the system will go through each one until successful.

Step 4 Select **PAL** or **NTSC** from the **Video Standard** drop-down list, 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.

4.7.5.2 Table Configuration

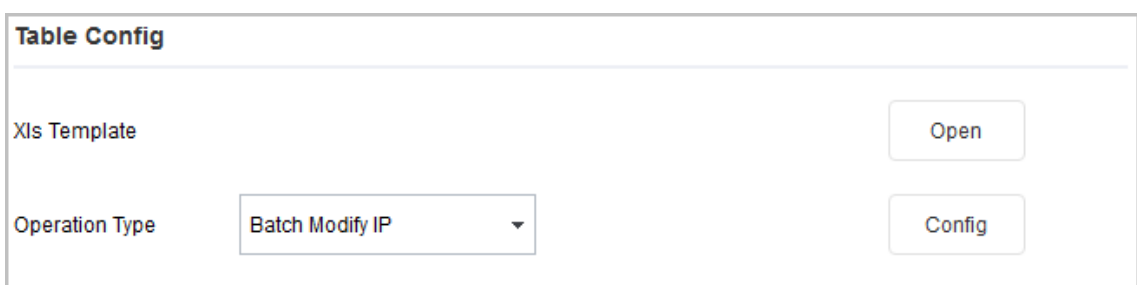
The **Table Config** function enables you to perform some device configurations in batches. This is applicable when you have a lot of devices to configure. Configurations include modifying IP, creating and modifying password, upgrading devices, adding allowlist and blocklist, and setting encoding parameters.

Procedure

Step 1 Click  System Settings.

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

Figure 4-62 Table configuration



The screenshot shows a configuration window titled "Table Config". On the left, there is a label "Xis Template" and an "Open" button. Below that, there is a label "Operation Type" followed by a dropdown menu with "Batch Modify IP" selected. To the right of the dropdown is a "Config" button.



- If the device is not on 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, and then 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. You do not need to enter.

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

Figure 4-63 Import template

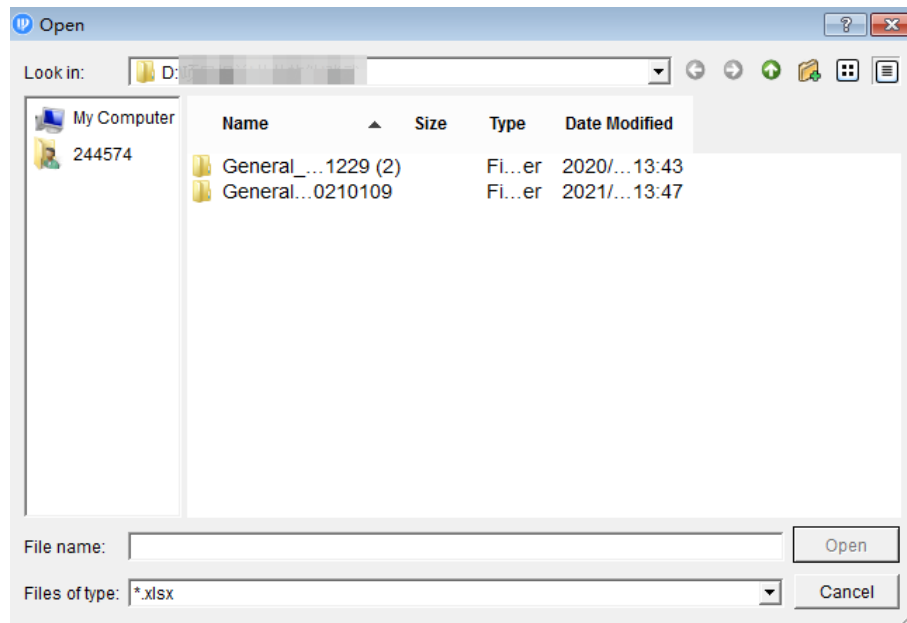



Table 4-19 Description of the operation type

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.

Operation Type	Description
VTO Password	Change the VTO password of engineering, duress, unlock and issuing card in batches.
Batch Modify Active Registration	Modify the active registration of the devices in batches.


Step 5 Open the template to confirm the result, and then view the **Result** column.

4.7.6 License

4.7.6.1 Update the Device License





If there is a problem with the device license, you need to update the license. Through this method, you need to contact technical support to apply for a license through the license application electronic flow.

Procedure

Step 1 Click  **System Settings**, and then select **License > General**.

Step 2 Select one or more devices to be authorized in the device list.

Step 3 Click **Export** to export the device configuration information to the computer.

If the export configuration is successful,  is displayed on the right side of the device; if the export configuration fails,  is displayed on the right side of the device. Click  or  to view the detail information.

Step 4 Contact your technical support personnel to obtain the license.



License needs to bind the device configuration information. Please provide your device configuration information when you contact the technical support personnel.

Step 5 Export the license to the device.

- Click **Select** to select the applied license.
- Click **Import** to import the license to the device.

Figure 4-64 Update the device license

License

General
Repair

Export Path Export

Import Path Select Import

4.7.6.2 One-click Grant Device License


You can use this method when the company's R&D personnel need to temporarily grant a device license. Through this method, you can directly grant a license to a device without applying for a license through the electronic flow. The license validity period is 30 days.

Background Information



- Only company employees have the permission to perform this operation.
- Perform operations on the Intranet of the company.
- The authorization content is the configuration of the filled P/N.

Procedure

Step 1 Click  **System Settings**, and then select **License > Repair**.

Step 2 (Optional) If you have not logged in, click **Login**, enter the **Job Number** and the **Password** in the pop-up dialog box, and then click **OK**.

Step 3 Select one or more devices to be authorized in the device list.

Step 4 Enter the P/N of the device, and then click **One-click reset**.





