ConfigTool (Mac Version)

User's Manual

V1.0.0

Foreword

General

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

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	June 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.

- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Table of Contents

1 Overview

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 abnormities.

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 by local.

2 Basic Operations

2.1 Starting ConfigTool

On the desktop, double-click , and then main interface is displayed.

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

Figure 2-1 Main interface

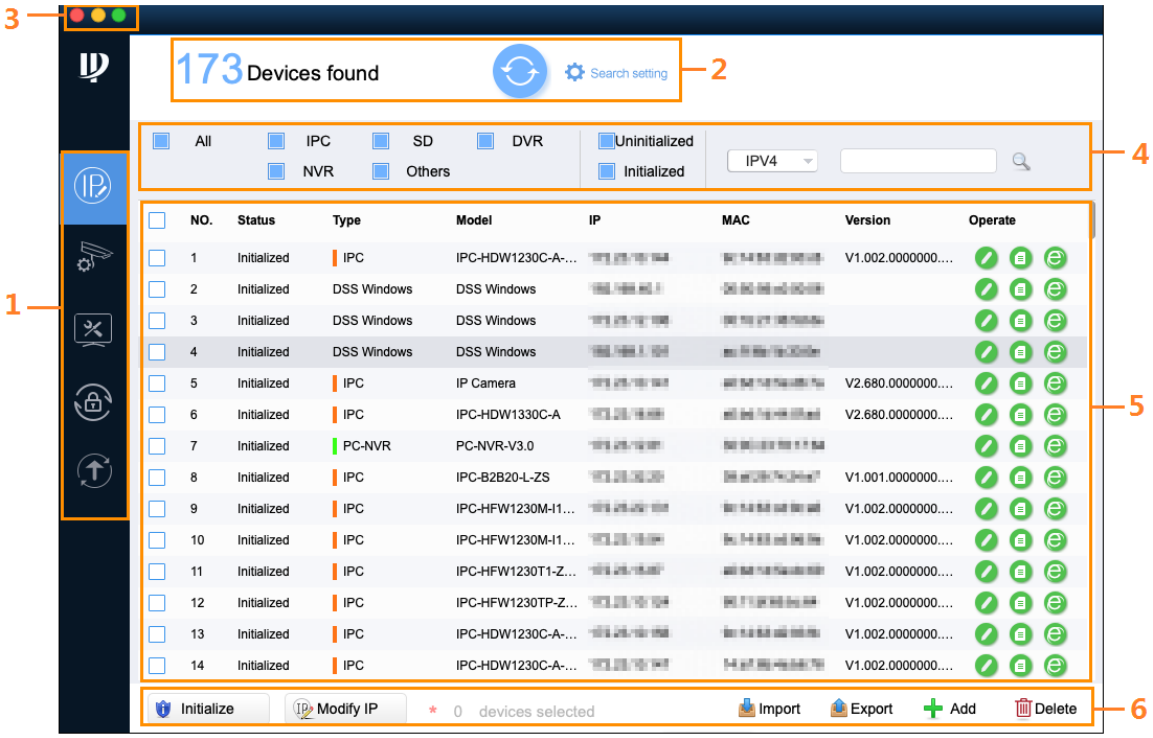


Table 2-1 Main interface description

No.	Function	Description
1	Menu	Includes six tabs: **Modify IP**, **Device Config**, **System Settings**, **Password Reset**, and **Upgrade**. ● Modify IP ( ): Modify IP of one device or multiple devices. ● Device Config ( ): Modify device default password, and configure encoding, image, and profile management. ● System Settings ( ): Set device system time, reboot device, restore device, modify password and reset password. ● Password Reset ( ): Reset the password the QR coed and XML file. ● Upgrade ( ): Upgrade one device or multiple devices.
2	Search setting	You can search the devices within the current network segment or other network segments. Click to refresh the device list that is displayed in the main interface.
3	Help	Provides access to check the **Help** file and software version, set network parameters and upgrade parameters, minimize or exit the software. ● Click to check the **Help** file and software version. Select **Setting** to set network parameters and upgrade parameters. ● Click to minimize the software. ● Click to exit the software.
4	Filtering	Filter by selecting device type and IP version (IPV4 or IPV6) to find the devices quickly. You can also manually enter the conditions such as type, IP address, model, MAC address and version number to search the devices.
5	Device list	Shows the searched devices and their information such as type, mode, IP, MAC and version. The **Operate** column provides the following functions: ● Click to modify device IP. ● Click to view device details. ● Click to open device WEB configuration interface. Under IPV6, modifying IP or viewing device details is not supported.

No.	Function	Description
6	Function buttons	Includes the following buttons: ● Select one or multiple devices and click Initialize to start initializing. ● Select one or multiple devices and click Modify IP to modify the IP addresses. ● Click Import to import one or multiple devices through template. ● Select one or multiple devices and click Export to export the device details. ● Select one or multiple devices and click Delete to remove from the list.

2.2 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.

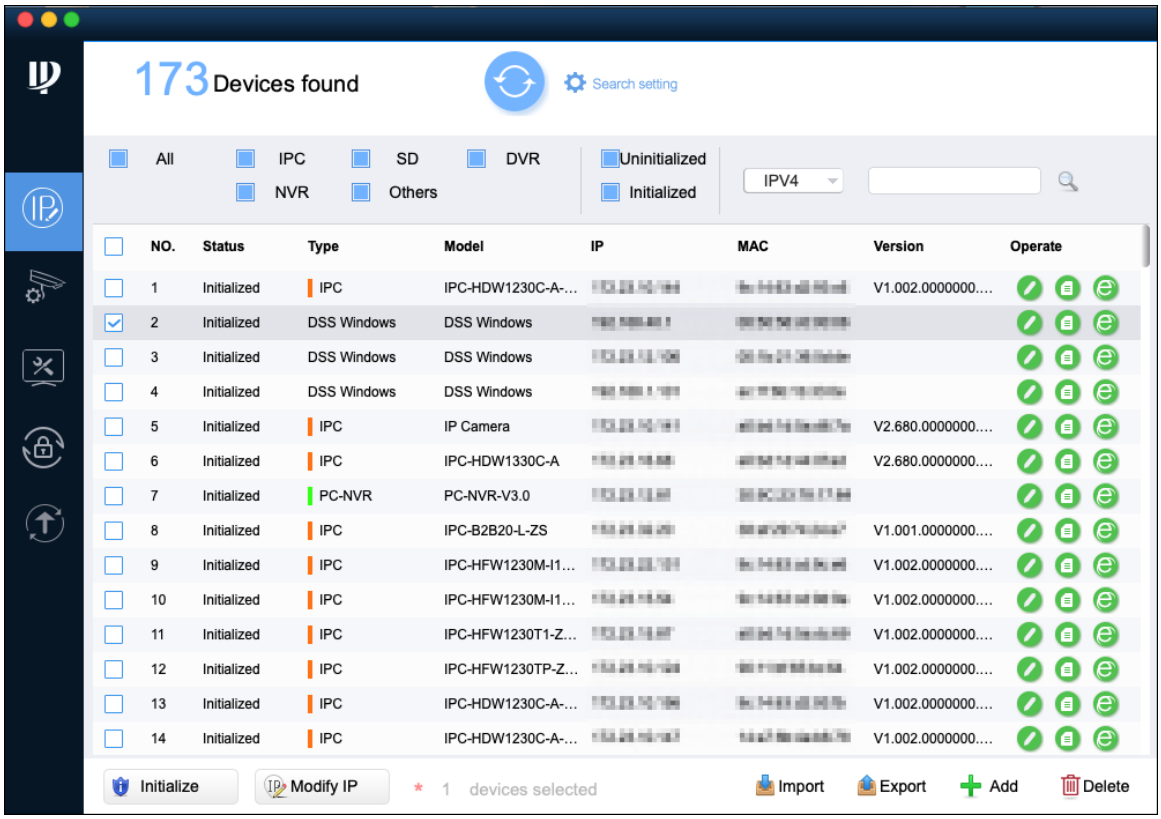
2.2.1 Adding One Device

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

Step 1 Click .

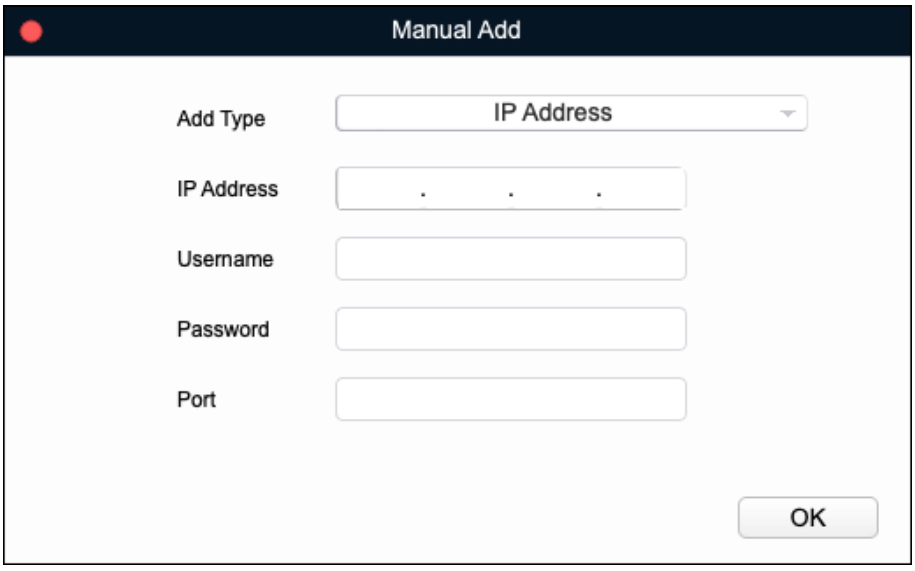
The **Modify IP** interface is displayed.

Figure 2-2 Modify IP Interface



Step 2 Click Add to add device manually.

Figure 2-3 Manually add



Step 3 Set the device parameters.

Table 2-2 Manual add parameters

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

Step 4 Click **OK**.

The newly added device appears in the device list.

