VDPConfig
(Windows version)
User's Manual

V1.2.2

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get "hacked" is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

"Nice to have" recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

- Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system's credentials. You will need to either update the camera's firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a

different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

- UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
- If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

Foreword

General

This user's manual (hereinafter referred to be "the Manual") introduces the functions and operations of the VDPConfig (hereinafter referred to be "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

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	February 26, 2016
2	V1.0.1	Update the structure of the Basic Operations chapter.	December 1, 2016
3	V1.0.2	1. Update "Basic Operations". 2. Add "Initializing Devices".	May 5, 2017
4	V1.1.0	1. Add "Cybersecurity Recommendations" and "Online Upgrade". 2. Update "The Main User Interface".	October 25, 2017
5	V1.2.0	1. Add "Project Configuration". 2. Add "Configuring Alarm" and "Configuring Arm/Disarm Settings".	January 15, 2018
6	V1.2.1	1. Add "Privacy Protection Notice". 2. Update "About the Manual".	May 3, 2018

No.	Version	Revision Content	Release Time
7	V1.2.2	1. Move the content of "configuring device" to the Project Configuration as "2.9.2 Maintenance". 2. Modify the SIP template. 3. Delete the VT system function of the Project Configuration.	September 5, 2018

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

1 Overview

CAUTION

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

1.1 General

The Tool configures and maintains the video intercom machines for home and outdoor use by providing the following operations:

- Initialize device.
- Modify device IP.
- Sync device time, reboot device, restore system default, modify password, reset device password, and configure alarm and arm/disarm.
- Export the configurations for video, audio, indoor machine, card management, access password, and access QR code.
- Upgrade device.
- Quickly configure VTO, VTH and IPC under the same unit and configure corresponding matching relationship.

1.2 The Main User Interface

For the main user interface of the Tool, see Figure 1-1, and for the details description, see Table 1-1.

NOTE

- The Tool will search the devices according to the network segments setting in **Search setting** once it is launched.
- After the Tool is installed, the **Current Segment Search** check box is selected by default in the **Search setting** in the first launch.