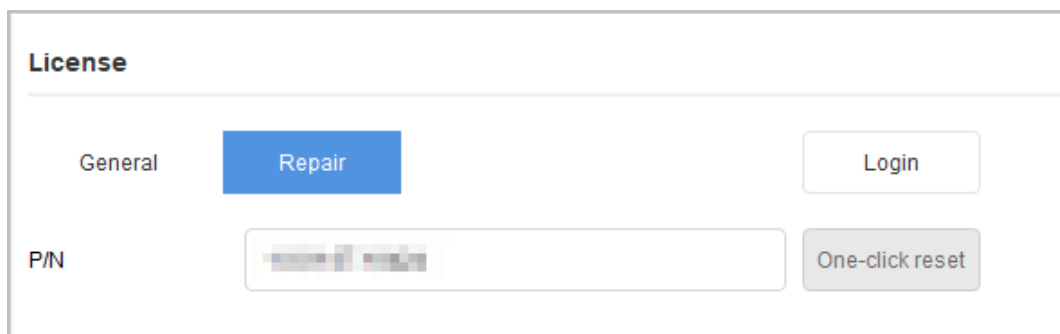
If one-click reset is successful,  is displayed on the right side of the device; if the one-click reset fails,  is displayed on the right side of the device. Click  or  to view the detail information.

Figure 4-65 One-click reset



4.7.6.3 Online Upgrade

Procedure


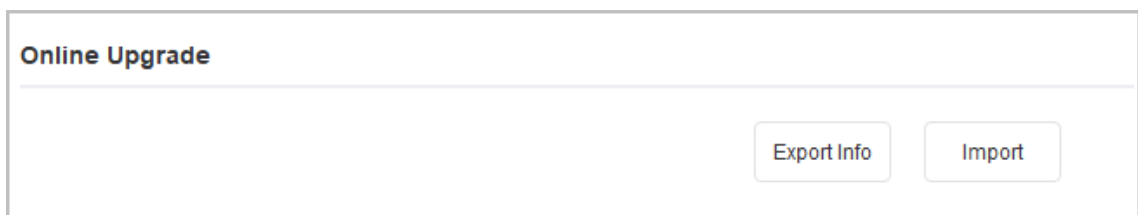
Step 1 Click  **System Settings**, and then select **License > Online Upgrade**.

Figure 4-66 Online Upgrade



Step 2 Click **Export Info** to export the PC information to a dat file.

Step 3 Apply for a license file with the exported dat file.

Step 4 Click **Import**, select the license file you applied for, and then wait for the activation to complete.

After the activation is complete, go to the **Online Upgrade** page to check whether the online upgrade function is available. For details, see "4.5 Online Upgrade".

4.7.7 LLDP

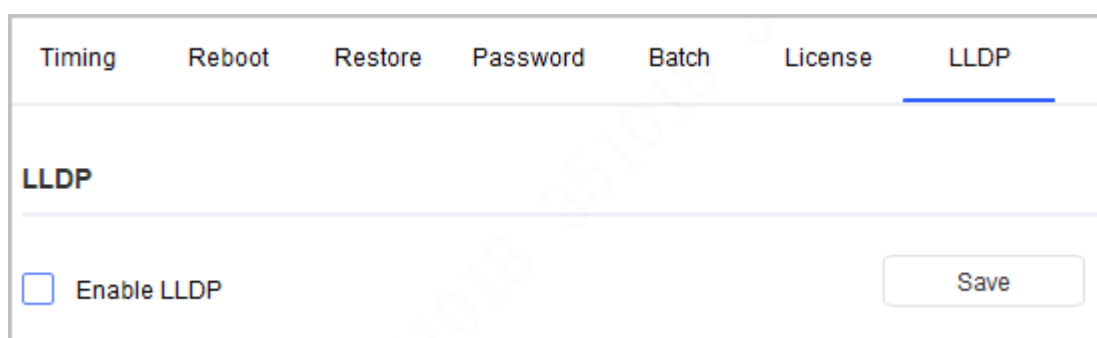
LLDP is used to get the neighbor information of the devices and discover the network topology.

Procedure

Step 1 Select **System Settings** > **LLDP**.

Step 2 Select devices on the device tree.

Figure 4-67 LLDP





Step 3 Enable LLDP function.



If this function is disabled, it will take approximately 2 minutes for the network topology to update.

Step 4 Click **Save**.

Results

- The device displays , which means LLDP is successfully enabled.
- The device displays , which means LLDP is failed to enable. You can click this icon to view failure details.

4.8 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.

4.8.1 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.

Procedure


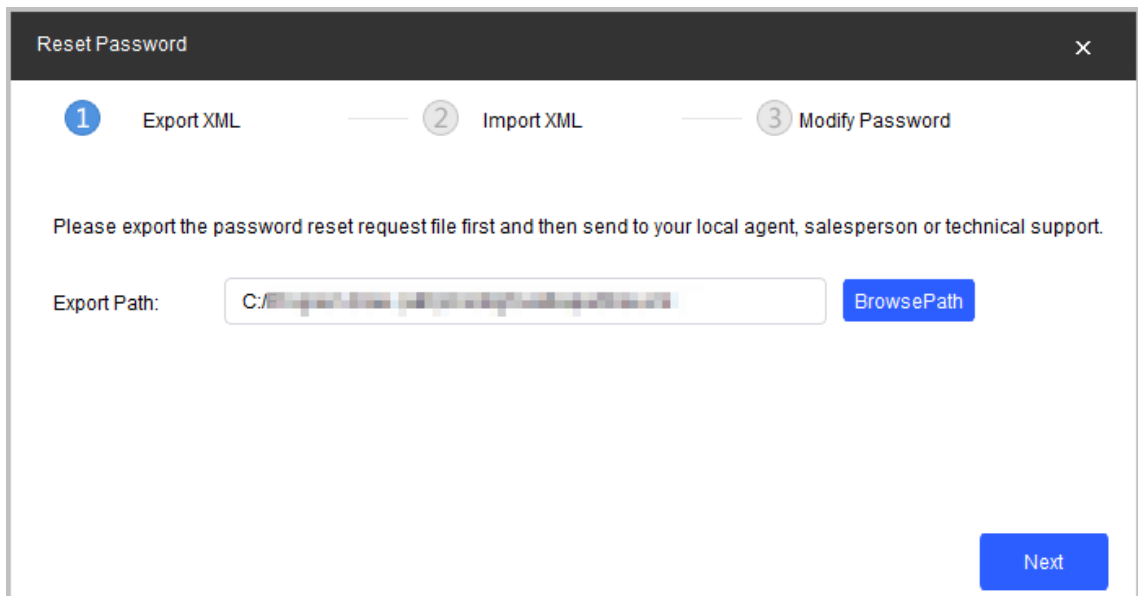
- Step 1** Click  Password Reset.
- Step 2** Select the devices that need to reset password, click **Batch Reset**, and then click **Agree** and **OK**.
- Step 3** Export XML.
1. Click **BrowsePath** to select the save path for the exported XML file.
2. Click **Next** to export the file.
- Step 4** Use 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 4-68 Reset ExportFile.xml