2.2.2 Adding by Searching

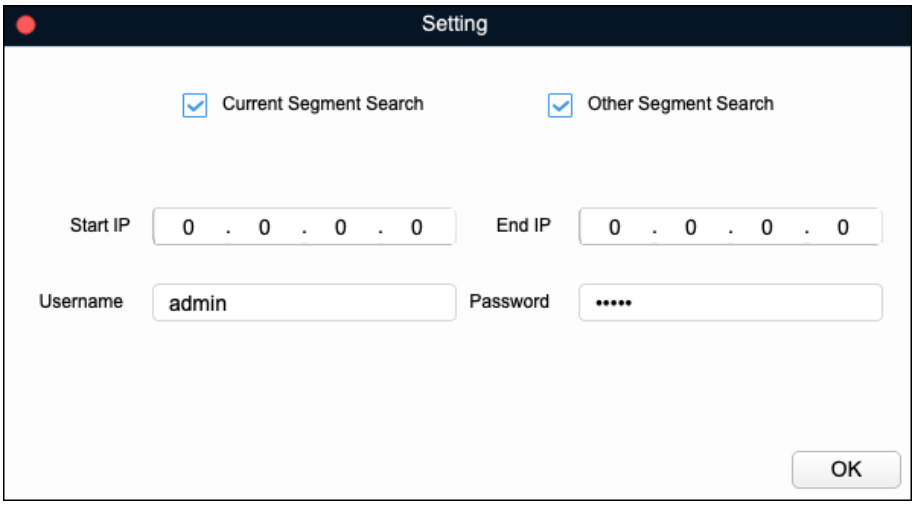
You can add multiple devices through searching devices, if you know the network segment where the device is located.

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

Step 1 Click Search setting.

The **Setting** interface is displayed.

Figure 2-4 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.

2.3 Initializing Devices

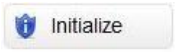
You can initialize one or multiple devices according to your actual needs.

- 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  .

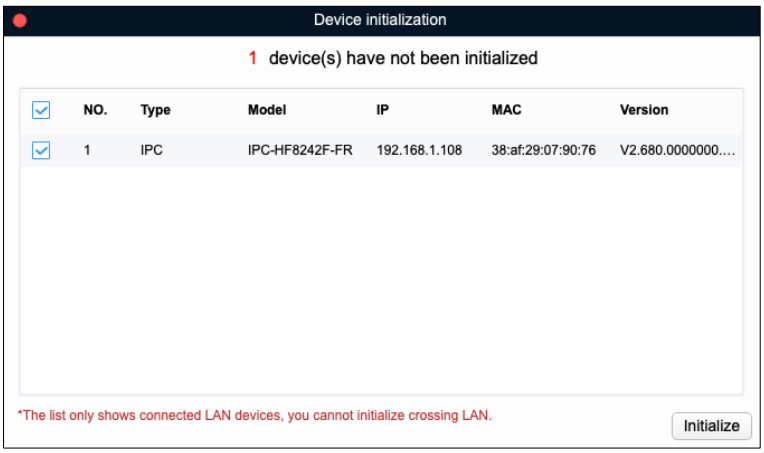
The **Modify IP** interface is displayed.

Step 2 Select one or several uninitialized devices.

Step 3 Click  .

The **Device initialization** interface is displayed.

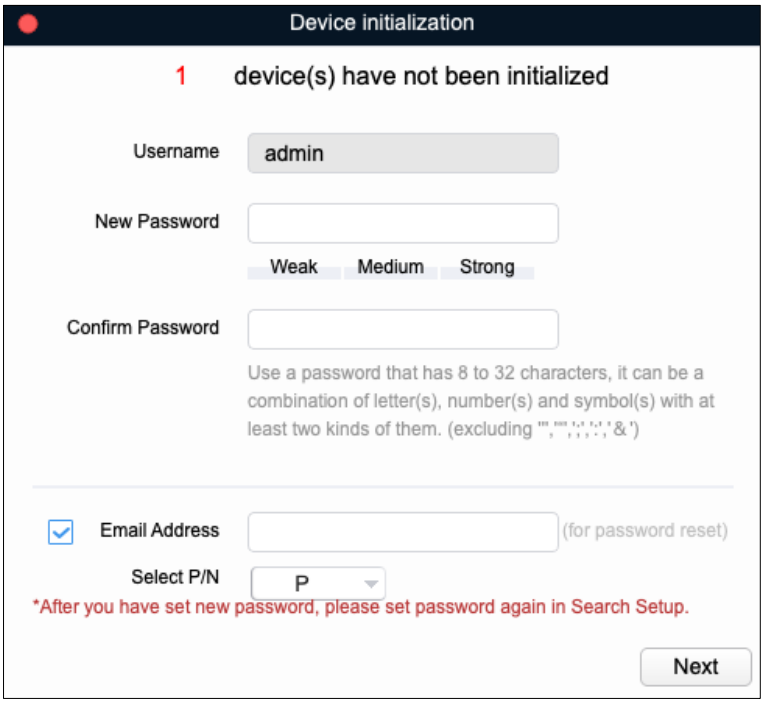
Figure 2-5 Device initialization (1)



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

- 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 2-6 Device initialization (2)



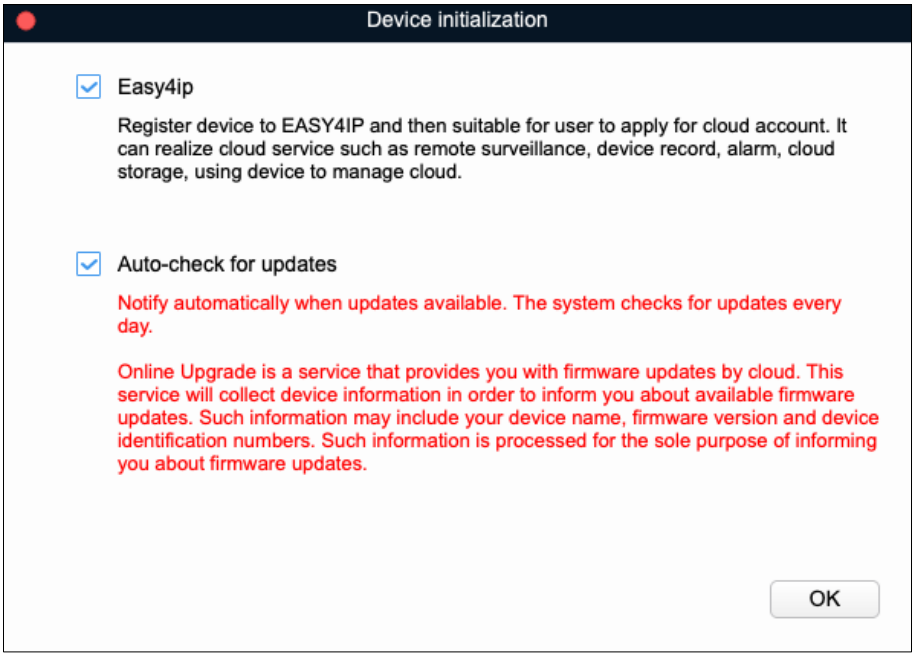
Step 5 Set the initialization parameters for the device.

Table 2-3 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**.

Figure 2-7 Device initialization (3)

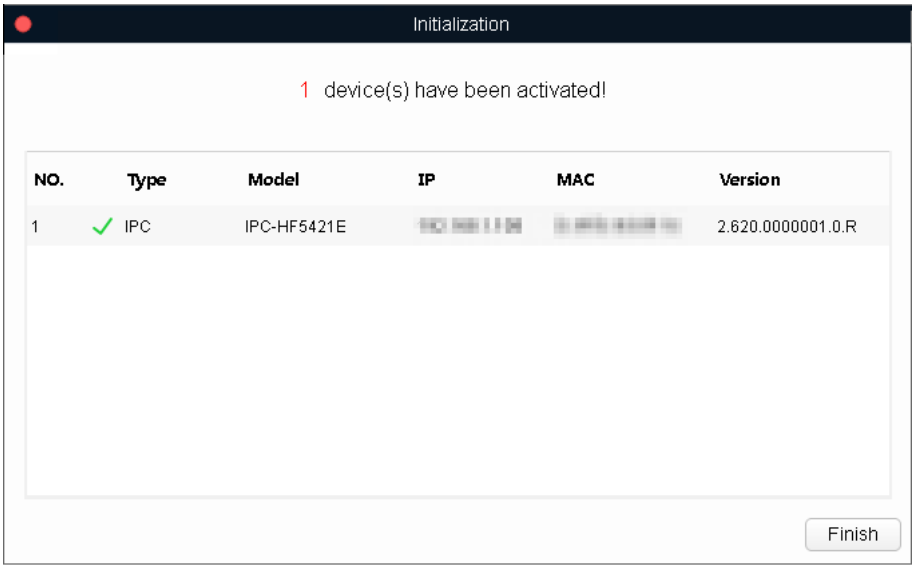


Step 7 Select **Easy4ip** or select **Auto-check for updates** according to the actual needs.

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

The **Initialization** interface is displayed after initializing is completed. Click the success icon ( ) or click the failure icon ( ) for the details.

Figure 2-8 Succeed to 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.

2.4 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.

2.4.1 Modifying One IP

Step 1 Click .

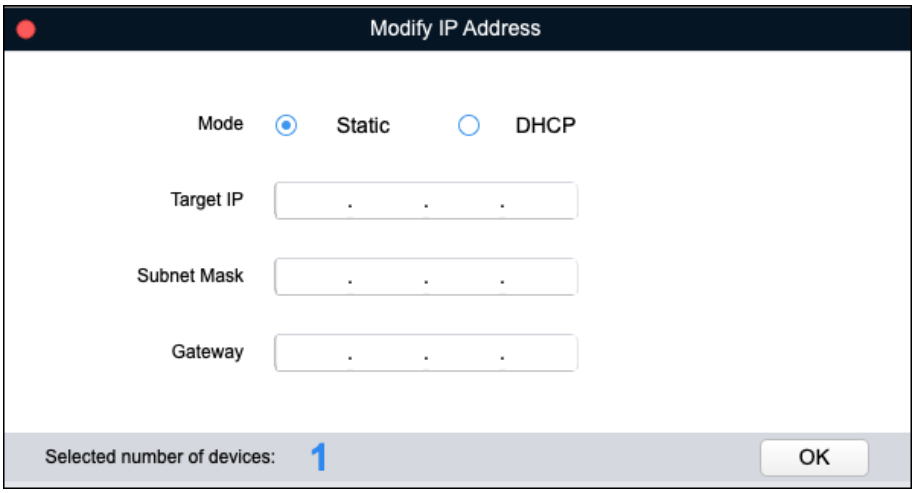
The **Modify IP** interface is displayed.

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

The **Modify IP Address** interface is displayed.

If the device is not in the device list, perform searching again. For details, see "2.2 Adding Devices."

Figure 2-9 Modify IP address of one device



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.

2.4.2 Modifying IP in Batches

Step 1 Click .

The **Modify IP** interface is displayed.

