



ConfigTool

(Windows Version)

User's Manual

V1.0.6





Foreword

General

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

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potentially hazardous situation which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.6	1. Update "3.7 Resetting Device Password."	July 2019
V1.0.5	1. Update the pictures in "3.6 Configuring System Settings." 2. Change the notice box to the new one in "3.8 Local Upgrade", and "3.9 Online Upgrade." 3. Update the template management interface, and add the description of profile management in "3.5 Configuring the Device Parameters" in "3.10 Configuring the Template."	March 2019

Version	Revision Content	Release Time
V1.0.4	<ol style="list-style-type: none"> 1. Add a notice box when you click reset password in the reset password menu. 2. Add a notice box when click batch download and upgrade detect in the online upgrade menu. 3. Add the function to get back video password in the system settings menu. 	April 2018
V1.0.3	Add cybersecurity recommendations and online upgrade section.	September 2017
V1.0.2	Modify the basic operations section.	March 2017
V1.0.1	<ol style="list-style-type: none"> 1. Add the description of uninstallation. 2. Modify 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 personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Table of Contents

Foreword	II
1 Overview.....	1
2 Installation and Uninstallation	2
2.1 Installation	2
2.2 Uninstallation.....	4
3 Basic Operations.....	5
3.1 Starting ConfigTool.....	5
3.2 Adding Devices	7
3.2.1 Adding One Device	7
3.2.2 Adding Multiple Devices	9
3.3 Initializing Devices	13
3.4 Modifying IP	16
3.4.1 Modifying One IP	17
3.4.2 Modifying IP in Batches	18
3.5 Configuring the Device Parameters.....	18
3.5.1 Accessing the Configuration Interface.....	19
3.5.2 Configuring the Parameters.....	20
3.6 Configuring System Settings	25
3.6.1 Timing	25
3.6.2 Rebooting.....	27
3.6.3 Restoring.....	28
3.6.4 Device Password	29
3.6.5 Video Password.....	30
3.7 Resetting Device Password.....	33
3.8 Local Upgrade.....	38
3.8.1 Upgrading One Device	38
3.8.2 Upgrading Devices in Batches	39
3.9 Online Upgrade.....	40
3.9.1 Enabling Online Upgrade	40
3.9.2 Performing Online Upgrade.....	42
3.10 Configuring the Template.....	53
3.10.1 Creating a Template.....	53
3.10.2 Applying the Template	59
Appendix 1 Cybersecurity Recommendations	62

1 Overview



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 abnormalities.

The Tool provides the following functions to configure and maintain the devices such as IPC and NVR:

- Initialize the device.
- Modify device IP.
- Set the code parameters or video parameters for the device.
- Synchronize device time, reboot device, restore system default, modify device password and reset password.
- Upgrade device, including local upgrade and online upgrade.

2 Installation and Uninstallation

This chapter introduces how to install and uninstall the Tool.

2.1 Installation

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

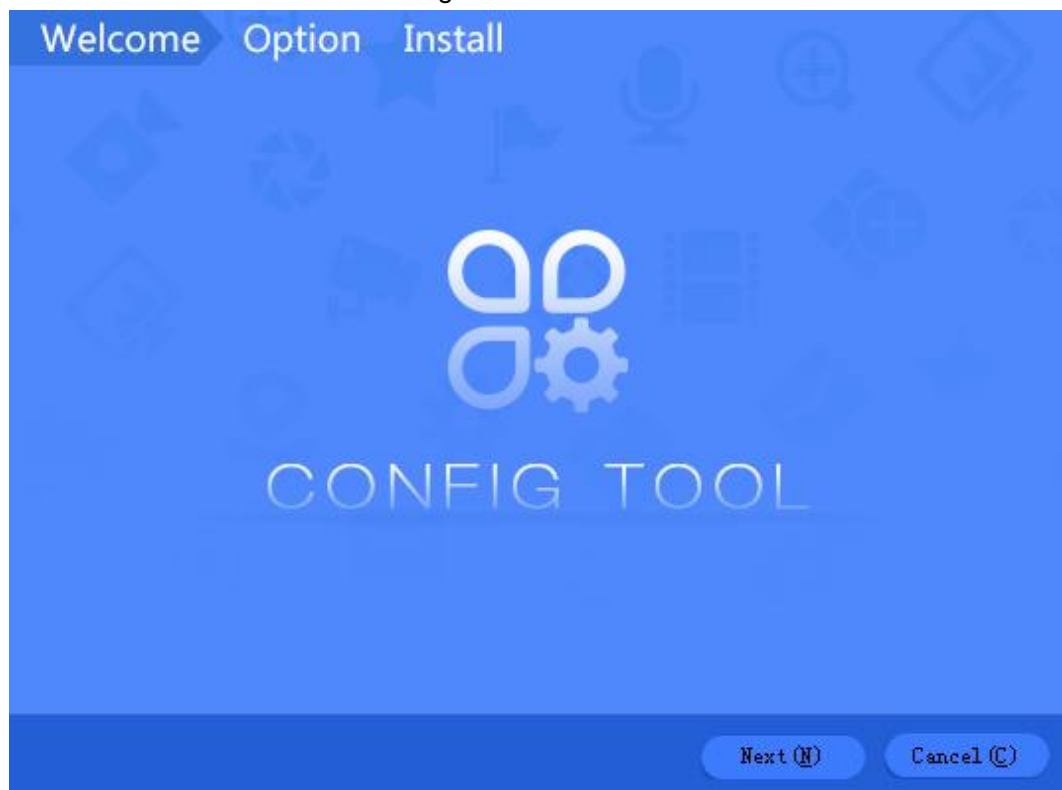
Step 1 Double-click the installation package.

The **Installer Language** dialog box is displayed.

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

The **Welcome** interface is displayed. See Figure 2-1.

Figure 2-1 Welcome



Step 3 Click **Next**.

The **Option** interface is displayed. See Figure 2-2.

Figure 2-2 Option

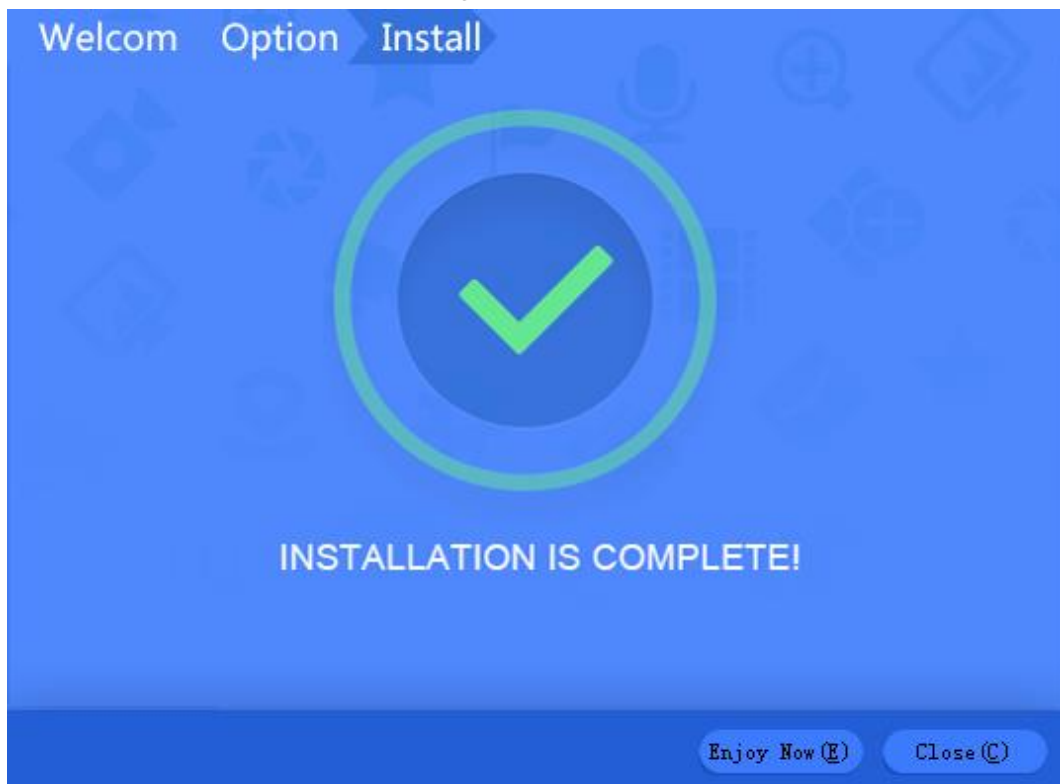


Step 4 Read the *User License Agreement*, select the **I agree** check box, and then click **Browse** to select the save path.

Step 5 Click **Install** to install the Tool.

After the installation is completed, the **Install** interface is displayed. See Figure 2-3.

Figure 2-3 Install



Step 6 Click **Close** to complete the installation.

2.2 Uninstallation

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

The **Uninstall** interface is displayed. See Figure 2-4.

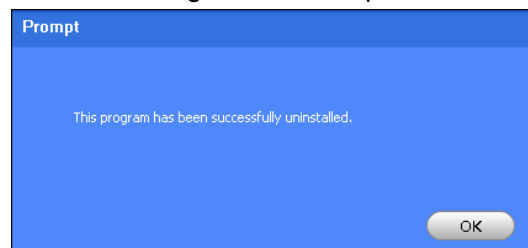
Figure 2-4 Uninstall



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

After the uninstallation is completed, the **Prompt** interface is displayed. See Figure 2-5.


Figure 2-5 Prompt



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

3 Basic Operations

3.1 Starting ConfigTool

On the desktop, double-click , the main interface is displayed. See Figure 3-1 and Table 3-1.



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

Figure 3-1 Main interface

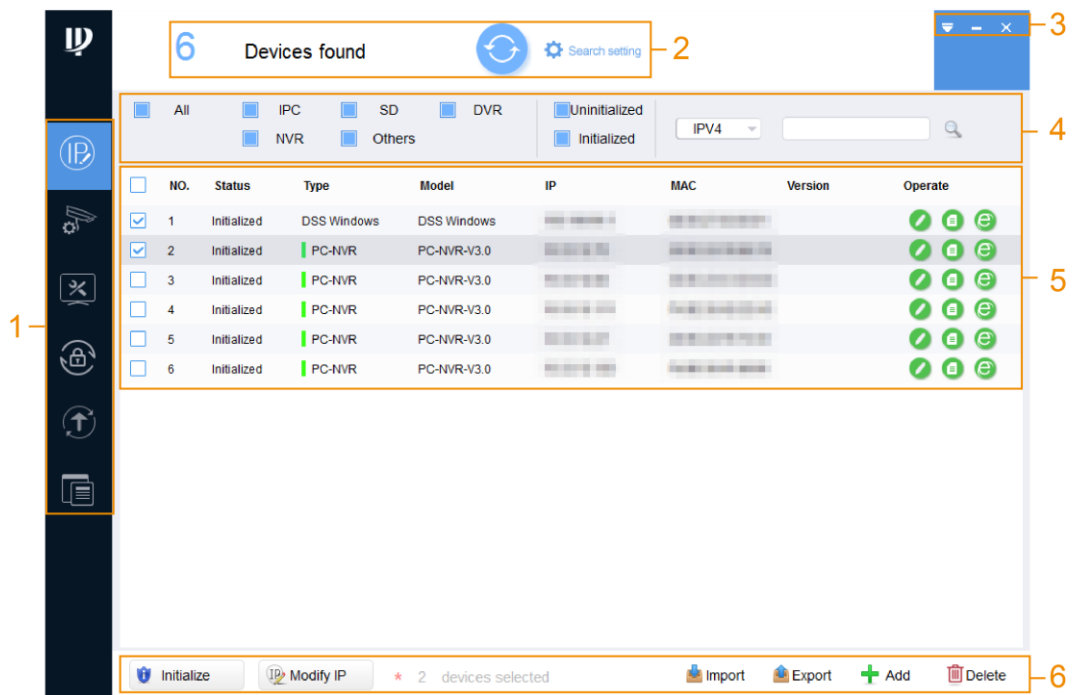








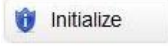
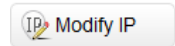
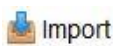




Table 3-1 Main interface Description

No.	Function	Description
1	Menu	<p>Includes six tabs: Modify IP, Device Config, System Settings, Password Reset, Upgrade, and Template Setup.</p> <ul style="list-style-type: none"> • Modify IP ( to refresh the device list that is displayed in the main interface.
3	Help	<p>Provides access to check the Help file, QA file and software version, set network parameters and upgrade parameters, minimize or exit the software.</p> <ul style="list-style-type: none"> • Click  to check the Help file, QA file and software version. Select Setting to set network timeout and online upgrade, including enable online upgrade, for detail, see "3.9.1 Enabling Online Upgrade." • Click  to minimize the software. • Click  to exit the software.
4	Filtering	<p>Filter by selecting device type and IP version (IPv4 or IPv6) to find the devices quickly.</p> <p>You can also manually enter the conditions such as type, IP address, model, MAC address and version number to search the devices.</p>

No.	Function	Description
5	Device list	<p>Shows the searched devices and their information such as type, mode, IP, MAC and version.</p> <p>The Operate column provides the following functions:</p> <ul style="list-style-type: none"> Click  to modify device IP. Click  to view device details. Click  to open device WEB configuration interface. <p></p> <p>Under IPV6, modifying IP or viewing device details is not supported.</p>
6	Function buttons	<p>Includes the following buttons:</p> <ul style="list-style-type: none"> Select one or multiple devices and click  to start initializing. Select one or multiple devices and click  to modify the IP addresses. Click  to import one or multiple devices through template. Select one or multiple devices and click  to export the device details. Select one or multiple devices and click  to remove from the list.

3.2 Adding Devices

You can add one or multiple devices according to your actual needs.



Make sure the network is interworking between the device and the PC installed with the Tool; otherwise the Tool cannot find the device.

3.2.1 Adding One Device

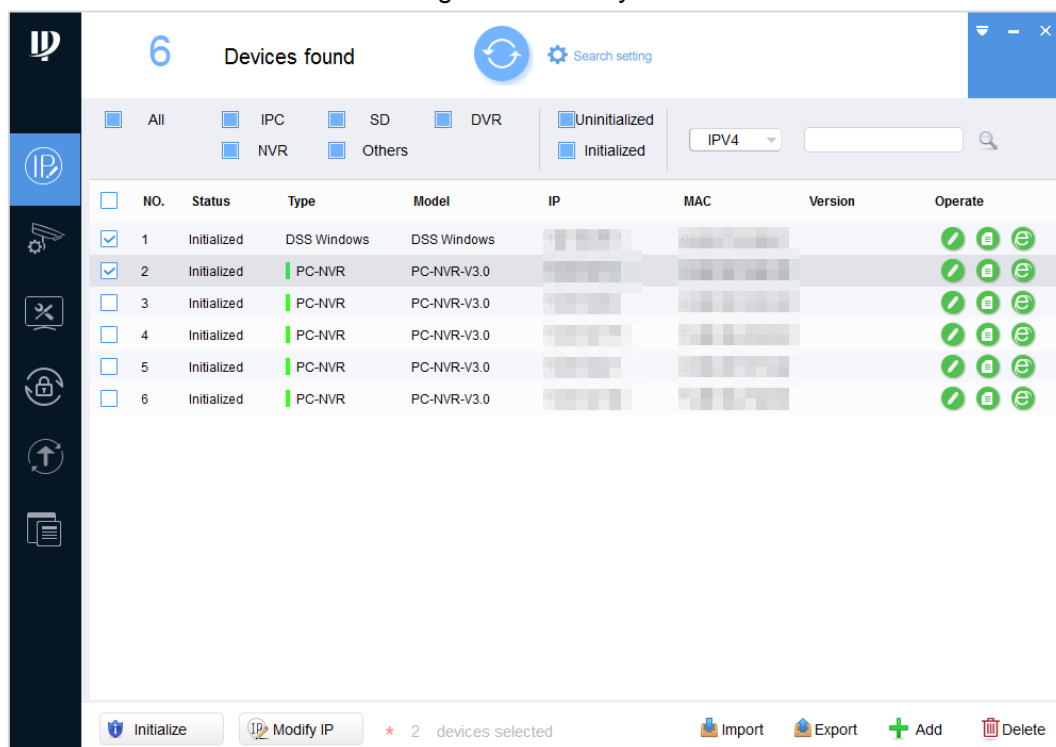


You can set the filtering conditions to search the wanted device quickly.

Step 1 Click .

The **Modify IP** interface is displayed. See Figure 3-2.

Figure 3-2 Modify IP



Step 2 Click  **Add**.

The **Manual Add** interface is displayed. Select **IP Address** or **Device SN** from **Add Type** list. See Figure 3-3 and Figure 3-4.

Figure 3-3 Manual add (IP address)

The 'Manual Add' dialog box is shown with a dark header and a close button. It contains the following fields:

- Add Type:** A dropdown menu currently set to 'IP Address'.
- IP Address:** A text input field with a placeholder showing three dots.
- Username:** A text input field.
- Password:** A text input field.
- Port:** A text input field.
- OK:** A button at the bottom right.

Figure 3-4 Manual add (Device SN)

Step 3 Set the device parameters. See Table 3-2.

Table 3-2 Manual add parameters

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

Step 4 Click **OK**.

The newly added device appears in the device list.

3.2.2 Adding Multiple Devices

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

- If you know the network segment where the device is located, add the devices through searching. For details, see "3.2.2.1 Adding by Searching."
- If you have the template data of the device, add the devices through importing the template. For details, see "3.2.2.2 Adding by Template."

3.2.2.1 Adding by Searching

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

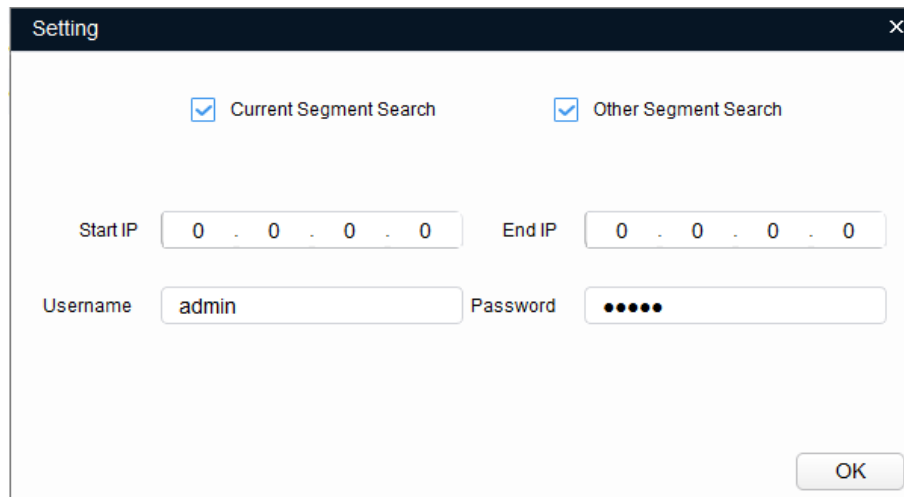


You can set the filtering conditions to search the wanted device quickly.

Step 1 Click  [Search setting](#).

The **Setting** interface is displayed. See Figure 3-5.

Figure 3-5 Setting



Step 2 Select the searching way. Both the following two ways are selected by default.

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




- If you select both the **Current Segment Search** check box and the **Other Segment Search** check box, the system searches devices under the both conditions.
- The user name and the password are the ones used to login when you want to modify IP, configure the system and update the device.

Step 3 Click **OK** to start searching devices.

The searched devices will appear in the device list on the main user interface.



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

3.2.2.2 Adding by Template

You can quickly add devices by using the template.



Make sure your PC is installed with Microsoft Excel.

3.2.2.2.1 Accessing to the Template

You can either manually fill in the template or export the device details file from the system.

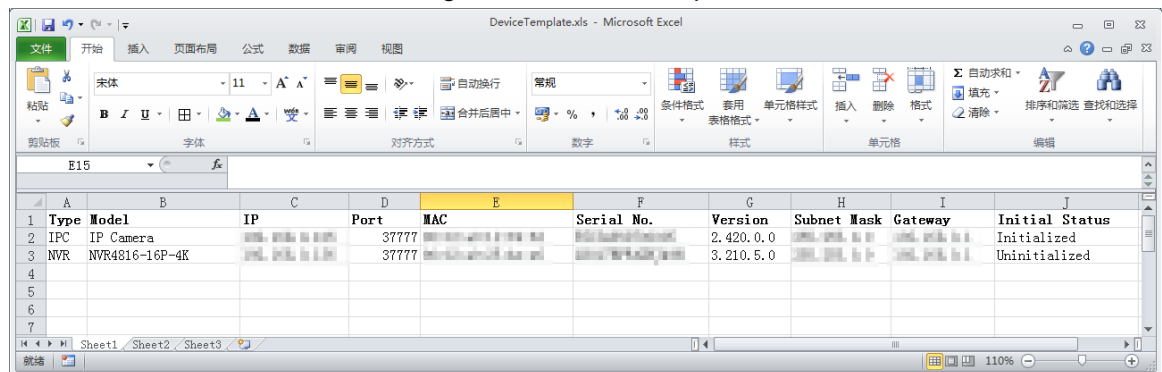


- The template (DeviceTemplate.xls) must be opened and edited by Excel.
- To delete the record in the template, right-click the line with the record, and then select **Delete**.

Filling in the Template

Step 1 Find the device template in the Tool save path and open it. See Figure 3-6.

Figure 3-6 Device template



Step 2 Enter the device parameters. See Table 3-3.

Table 3-3 Device parameters

Parameter	Description
Type	Optional. Device type, such as IPC and NVR.
Model	Optional. Device model.
IP	Required. IP address of device.
Port	Required. Port number of device.
MAC	Required. Device MAC address that can be obtained from the device label.
Serial No.	Optional. Device serial number.
Version	Optional. Device version number.
Subnet Mask	Required. Device subnet mask.
Gateway	Required. Device gateway.
Initial Status	Required. Device initialization status: Initialized or uninitialized.

Step 3 Save and close the template.

Exporting the Device Details File

You can export the device details file and use it as a template to add or back up the device details.

Step 1 Click .