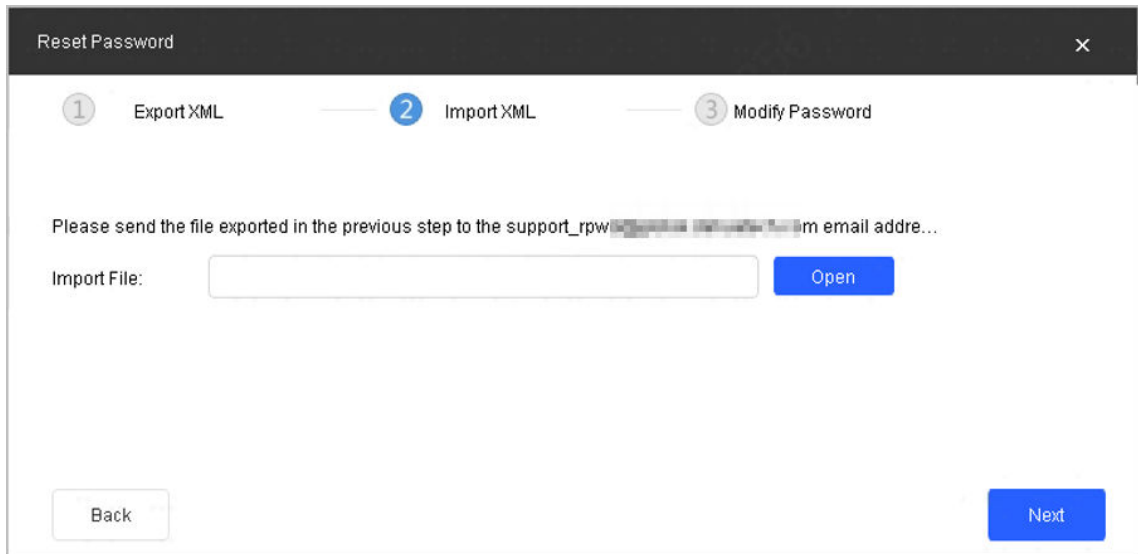
- Step 5** Import XML.



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

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

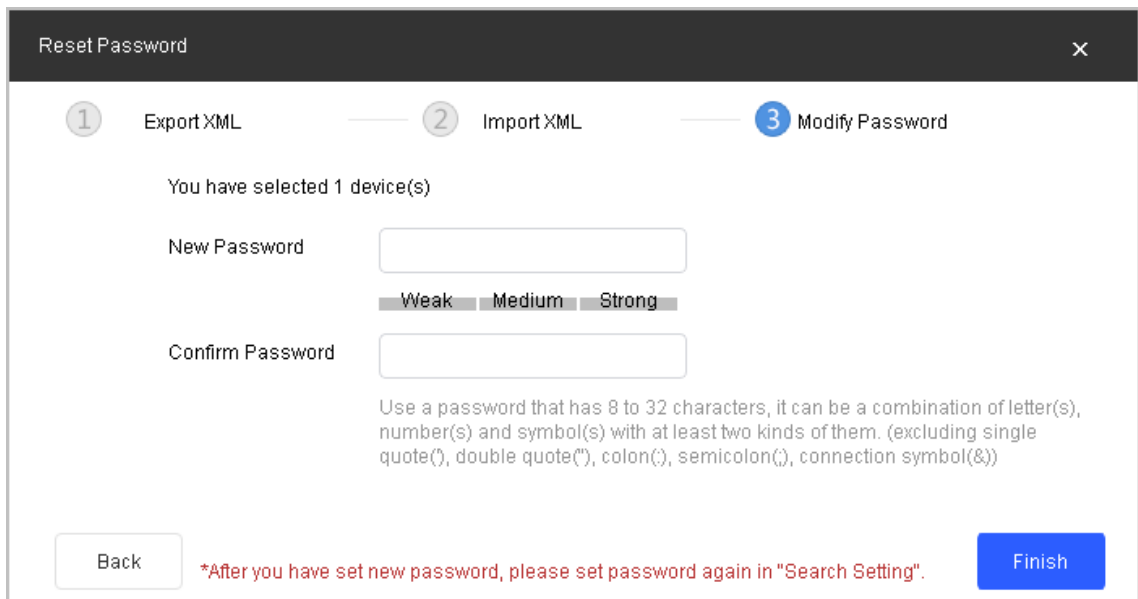
Figure 4-69 Reset password



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

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

Figure 4-70 Reset password-modify password



Step 6 Enter the new password, and then confirm the password.

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.

4.8.2 Resetting Password of One Device

This operation is only applicable to a single device.

Procedure

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 "4.8.1 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.