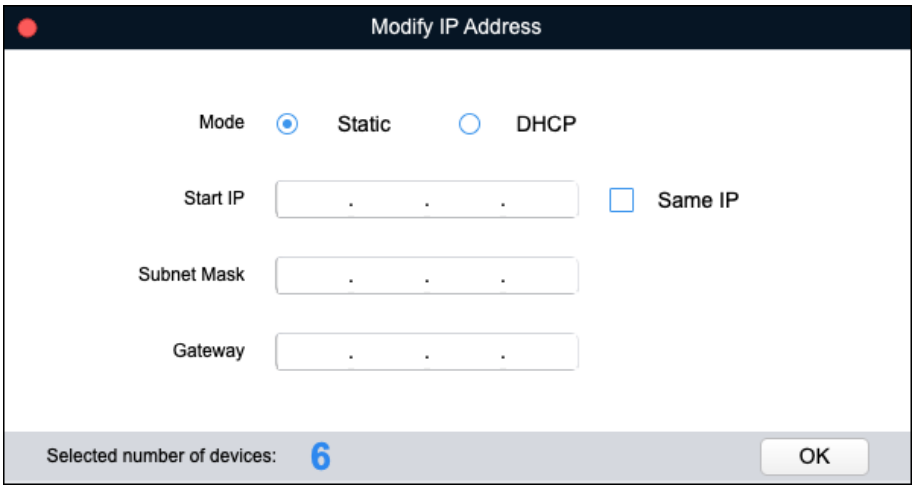
Step 2 Select the devices that you want to modify IP.

If the device is not in the device list, perform searching again. For the details about how to search devices, see "2.2 Adding Devices."

Step 3 Click Modify IP.

The **Modify IP Address** interface is displayed.

Figure 2-10 Modify IP address in batches



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.

2.5 Configuring the Device Parameters

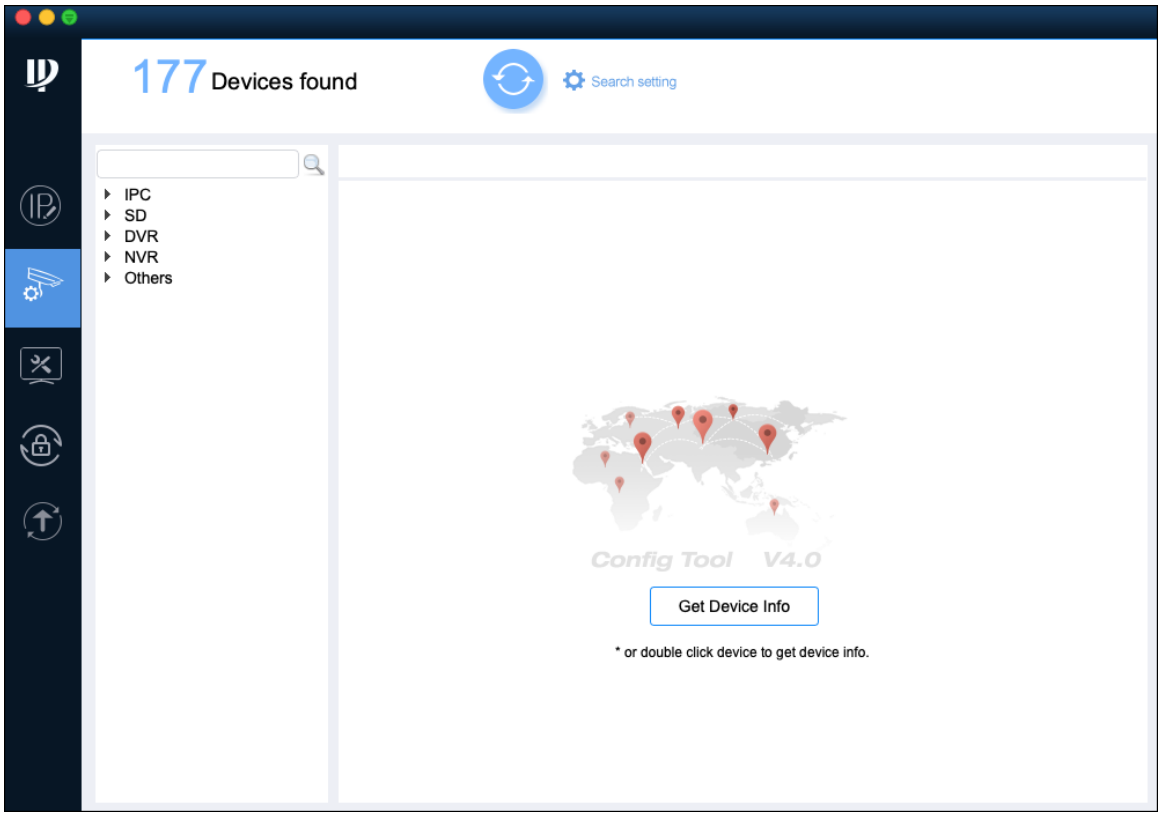
You can configure the encoding parameters, video parameters, and profile management.

2.5.1 Accessing the Configuration Interface

Step 1 Click  .

The **Device Config** interface is displayed.

Figure 2-11 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 **Login** 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 "2.2 Adding Devices."

Step 3 Enter username and password, and then click **OK**.

The **Encode** interface is displayed.

Figure 2-12 Login

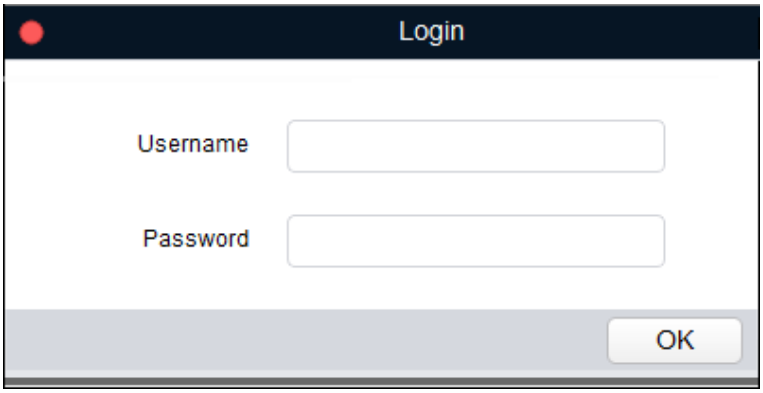
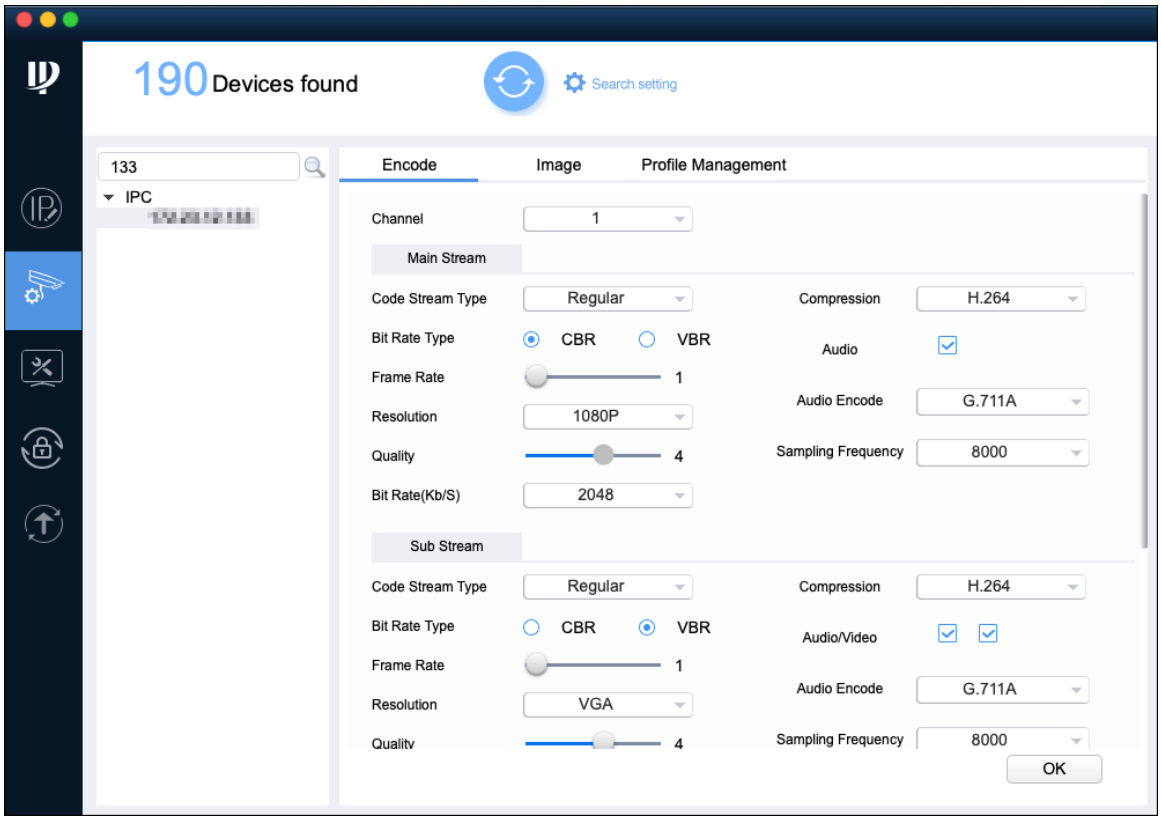


Figure 2-13 Encode



2.5.2 Configuring the Parameters

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

2.5.2.1 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.

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

Table 2-4 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: ● 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: ● 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. When the compression is set as **MJPG**, the bit rate can only be **CBR**.
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	● To enable the audio function, select the **Audio** check box. ● To monitor with the sub stream, select the **Video** check box. For the sub stream, you can enable the audio function only after the video function is already enabled.
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.