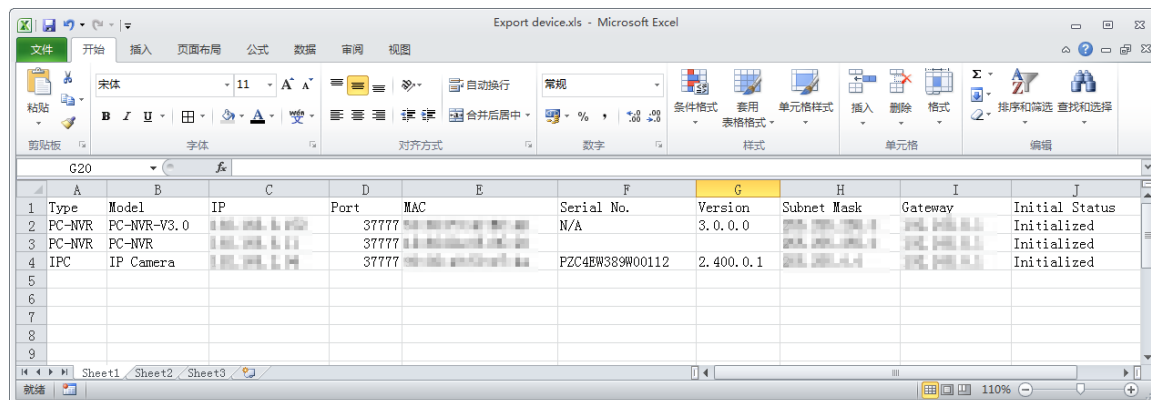
The **Modify IP** interface is displayed.

Step 2 Select the devices to be exported, and then click  **Export**.

The **Save As** interface is displayed.

- Step 3** Select the save path, enter the file name in the **File name** box, and then click **Save**.
The system starts exporting the device details. After the exporting is completed, a success notice is displayed.
- Step 4** Click **OK** to complete exporting.
You can check the exported device details in the save path. See Table 3-4.

Table 3-4 Exported device details



Type	Model	IP	Port	MAC	Serial No.	Version	Subnet Mask	Gateway	Initial Status
PC-NVR	PC-NVR-V3.0	192.168.1.1	37777	08:00:27:00:00:00	N/A	3.0.0.0	255.255.255.0	192.168.1.1	Initialized
PC-NVR	PC-NVR	192.168.1.2	37777	08:00:27:00:00:00			255.255.255.0	192.168.1.1	Initialized
IPC	IP Camera	192.168.1.3	37777	08:00:27:00:00:00	FZC4EW389W00112	2.400.0.1	255.255.255.0	192.168.1.1	Initialized

3.2.2.2.2 Importing Devices

After getting the template, you can add the devices details into the template, and then import the template to the Tool. The devices in the template will display on the device list.



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

- Step 1** Click .

The **Modify IP** interface is displayed.

- Step 2** Click  **Import**.

The **Open** interface is displayed.

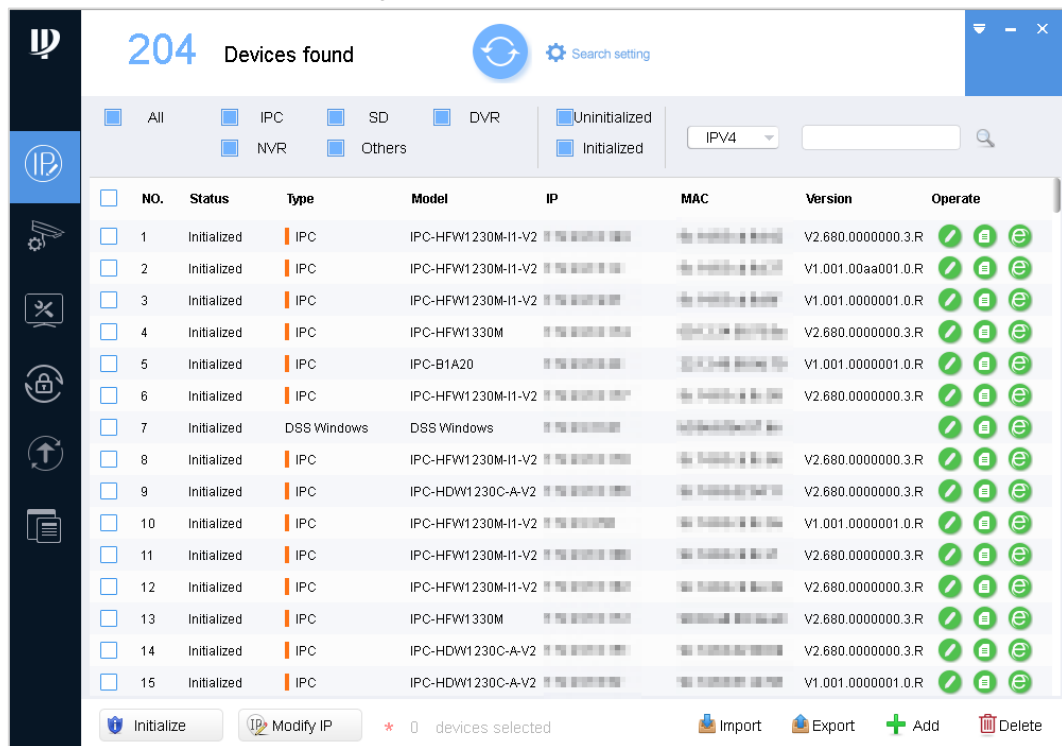
- Step 3** Select the template and click **Open**.

The system starts importing the devices details. After the importing is completed, a success notice is displayed.

- Step 4** Click **OK**.

The newly imported devices appear in the device list. See Figure 3-7.

Figure 3-7 Imported device list



3.3 Initializing Devices

You can initialize one or multiple devices according to your actual needs.

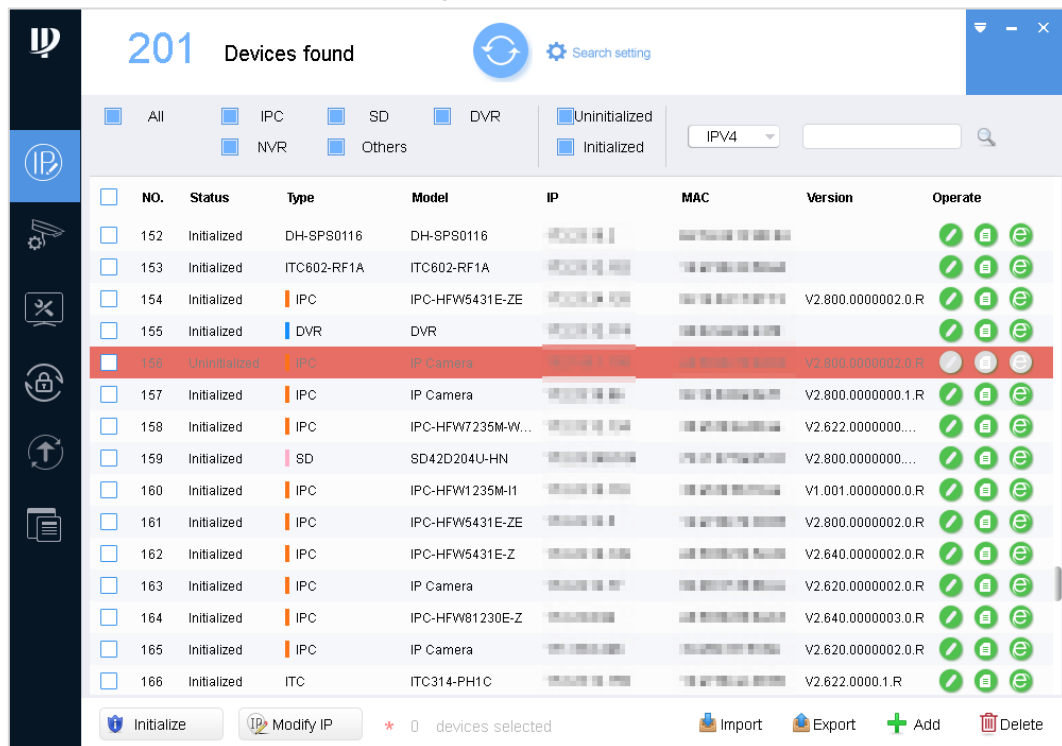


- This function is available on select models.
- The initializing operation can only be performed to the devices within the local area network.
- The operations cannot be performed to the uninitialized devices that are shown in gray background. And the uninitialized devices do not appear on other interfaces of the Tool.

Step 1 Click .

The **Modify IP** interface is displayed. See Figure 3-8.

Figure 3-8 Modify IP

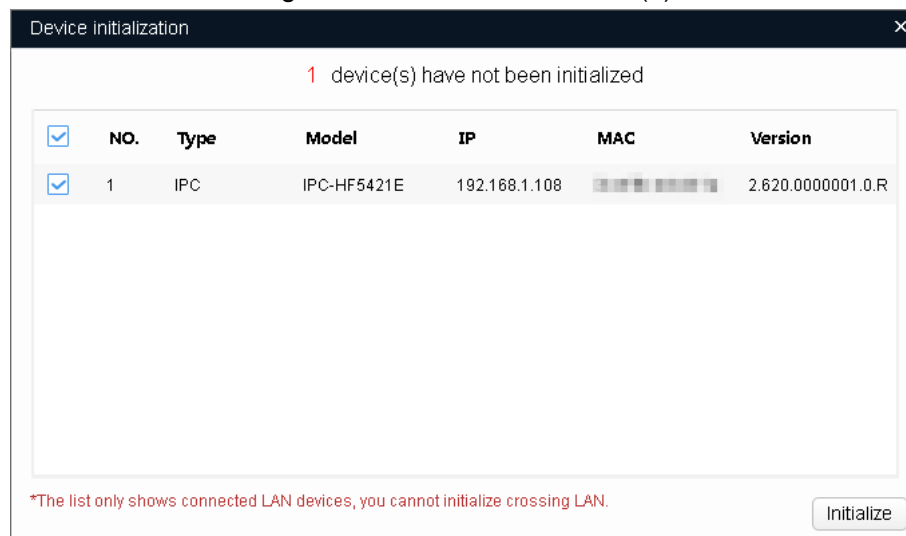


Step 2 Select one or several uninitialized devices.

Step 3 Click Initialize.

The **Device initialization** interface is displayed. See Figure 3-9.

Figure 3-9 Device initialization (1)



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

The **Device initialization** interface is displayed. See Figure 3-10.



- The interface might vary with different models, and the actual product shall prevail.
- If you do not provide the reserve information for password reset, you can reset the password only through XML file.
- When initializing multiple devices, the Tool initializes all devices based on the password reset mode of the first selected device.

- After setting the new password is completed, reset the password in **Search setting** interface.

Figure 3-10 Device initialization (2)

Device Initialization

X

1 device(s) have not been initialized

Username

admin

New Password

WeakMediumStrong

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 " , ' , . , , , , & ')

☒

Email Address

(for password reset)

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

Next

Step 5 Set the initialization parameters for the device. See Table 3-5.

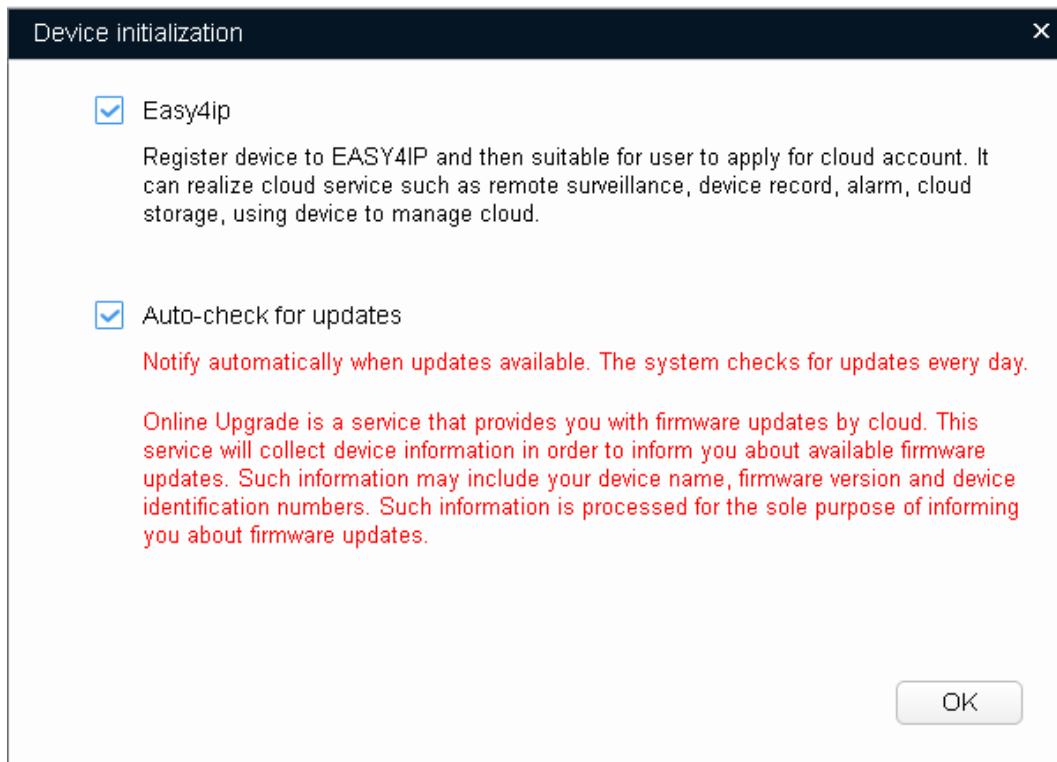
Table 3-5 Initialization parameters

Parameter	Description
Username	The user name is admin by default.
New Password	Enter the new password. There is an indication for the strength of the new password. The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
Confirm Password	Confirm the new password.
Email Address	Selected by default. The email address will be used for password reset.

Step 6 Click Next.

The **Device initialization** interface is displayed. See Figure 3-11.

Figure 3-11 Device initialization (3)



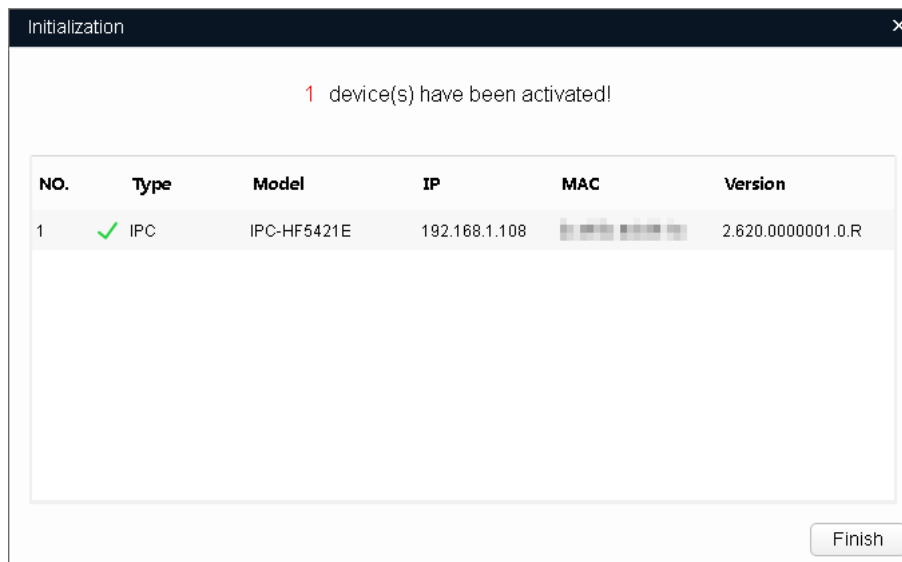
Step 7 Select **Easy4ip** or select **Auto-check for updates** according to the actual needs.

Step 8 Click **OK** to initialize the device.

The **Initialization** interface is displayed after initializing is completed. See Figure 3-12.

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

Figure 3-12 Initialization



Step 9 Click **Finish** to finish initialization.

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

3.4 Modifying IP

You can modify IP for one or multiple devices in one time.

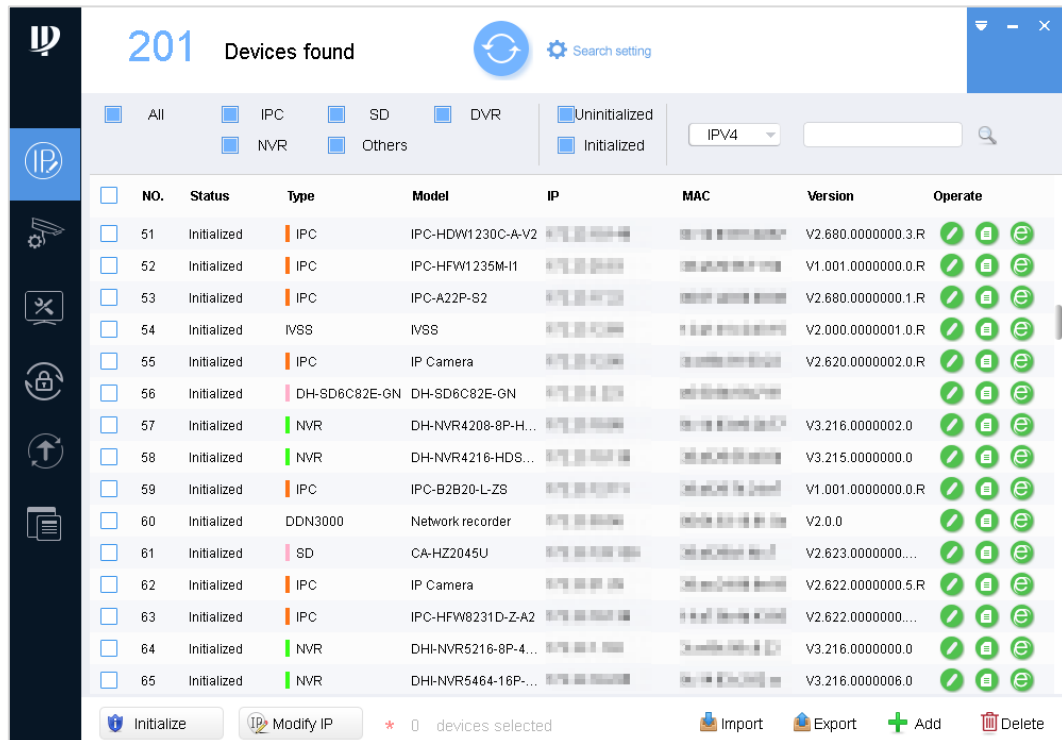
You can modify IP in batches only if the device login passwords are the same; otherwise you can modify one IP at a time.

3.4.1 Modifying One IP

Step 1 Click .

The **Modify IP** interface is displayed. See Figure 3-13.

Figure 3-13 Modify IP address (1)



Step 2 Select the device that you want to modify IP, and then click the .

The **Modify IP Address** interface is displayed. See Figure 3-14.



If the device is not in the device list, perform searching again. For details, see "3.2 Adding Devices."

Figure 3-14 Modify IP address (2)

Modify IP Address

Mode: ☒ Static ☐ DHCP

Target IP:

Subnet Mask:

Gateway:

Selected number of devices: 1

OK

Step 3 Select the mode for setting the IP address according to the actual needs.

- 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 modified to be the one you set.

Step 4 Click **OK** to complete modification.

3.4.2 Modifying IP in Batches

Step 1 Click .

The **Modify IP** interface is displayed.

Step 2 Select the devices that you want to modify IP.

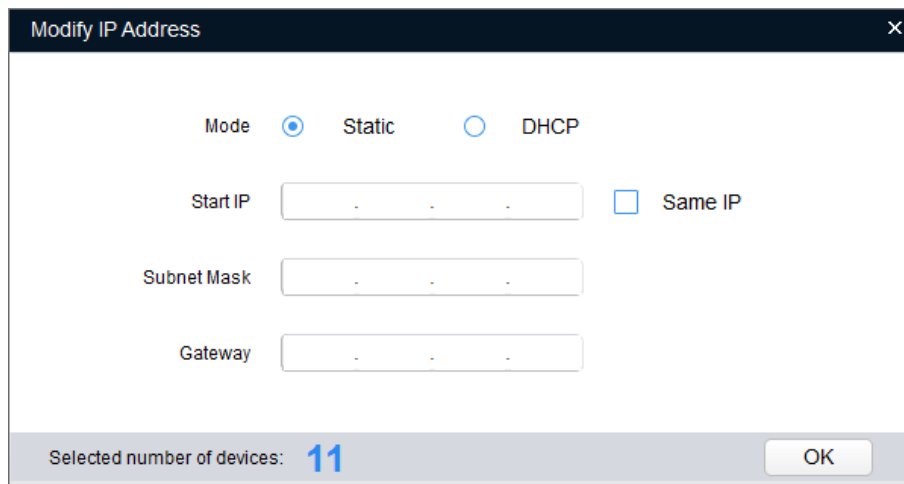


If the device is not in the device list, perform searching again. For the details about how to search devices, see "3.2 Adding Devices."

Step 3 Click .

The **Modify IP Address** interface is displayed. See Figure 3-15.

Figure 3-15 Modify IP address (3)



Step 4 Select the mode for setting the IP address according to the actual needs.

- 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 address of the devices will be modified successively starting from the entered start IP.