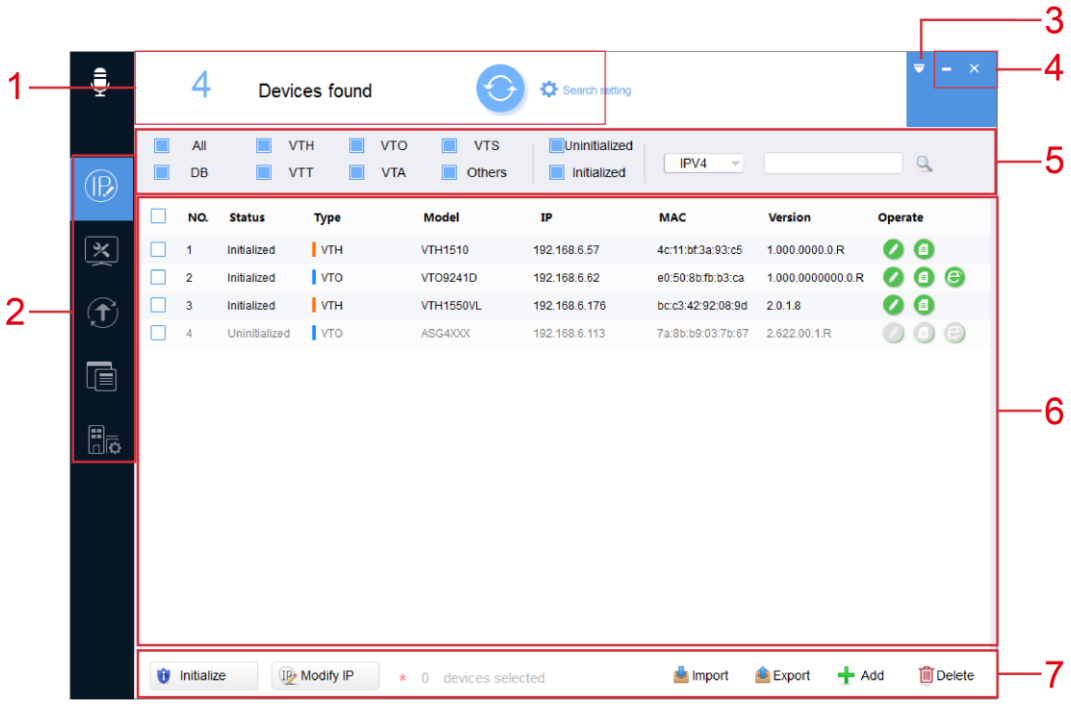


Figure 1-1

No.	Function	Description
1	Search setting	You can search the devices within the current network segment or other network segment. Click to refresh the searched device list.
2	Menu	This function includes Modify IP, Device Config, Upgrade, Template Setup and Project Configuration. • Modify IP ( ): Modify IP for one device or multiple devices. • Device Config ( ): Set device system time, reboot device, restore device, modify password and reset password. • Upgrade ( ): Upgrade local devices individually or in batches. • Template Setup ( ): Manage and apply the template. The template includes the information such as encoding and video configuration information. • Project Configuration ( ): Quickly configure VTO, VTH and IPC under the same unit and configure corresponding matching relationship.
3	System Settings	This function provides access to check the **Help** file and software version, and set network timeout and online upgrade, including enabling online upgrade. For details, see "2.7.1 Enabling Online Upgrade."

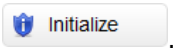
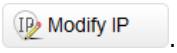
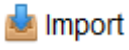
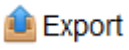
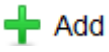
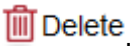
No.	Function	Description
4	Window Control Button	• Click  to minimize the software. • Click  to exit the software.
5	Filtering	This function provides filtering by selecting device type, initial status, and IP version (IPV4 or IPV6) to find the devices quickly. You can also manually enter the conditions such as device type, IP address, model, MAC address and version number to search the devices.
6	Device list	This function shows the searched devices and their information such as type, model, 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.  NOTE It is not supported to modify IP or view device details under IPv6.
7	Function buttons	You can operate the following functions: • Initialization: Select one device and click  . • Batch IP modification: Select devices and click  . • Device import: Click  to import one or multiple devices through template. • Device details export: Select one or multiple devices and click  . • Device addition: Click  to add one or multiple devices manually. • Device deleting from the list: Select one or multiple devices and click  .

Table 1-1

2 Basic Operations

2.1 Searching Devices

You can search the devices through setting the current segment or other segment.

NOTE

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

Step 1 Click .

The **Modify IP** interface is displayed. See Figure 2-1.