2.5.2.2 Configuring Video Parameters

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

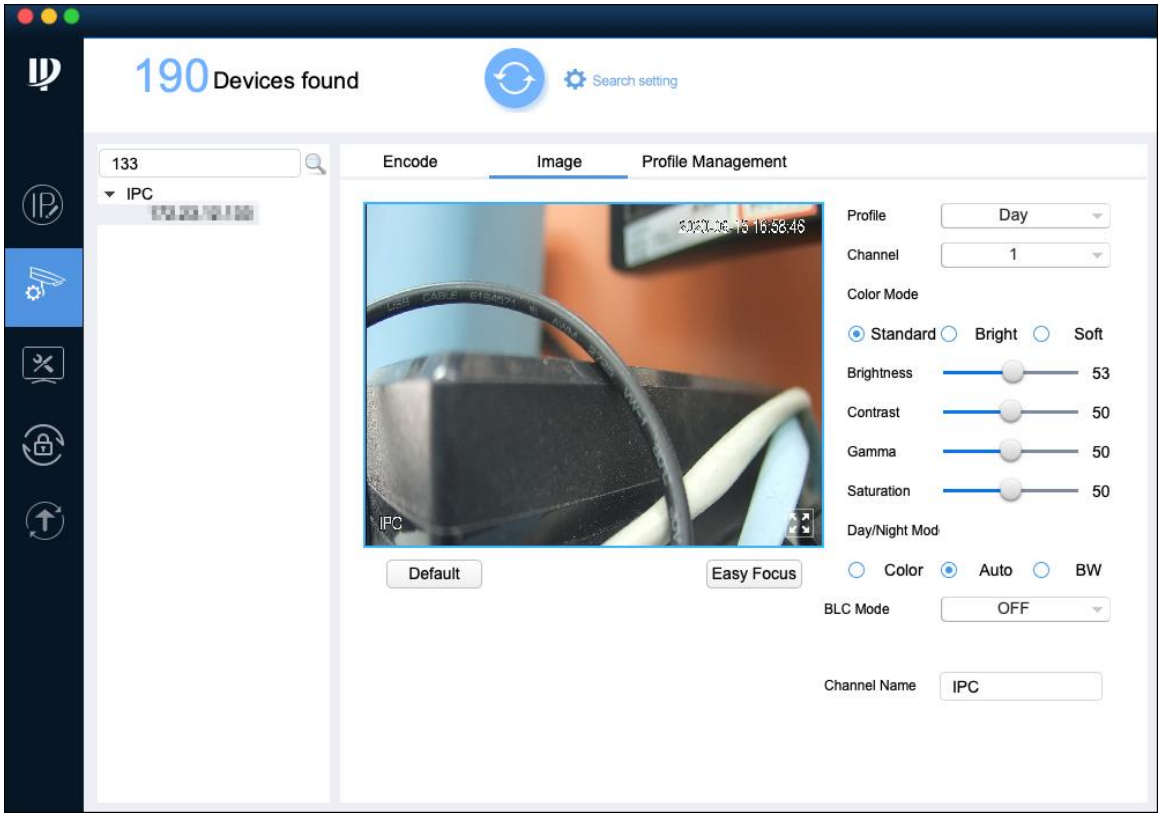
Step 1 Click the **Image** tab.

The **Image** interface is displayed.

- 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 2-14 Image



Step 2 Set the video parameters.

Table 2-5 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: ● 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	● 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.

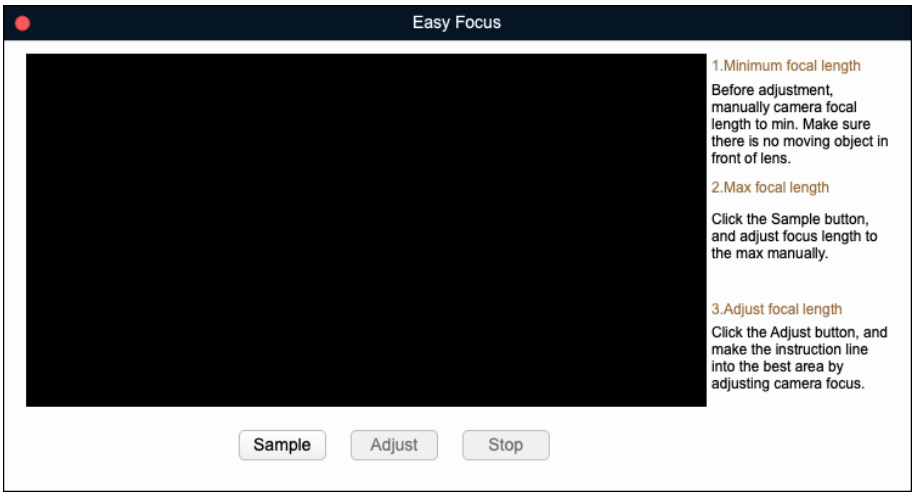
Step 3 (Optional) Set the **Easy Focus** function.

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

1) Click **Easy Focus**.

The **Easy Focus** interface is displayed.

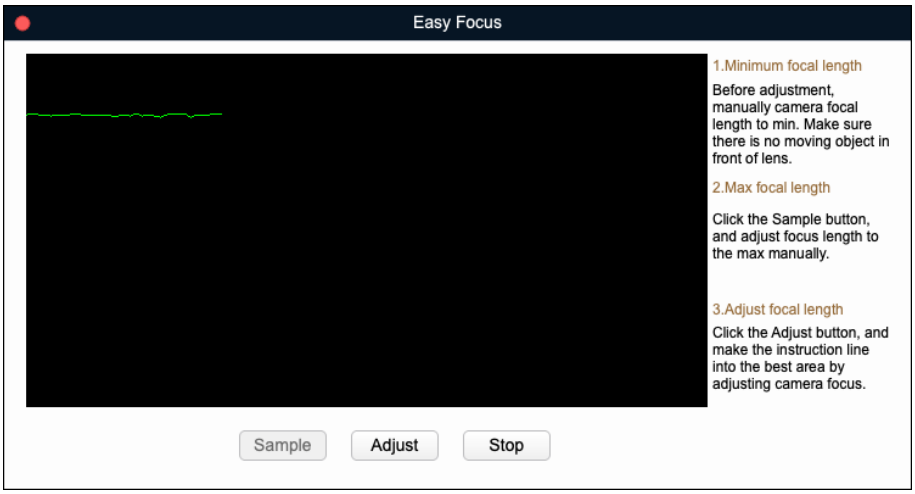
Figure 2-15 Easy focus



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.

Figure 2-16 Sampling

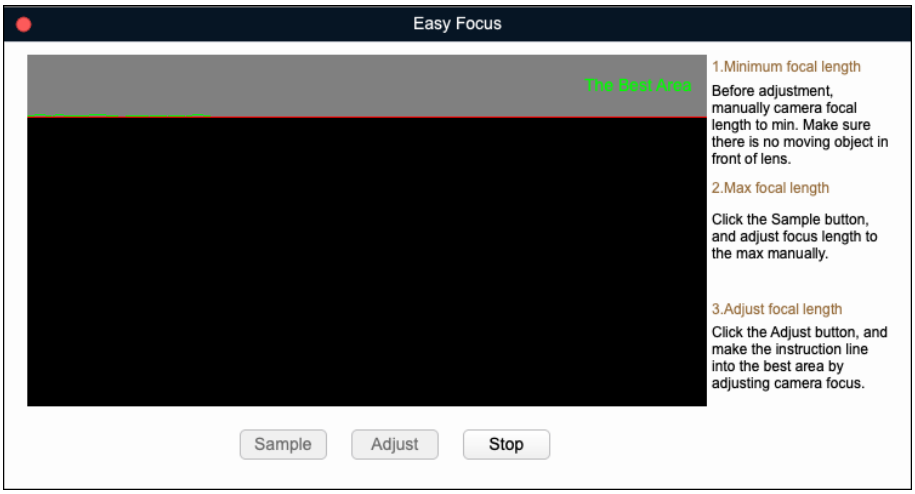


3) Click **Adjust**.

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

- 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 2-17 Final result



2.5.2.3 Configuring the Profile Management

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

Step 1 Click the **Profile Management** tab.

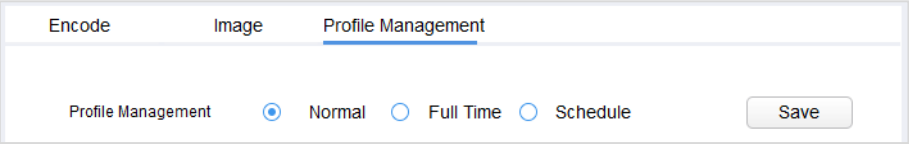
The **Profile Management** interface is displayed.

Step 2 Set the management profile.

- Select **Normal**.

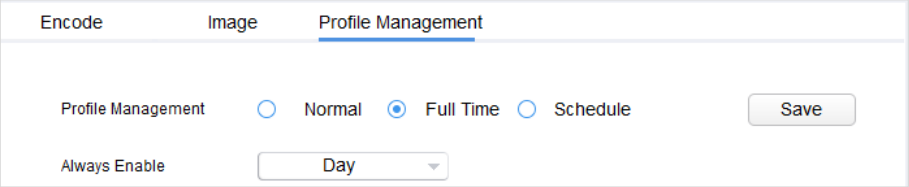
  The system monitors according to the normal configuration.

Figure 2-18 Normal



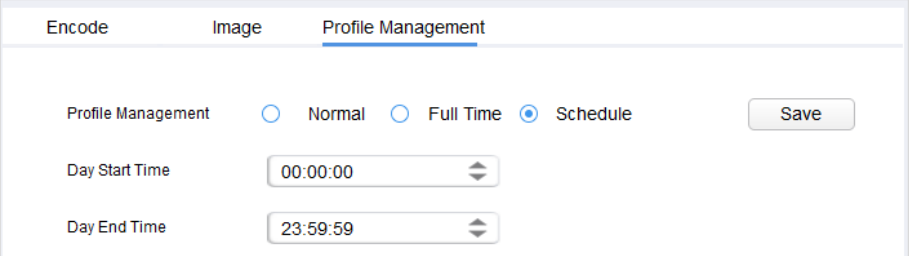
- Select **Full Time**, and then select **Day** or **Night**.
  The system monitors according to the corresponding settings.