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

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

3.5 Configuring the Device Parameters

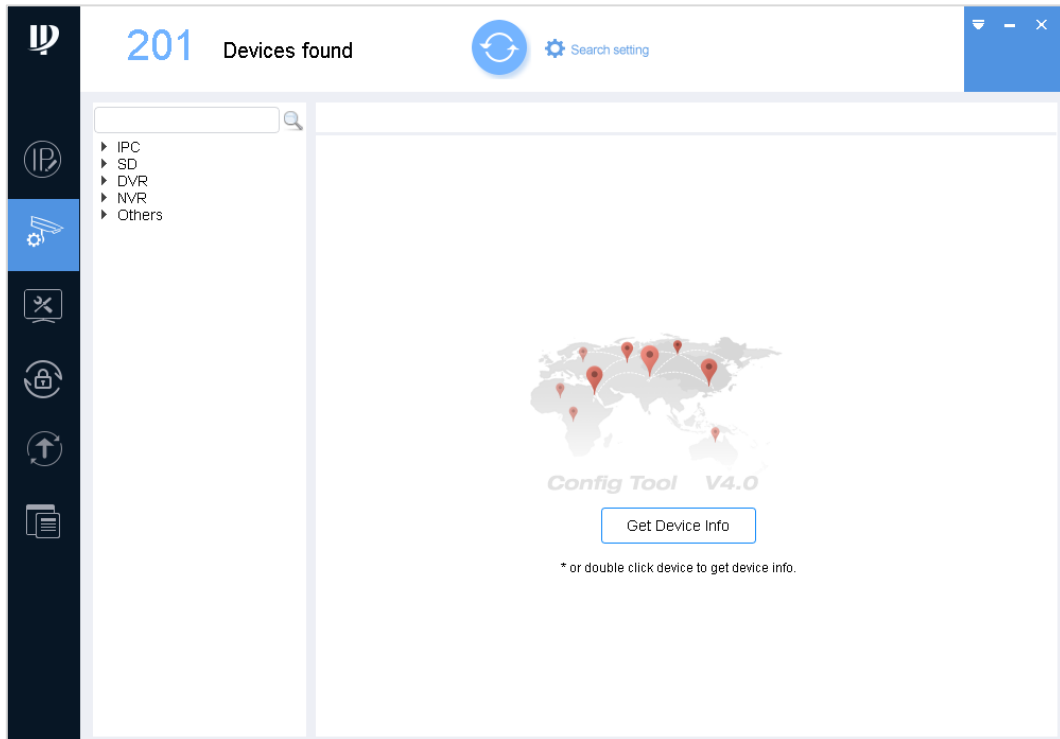
You can configure the encoding parameters, video parameters, and profile management.

3.5.1 Accessing the Configuration Interface

Step 1 Click .

The **Device Config** interface is displayed. See Figure 3-16.

Figure 3-16 Device Config



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

The **Notice** dialog box is displayed.



If the device is not in the device list, perform searching again. For the details about how to search devices, see "3.2 Adding Devices."

Step 3 Click **OK** or click **Cancel**.

- Click **OK** to enter the **Login** interface on which you can change the initial password of the device. See Figure 3-17.

Figure 3-17 Login

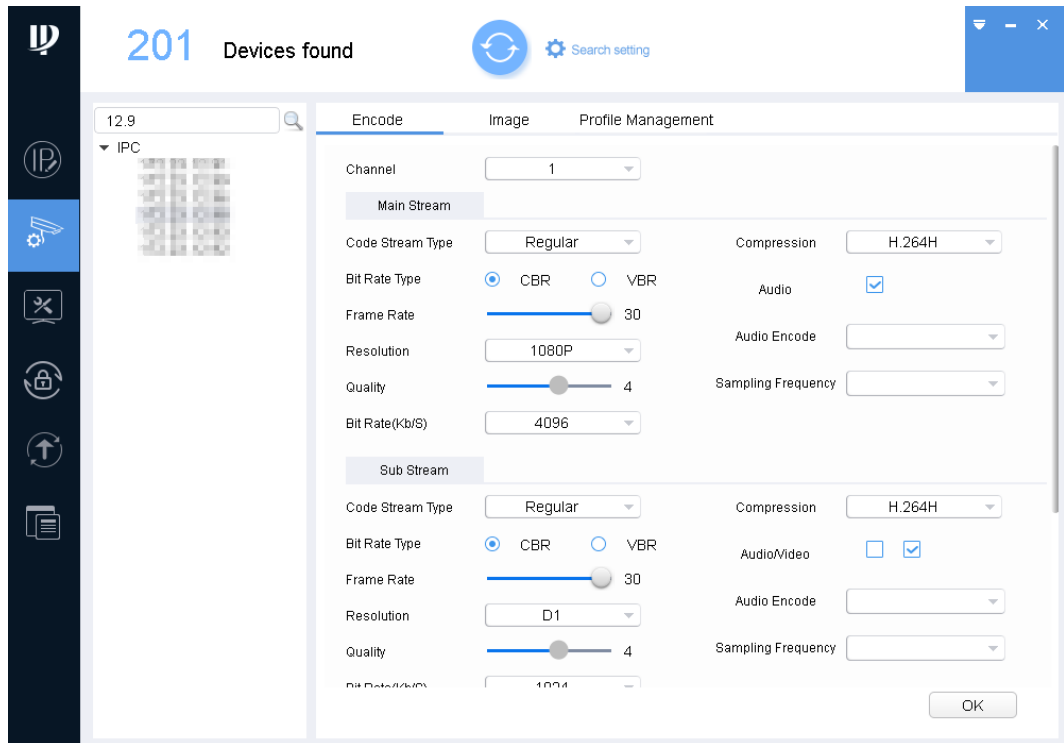
Enter the username and password, and then Click **OK**.

The **Encode** interface is displayed. See Figure 3-18.

- Click **Cancel**.

The **Encode** interface is displayed. See Figure 3-18.

Figure 3-18 Encode



3.5.2 Configuring the Parameters

After accessing the Device Config interface, you can configure the encoding parameters, video parameters, and profile management.

3.5.2.1 Configuring Encoding Parameters

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


Step 1 On the **Encode** interface, set the parameters for main stream and sub stream. See Table 3-6.



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

Table 3-6 Encode parameters

Parameter	Description
Channel	Select the channel number.
Code Stream type	Includes Regular , Motion , and Alarm . The sub stream only supports Regular type.

Parameter	Description
Compression	Includes the following video encoding modes: <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 higher bit rate to ensure video quality. It is recommended to use the maximum bit rate value to get the best results.
Bit Rate Type	Includes the following two types of bit rate: <ul style="list-style-type: none"> • Constant Bit Rate (CBR): The bit rate is fluctuating around the set value without big changes. • Variable Bit Rate (VBR): The bit rate is changing along with the monitoring environment.  <p>When the compression is set as MJPG, the bit rate can only be CBR.</p>
Frame Rate	The total frames per second. The higher the frame rate, the more clear and smooth the image will become.
Resolution	The video resolution. The maximum video resolution might be different dependent on your device model.
Quality	The video image quality level. You can configure this parameter when the bit rate type is set as VBR .
Bit Rate (Kb/S)	Select the suitable value according to the actual needs. You can configure this parameter when the bit rate type is set as CBR.
Audio/Video	<ul style="list-style-type: none"> • To enable the audio function, select the Audio check box. • To monitor with the sub stream, select the Video check box. <p>For the sub stream, you can enable the audio function only after the video function is already enabled.</p>
Audio Encode	Indicates audio encoding mode that includes G.711A, G.711Mu, G.726, and AAC. The setting of audio encoding mode will simultaneously apply to both audio and voice intercom.
Sampling Frequency	Indicates the sampling frequency of the audio.

Step 2 Click **OK** to complete settings.

3.5.2.2 Configuring Video Parameters

You can check the live monitoring picture and set the video effects.

Step 1 Click the **Image** tab.

The **Image** interface is displayed. See Figure 3-19.



- Click **Default** to restore the default parameters settings.
- Rotate mouse wheel on the image to zoom in or zoom out. Right-click on the image to return to the default size.



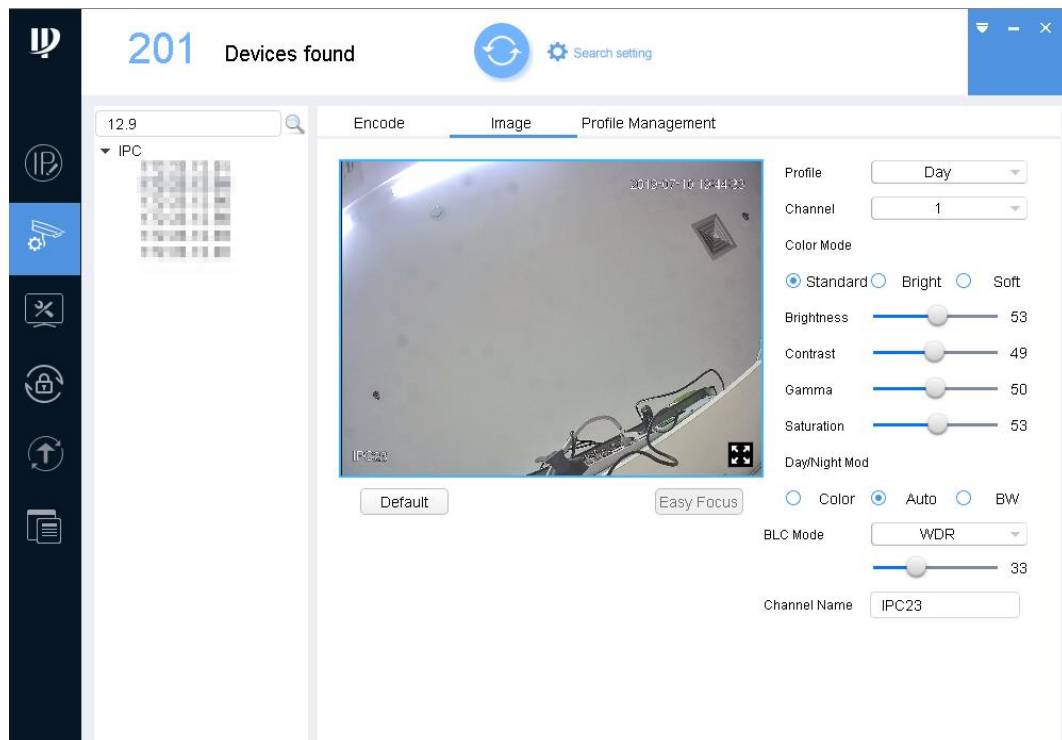
- On the image, click  to display in full screen, and click  on full screen to restore the default.

Figure 3-19 Image



Step 2 Set the video parameters. See Table 3-7.

Table 3-7 Video parameters

Parameter	Description
Profile	Select the device profile from Day , Night , and Normal .
Channel	Select the channel number.
Color Mode	Select the image color mode from Standard , Bright , and Soft .
Brightness	Adjust the image brightness. The bigger the value, the brighter the image.
Contrast	Adjust the image contrast. The bigger the value, the more obvious the contrast between the light area and dark area.
Gamma	Adjust the image brightness in a non-linear way to improve the dynamic display range. The bigger the value, the brighter the image.
Saturation	Adjust the color shades. The bigger the value, the lighter the color. This value does not affect the general image lightness.
Day/Night Mode	Includes the following three options: <ul style="list-style-type: none"> Color: Select this option to set the color image. 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.

Parameter	Description
BLC Mode	<ul style="list-style-type: none"> • OFF: Turn off the backlight compensation mode. • BLC: Backlight compensation. In the backlighting environment, the compensation function can avoid silhouette of the dark part when taking a picture. • WDR: Wide Dynamic Range. In the strong illumination contrast, this function can suppress the area with excessive brightness and compensate the area with excessive darkness so as to make the image clearer in general. • HLC: Highlight Compensation. This function can weaken the strong light to reach the brightness balance.
Channel Name	Set the device channel name. The input cannot be null character.

Step 3 (Optional) Set the **Easy Focus** function.

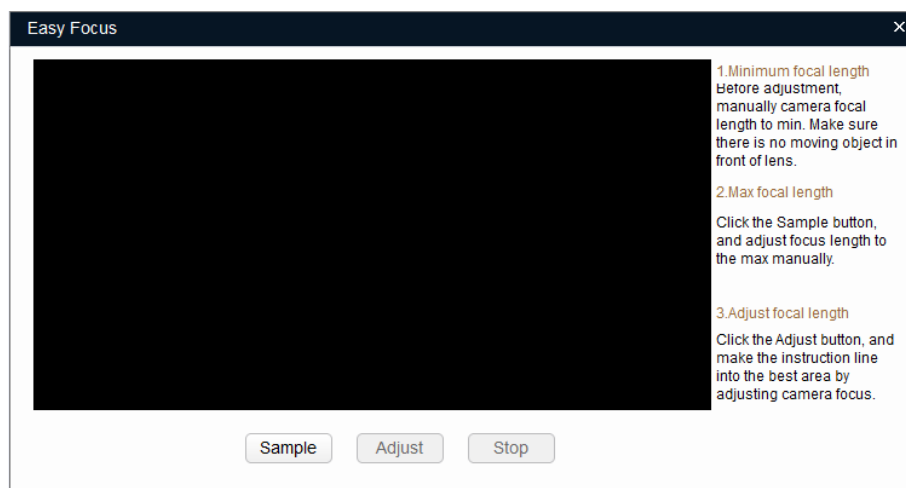


Do this step when you need to do fine adjustment to the focal distance.

1) Click **Easy Focus**.

The **Easy Focus** interface is displayed. See Figure 3-20.

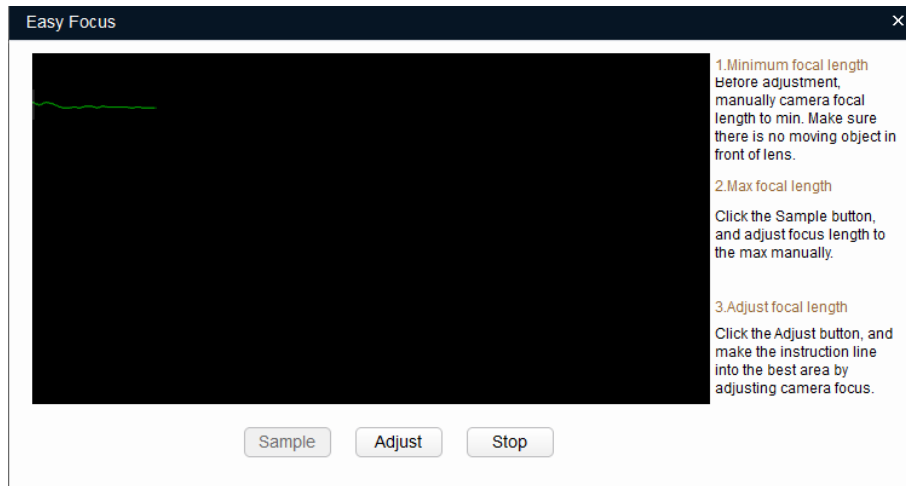
Figure 3-20 Easy focus



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.

The sampling started. See Figure 3-21.

Figure 3-21 Sampling



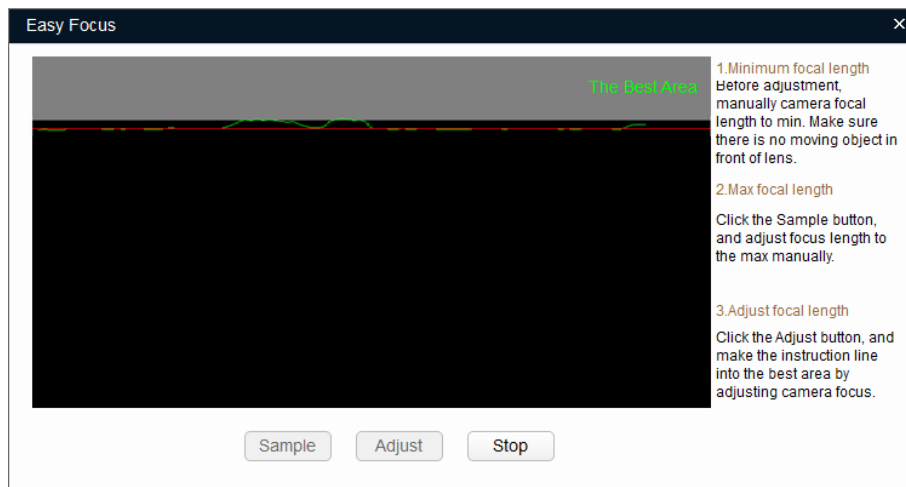
3) Click **Adjust**.

The **The Best Area** interface is displayed. Manually adjust the focus till the focal length indicating line has entered the best area. See Figure 3-22.



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

Figure 3-22 Final result



3.5.2.3 Configuring the Profile Management

You can manage the profiles through **Normal**, **Full Time**, and **Schedule**.

Step 1 Click **Profile Management** tab.

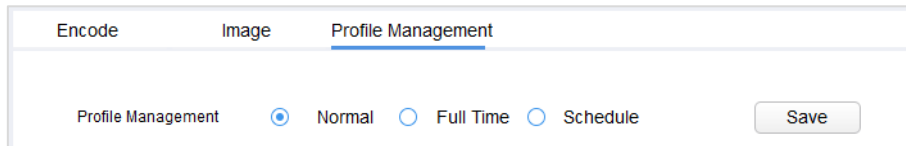
The **Profile Management** interface is displayed.

Step 2 Set the management profile.

- Select **Normal**.

The system monitors according to the normal configuration. See Figure 3-23.

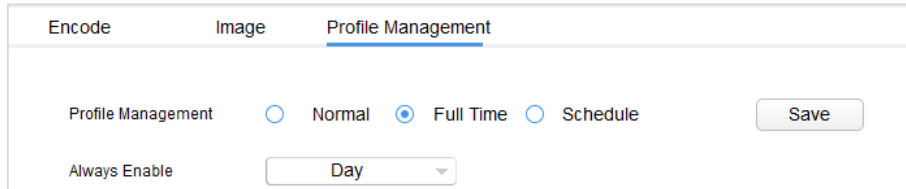
Figure 3-23 Normal



The screenshot shows a web interface with three tabs: 'Encode', 'Image', and 'Profile Management'. The 'Profile Management' tab is active. Below the tabs, there are three radio buttons: 'Normal' (selected), 'Full Time', and 'Schedule'. To the right of these buttons is a 'Save' button.

- Select **Full Time**, and then select **Day** or **Night**.
The system monitors according to the corresponding settings. See Figure 3-24.

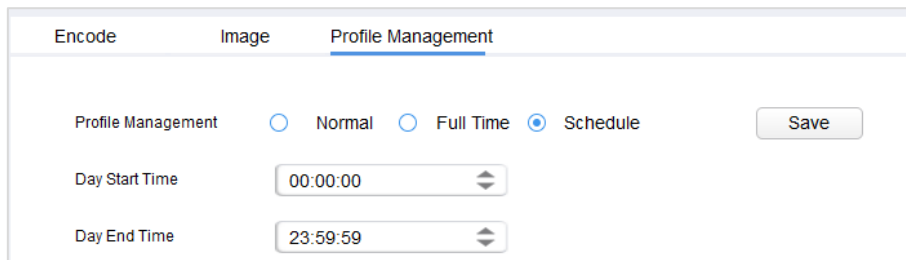
Figure 3-24 Full time



The screenshot shows the same web interface as Figure 3-23, but now the 'Full Time' radio button is selected. Below the radio buttons, there is a label 'Always Enable' and a dropdown menu currently showing 'Day'. The 'Save' button is still present.

- Select **Schedule**, and then type **Day Start Time** and **Day End time**. The rest time is night. For example, if you set 8:00–17:00 as day, so 0:00–8:00 and 18:00–24:00 are night.
The system monitors according to the corresponding settings. See Figure 3-25.

Figure 3-25 Schedule



The screenshot shows the same web interface, but now the 'Schedule' radio button is selected. Below the radio buttons, there are two input fields: 'Day Start Time' with the value '00:00:00' and 'Day End Time' with the value '23:59:59'. The 'Save' button is still present.

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

3.6 Configuring System Settings

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


3.6.1 Timing

You can calibrate the device time through configuration.

Step 1 Click .

The **Timing** interface is displayed. See Figure 3-26.

Figure 3-26 Timing

Step 2 Click  next to the device type.

The device list is displayed.

Step 3 Select one or multiple devices.



If the device is not in the device list, perform searching again. For the details about how to search devices, see "3.2 Adding Devices."

Step 4 Select the time sync way for the device.

- Manual sync: Type the time and select the time zone, and then click **Manual Sync**. The device time will sync with the setting.
- PC sync: Click **Sync PC**. The device time will sync with the PC time.
- NTP sync: Select **Synchronize with NTP** check box and set the parameters. See Table 3-8.

Table 3-8 NTP Parameters

Parameter	Description
NTP Sever	Enter the IP address or domain name of the corresponding NTP server.
NTP Port	Enter the port number of corresponding NTP server.
Update Period	Enter the time interval that device sync with the NTP.

Step 5 (Optional) Select **DST Enable** (Daylight Saving Time) check box and set the parameters. See Table 3-9.



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

Table 3-9 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 6 Click **Save** to complete settings.

3.6.2 Rebooting

You can manually or automatically reboot the device.



Reboot will interrupt operations, so reboot the device when the operation is not so frequent.

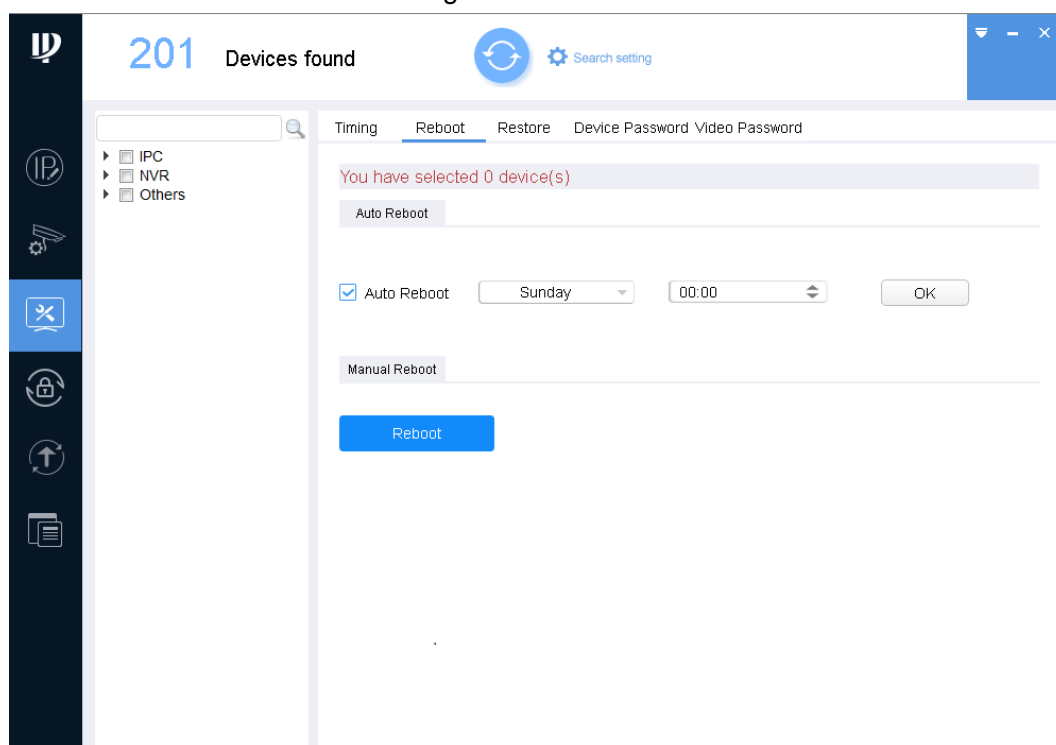
Step 1 Click .