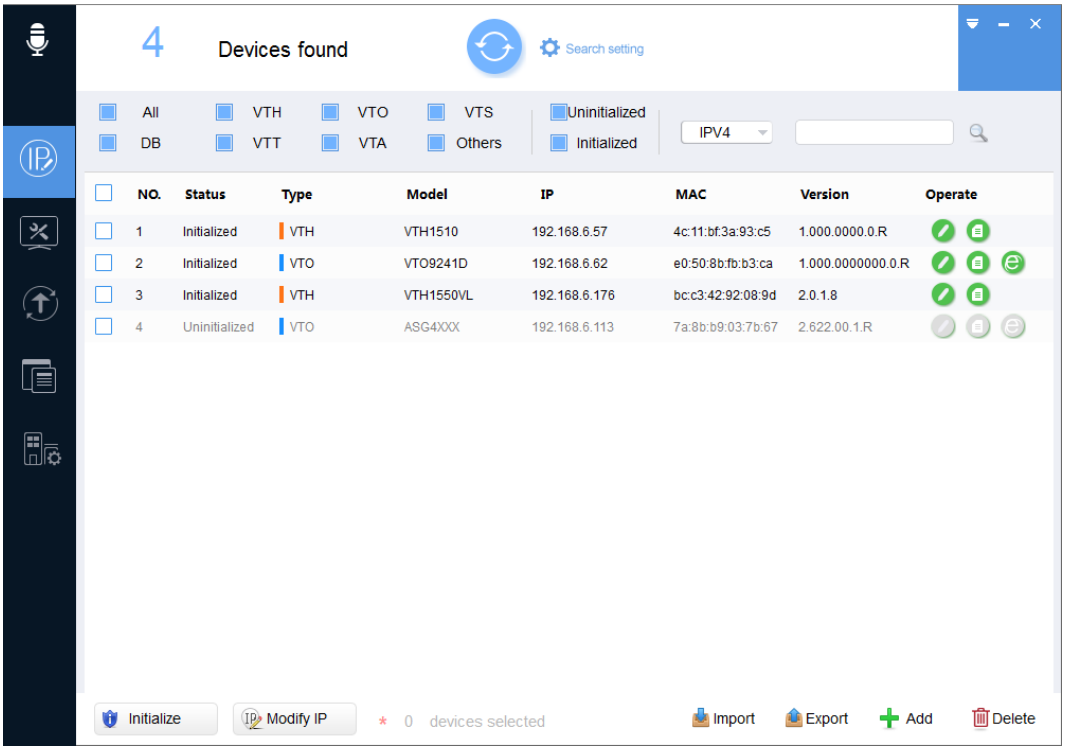


Figure 2-1

Step 2 Click Search setting.

The **Setting** dialog box is displayed. See Figure 2-2.

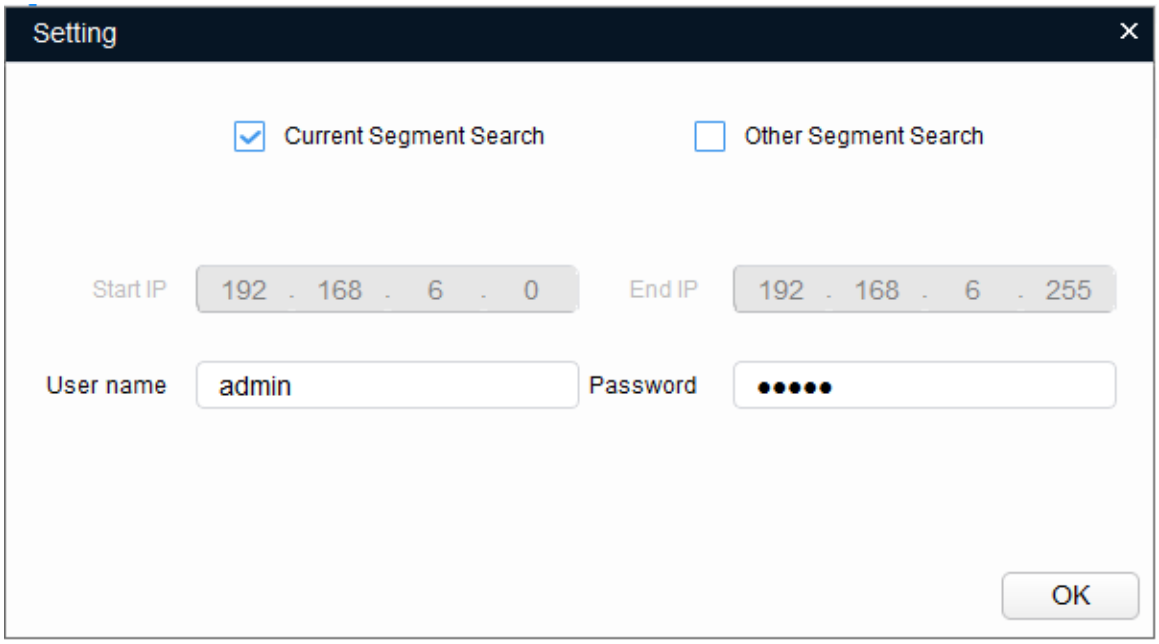


Figure 2-2

Step 3 Select the searching way.

- 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 **Current Segment Search** check box is selected by default.
  The **Current Segment Search** indicates the LAN search. When you select the **Current Segment Search** check box, the system will search the devices in the LAN.
- 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.
  When you select the **Other Segment Search** check box, make sure the network is connected between the PC and the device, and then the system will search the devices by IP address.

NOTE

- 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 also used to login the device when you want to modify IP, configure the system and update the device.

Step 4 Click **OK** to start searching the devices.

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

NOTE

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

2.2 Adding Devices

You can add one or multiple devices according to the actual situation.

CAUTION

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 choose this procedure for adding one device.

NOTE

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

Step 1 Click .

The **Modify IP** interface is displayed.

Step 2 Click Add.

The **Manual Add** dialog box is displayed. See Figure 2-3.