Figure 2-19 Full time



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

Figure 2-20 Schedule



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

2.6 Configuring System Settings

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

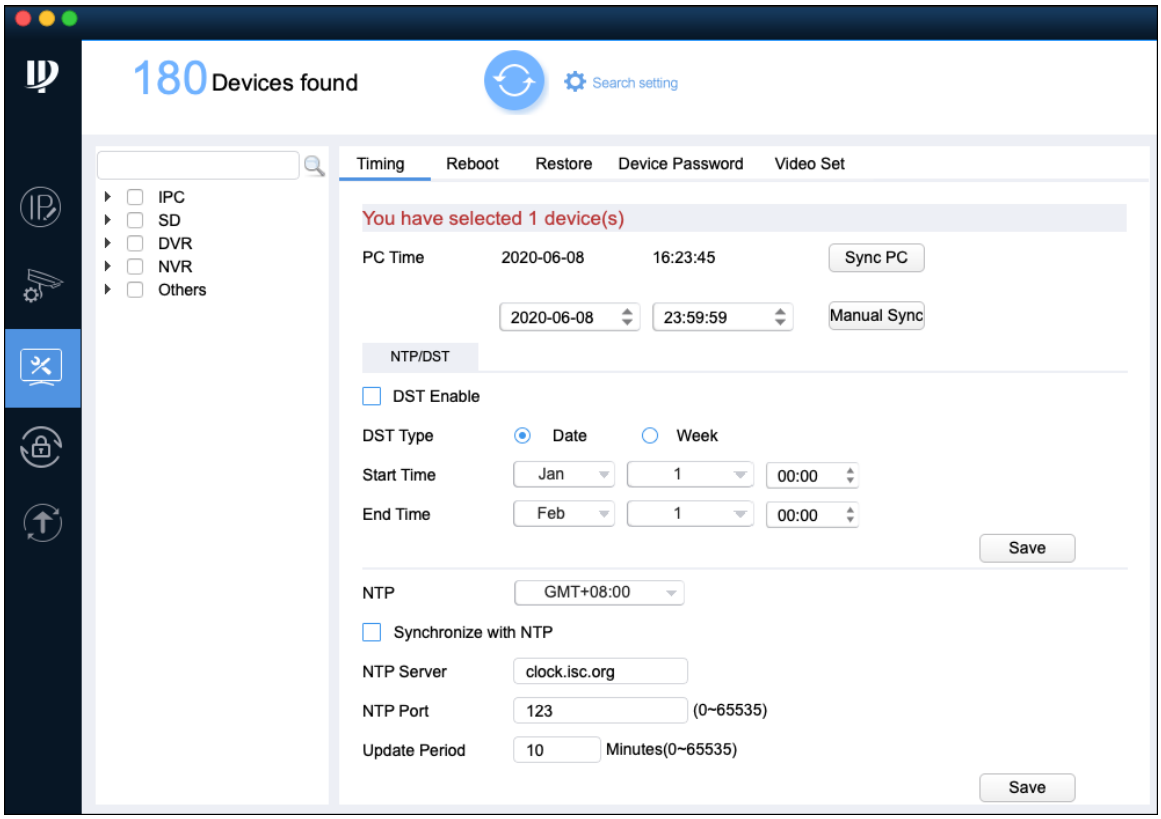
2.6.1 Timing

You can calibrate the device time through configuration.

Step 1 Click  .

The **Timing** interface is displayed.

Figure 2-21 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 "2.2 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.

Table 2-6 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.

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

Table 2-7 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.

2.6.2 Rebooting

You can manually or automatically reboot the device.

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

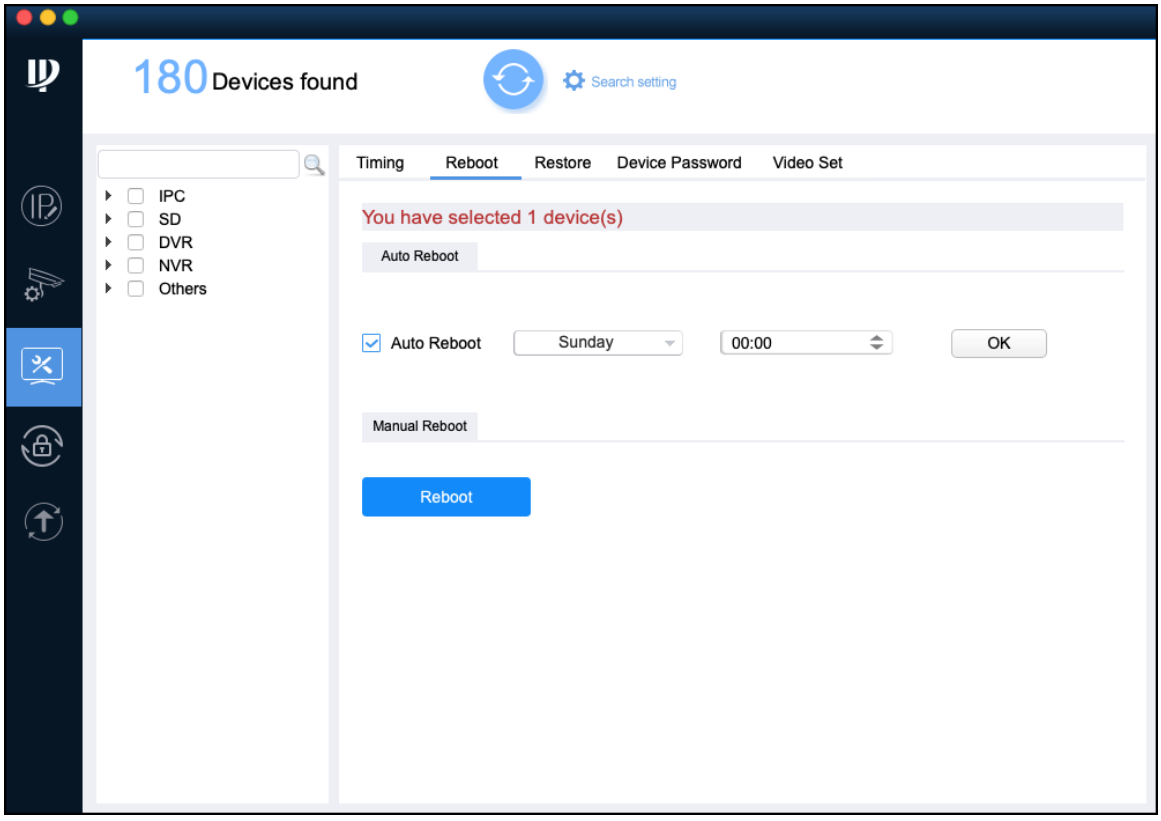
Step 1 Click  .

The **Timing** interface is displayed.

Step 2 Click the **Reboot** tab.

The **Reboot** interface is displayed.

Figure 2-22 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 "2.2 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.

2.6.3 Restoring

2.6.3.1 Restoring Default Configurations of Device

You can restore the default configurations. And then other configurations will be recovered to default except network IP address, user management and so on.

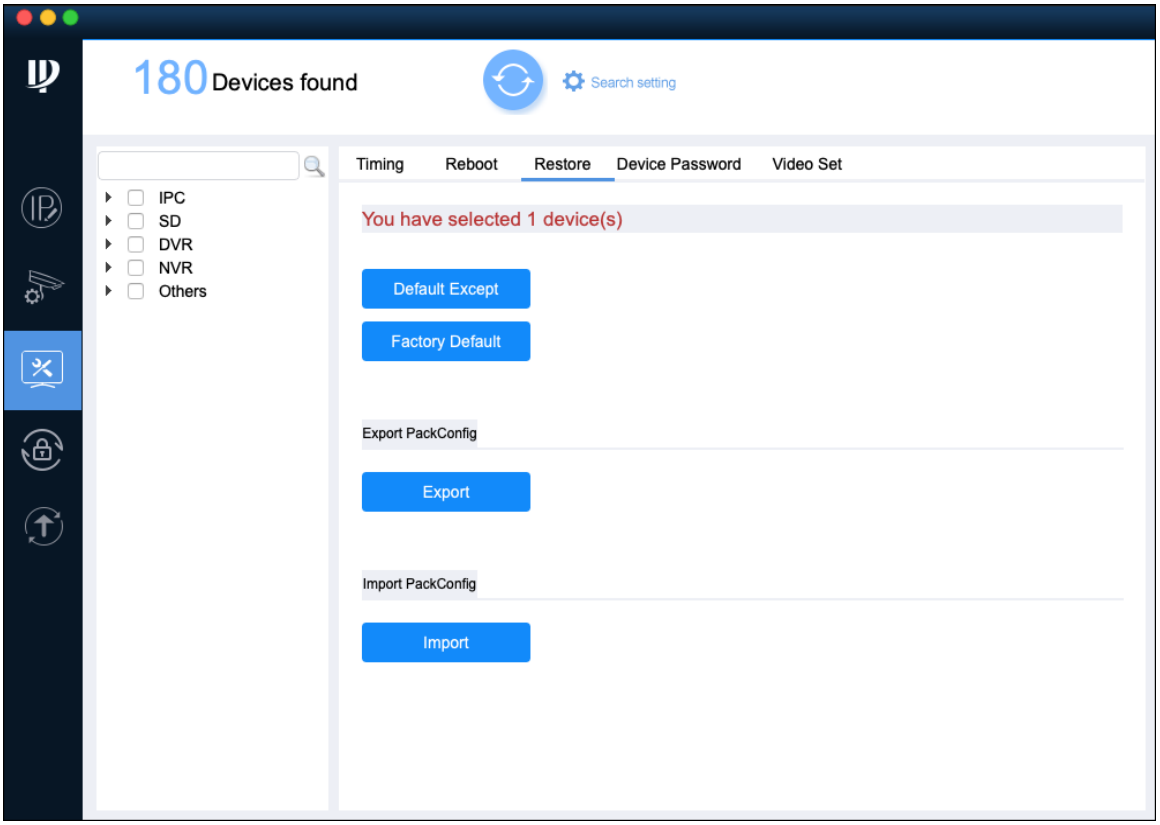
Step 1 Click  .

The **Timing** interface is displayed.

Step 2 Click the **Restore** tab.

The **Restore** interface is displayed.

Figure 2-23 Restore default configurations



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 "2.2 Adding Devices."

Step 4 Select one or multiple devices.

Step 5 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.

2.6.3.2 Restoring Factory Configurations of Device

You can restore the factory default configurations. And then you can completely recover device parameters to factory default

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

Step 5 Click **Factory Default** and click **OK** to restore factory configurations.

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

2.6.3.3 Export Configurations

Step 1 Click  .

The **Timing** interface is displayed.

Step 2 Click the **Restore** tab.

The **Restore** interface is displayed.

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 "2.2 Adding Devices."

Step 4 Select one or multiple devices.

Step 5 Click **Export**, select saving path and enter the file name. Then click **OK**.

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

2.6.3.4 Import Configurations

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

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

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

2.6.4 Device Password

You can modify the device login password.