The **Timing** interface is displayed.

Step 2 Click the **Reboot** tab.

The **Reboot** interface is displayed. See Figure 3-27.

Figure 3-27 Reboot



Step 3 Click  next to the device type.

The device list is displayed.

Step 4 Select one or multiple devices.



If the device is not in the device list, perform searching again. For the details about how to search devices, see "3.2 Adding Devices."

Step 5 Select the reboot type for the device according to your actual needs.

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

3.6.3 Restoring

You can restore the default parameters value, including normal configuration, encoding configuration, video configuration, serial port configuration, alarm setup, video detection, and Pan Tilt Zoom (PTZ) control.

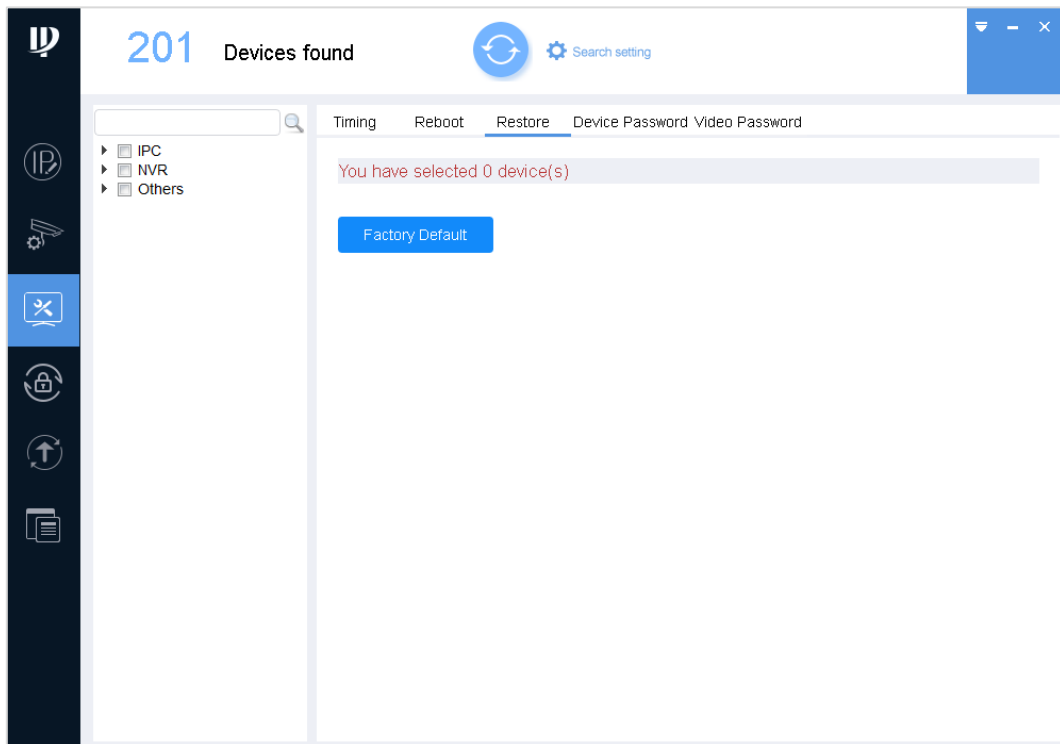
Step 1 Click .


The **Timing** interface is displayed.

Step 2 Click the **Restore** tab.

The **Restore** interface is displayed. See Figure 3-28.

Figure 3-28 Restore



Step 3 Click  next to the device type.

The device list is displayed.

Step 4 Select one or multiple devices.



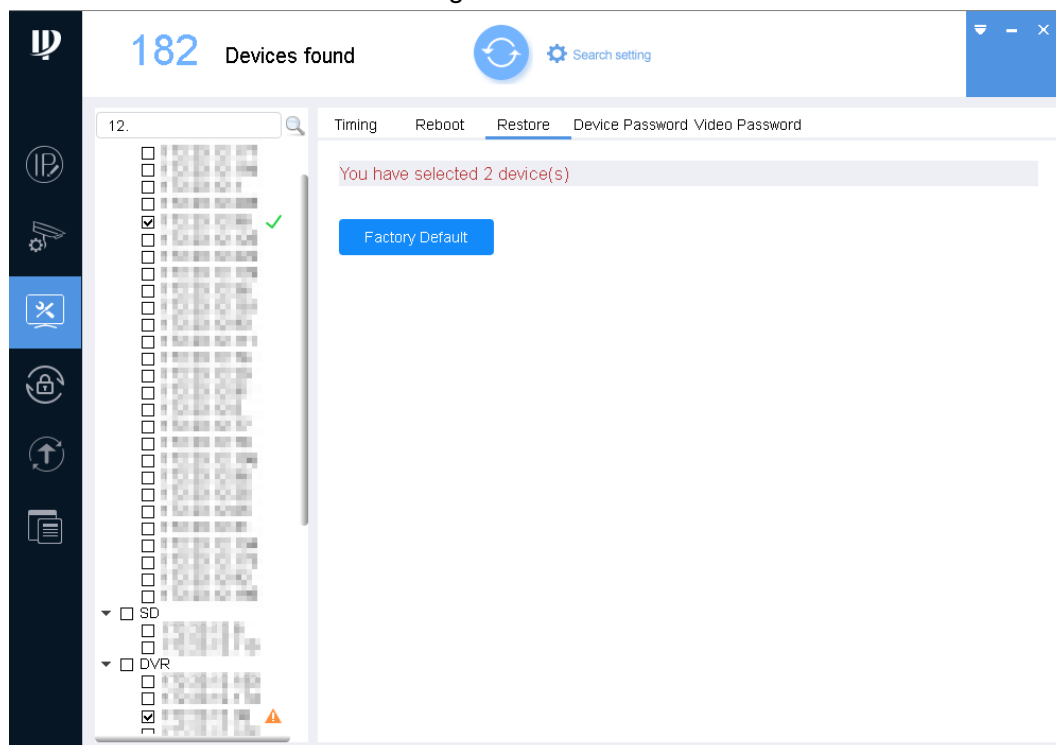
If the device is not in the device list, perform searching again. For the details about how to search devices, see "3.2 Adding Devices."

Step 5 Click **Factory Default** to start restoring the selected devices.

The result is displayed next to the device after restoring is completed. See Figure 3-29.

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

Figure 3-29 Result



3.6.4 Device Password

You can modify the device login password.

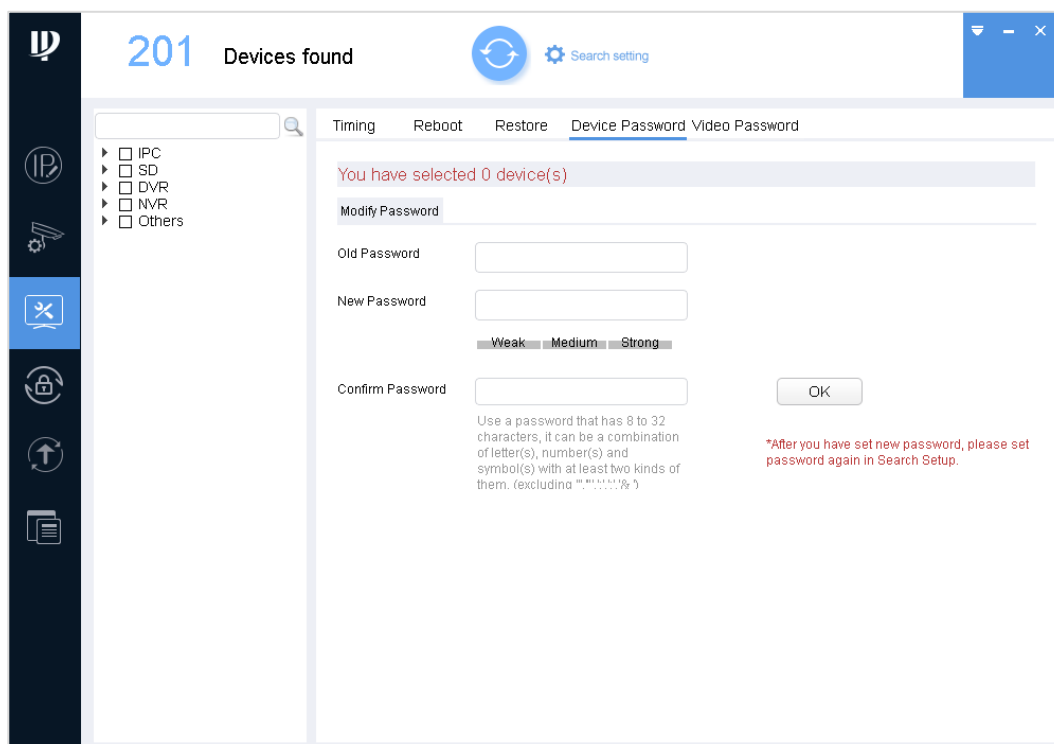
Step 1 Click .

The **Timing** interface is displayed.

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

The **Device Password** interface is displayed. See Figure 3-30.

Figure 3-30 Device password



Step 3 Click  next to the device type.

The device list is displayed.

Step 4 Select one or multiple devices.



- If you select multiple devices, the login passwords must be the same.
- If the device is not in the device list, perform searching again. For the details about how to search devices, see "3.2 Adding Devices."

Step 5 Set the password parameters. See Table 3-10.

Table 3-10 Password parameters

Parameter	Description
Old Password	Enter the device old password.
New Password	Enter the new password for the device. There is an indication for the strength of the password. The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
Confirm Password	Confirm the new password.



- After setting the new password is completed, reset the password in **Search setting** interface.
- If the new password is the same with the old password, a **Notice** dialog box is displayed after clicking **OK**. Then you need to click **OK** to go back and reset the new password.

Step 6 Click **OK** to complete modification.

3.6.5 Video Password

You can get back password for video files.

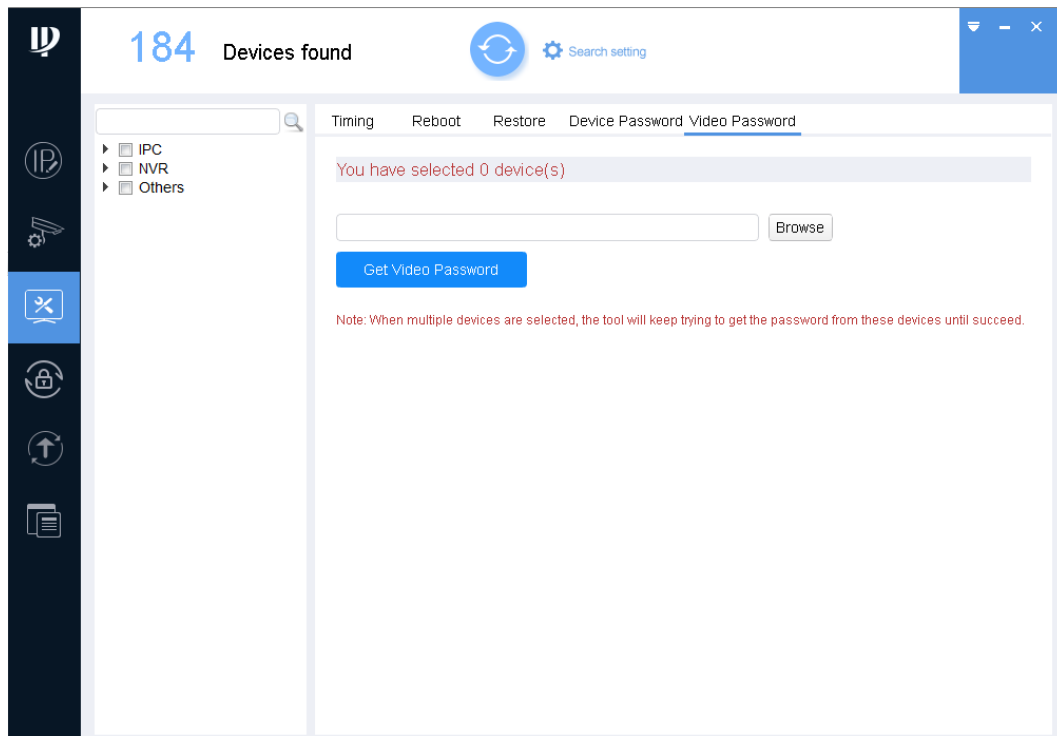
Step 1 Click .

The **Timing** interface is displayed.

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

The **Video Password** interface is displayed. See Figure 3-31.

Figure 3-31 Video password



Step 3 Click ► next to the device type.

The device list is displayed.



If the device is not in the device list, perform searching again. For the details about how to search devices, see "3.2 Adding Devices."

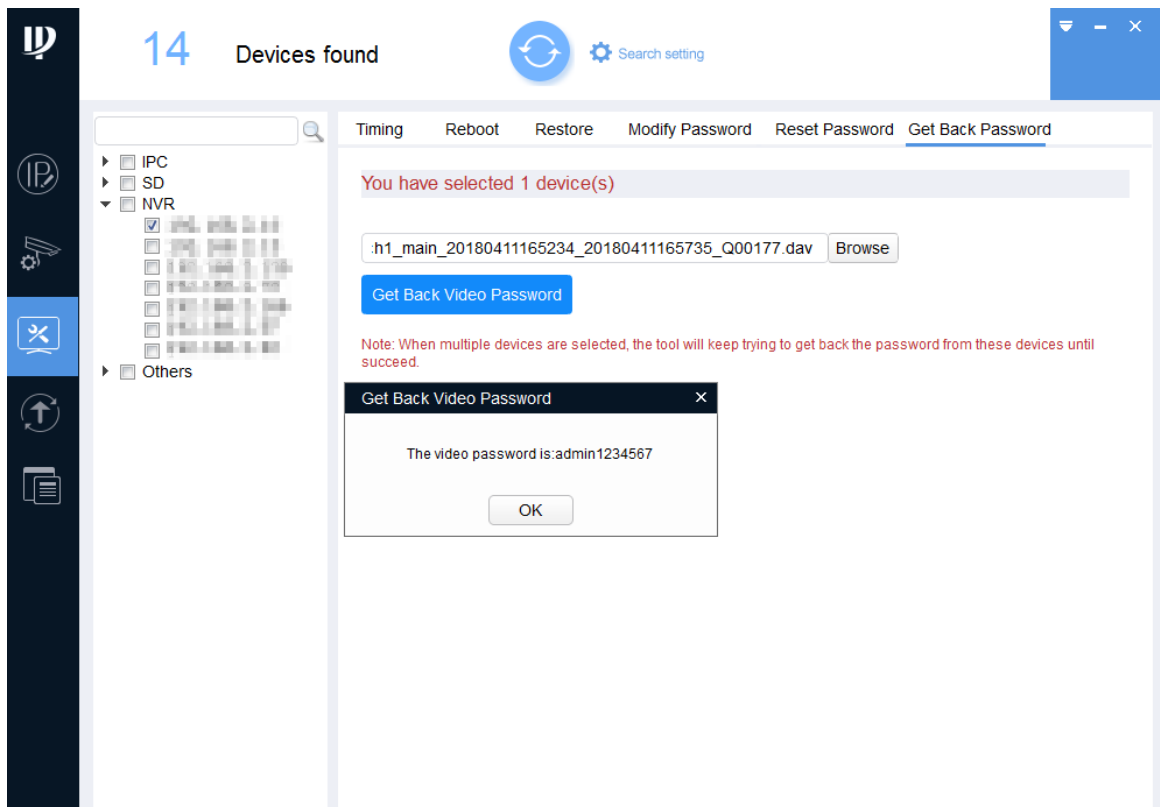
Step 4 Select one or multiple devices.

Step 5 Click **Browse** to select a video file.

Step 6 Click **Get Video Password**.

The **Video Password** interface is displayed. See Figure 3-32.

Figure 3-32 Video password

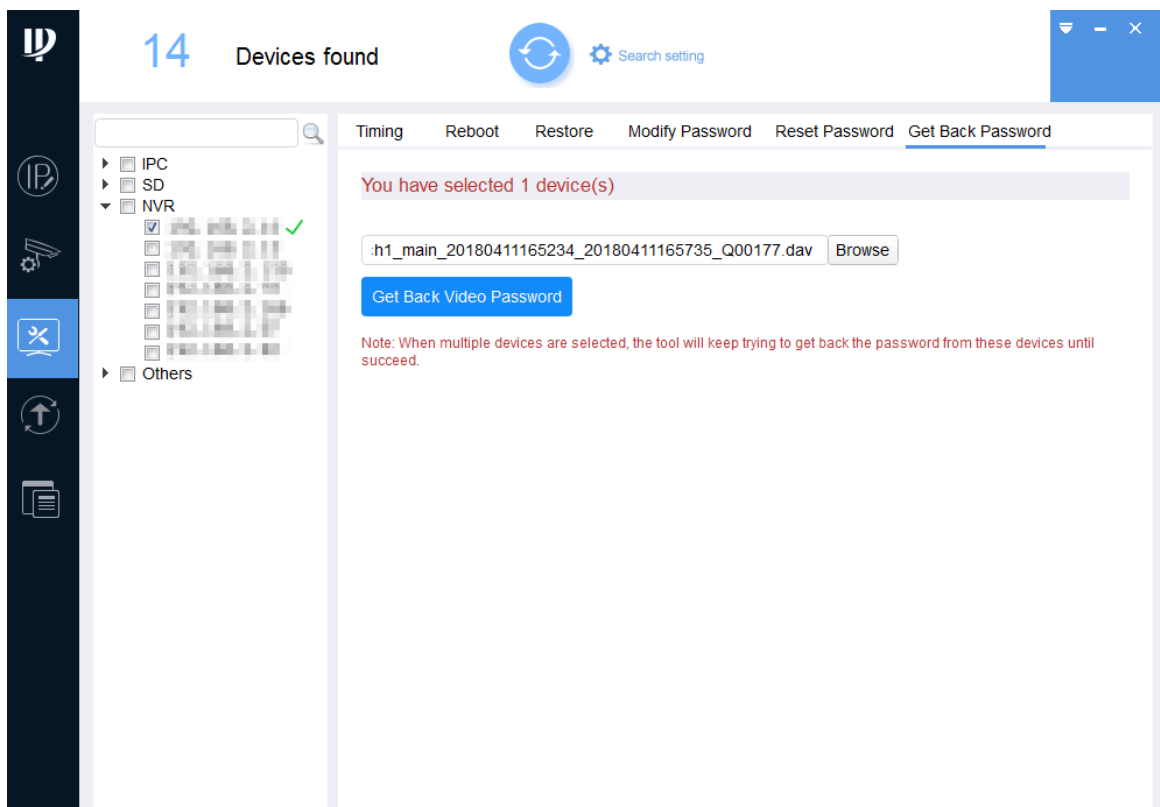


Step 7 Click **OK**.

The result is displayed next to the device after getting back video password is completed. See Figure 3-33.

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

Figure 3-33 Result



3.7 Resetting Device Password

You can reset the password through the quick response code (QR code) or XML file.



- NVR and DVR devices do not support this function.
- The password resetting operation can only be performed to the devices within the local area network.
- If you did not type the reserve information for password reset during device initializing, you can reset the password only through XML file.

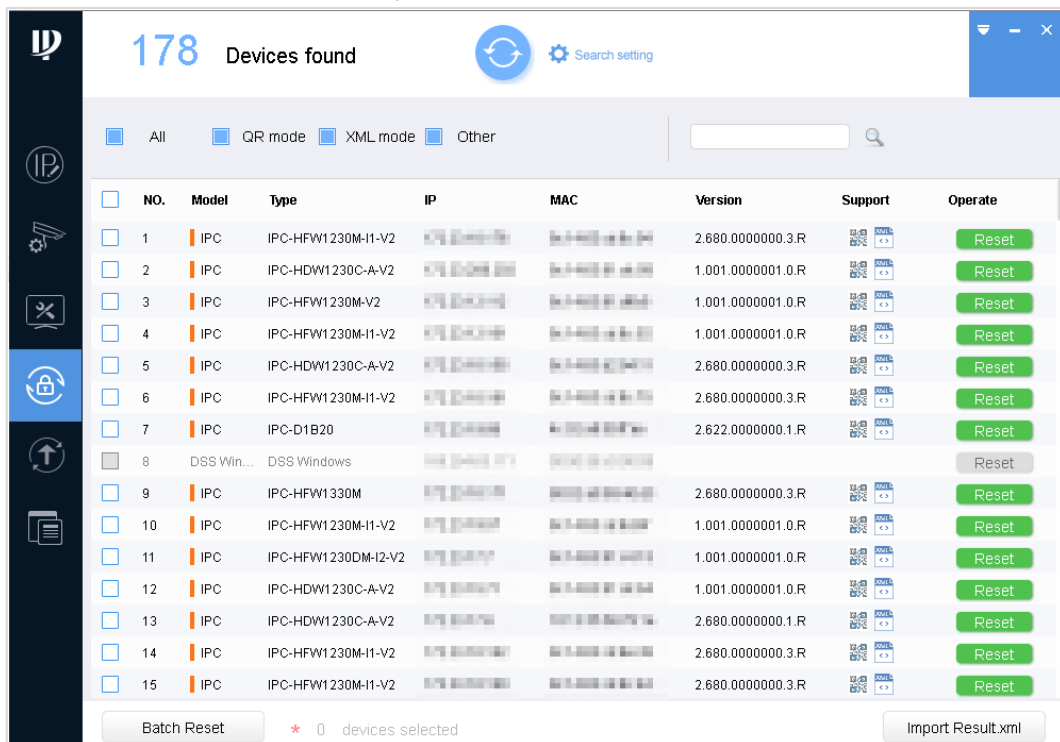
3.7.1.1.1 Using the QR Code

You can reset the password by scanning the QR code. This procedure is only applicable to a single device situation.

Step 1 Click .


The **Password Reset** interface is displayed. See Figure 3-34.

Figure 3-34 Password reset



Step 2 Select the device that needs to reset the password.



The supported formats are displayed in **Support**:  means QR code, and  means XML file.

Step 3 Click **Reset**.