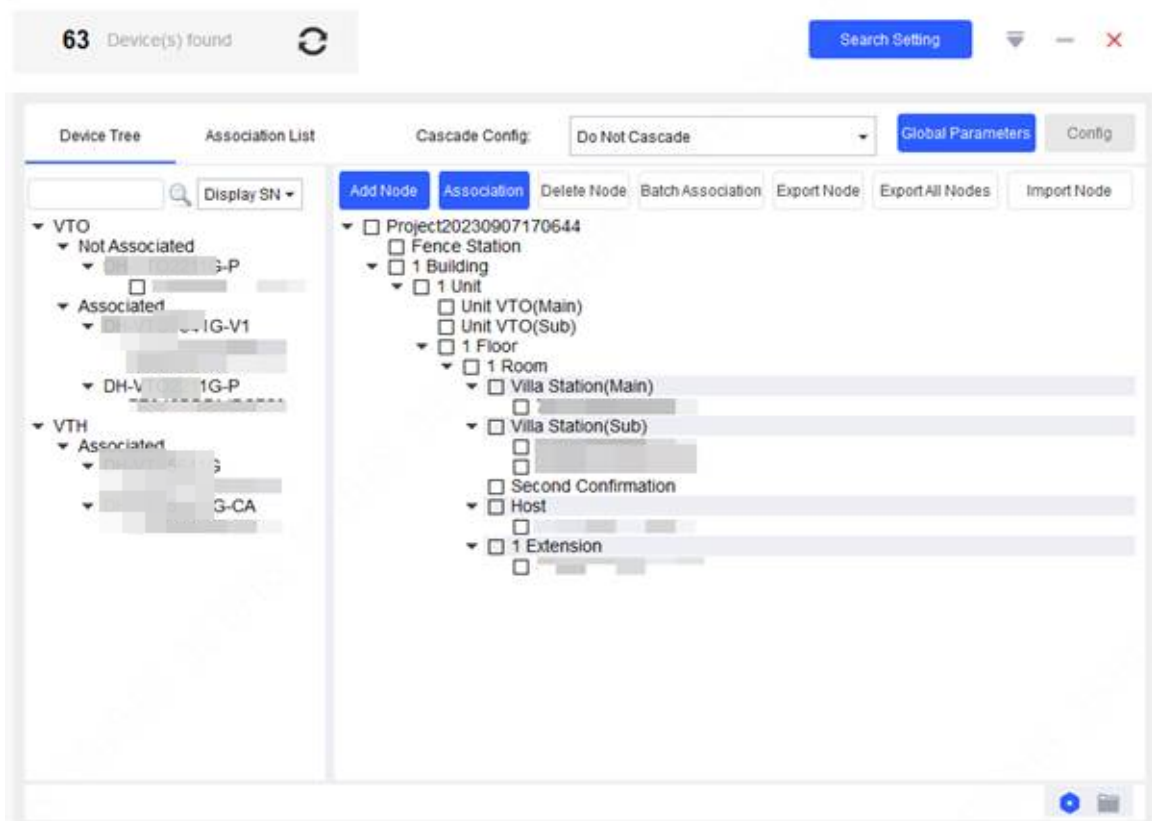
4.9 Building Configuration

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



- Building configuration supports two modes: generating configuration and distributing, and importing configuration and distributing. You can switch the mode on the lower-right corner of the page.
- The device tree supports viewing by IP and SN. You can switch the display mode through the drop-down list.

Figure 4-71 Building configuration page



4.9.1 Generating Configuration and Distributing

4.9.1.1 Configuring Global Parameters

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

Procedure

Step 1 Select **Building Config > Device Tree**.

Step 2 Configure device information.

Figure 4-72 Global parameters

Table 4-20 Global parameters 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	Enter server username. By default, the username is admin.
Server Password	Enter server password.
SIP Domain	Enter the SIP domain and registration password. They are VDP and 123456 by default.
Registered PWD	Enter the registered password.
VTO/VTH Username and Password	<ul style="list-style-type: none"> The username and password are admin and admin123 for VTO. The username and password are admin and 123456 for VTH.

Step 3 Click **Save**.

4.9.1.2 Adding Organization Node

Procedure

- Step 1 Select **Building Config** > **Device Tree**.
Step 2 Click **Add Node** to add building organization node.

Figure 4-73 Add nodes

Organization tree node

Building Unit Floor

Building Start Building Number Fence Station

Unit Start Unit Number Unit VTO(Main) Unit VTO(Sub)

Floor Start Floor Number Second Confirmation

Room Start Room Number Villa Station(Main) Villa Station(Sub)

Extension Number

*The maximum number of device nodes allowed is 10,000.

OK

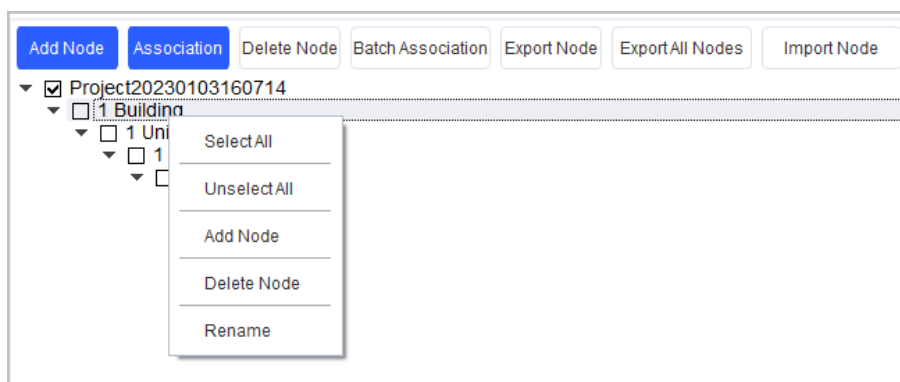


Enable **Building**, **Unit** and **Floor** when you need to select them.

- 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.
- The maximum number of device nodes allowed is 10,000.
- The host is created in the project node by default.
- The villa station is divided into the main villa station and sub villa station, among which the sub villa station can associate multiple devices.