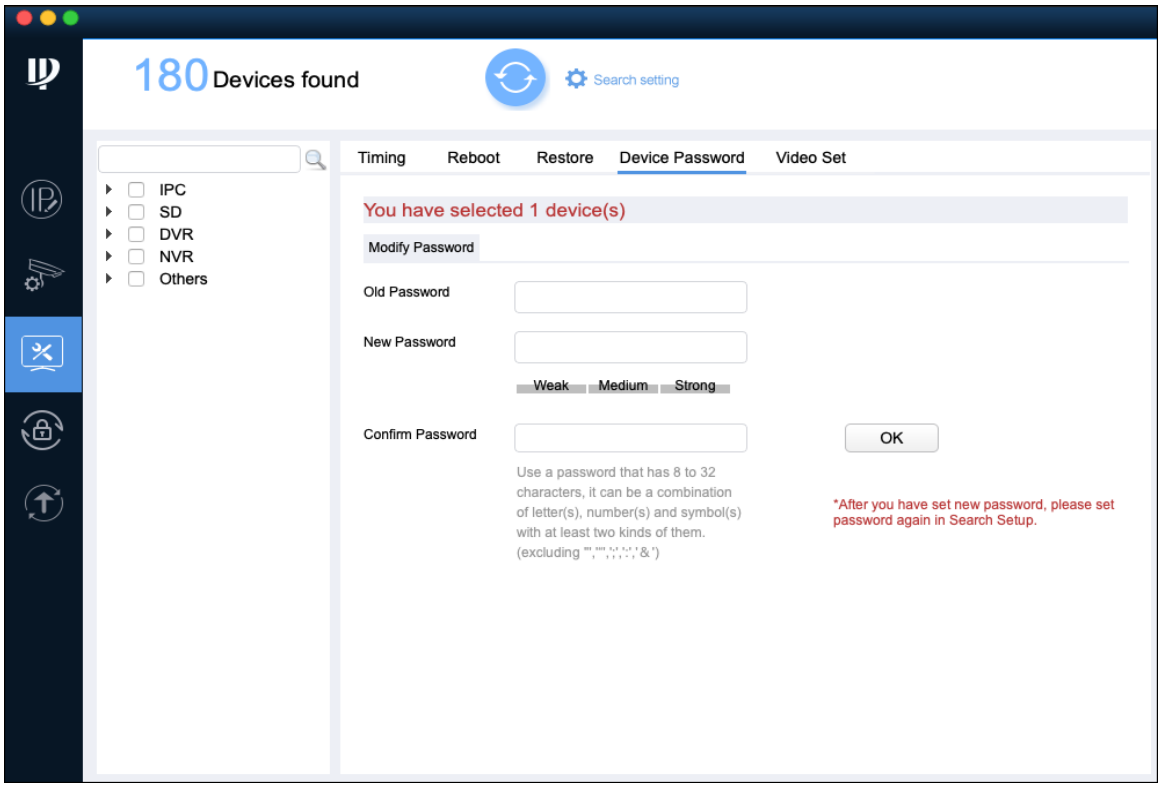
Step 1 Click  .

The **Timing** interface is displayed.

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

The **Device Password** interface is displayed.

Figure 2-24 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 "2.2 Adding Devices."

Step 5 Set the password parameters.

Table 2-8 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.

2.6.5 Video Settings

2.6.5.1 Getting Video Password

You can get back password for video files.

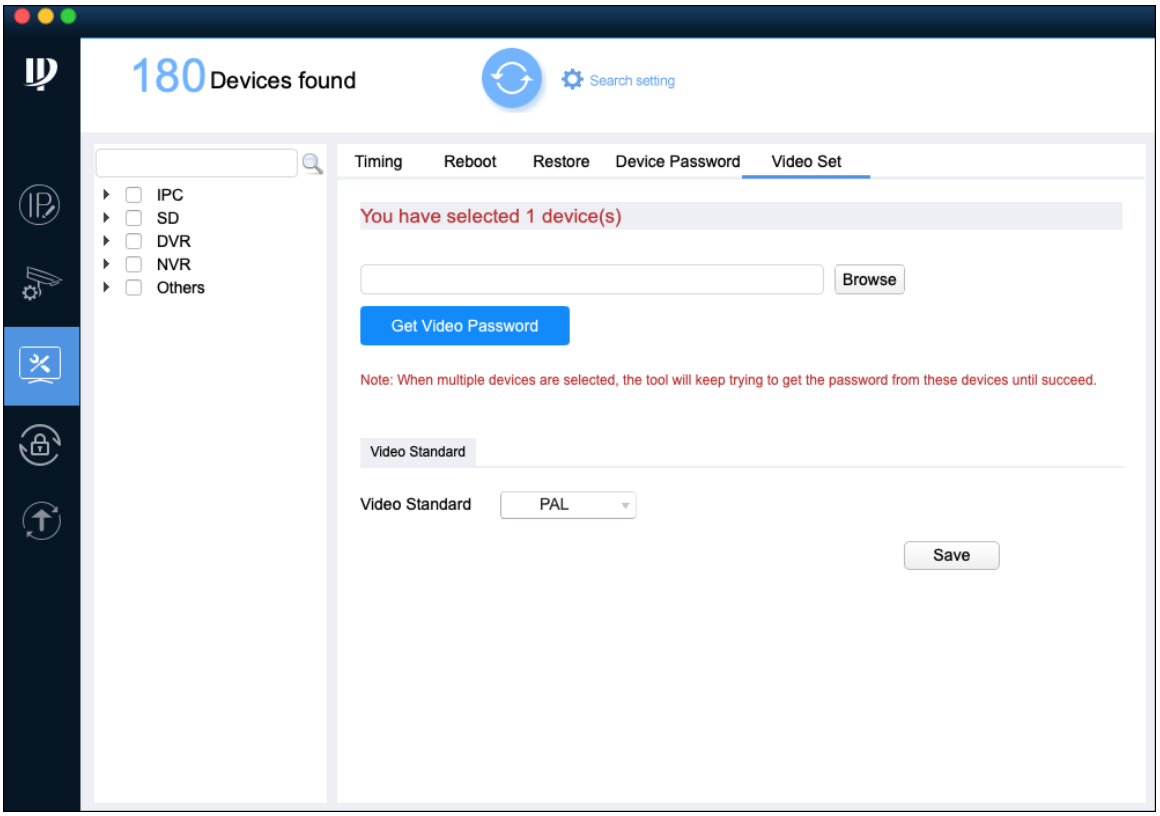
Step 1 Click  .

The **Timing** interface is displayed.

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

The **Video Set** interface is displayed.

Figure 2-25 Get video password (1)



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 "2.2 Adding Devices."

Step 4 Select one or multiple devices.

If you do not know which device the video file is exported from, you can select multiple devices so that the system will try them one by one until succeeds.

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

Step 6 Click **Get Video Password** to get video password.

Step 7 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.

2.6.5.2 Setting Video Standard

There are two video standards, PAL and NTSC. Select the needed one according to needs.

Step 1 Click  .

The **Timing** interface is displayed.

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

The **Video Set** interface is displayed.

Step 3 Select the needed video standard according to situations. 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.

2.7 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.

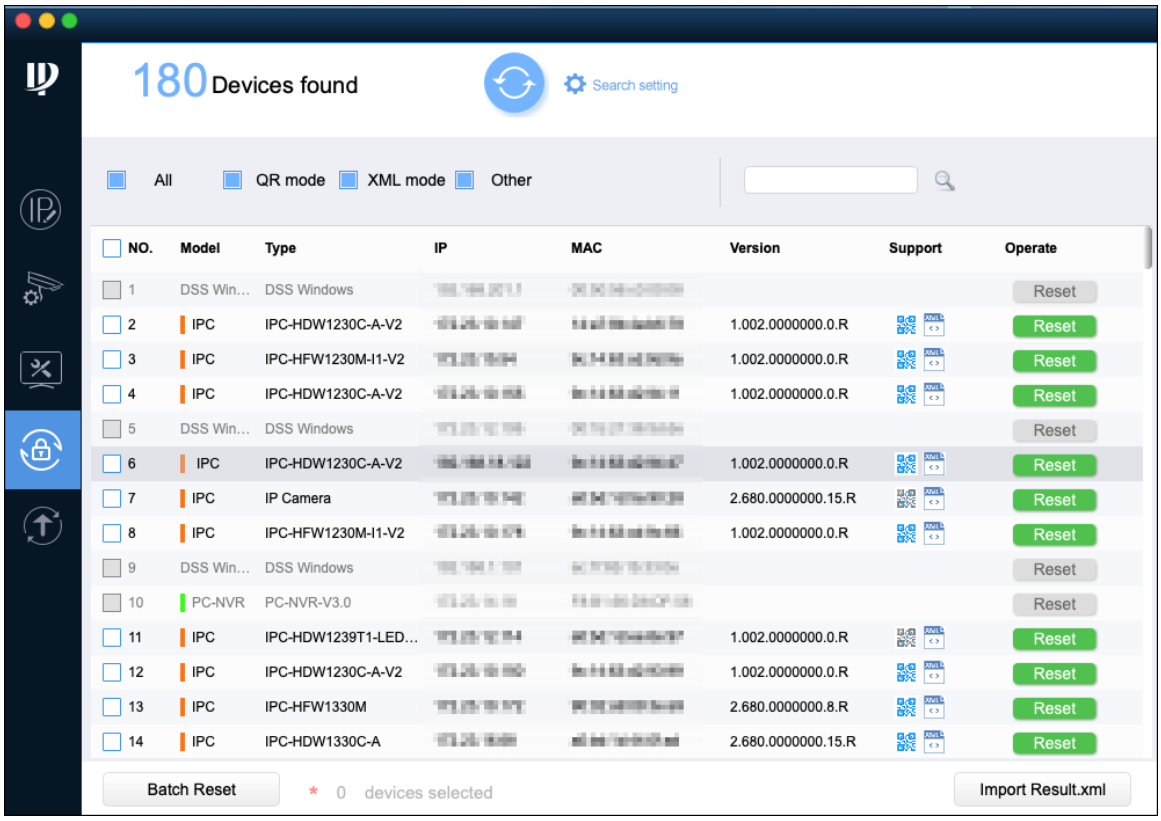
2.7.1 Using the QR Code

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.

Figure 2-26 Password reset



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

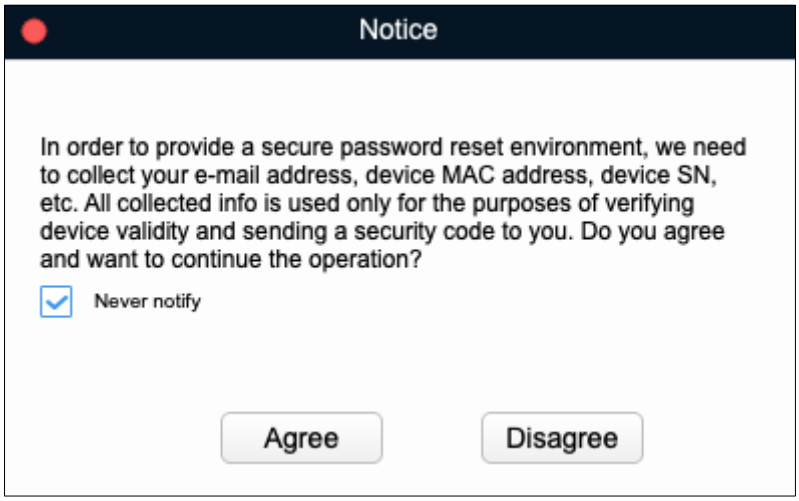
The supported formats are displayed in **Support**: means QR code, and means XML file. and are different icons of bin version.