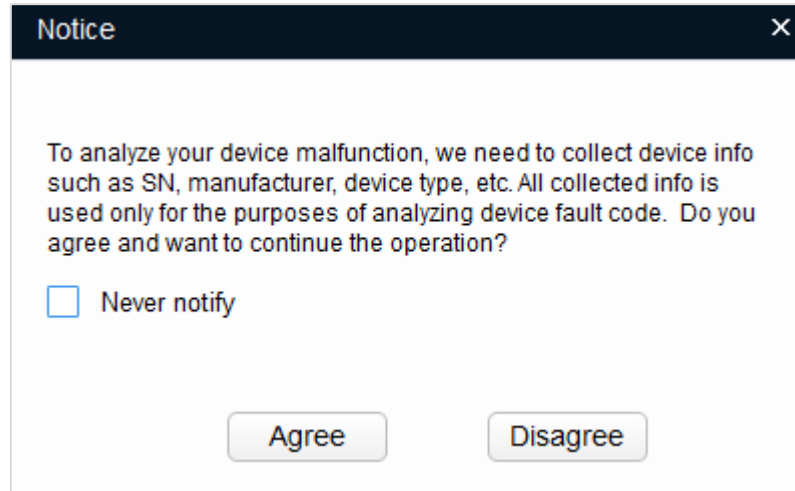
A **Notice** box will be displayed. See Figure 3-35.



- The interface might vary with different models, and the actual product shall prevail.

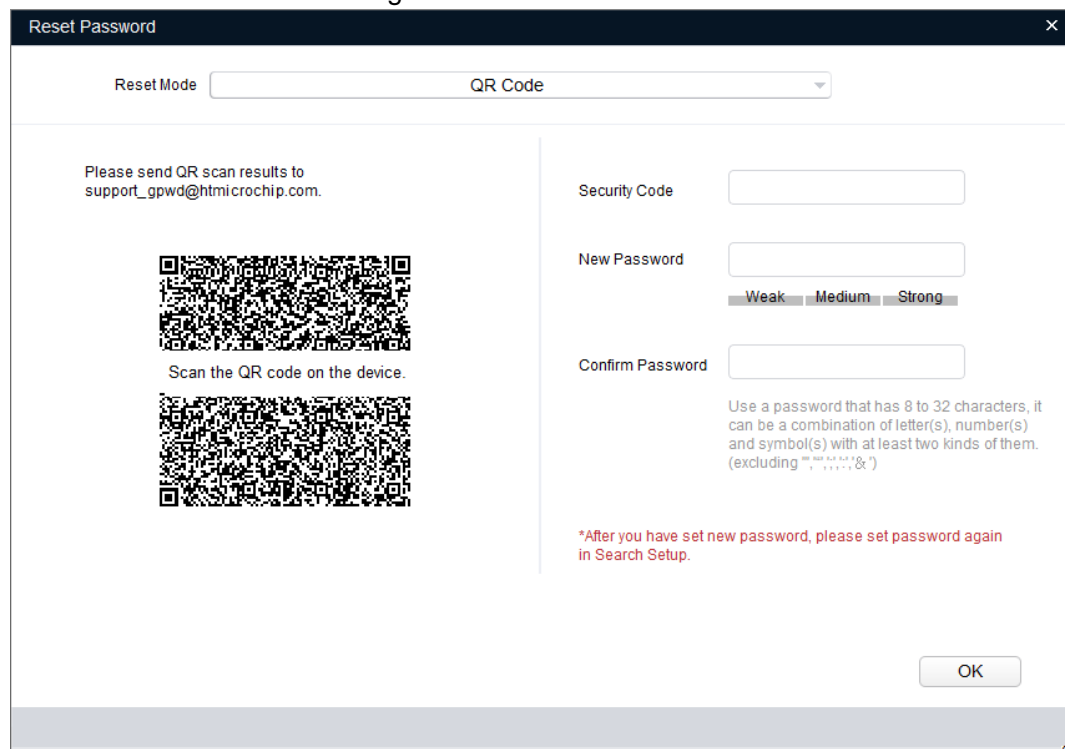
- If the device does not support this function, the reset button displays gray (Reset).
- If the device supports this function, the reset button displays green (Reset).

Figure 3-35 Notice



Step 4 Click **Agree**, the **Reset Password** interface is displayed. See Figure 3-36.

Figure 3-36 Reset Password



Step 5 Under **Reset Mode**, select **QR code**.

Step 6 Perform operations according to the instructions on the interface to obtain the security code.

Step 7 Enter old password, new password, and confirm password.



The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' ' ; : &).

Step 8 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.

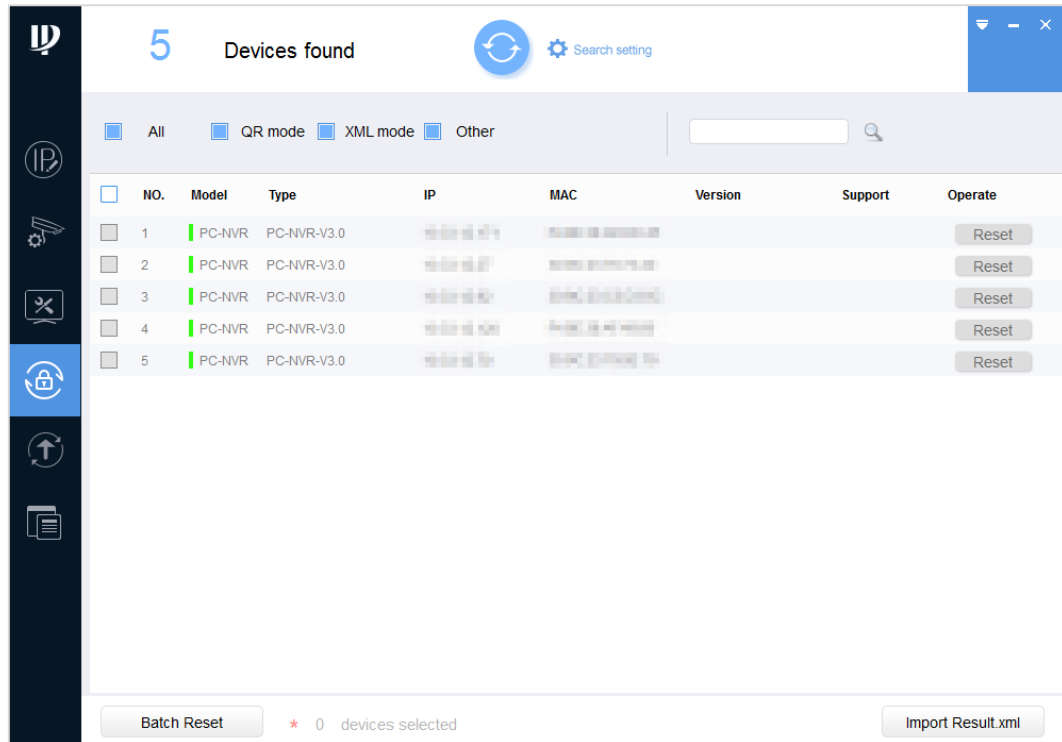
3.7.1.1.2 Using the XML File

You can reset the password by XML file for one device or multiple devices.

Step 1 Click .

The **Password Reset** interface is displayed. See Figure 3-37.

Figure 3-37 Device Password



Step 2 Select one device or multiple devices that need to reset the password.

Step 3 Click **Reset** or **Batch Reset**.

If the device does not support this function, a message is displayed to provide such indication. If the device supports this function, a **Notice** dialog box will be displayed. See Figure 3-38. Click **Agree**, the **Reset Password** interface is displayed. See Figure 3-39.



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

Figure 3-38 Notice

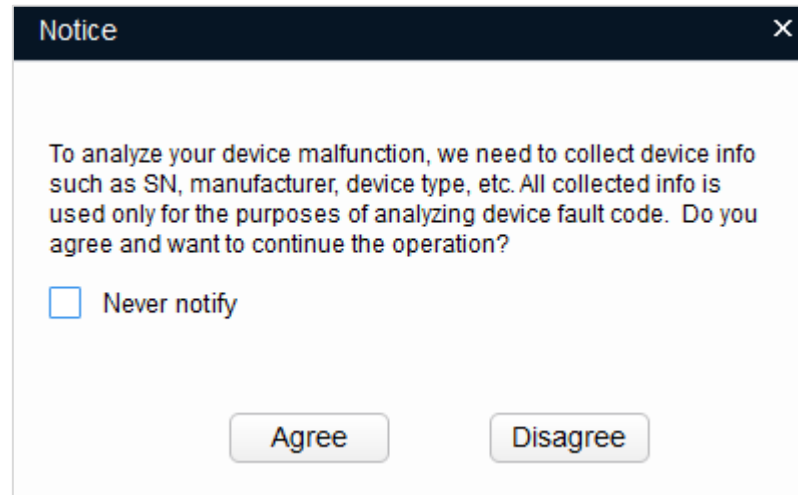
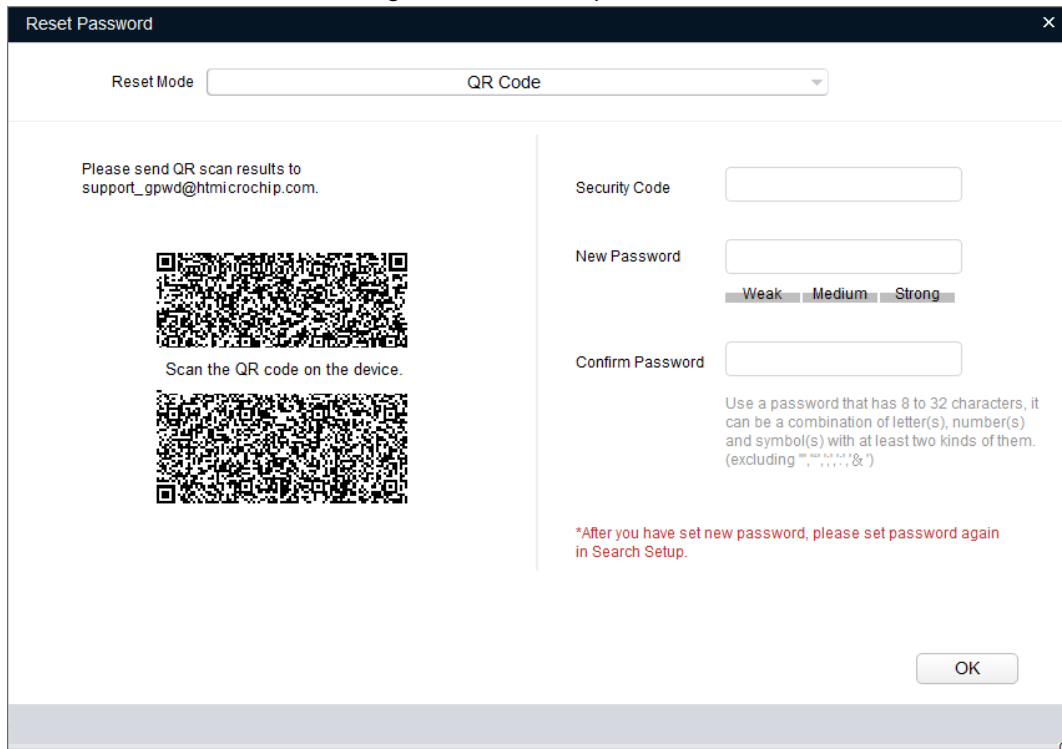


Figure 3-39 Reset password



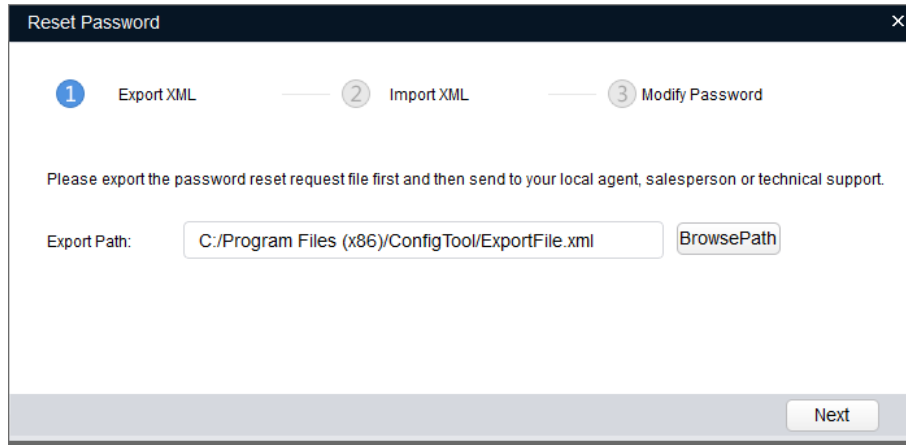
Step 4 Under **Reset Mode**, select **XML File**.

The **Reset Password-Export XML** interface is displayed. See Figure 3-40.



- The interface might vary with different models, and the actual product shall prevail.
- If you reset the passwords for multiple devices, the operation will be performed through the XML file interface supported by the first device in the list.

Figure 3-40 Reset password-export XML



Step 5 Export XML.

- 1) Click **Browse** to select the save path for the exported XML file.
 - 2) Click **Next** to start exporting.
After the exporting is completed, a **Notice** dialog box will be displayed.
 - 3) Click **OK** to complete exporting.
After completing exporting the XML, the import XML interface is displayed.
- Find the **ExportFile.xml** under the save path and send it as an attachment to the local technical support team. Then you will receive a **result.xml** file from the team.

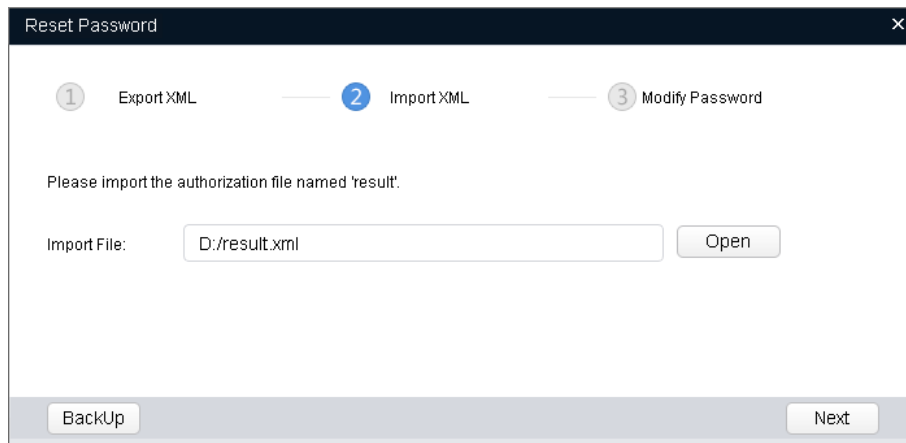
Step 6 Import XML.



If the **Reset Password-Import XML** interface is closed, select **System Settings > Reset Password**. On the **Reset Password** tab, click **Note: To reset password, please connect device to LAN of the host!** to continue the operation.

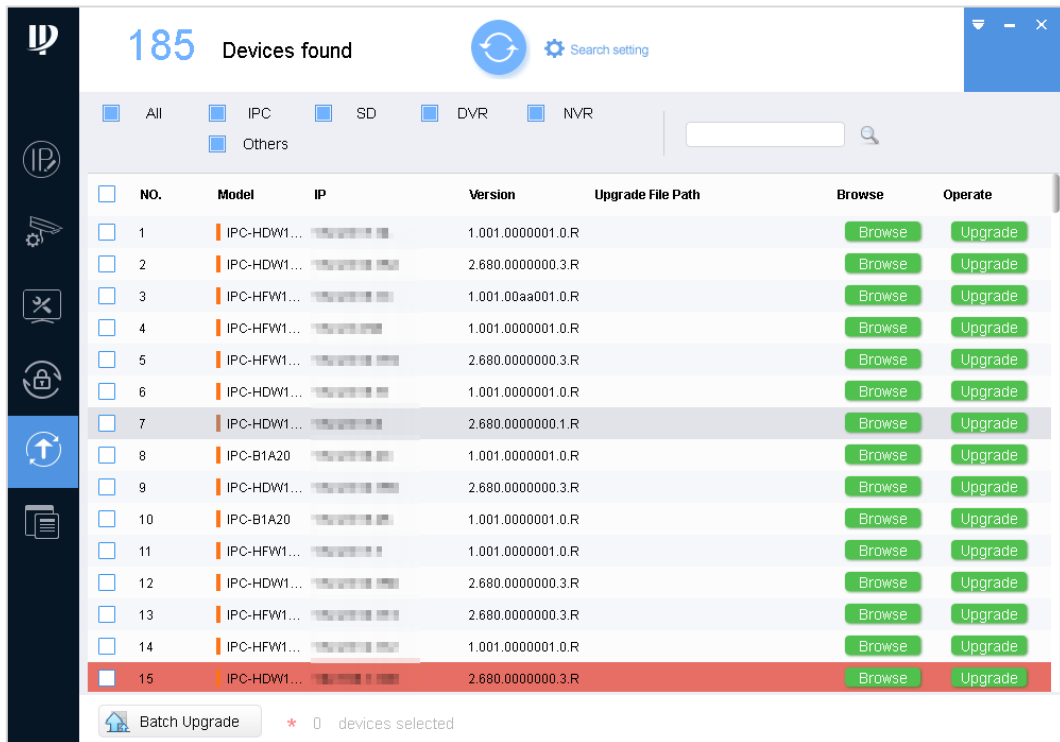
- 1) Click **Open** to import the **result.xml** file from the save path. See Figure 3-41.

Figure 3-41 Reset password



- 2) Click **Next** to start importing.
After completing exporting the XML, the **Reset Password-Modify Password** interface is displayed. See Figure 3-42.

Figure 3-43 Upgrade



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



If the device is not in the device list, perform searching again. For the details about how to search devices, see "3.2 Adding Devices."

Step 3 Click **Upgrade** to start upgrading.

After upgrading is completed, a **Notice** dialog box will be displayed indicating the device will be rebooted. Then the device reboots automatically.

3.8.2 Upgrading Devices in Batches

You can upgrade multiple devices to the same software version.

Step 1 Click .

The **Upgrade** interface is displayed.

Step 2 Select the devices that need to be upgraded.

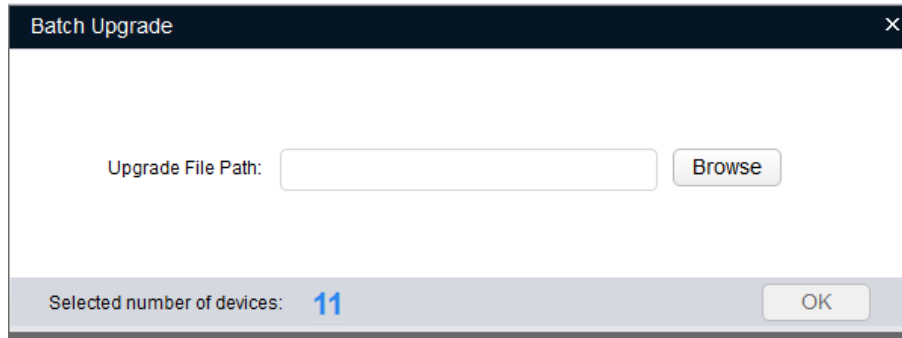


- If the device is not in the device list, perform searching again. For the details about how to search devices, see "3.2 Adding Devices."
- Make sure the selected devices are subject to be upgraded to the same software version.

Step 3 Click  **Batch Upgrade**.

The **Batch Upgrade** dialog box is displayed. See Figure 3-44.

Figure 3-44 Batch Upgrade

A dialog box titled "Batch Upgrade" with a close button (X) in the top right corner. It contains a text input field labeled "Upgrade File Path:" followed by a "Browse" button. At the bottom, there is a status bar showing "Selected number of devices: 11" and an "OK" button.

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


Step 5 Click **OK** to start upgrading.

3.9 Online Upgrade

You can download upgrade package from the upgrade server to upgrade the device.

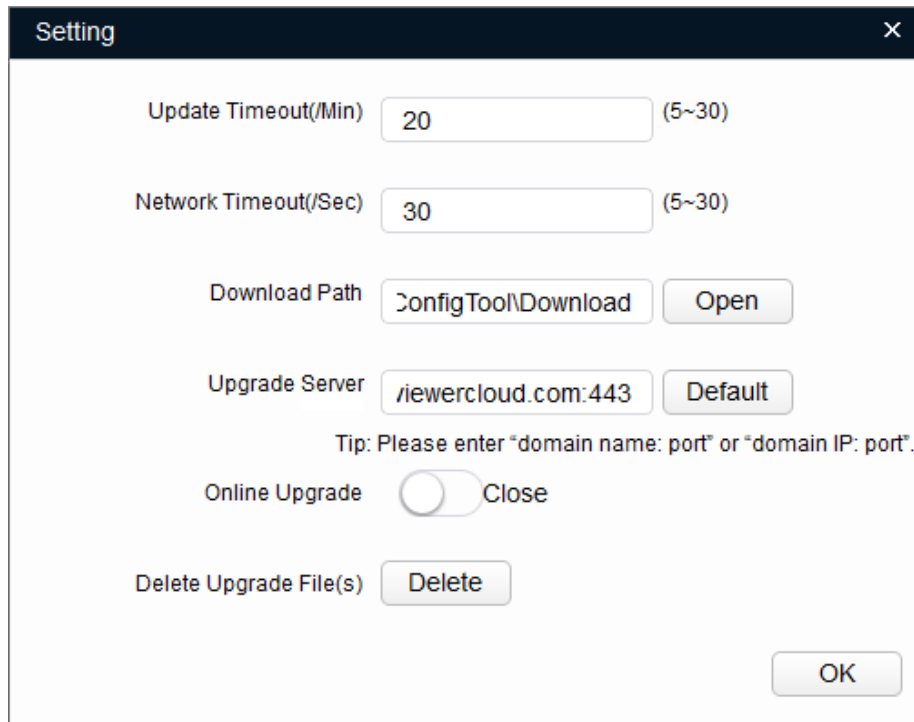
3.9.1 Enabling Online Upgrade

The online upgrade is hidden by default and you need to manually enable it.

Step 1 On the main user interface, click , and then select **Setting**.

The **Setting** interface is displayed. See Figure 3-45.