- Step 3 Right-click the node to rename, add, delete nodes.

Figure 4-74 Node operations



Step 4 Click **OK**.

Related Operations

- **Delete nodes**
Select the node that you want to delete, and then click **Delete Node** to delete the node.
- **Export nodes**
Select the node you want to export, and then click **Export Node** to export the corresponding node, or click **Export All Node** to export all nodes.
- **Import modes**
If the node tree is not created, you can click **Import Node**, and then select the previously exported node tree file to automatically create the node tree.

4.9.1.3 Configuring Linkage

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

Procedure

Step 1 Select **Building Config > Device Tree**.

Step 2 Select a cascade mode.

- **Do not Cascade:** Do not cascade second confirmation station to the main VTH.
- **Cascade Second Confirmation Station:** Cascade second confirmation station to main VTH.

Step 3 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 4 Click **Association List**, select devices to be sent, and then click **Config**.

- means that the linkage sent successfully.
- means that the linkage sent failed. Click to check for the reasons.

Figure 4-75 Association list

NO.	Model	Device node	Serial No.	IP : Port	Operate	QR code
1					✓	
2					✓	

4.9.1.4 Linking Devices in Batches

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

Procedure

- Step 1** Select **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 then click **Save**.
- Step 4** Open the table, enter the serial number of each device linking with each node, and then 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 then select the finished table.
- Step 6** Click **Association List**, select devices to be sent, and then click **Config**.
 - ✓ means that the linkage sent successfully.
 - ⚠ means that the linkage sent failed. Click ⚠ to check for the reasons.

Figure 4-76 Association list

NO.	Model	Device node	Serial No.	IP : Port	Operate	QR code
1					✓	
2					✓	

4.9.1.5 Exporting Related Information

You can export related information table to your PC.


Procedure

- Step 1** Select **Building Config > Association List**.
- Step 2** Select devices to be exported, and then click **Export Table**.
- Step 3** Select storage path, and then click **Save**.
- Step 4** Open the table on local, and then you can view the related linkage information.

4.9.2 Importing Configuration and Distributing

Procedure

Step 1 Click  Building Config.

Step 2 Click  on the lower-right corner of the page to switch to importing configuration mode.

Step 3 Click **Download** to download the template file, and then enter configuration information in the file.



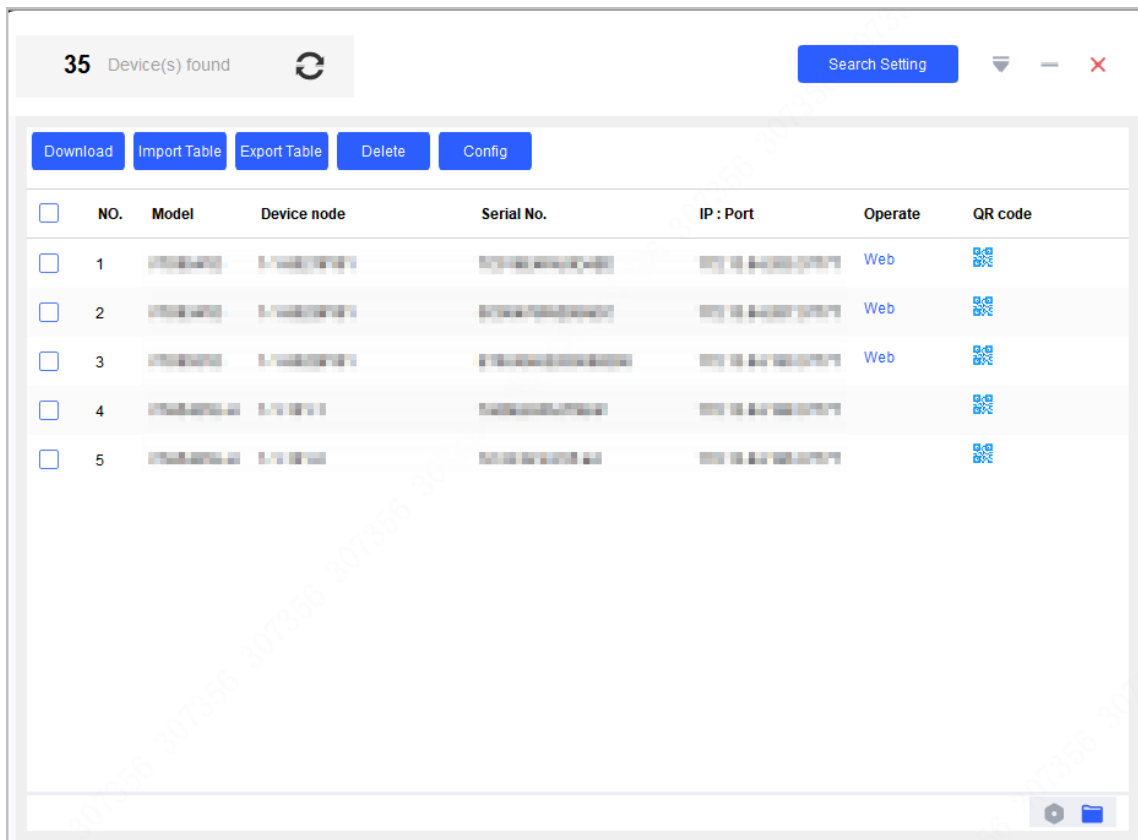
Supports setting VTS/VTO/VTH configuration. View details in the download template.

Step 4 Click **Import Table** to import the configuration file into the Tool.



If there are uninitialized devices in the file, the tool will automatically initialize them and assign IP to them.

Figure 4-77 Import configuration file



Step 5 Select the device to be configured, and then click **Config** to apply the configurations.

After the configuration is complete, each device displays the corresponding configuration result, and you can click and view it.

4.10 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 prompt **Operation via http is not safe** will appear.