Step 3 Click **Reset**.

A **Notice** box will be displayed.

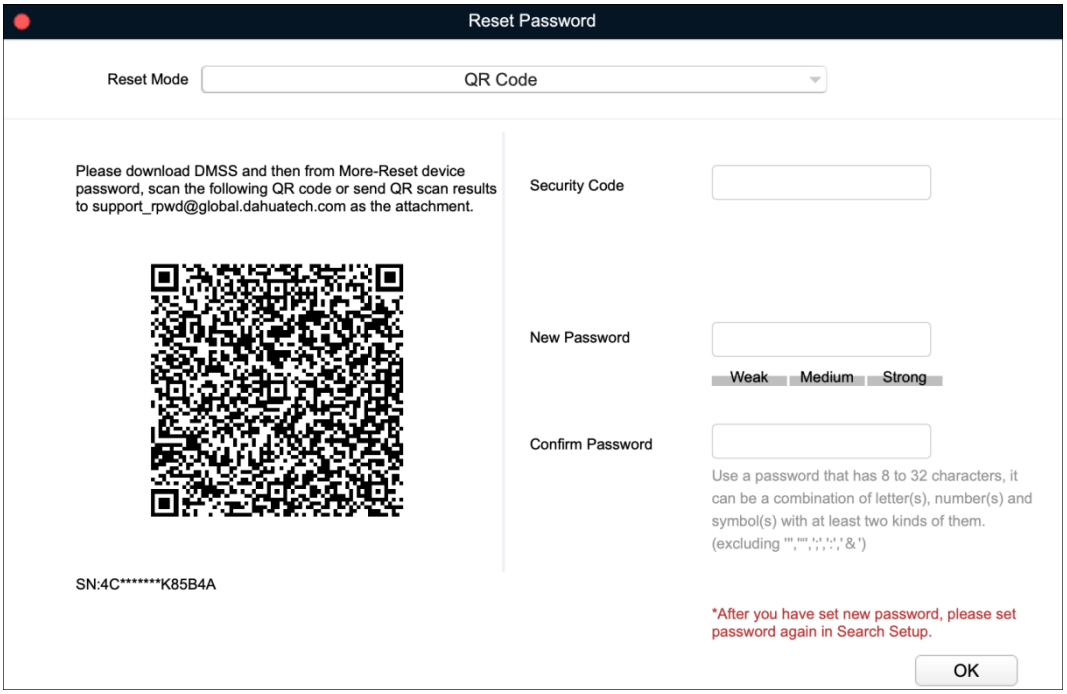
- The interface might vary with different models, and the actual product shall prevail.
- If the device does not support this function, the reset button displays gray (Reset).a If the device supports this function, the reset button displays green (Reset).

Figure 2-27 Notice



Step 4 Click **Agree**, the **Reset Password** interface is displayed.

Figure 2-28 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.

2.7.2 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.

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 2-29. Click **Agree**, the **Reset Password** interface is displayed. See Figure 2-30.

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

Figure 2-29 Notice

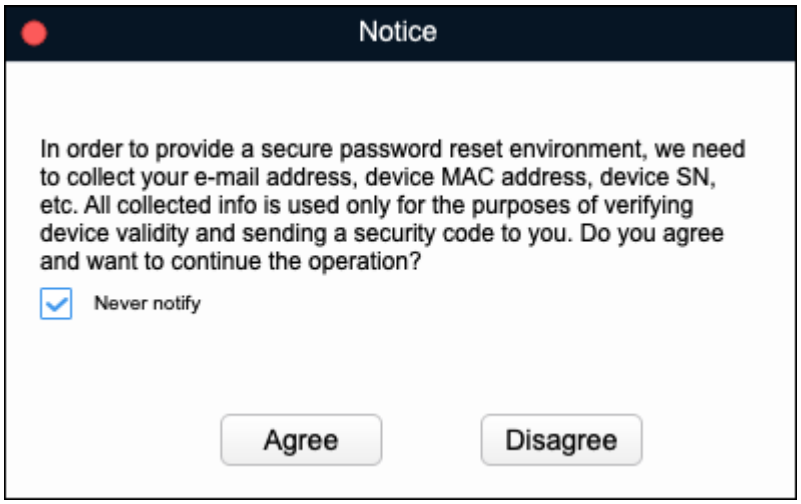
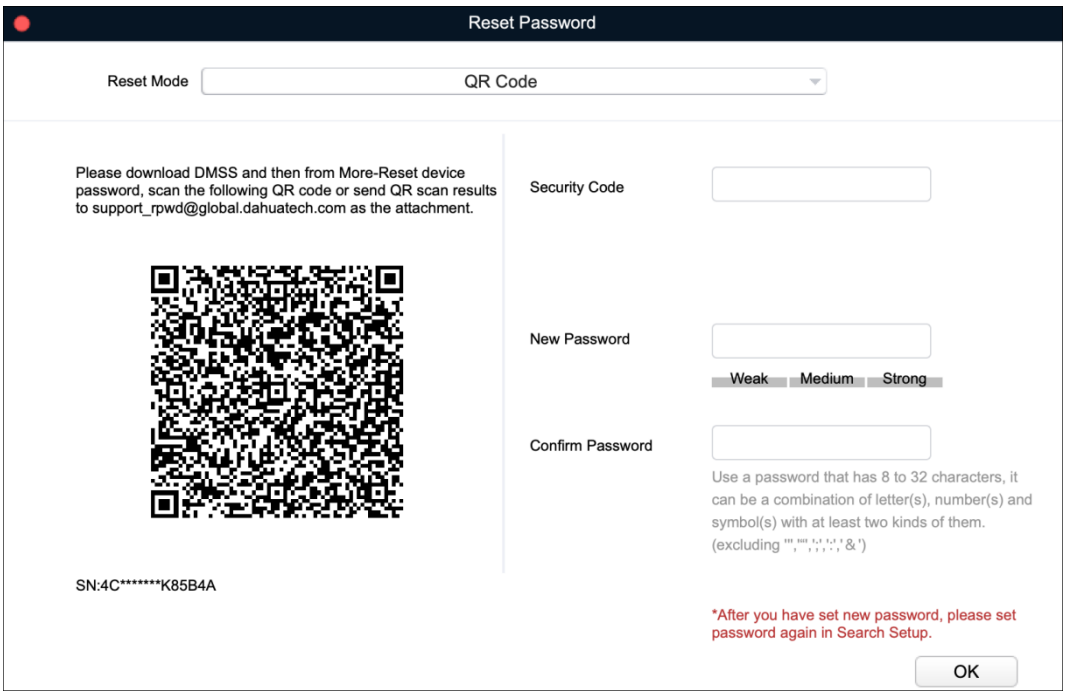


Figure 2-30 Reset password

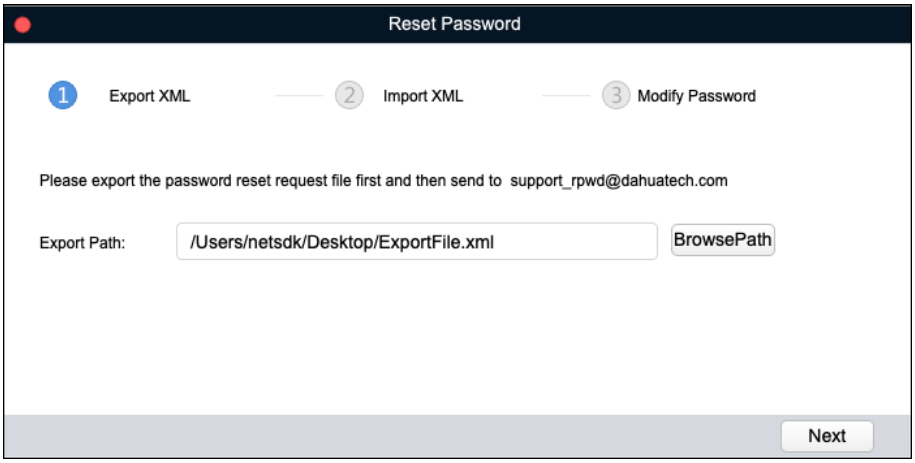


Step 4 Under **Reset Mode**, select **XML File**.

The **Reset Password-Export XML** interface is displayed.

- 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 2-31 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.

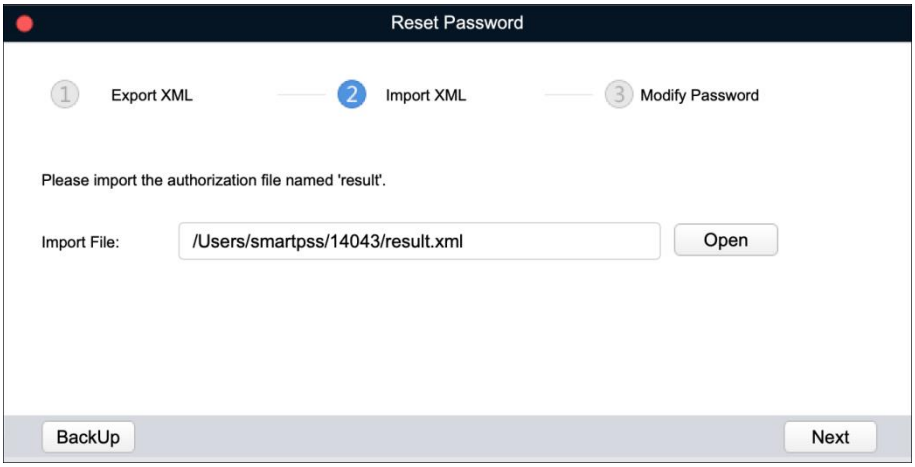
Find the **ExportFile.xml** under the save path and send it as an attachment to the local technical support team. Then you will receive a **result.xml** file from the team.

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.