Figure 3-45 Setting

A dialog box titled "Setting" with a close button (X) in the top right corner. It contains several configuration options: "Update Timeout(/Min)" with a value of 20 and a range of (5~30); "Network Timeout(/Sec)" with a value of 30 and a range of (5~30); "Download Path" with a text field containing "ConfigTool\Download" and an "Open" button; "Upgrade Server" with a text field containing "viewercloud.com:443" and a "Default" button; a tip message "Tip: Please enter 'domain name: port' or 'domain IP: port'."; "Online Upgrade" with a toggle switch currently turned off and labeled "Close"; and "Delete Upgrade File(s)" with a "Delete" button. An "OK" button is located at the bottom right.

Step 2 Set the system parameters. See Table 3-11.

Table 3-11 Online upgrade parameters

Parameter	Description
Update Timeout (/Min)	The maximum updating time for a single device. When the updating time is longer than the set value, the updating fails.
Network Timeout (/Sec)	The maximum time for network connecting during device updating. When the network connecting time is longer than the set value, the updating stops.
Download Path	The save path for saving the upgrade package downloaded from upgrade server. Click Open to set the save path.
Upgrade Server	The default address for upgrade server. The upgrade server bases on device information to detect whether there is a new version. It is recommended to keep the default address, unless you have deployed another standalone upgrade server within the LAN.
Delete Upgrade File(s)	Click Delete to delete upgrade files in the download directory.

Step 3 Enable **Online Upgrade**. See Figure 3-46.

Figure 3-46 Enable

Step 4 Click **OK** to complete setting.


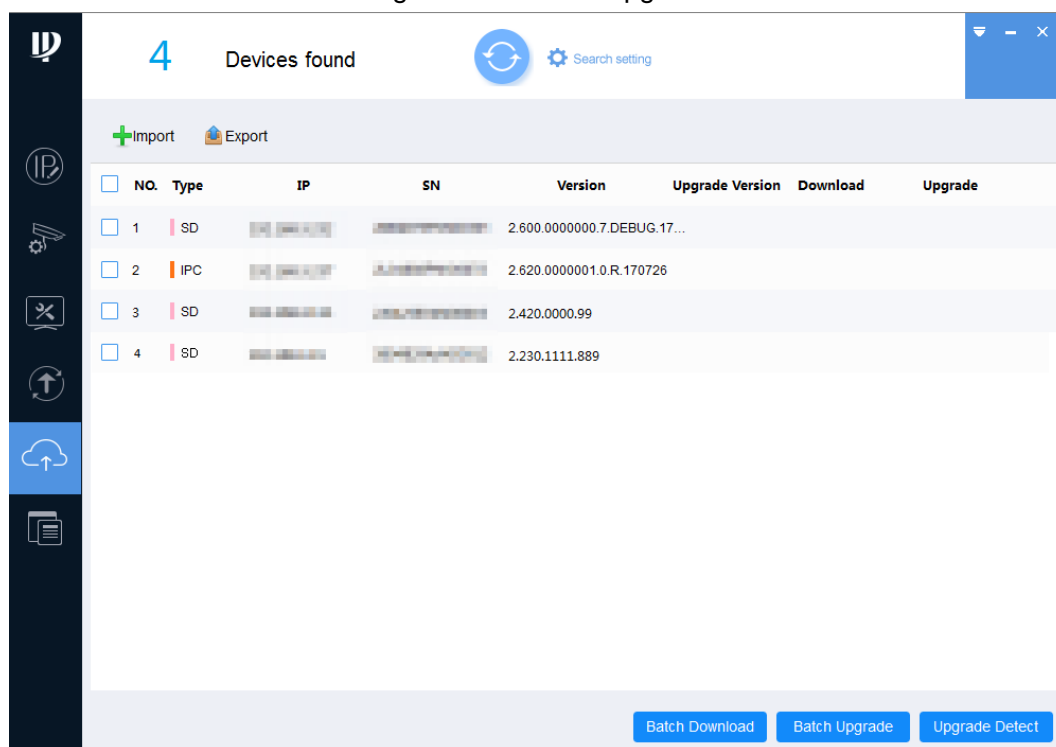
The online upgrade icon () appears in the menu. The searched devices are display on the online upgrade interface. See Figure 3-47.

Figure 3-47 Online upgrade



3.9.2 Performing Online Upgrade



The online upgrade operation such as detecting, downloading, and upgrading, can affect the normal operation of other functions of the Tool. For example, if you modify IP, a notice is displayed indicating **Detecting, please wait...**

According to the network features of the PC where the Tool is located and the detected devices the online upgrade operation is divided into synchronous operation and asynchronous operation. Select the upgrade method according to the actual needs.

- Synchronous operation means that you can complete the upgrade detection, upgrade package download and upgrade on the PC where the Tool is located. The applications are as follows:
 - ◇ The PC where the Tool is located and the detected devices have accessed the Internet.
 - ◇ The PC where the Tool is located and the detected devices are located in the same LAN, and the PC has double network card that can access the Internet at the same time.
 - ◇ The PC where the Tool is located and the detected devices are located in the same LAN, and you can change the PC cable to access the Internet.
- Asynchronous operation means that you cannot complete the upgrade operation on the PC where the Tool is located, and you need to migrate the data. The application is as follows:
 - ◇ The PC where the Tool is located and the detected devices are located on the same LAN and neither of them can access the Internet. You can download the upgrade package through the Tool on another PC connected to the Internet.

3.9.2.1 Performing Synchronous Operation

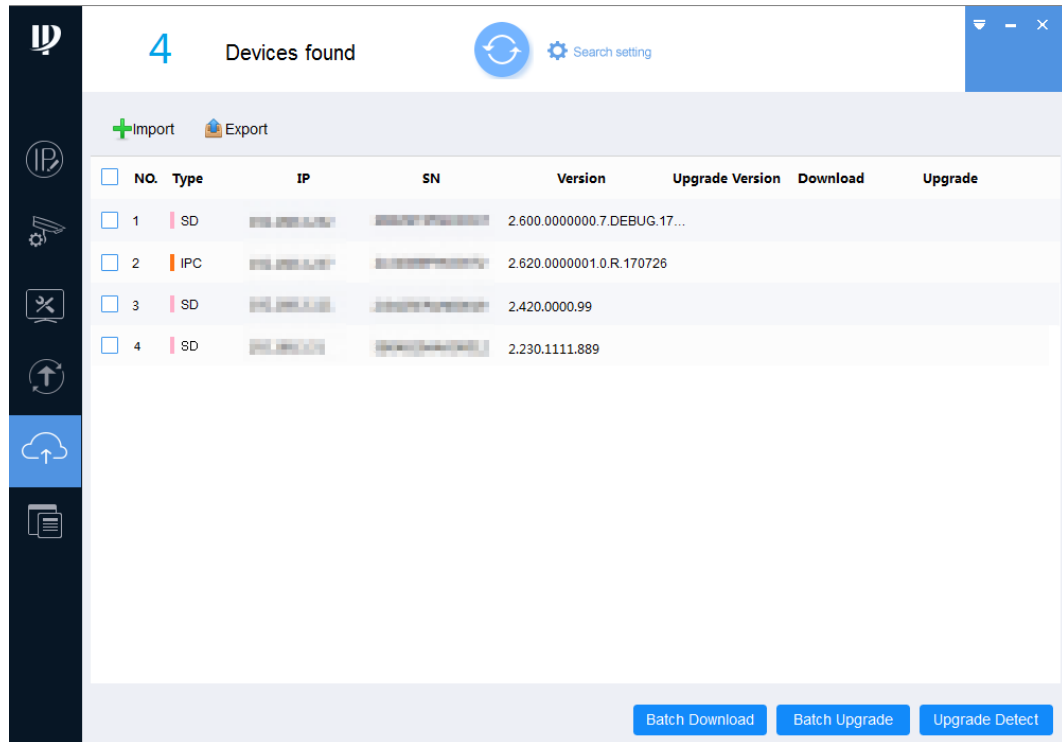


Confirm that the PC where the Tool is located has accessed the Internet.

Step 1 Click .

The online upgrade interface is displayed. See Figure 3-48.

Figure 3-48 Online upgrade



Step 2 Select one or multiple devices.



If the device is not in the device list, perform searching again. For the details about how to search devices, see "3.2 Adding Devices."

Step 3 Click **Upgrade Detect**.

A **Notice** interface is displayed. See Figure 3-50. Click **Agree**, the **Download** button is displayed after the detection is completed. See Figure 3-49.



After clicking **Upgrade Detect**, the button changes to **Stop Checking**. Click **Stop Checking** to stop version detection for all devices.

Figure 3-49 Notice

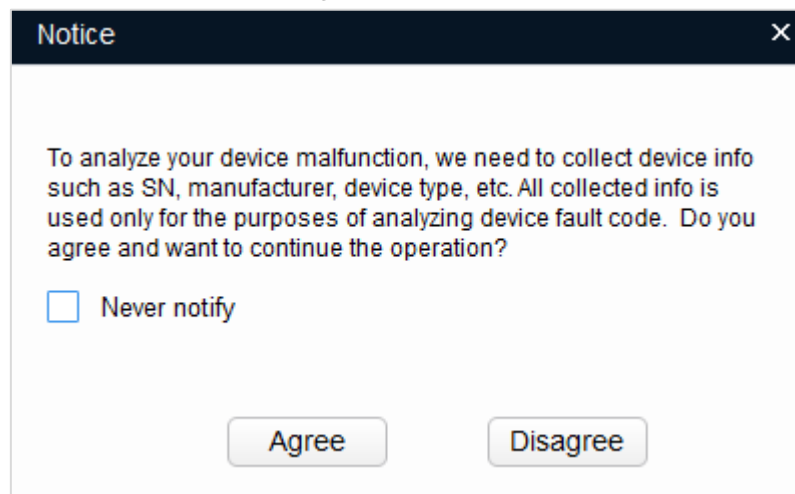
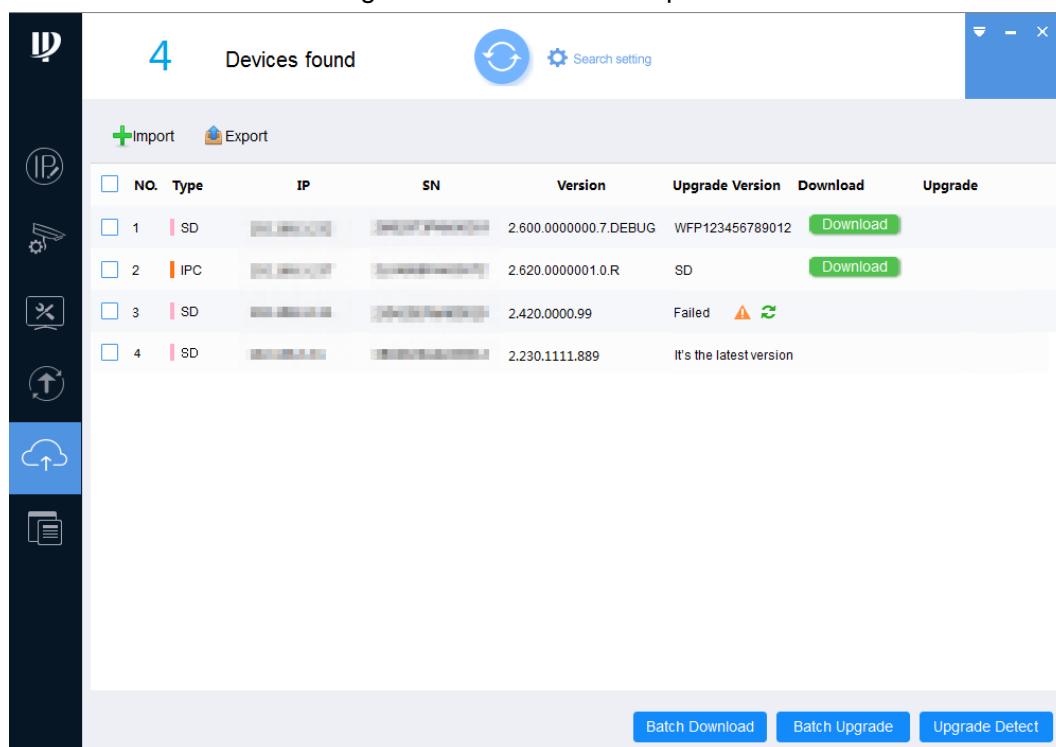



Figure 3-50 Detection completed



If the detection is successful, skip Step 4.

Step 4 Click  to see the details for the failed detection individually.

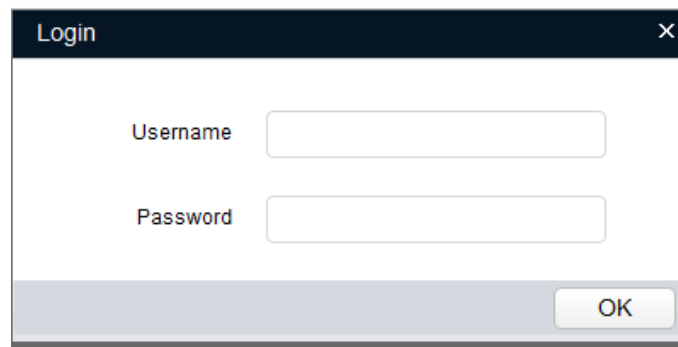
The **Details** interface is displayed.


- If the **Config Result** shows **Connection failed** or **network error, maybe timeout**, please perform upgrade detection again.
- If the **Config Result** shows **Incorrect password**, please perform the following steps:

- 1) Click .

The **Login** interface is displayed. See Figure 3-51.

Figure 3-51 Login

A login dialog box with a dark blue title bar containing the text 'Login' and a close button (X). The main area is white and contains two input fields: 'Username' and 'Password'. Below the 'Password' field is an 'OK' button.

- 2) Enter the user name and password for the device.
- 3) Click **OK** to start automatic detection.
 - ◇ If succeeded, the **Download** button will display in the **Download** column when there is an upgraded version; and the **Upgrade Version** column will show **It's the latest version** when no upgrade is available.
 - ◇ If failed, click  to see the details. If the **Config Result** still shows **Incorrect password**, please obtain the correct user name and password and repeat the above steps.



If the password error occurs for multiple times, the user account will be locked.

- If the **Config Result** shows information other than the previous two cases, follow the prompts.

Step 5 Download the upgrade package.

- Download one upgrade package: Click **Download** next to the device that you want to upgrade.
- Download upgrade packages in batches: Select the devices with the **Download** button, and then click **Batch Download**.

A **Notice** box will be displayed. See Figure 3-52. Click **Agree**, the **Upgrade** button is displayed after the downloading is completed. See Figure 3-53.



After clicking **Batch Download**, the button changes to **Stop Downloading**. Click **Stop Downloading** to stop downloading the upgrade package for all devices.

Figure 3-52 Notice

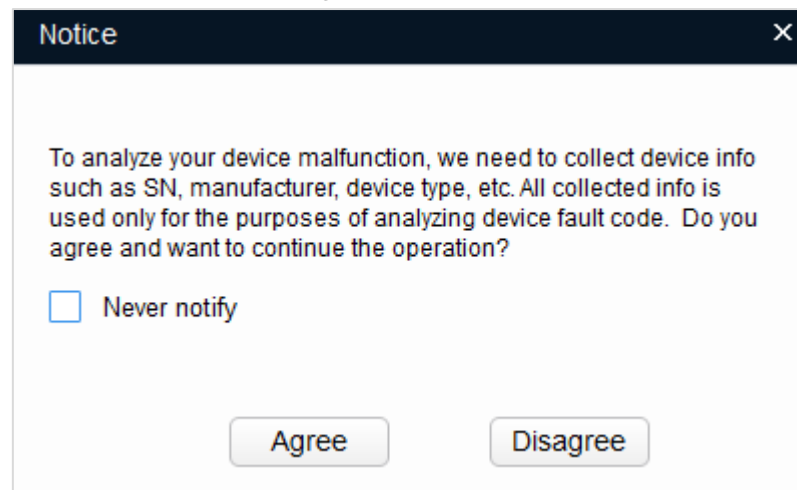
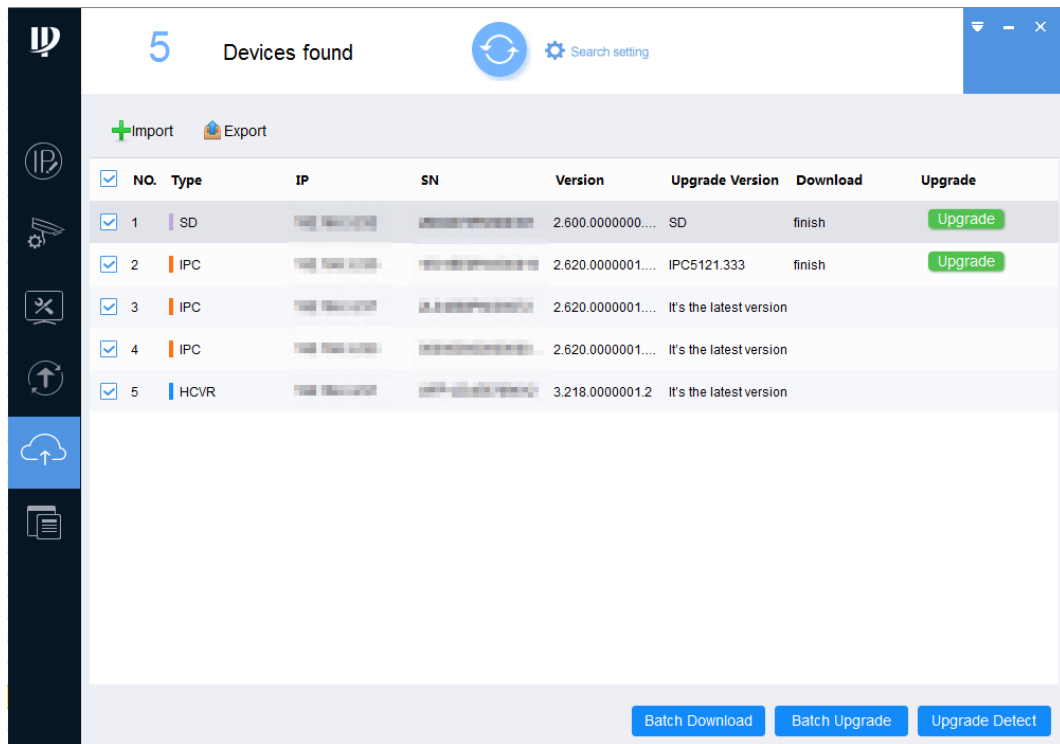
A notice dialog box with a dark blue title bar containing the text 'Notice' and a close button (X). The main area is white and contains the following text: 'To analyze your device malfunction, we need to collect device info such as SN, manufacturer, device type, etc. All collected info is used only for the purposes of analyzing device fault code. Do you agree and want to continue the operation?'. Below this text is a checkbox labeled 'Never notify'. At the bottom are two buttons: 'Agree' and 'Disagree'.

Figure 3-53 Upgrade package downloading completed



Step 6 Upgrade device.

Upgrade one device: Click **Upgrade** next to the device that you want to upgrade.

Upgrade devices in batches: Select the devices with the **Upgrade** button, and click **Batch Upgrade**.

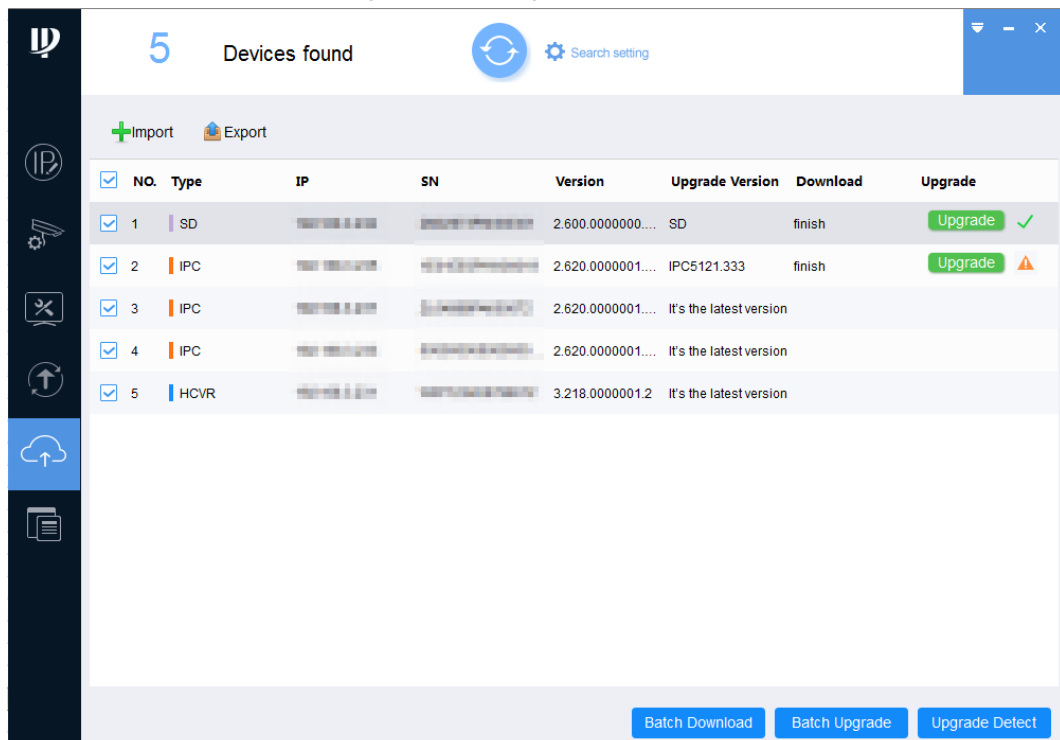


After clicking **Batch Upgrade**, the button changes to **Stop Upgrading**. Click **Stop Upgrading** to stop upgrading for all devices.

The upgrade result is displayed after the upgrading is completed. See Figure 3-54.

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

Figure 3-54 Upgrade completed



3.9.2.2 Performing Asynchronous Operation

Prerequisite:

- Asynchronous operation is applicable to the situation that PC (hereinafter referred to be "PC1") where the Tool is located and the detected devices are located on the same LAN and neither of them can access the Internet. Please prepare another PC (hereinafter referred to be "PC2") that has accessed the Internet and installed the Tool.
- Make sure the user name and password of devices for the asynchronous operation are the same; otherwise the upgrade will fail.