4.10.1 CGI Command Configuration

Procedure

Step 1 Click  CGI Protocol.

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


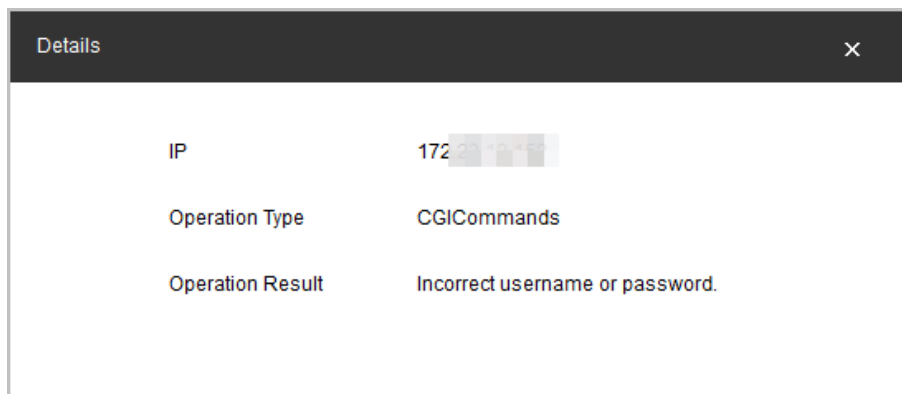
1. If  shows next to the device IP, it means that the configuration failed. You can click the icon to see details.

Figure 4-78 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 4-79 CGI command success

<input type="checkbox"/>	NO.	Model	IP		Url Path	Operate
<input type="checkbox"/>	1	IPC-HDBW1...	172.20.10.10		nager.cgi	Config

4.10.2 Changing CGI Commands in batches

Procedure

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 4-80 Batch CGI commands

4.10.3 Table Configuration

Procedure


- Step 1** Click  **Table Configuration**.
- Step 2** Click **Open Template**, and then enter IP address, port No., username, password, and CGI commands content.
- Step 3** Save the template, and then close it.

Figure 4-81 Template

IP Address	Port	Username	Password	CGI Commands Content	protocol (0 - http, 1 - https)	Result
192.168.1.1	80	admin	admin	/cgi/...	0	0
192.168.1.1	80	admin	admin	/cgi/...	0	0
192.168.1.1	80	admin	admin	/cgi/...	1	1

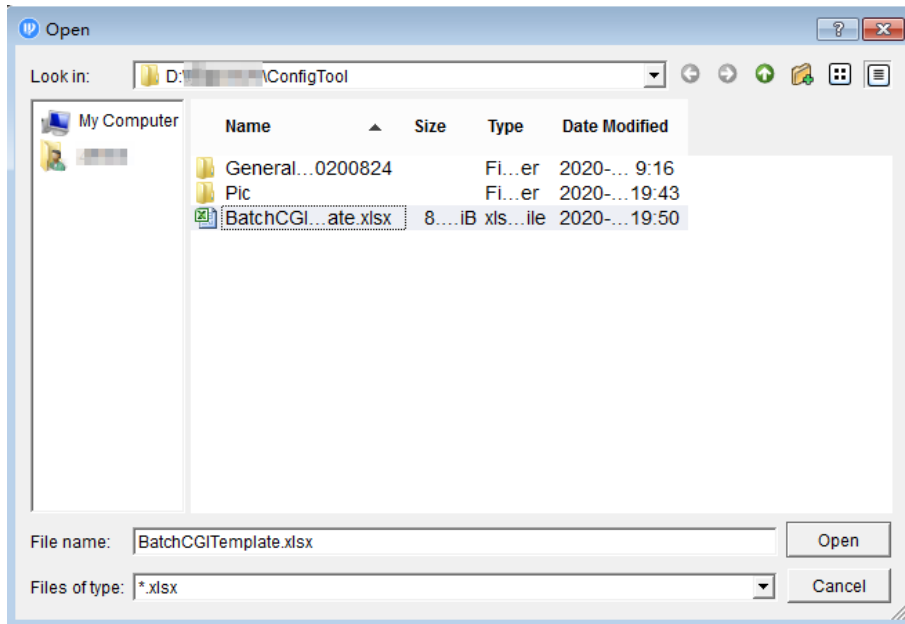
Table 4-21 Parameter description of the template

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 4** Return to CGI protocol page, and then click **Table Configuration**.
- Step 5** Select the completed template, and then click **Open** to import the template. The devices in the template will be configured as the template.

After the configuration is completed, the success prompt is displayed. You can check the result in the template.



Figure 4-82 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.

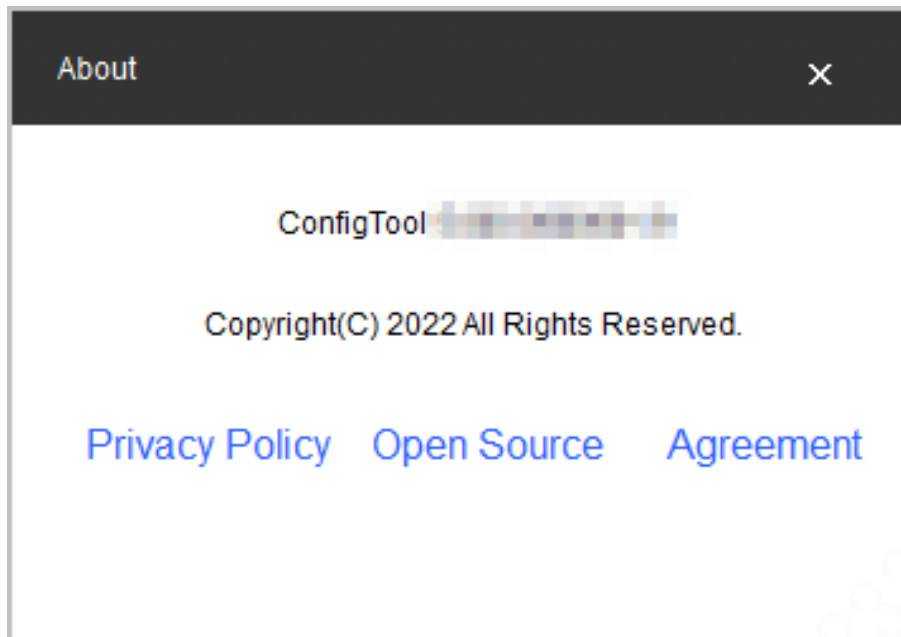
5.1 Help File

- Click  at 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 privacy policy, open source and software version.