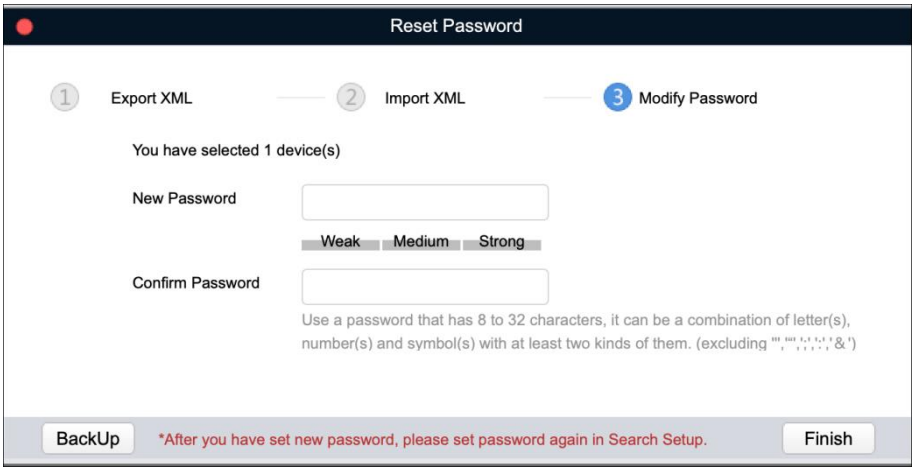
1) Click **Open** to import the **result.xml** file from the save path.

Figure 2-32 Reset password



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

Figure 2-33 Reset password-modify password



Step 7 Modify password.

1) Enter the 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 ' " ; : &).

2) Enter the registered email address, and you can check the **Set to reserved phone** check box to set it as the reserved phone number.
3) Click **Finish** to starting 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.

2.8 Local Upgrade

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

If the device is disconnected during upgrading, the Tool will prompt the disconnection and the device might reboot.

- If the upgrade progress does not exceed 50%, the upgrade package is not completed. Please search and upgrade again after reconnecting the device.
- If the upgrade progress exceeds 50%, the upgrade package is completed and the device will be upgraded successfully. The upgraded device will display after searching once the device is reconnected.

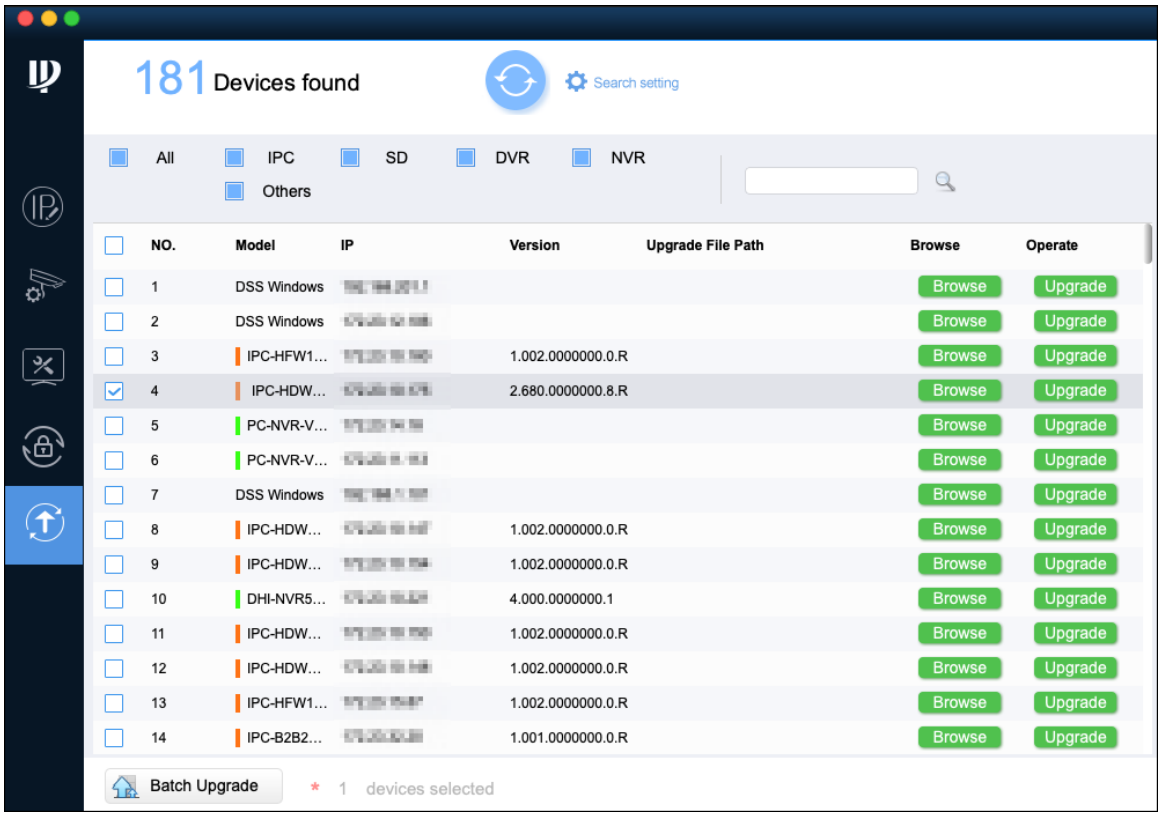
2.8.1 Upgrading One Device

You can choose this procedure for upgrading one device.

Step 1 Click .

The **Upgrade** interface is displayed.

Figure 2-34 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 "2.2 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.

2.8.2 Upgrading Devices in Batches

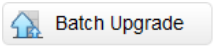
You can upgrade multiple devices to the same software version.

Step 1 Click  .

The **Upgrade** interface is displayed.

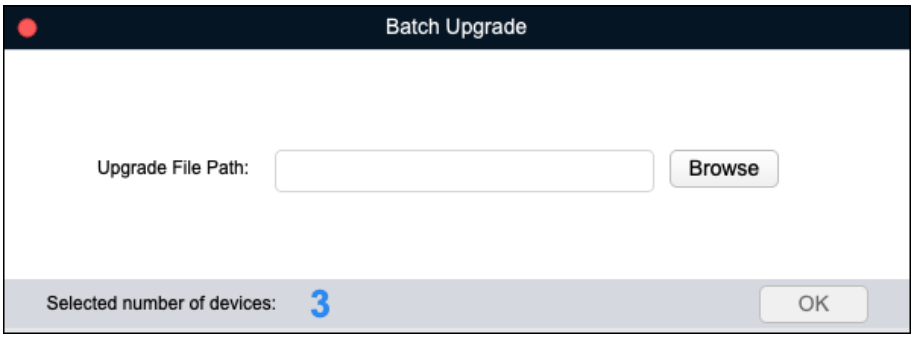
Step 2 Select the devices that need to be upgraded.

- If the device is not in the device list, perform searching again. For the details about how to search devices, see "2.2 Adding Devices."
- Make sure the selected devices are subject to be upgraded to the same software version.

Step 3 Click  .

The **Batch Upgrade** dialog box is displayed.

Figure 2-35 Batch Upgrade



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

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

3 Help

This chapter introduces how to view Help file and software version, how to set network parameters and upgrade parameters, and minimize or exit the software.

3.1 Help File

Click  at the upper-right corner, and then select **Help** to view the *User's Manual.*

3.2 Software Version

Click  and then select **About** to view software version.

3.3 Setting

Click  and then select **Setting**. The **Setting** interface is displayed.

Figure 3-1 Setting

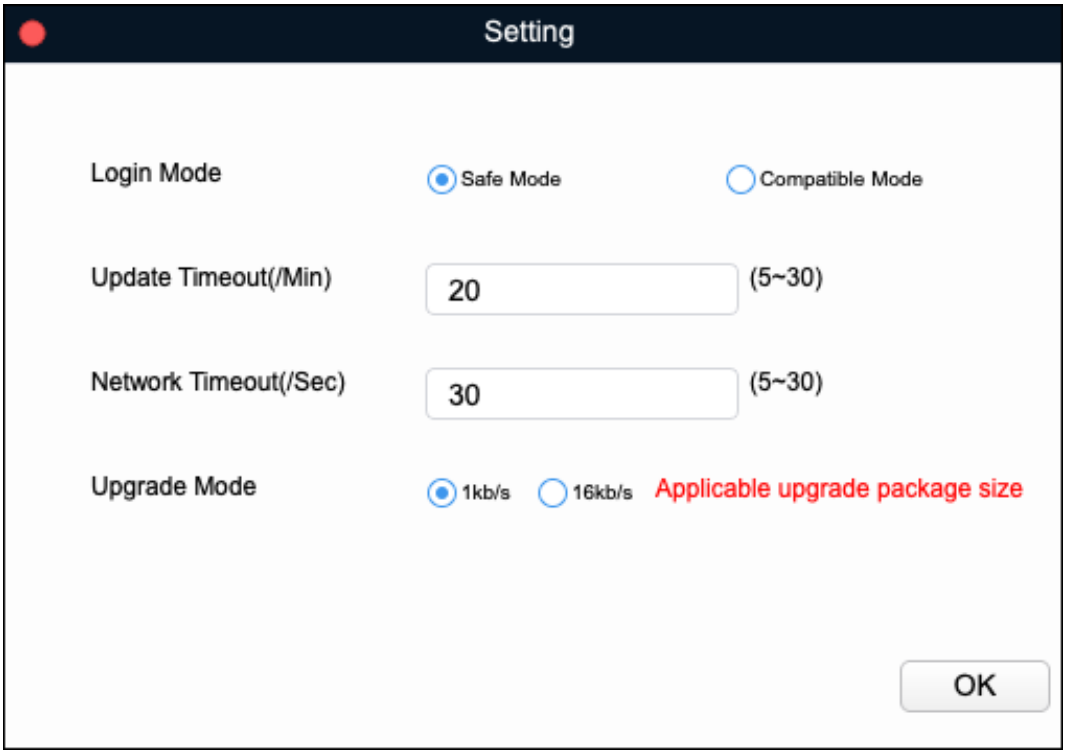


Table 3-1 Setting Parameters

Parameter	Description
Login Mode	● **Security Mode** (default): Log in only with secure authentication method. ● **Compatibility Mode**: Try to log in with secure or insecure authentication method in turn. It has potential risks and is not recommended to use.  Compatibility mode has potential security risks. It is recommended to log in with security mode.
Update Timeout (/Min)	The maximum upgrade time for a single device when the device is upgraded. When the device upgrade time is longer than the set value, the system prompts that the upgrade fails.
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 Mode	Select the transmission speed when upgrading, **1Kb/s** or **16Kb/s**. ● 1Kb/s: Transmit 1Kb data for each time. ● 16Kb/s: Transmit 16Kb data for each time.  Select transmission speed according to upgrade files.

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.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.