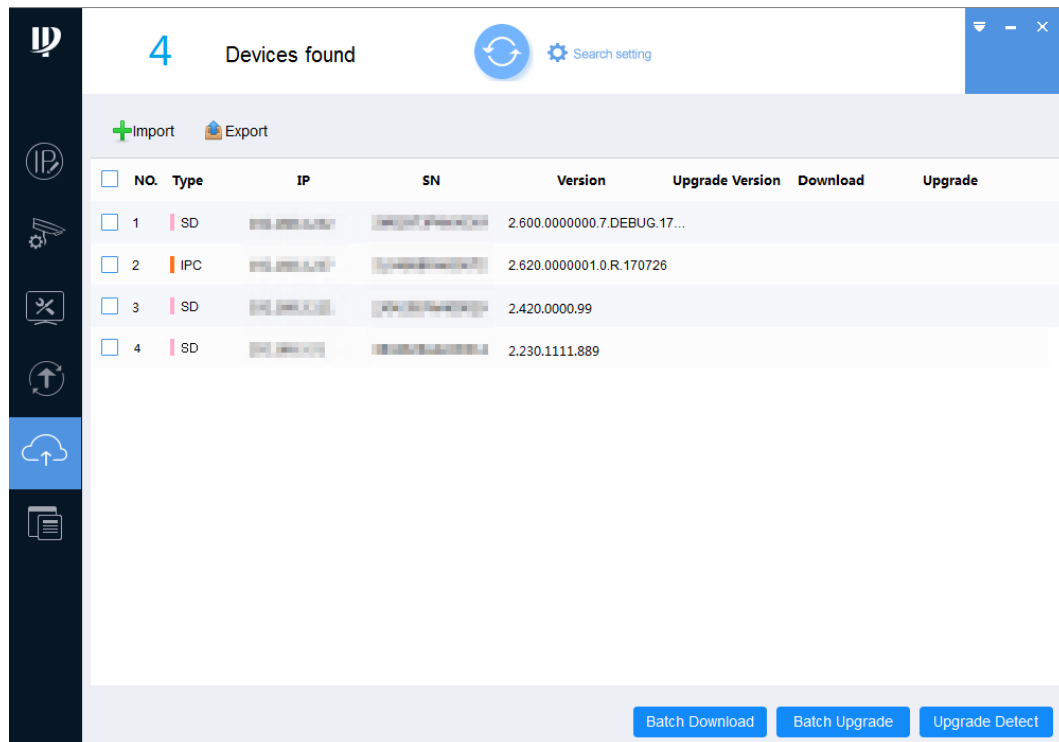
The import and export file types mentioned in this section support only **.7z** format.

Exporting PC1 Device Information

Step 1 On the main interface on PC1, click .

The online upgrade interface is displayed. See Figure 3-55.

Figure 3-55 Online upgrade



Step 2 Select one or multiple devices.



If the device is not in the device list, perform searching again. For the details about how to search devices, see "3.2 Adding Devices."



Click **Upgrade Detect** to obtain device information. If you ignore this step and export device information directly, the upgrade detection will fail on the PC2.

Step 3 Click **Upgrade Detect**.

A **Notice** box is displayed. See Figure 3-56. Click **Agree**, the detection result is displayed after the detection is completed. See Figure 3-57.



After clicking **Upgrade Detect**, the button changes to **Stop Detecting**. Click **Stop Detecting** to stop version detection for all devices.

Figure 3-56 Notice

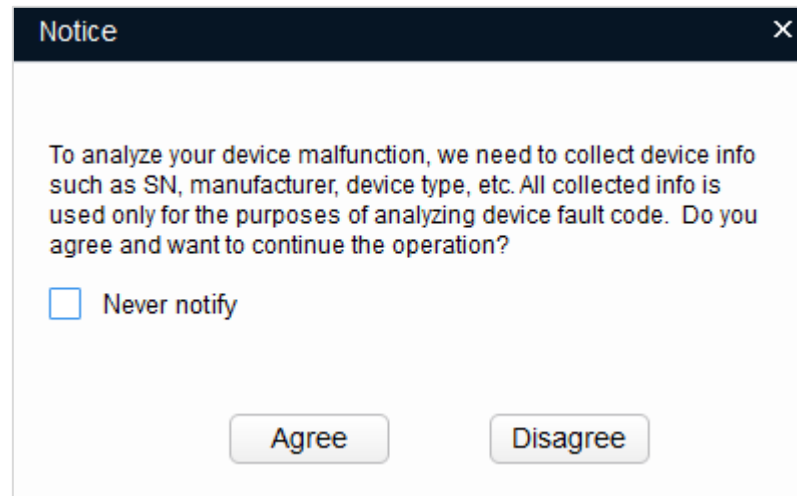
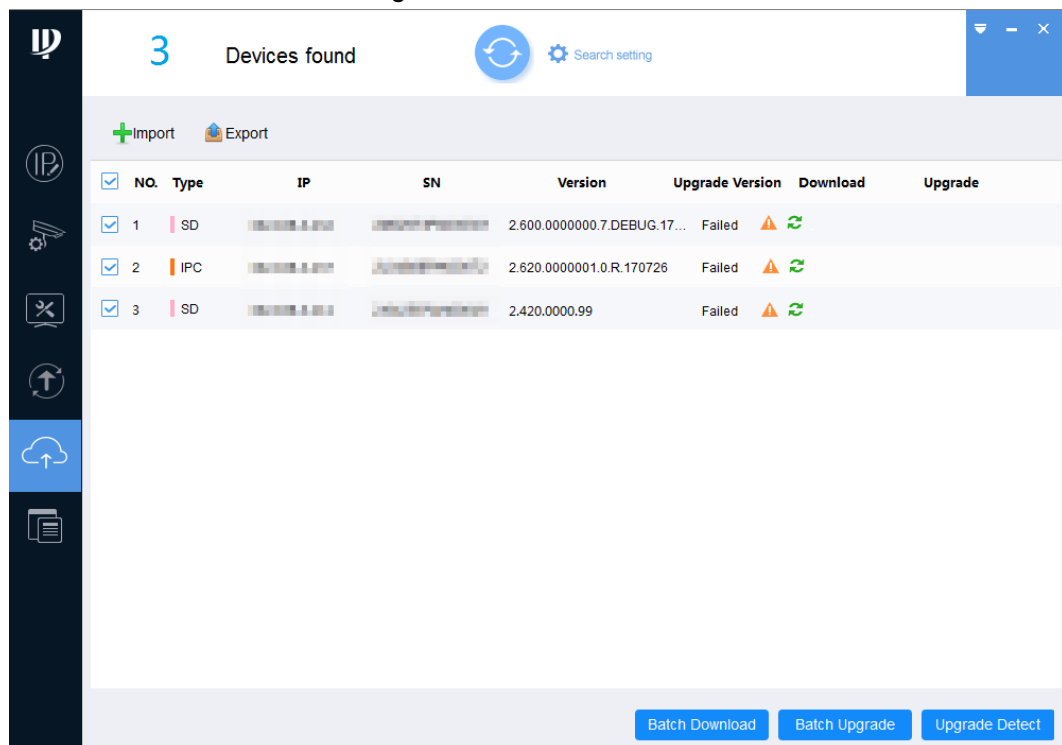


Figure 3-57 Detection result



Step 4 Click ⚠️ to see the details for the failed detection individually.


The **Details** dialog box is displayed.

- If the **Config Result** shows **Connection failed** or **network error, maybe timeout**, you can export devices information by going to Step 5.
- If the **Config Result** shows **Incorrect password**, you cannot export devices information at once but need to perform the following steps first:

- 1) Click ⚙️ [Search setting](#).

The **Setting** dialog box is displayed.

- 2) Enter the user name and password for the device.

- 3) Click **OK** to search device.
- 4) After search is completed, click **Upgrade Detect** again.
After detection is completed, click  to see the details. If the **Config Result** no longer shows **Incorrect password**, you can export devices information according to Step 5. Otherwise, obtain the correct user name and password and repeat the above steps.



If the password error occurs for multiple times, the user account will be locked.

- If the **Config Result** shows information other than previous the two cases, follow the prompts.

Step 5 Click  **Export**.

The **Save as** dialog box is displayed.

Step 6 Select save path, enter **File name**, and then click **Save** to start exporting device information file.

The **Notice** dialog box is displayed after the exporting is completed.

Step 7 Click **OK**.

Importing PC1 Device Information into PC2

Step 1 Copy the exported file from PC1 to PC2 by storage devices such as a USB flash disk.

Step 2 Import PC1 device information into PC2.


- 1) Start the Tool, click  on the main interface and then select **Setting**.
The **Setting** interface is displayed.
- 2) Enable **Online Upgrade**. See Figure 3-58.

Figure 3-58 Enable online upgrade

The screenshot shows a 'Setting' dialog box with the following fields and controls:

- Update Timeout(/Min)**: Input field with value '20' and range '(5~30)'.
- Network Timeout(/Sec)**: Input field with value '30' and range '(5~30)'.
- Download Path**: Input field with value 'ConfigTool\Download' and an 'Open' button.
- Upgrade Server**: Input field with value '/iewercloud.com:443' and a 'Default' button.
- Tip**: Please enter "domain name: port" or "domain IP: port".
- Online Upgrade**: A toggle switch is turned on (blue) and is highlighted with a red rectangle. The label 'Open' is next to it.
- Delete Upgrade File(s)**: A 'Delete' button.
- OK**: A button at the bottom right.

- 3) Click **OK**.
The **Online upgrade** interface is displayed.

- 4) Click  **Import**.

The **Open** dialog box is displayed.

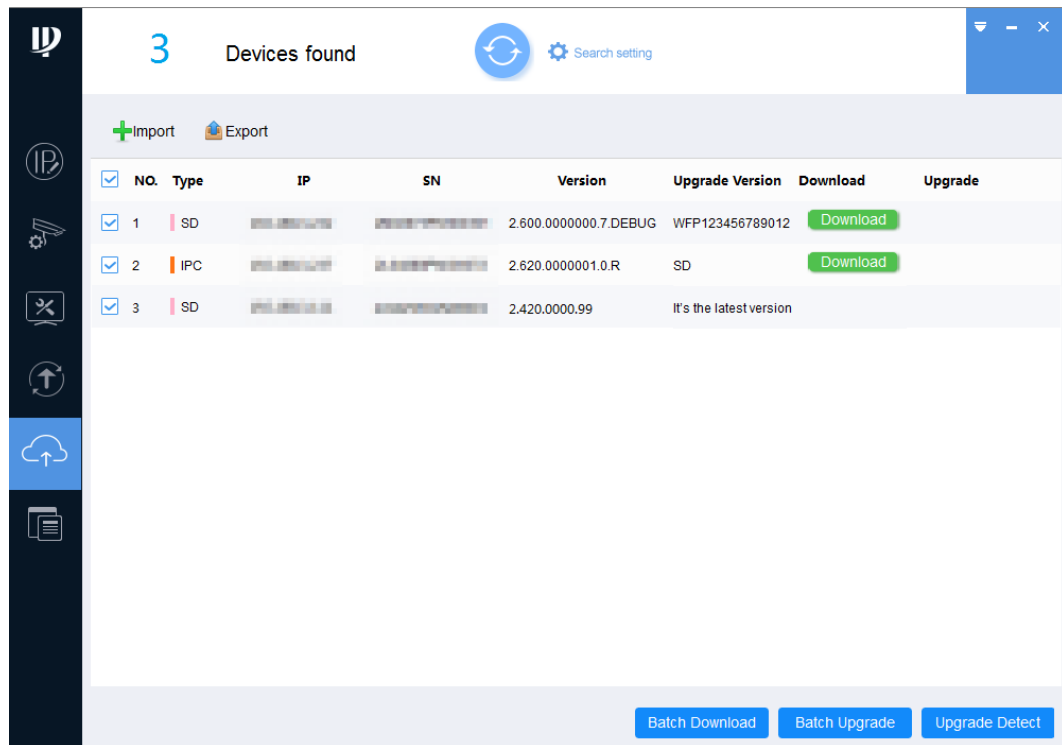
- 5) Select the exported file from PC1 and then click **Open** to start importing file.

The **Notice** dialog box is displayed after the importing is completed.

- 6) Click **OK** to start automatic detection.

The **Download** button is displayed after the detection is completed. See Figure 3-59.

Figure 3-59 Import completed



Downloading and Exporting Upgrade Package on PC2

Step 1 Select one or multiple devices on the interface shown in Figure 3-59.

Step 2 Download the upgrade package.

- Download one upgrade package: Click **Download** next to the device that you want to upgrade.
- Download upgrade packages in batches: Select the devices with the **Download** button, and then click **Batch Download**.

A **Notice** box is displayed. See Figure 3-60. Click **Agree**, the **Upgrade** button is displayed after the downloading is completed. See Figure 3-61.



After clicking **Batch Download**, the button changes to **Stop Downloading**. Click **Stop Downloading** to stop downloading the upgrade package for all devices.

Figure 3-60 Notice

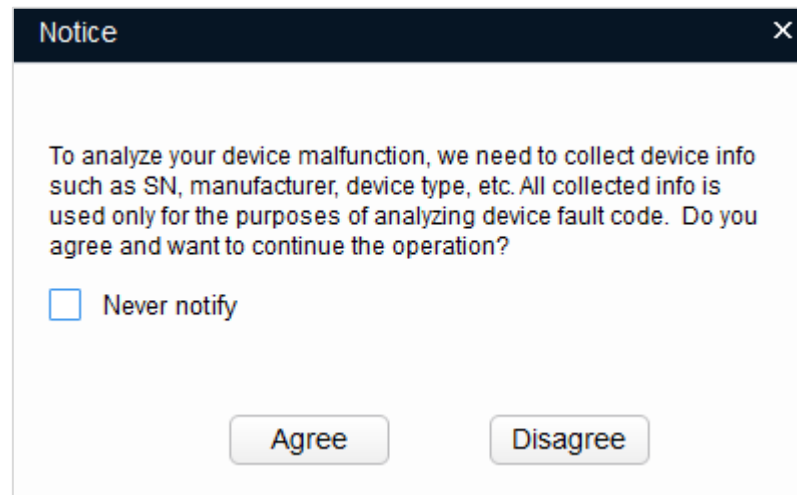
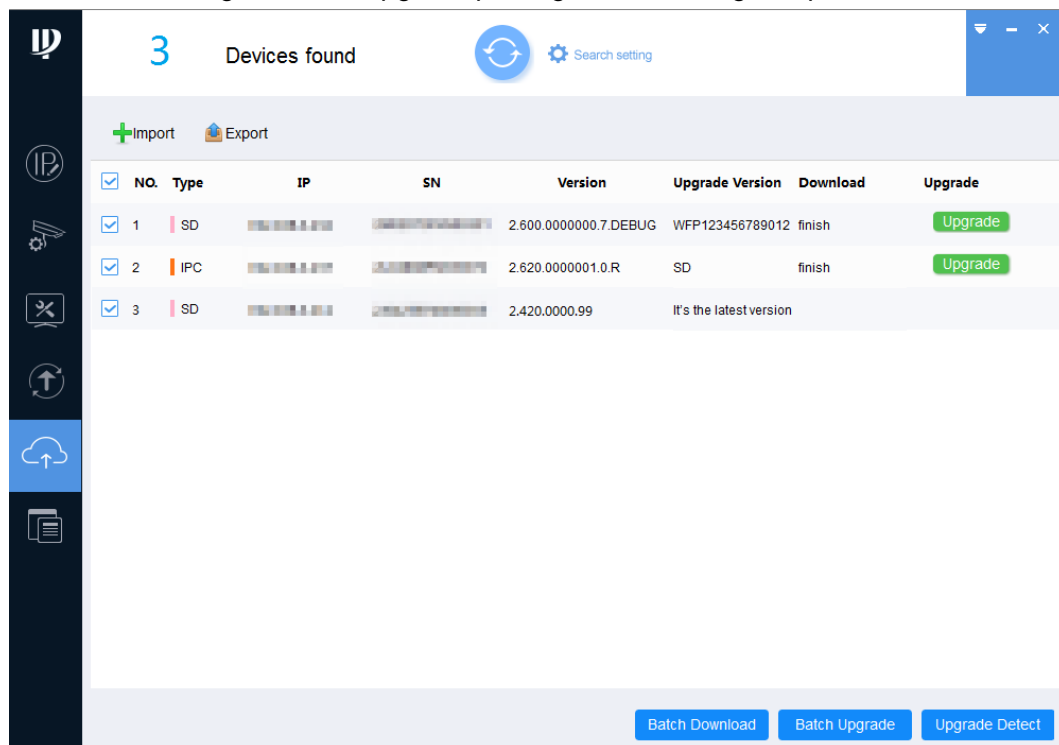


Figure 3-61 Upgrade package downloading completed



Step 3 Click **Export**.

The **Save as** dialog box is displayed.

Step 4 Select save path, enter **File name** and then click **Save** to start exporting file.

The **Notice** dialog box is displayed after the exporting is completed.

Step 5 Click **OK**.

Importing PC2 Upgrade Package into PC1

Step 1 Migrate the exported upgrade package from PC2 to PC1 by storage devices such as a USB flash disk.

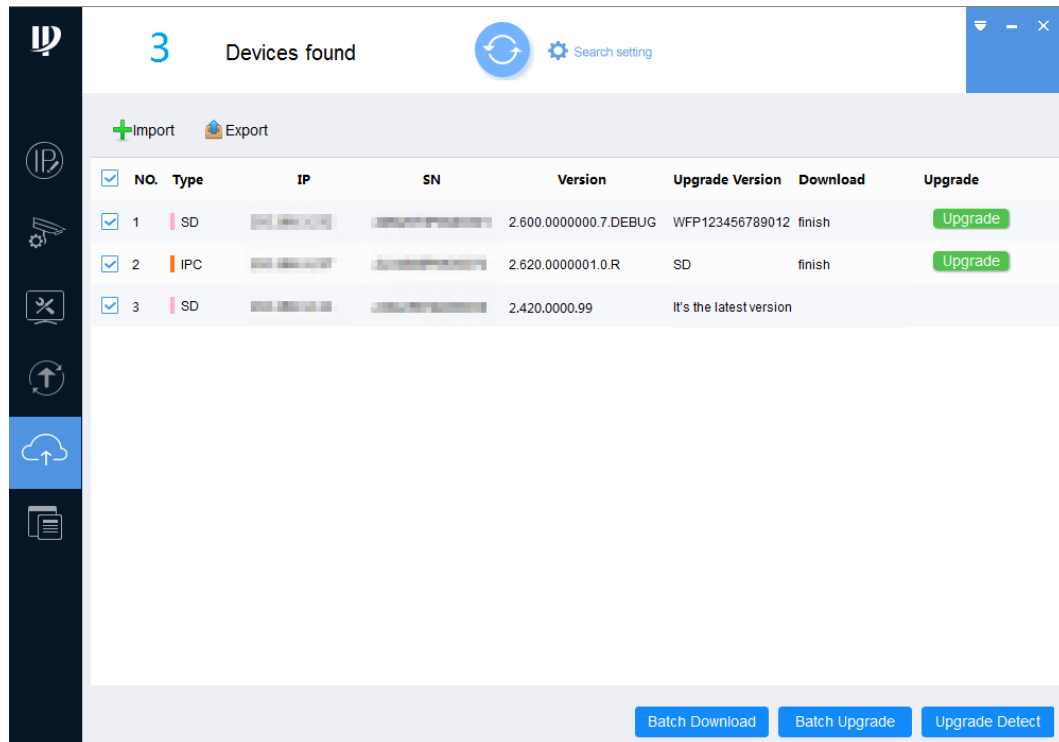
Step 2 Upgrade devices on PC1.

1) On **Online upgrade** interface of The Tool, click .

The **Open** dialog box is displayed.

- 2) Select the upgrade package file and click **Open** to start importing the file.
The **Notice** dialog box is displayed after the importing is completed.
- 3) Click **OK**. See Figure 3-62.

Figure 3-62 File import Completed



- 4) Upgrade device.
 - ◇ Upgrade one device: Click **Upgrade** next to the device that you want to upgrade.
 - ◇ Upgrade devices in batches: Select the devices with the **Upgrade** button, and then **Batch Upgrade**.

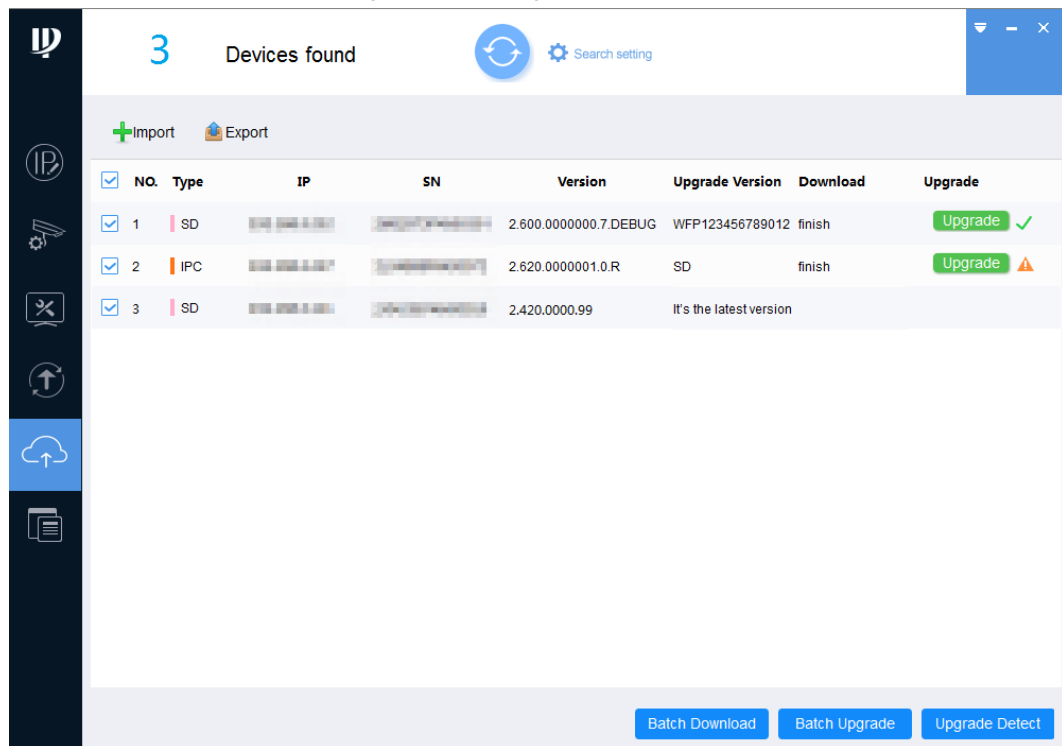


After clicking **Batch Upgrade**, the button changes to **Stop Upgrading**. Click **Stop Upgrading** to stop upgrading for all devices.