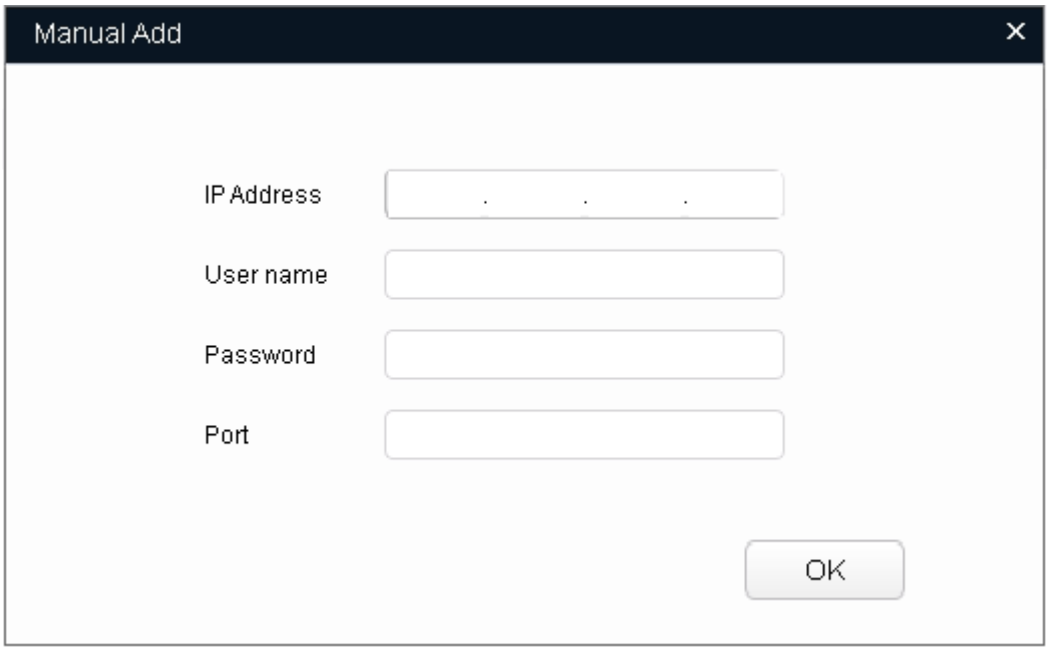


Figure 2-3

Step 3 Set the device parameters. See Table 2-1.

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

Table 2-1

Step 4 Click **OK**.

The newly added device appears in the device list.

2.2.2 Adding Multiple Devices

You can add multiple devices through importing the template.

CAUTION

Please use "Microsoft Excel" instead of "WPS Office", and the version of "Microsoft Excel" should be above "Microsoft Excel 2007".

2.2.2.1 Accessing the Template

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

Step 1 Click .

The **Modify IP** interface is displayed.

Step 2 Select one or multiple devices, and then click Export .

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

Step 3 Select the save path, and then enter file name in the **File name** box.

Step 4 Click **Save**.

After the exporting is completed, a **Notice** dialog box indicating export result is displayed.

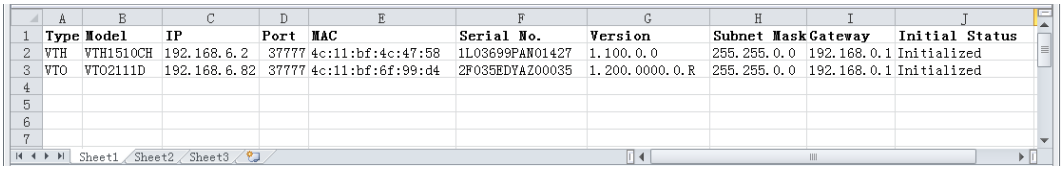
Step 5 Click **OK**.

2.2.2.2 Filling in the Template

Step 1 Find the template in the save path, and then open it. See Figure 2-4.

NOTE

- The example in the template is for reference only.
- To delete the record in the template, right-click the record line, and then select **Delete**.