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.

Procedure


- Step 1 Click  on the upper-right corner of the page, and then click **Setting**.
- Step 2 Configure the mode when logging in to the device and the parameters related to upgrading the device.
- Step 3 Click **OK**.

Figure 5-2 Setting

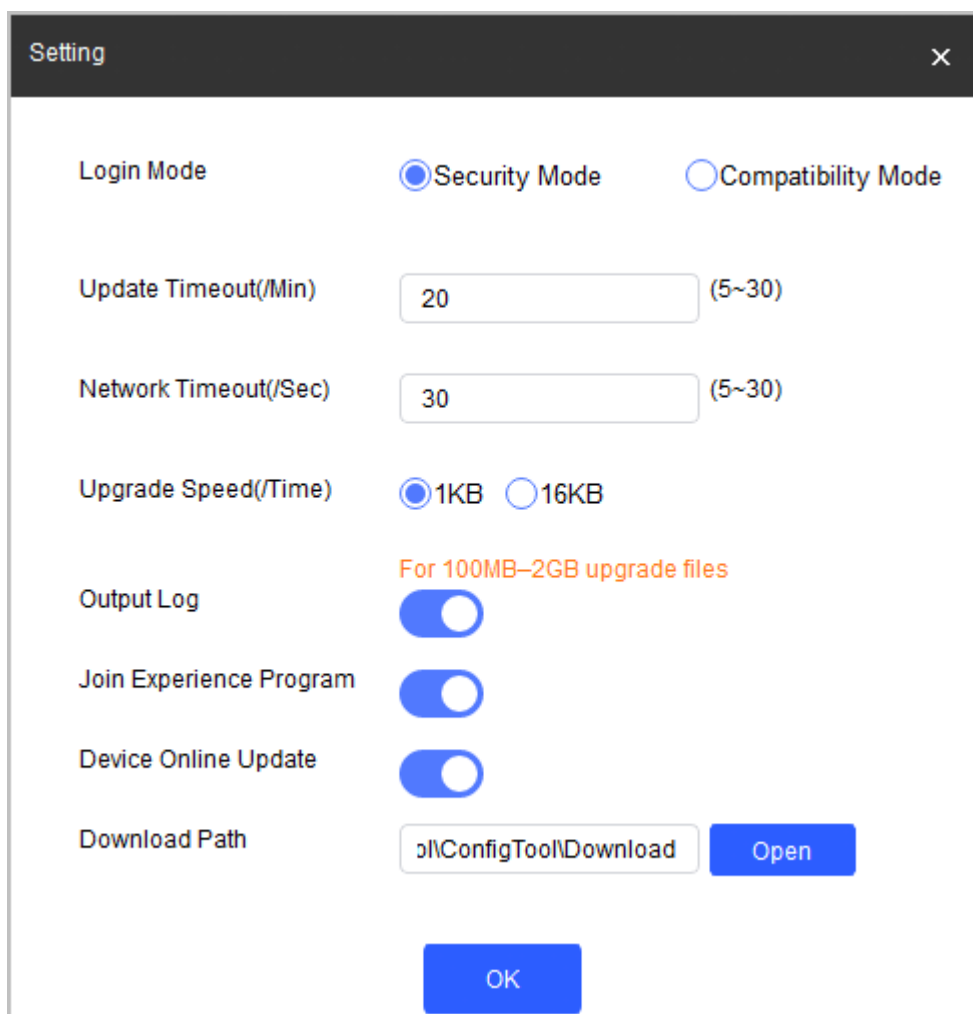



Table 5-1 Setting Parameters

Parameter	Description
Login Mode	<ul style="list-style-type: none"> ● 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. <p> Compatibility mode has potential security risks. It is recommended to log in with security mode.</p>
Update Timeout (/Min)	<p>The maximum upgrade time for a single device when the device is upgraded.</p> <p>When the device upgrade time is longer than the set value, the system notices that the upgrade failed.</p>

Parameter	Description
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.
Upgrade Speed (/Time)	Select the loading speed when upgrading. <ul style="list-style-type: none"> ● 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 Settings".
Output Log	Click <input type="checkbox"/> to enable the function, and click <input checked="" type="checkbox"/> to disable the function.
Join Experience Program	
Device Online Update	
Download Path	


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 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**.

- **Device program version is low. Please upgrade the device or enable [ConfigTool] 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, restarted and so on.



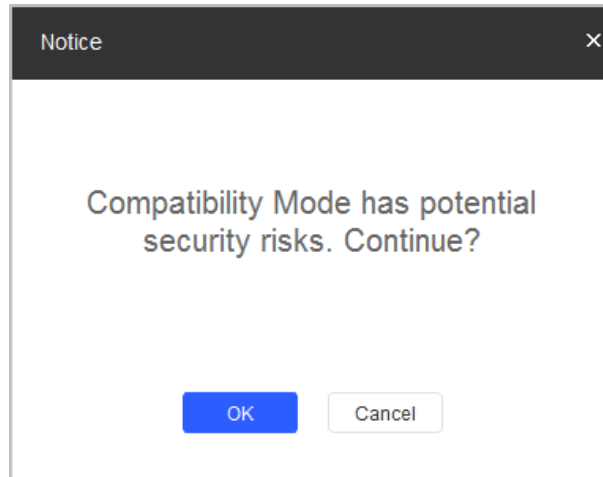
Operate according to the instructions and then repeat the failed operations when this hint appears. There are two methods. You can select one of them.