The result is displayed next to the device after the upgrading is completed. See Figure 3-63.

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

Figure 3-63 Upgrade completed



3.10 Configuring the Template

You can create and apply the templates.

- Creating the template: Back up or save the video and encoding parameters for the device.
- Applying the template: Restore or batch configuring the video and encoding parameters for the device.

3.10.1 Creating a Template

You can create a template through manual configuration or exporting a device template.

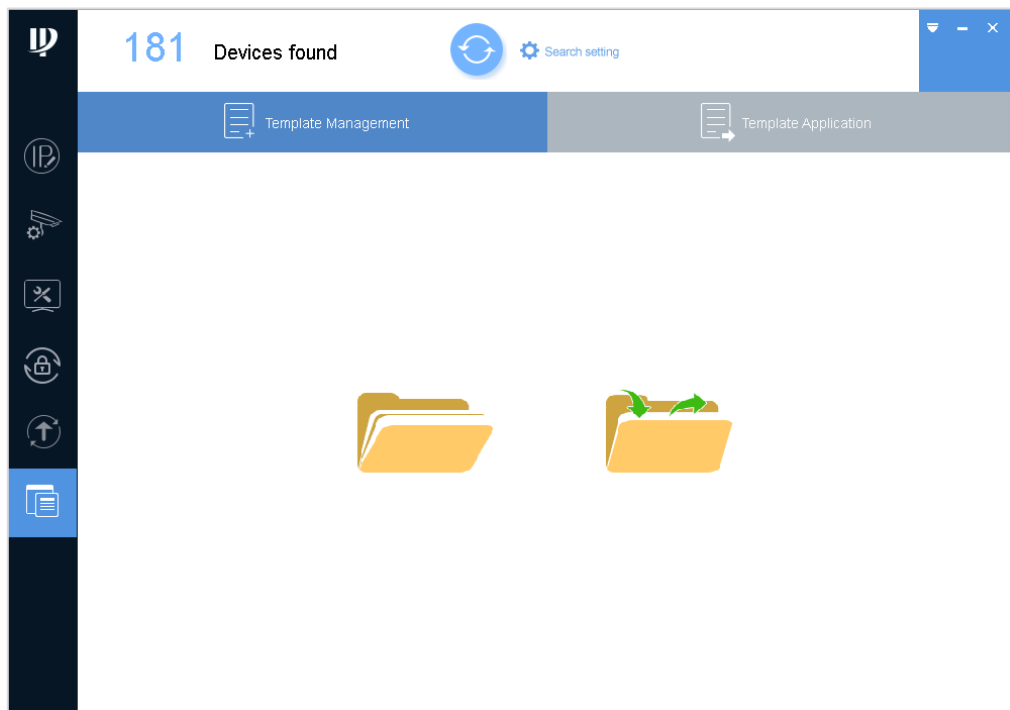
3.10.1.1 Manual Configuration

You can customize the template according to your actual needs.

Step 1 Click .

The **Template Setup** interface is displayed. See Figure 3-64.

Figure 3-64 Template setup



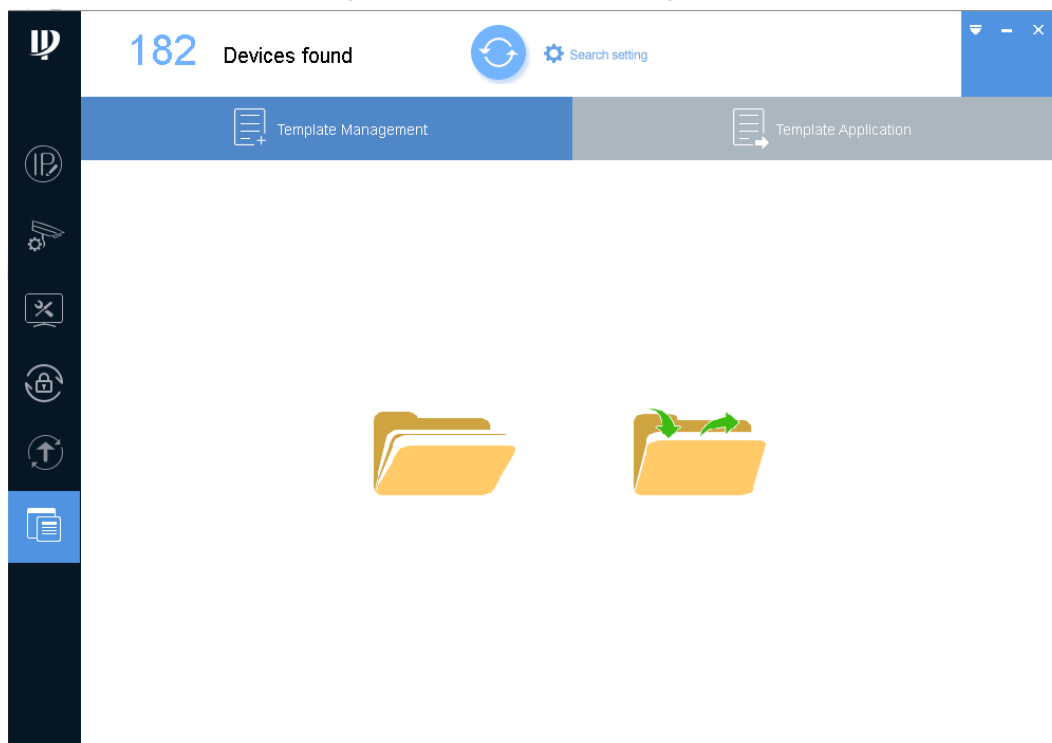
Step 2 Manually configure the template.

- 1) Click .

The **Load Template** dialog box is displayed. Click **OK**.

The **Template Management** interface is displayed. See Figure 3-65.

Figure 3-65 Template management




- 2) On the **Template Management** interface, select the template type, enter the template name, and then set the parameters accordingly. See Table 3-12.



After the template configuration is completed, click **Apply** to apply the template to the device. For the details about how to apply the template, see "3.10.2 Applying the Template."

Table 3-12 Template management parameters

Parameter	Description
Video Enable	Select the Video Enable check box to enable sub stream. Then the device monitors under the sub stream. This function is enabled by default.
Main Stream, Sub Stream	Indicates the stream type that includes Regular , Motion , and Alarm .
Encode Mode	Includes the following video encoding modes: <ul style="list-style-type: none"> • H.263: Low profile encoding. • H.264: Main profile encoding • H.264B: Baseline profile encoding • H.264H: High profile encoding • H.265: Main Profile encoding • MJPG: Short for MJPG. Under this mode, the video image requires higher bit rate to ensure video quality. It is recommended to use the maximum bit rate value to get the best results. • FCC_MPEG4: MPEG4 profile encoding certified by FCC. • MS_MPEG4: MPEG4 profile encoding developed by MS. • MPEG1, MPEG2, MPEG4: Profile encoding that complies with MPEG standard.
Video Standard	Select the video standard for the device: <ul style="list-style-type: none"> • PAL (Phase Alteration Line) • NTST (National Television System Committee)
Resolution	Indicates the video resolution. The maximum video resolution might be different according to your device model.
Frame Rate	Indicates the total frames per second. The higher the frame rate, the more clear and smooth the image will become.
Bit Stream Control	Includes the following two types of bit rate: <ul style="list-style-type: none"> • Constant Bit Rate (CBR): The bit rate is fluctuating around the set value without big changes. • Variable Bit Rate (VBR): The bit rate is changing along with the monitoring environment.  <p>When the compression is set as MJPEG, the bit rate can only be CBR.</p>
Bit Rate (kbps)	Select the suitable value according to the actual needs. You can configure this parameter when the bit rate type is set as CBR.
Audio Enable	The audio function can be enabled only when the video function has been enabled. Select the Audio Enable check box, the bit rate changes to the audio and video combined bit rate; otherwise the bit rate only includes video image.

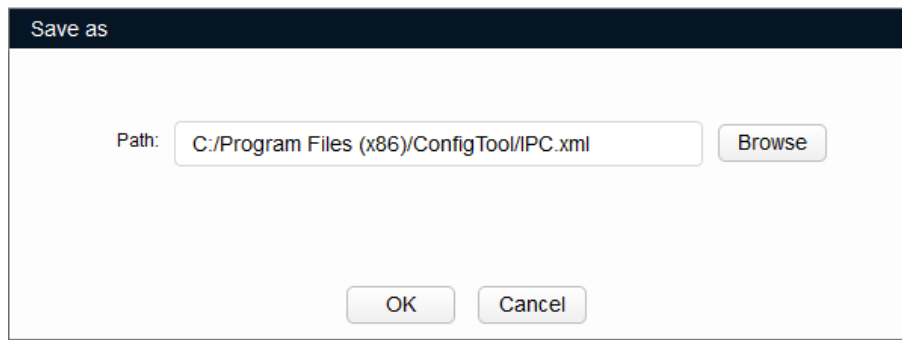
Parameter	Description
Audio Encode	Indicates audio encoding mode such as G.711A, G.711Mu, G.726, and AAC. The setting of audio encoding mode will simultaneously apply to both audio and voice call.
Color Mode	Select the image color mode from Standard, Bright, and Soft for the device.
Brightness	Adjust the image brightness. The bigger the value, the brighter the image is.
Contrast	Adjust the image contrast. The bigger the value is, the contrast between the light area and dark area is more obvious.
Gamma	Adjust the image brightness in a non-linear way to improve the dynamic display range. The bigger the value, the brighter the image will become.
Saturation	Adjust the color shades. The bigger the value, the lighter the color is. This value does not influence the general image lightness.
BLC Mode	<ul style="list-style-type: none"> • OFF: Turn off the backlight compensation mode. • BLC: Backlight compensation. In the backlighting environment, the compensation function can avoid silhouette of the dark part when taking a picture. • WDR: Wide Dynamic Range. In the strong illumination contrast, this function can suppress the area with excessive brightness and compensate the area with excessive darkness so as to make the image clearer in general. • HLC: Highlight Compensation. This function can weaken the strong light to reach the brightness balance.
Day/Night Mode	Includes the following three options: <ul style="list-style-type: none"> • Color: Select this option to set the color image. • 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.
Profile Management	Includes the following three options: <ul style="list-style-type: none"> • Normal: the system monitors according to the normal configuration. • Full Time: Select Day or Night from Always Enable list, the system monitors according to the configuration of Always Enable. • Schedule: Set Day Start Time and Day End Time, and the rest time is night. The system will monitor by the corresponding configuration in different periods.

Step 3 Save the template.

- 1) Click **Save as**.

The **Save as** dialog box is displayed. See Figure 3-66.

Figure 3-66 Save as



- 2) Click **Browse** to select the save path for the template.
- 3) Click **OK** to save the template.

3.10.1.2 Exporting the Device Template

You can export the template of the existing device and save it for further use.

Step 1 Click .

The **Template Setup** interface is displayed.

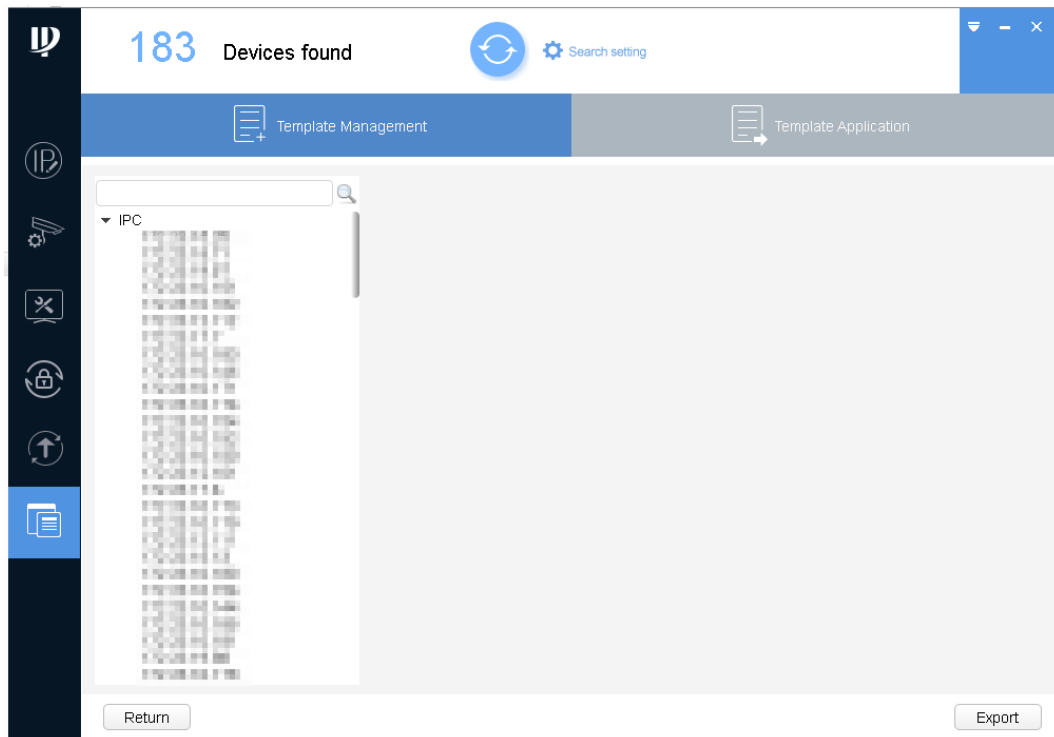
Step 2 Export the template.

- 1) Click .

The **Notice** dialog box is displayed. Click **OK**.

The **Export** interface is displayed. See Figure 3-67.

Figure 3-67 Export



- 2) Select the device and click **Export**.
The **Export** dialog box is displayed. Click **OK** to start exporting.
After exporting is completed, the **Template Management** interface is displayed.
See Figure 3-68.



If the device is not in the device list, perform searching again. For the details about how to search devices, see "3.2 Adding Devices."

Figure 3-68 Template management

- 3) Select the template type, type the template name, and then set the parameters accordingly.



After the template configuration is completed, click **Apply** to apply the template to the device. For the details about applying the template, see "3.10.2 Applying the Template."

Step 3 Save the template.

- 1) Click **Save as**.

The **Save as** dialog box is displayed. See Figure 3-69.

Figure 3-69 Save as

- 2) Click **Browse** to select the save path for the template.
- 3) Click **OK** to save the template.

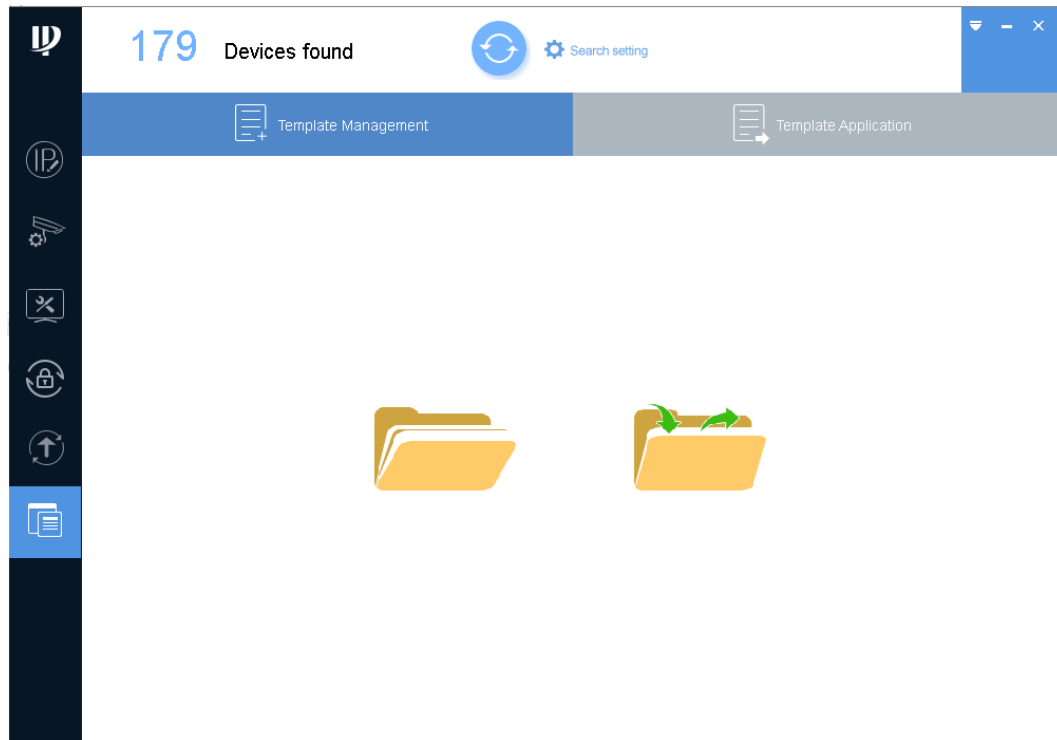
3.10.2 Applying the Template

You can load the template to restore or batch configuring the video parameters and encoding parameters for the device.

Step 1 Click .

The **Template Setup** interface is displayed. See Figure 3-70.

Figure 3-70 Template Setup



Step 2 Load the template.

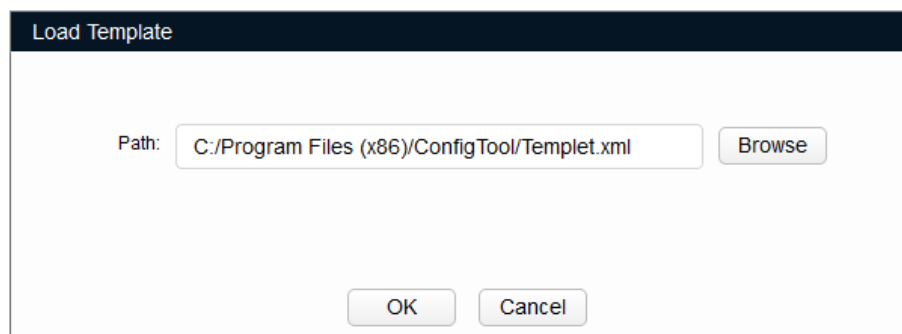
1) Click .

The **Load Template** dialog box is displayed. See Figure 3-71.



Make sure the template is already existing, if not, for the details about how to create a template, see "3.10.1 Creating a Template."

Figure 3-71 Load template



2) Click **Browse** to select the template.

3) Click **OK**.

The **Template Management** interface is displayed. See Figure 3-72.

Figure 3-72 Template management

Step 3 Apply the template.

- 1) Click the **Template Application** tab.

The **Template Application** interface is displayed. See Figure 3-73.



- Click **Other Template** to switch template.
- If the device is not in the device list, perform searching again. For the details about how to search devices, see "3.2 Adding Devices."

Figure 3-73 Template Application

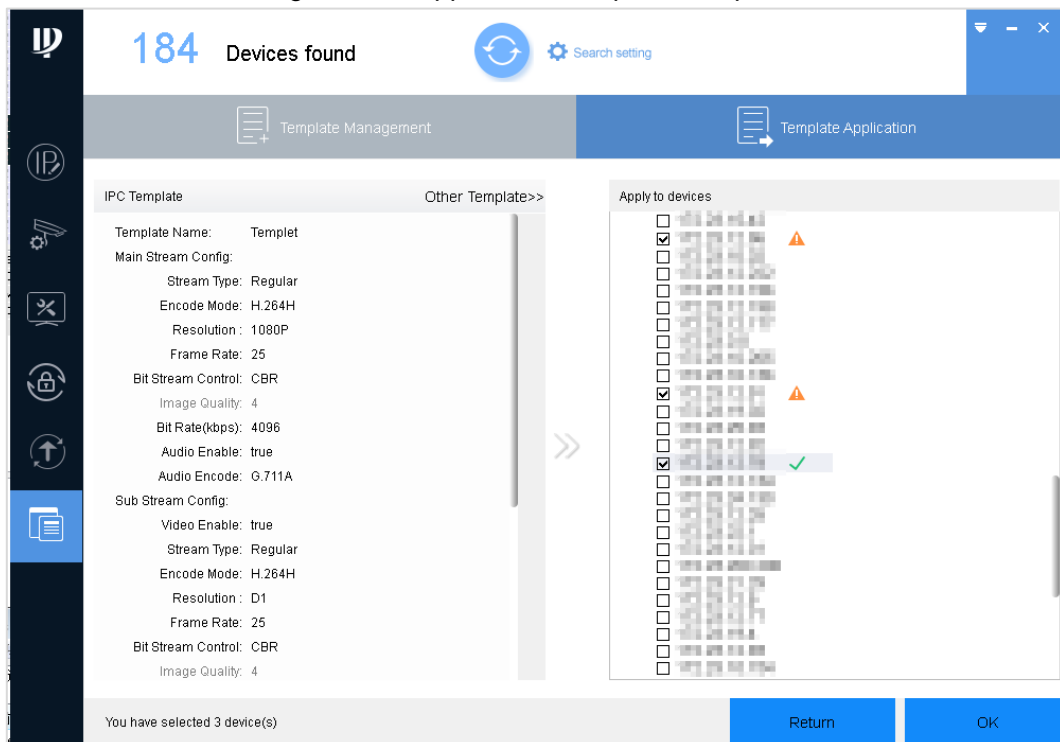
- 2) Select the one or multiple devices and click **OK**.

The **Application Template** dialog box is displayed. Click **OK** to start applying the template.

The result is displayed next to the device after applying is completed. See Figure 3-74.

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

Figure 3-74 Application Template completed



Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic equipment network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

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

2. Update Firmware and Client Software in Time

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

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

1. Physical Protection

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

2. Change Passwords Regularly

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

3. Set and Update Passwords Reset Information Timely

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

4. Enable Account Lock

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

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

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

7. Enable Whitelist

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

8. MAC Address Binding

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

9. Assign Accounts and Privileges Reasonably

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

10. Disable Unnecessary Services and Choose Secure Modes

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

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

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

11. Audio and Video Encrypted Transmission

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

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

12. Secure Auditing

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

13. Network Log

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

14. Construct a Safe Network Environment

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

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.

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