- ◇ 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)



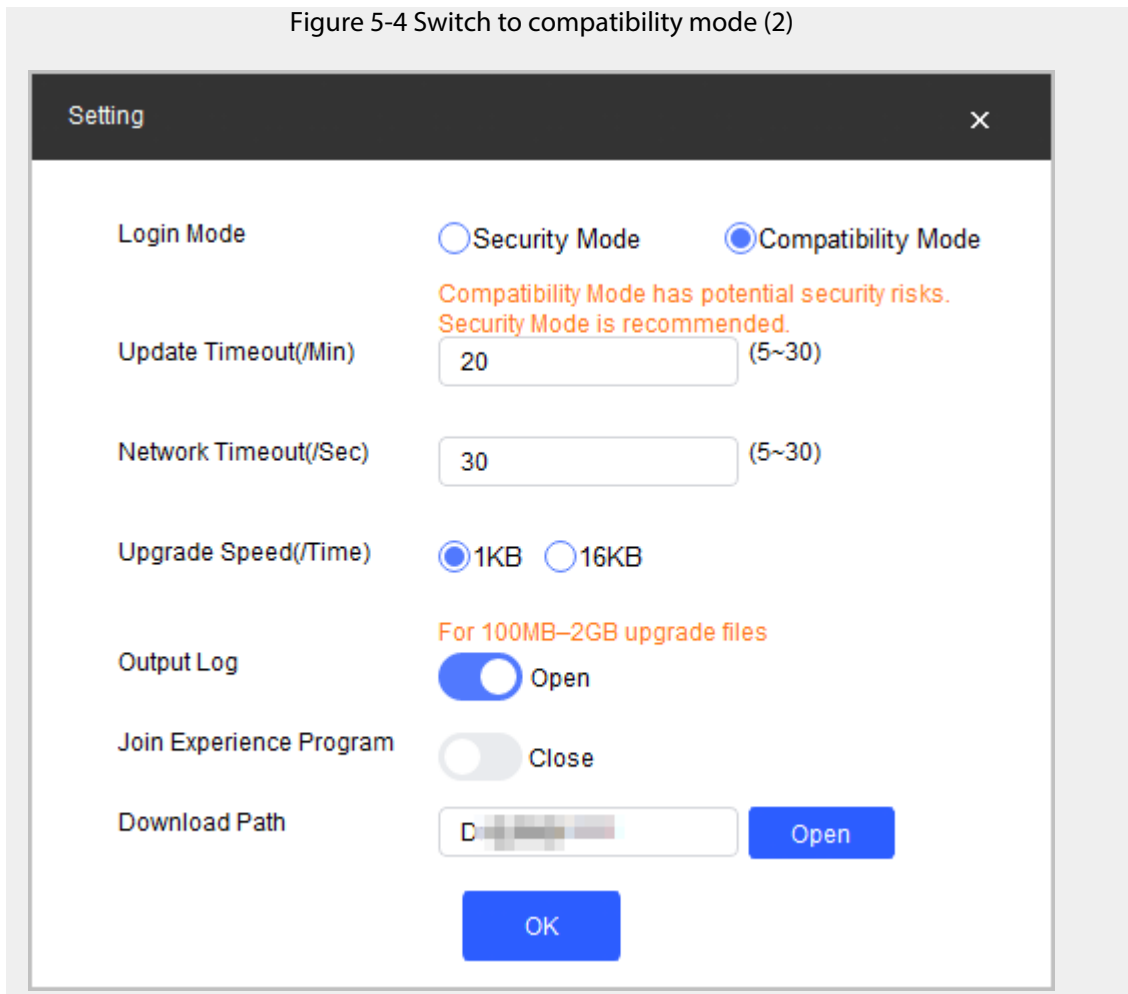
- **Compatibility Mode has potential security risks. Security Mode is recommended.**

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

The necessary measures to ensure the basic cyber security of the platform:

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. Customize the Answer to the Security Question

The security question setting should ensure the difference of answers, choose different questions and customize different answers (all questions are prohibited from being set to the same answer) to reduce the risk of security question being guessed or cracked.

Recommendation measures to enhance platform cyber security:

1. Enable Account Binding IP/MAC

It is recommended to enable the account binding IP/MAC mechanism, and configure the IP/MAC of the terminal where the commonly used client is located as an allowlist to further improve access security.

2. Change Passwords Regularly

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

3. Turn On Account Lock Mechanism

The account lock function is enabled by default at the factory, and it is recommended to keep it on to protect the security of your account. After the attacker has failed multiple password attempts, the corresponding account and source IP will be locked.

4. Reasonable Allocation of Accounts and Permissions

According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.

5. Close Non-essential Services and Restrict the Open Form of Essential Services

If not needed, it is recommended to turn off NetBIOS (port 137, 138, 139), SMB (port 445), remote desktop (port 3389) and other services under Windows, and Telnet (port 23) and SSH (port 22) under Linux. At the same time, close the database port to the outside or only open to a specific IP address, such as MySQL (port 3306), to reduce the risks faced by the platform.

6. Patch the Operating System/Third Party Components

It is recommended to regularly detect security vulnerabilities in the operating system and third-party components, and apply official patches in time.

7. Security Audit

- Check online users: It is recommended to check online users irregularly to identify whether there are illegal users logging in.
- 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.

8. The Establishment of a Secure Network Environment

In order to better protect the security of the platform and reduce cyber security risks, it is recommended that:

- Follow the principle of minimization, restrict the ports that the platform maps externally by firewalls or routers, and only map ports that are necessary for services.

- Based on actual network requirements, separate networks: if there is no communication requirement between the two subnets, it is recommended to use VLAN, gatekeeper, etc. to divide the network to achieve the effect of network isolation.