	A	B	C	D	E	F	G	H	I	J
1	Type	Model	IP	Port	MAC	Serial No.	Version	Subnet Mask	Gateway	Initial Status
2	VTH	VTH1510CH	192.168.6.2	37777	4c:11:bf:4c:47:58	1L03699PAN01427	1.100.0.0	255.255.0.0	192.168.0.1	Initialized
3	VTO	VTO2111D	192.168.6.82	37777	4c:11:bf:6f:99:d4	2F035EDYAZ00035	1.200.0000.0.R	255.255.0.0	192.168.0.1	Initialized
4										
5										
6										
7										

Sheet1 Sheet2 Sheet3

Figure 2-4

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

Parameter	Description
Type	Mandatory. Device type, enter VTH, VTO, VTS, DB, VTT, VTA or OTHER.
Model	Optional. Device model.
IP	Mandatory. IP address of device.
Port	Mandatory. Port number of device.
MAC	Mandatory. Device MAC address that can be obtained from the device label.
Serial No.	Optional. Device serial number.
Version	Optional. Device version number.
Subnet Mask	Mandatory. Device subnet mask.
Gateway	Mandatory. Device gateway.
Initial Status	Mandatory. Device initialization status: Initialized or uninitialized.
Room Num or VTO Num	Optional. Enter the VTH room number or the VTO number.

Table 2-2

Step 3 Save and close the template.

2.2.2.3 Importing Devices

You can import the filled template to add device.

CAUTION

Close the template file before importing.

Step 1 Click .

The **Modify IP** interface is displayed. See Figure 2-5.

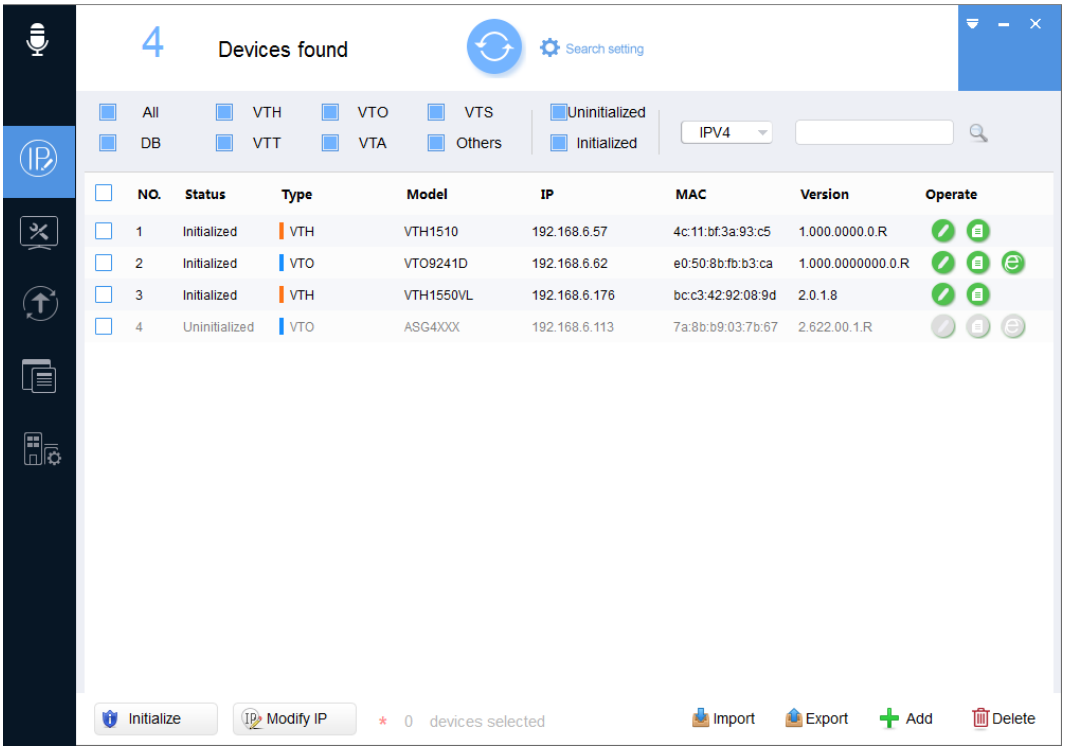


Figure 2-5

Step 2 Click Import.

The **Open** dialog box is displayed.

Step 3 Select the template, and then click **Open**.

After the importing is completed, a **Notice** dialog box indicating import result is displayed.

Step 4 Click **OK**.

The newly imported devices appear in the device list. See Figure 2-6.

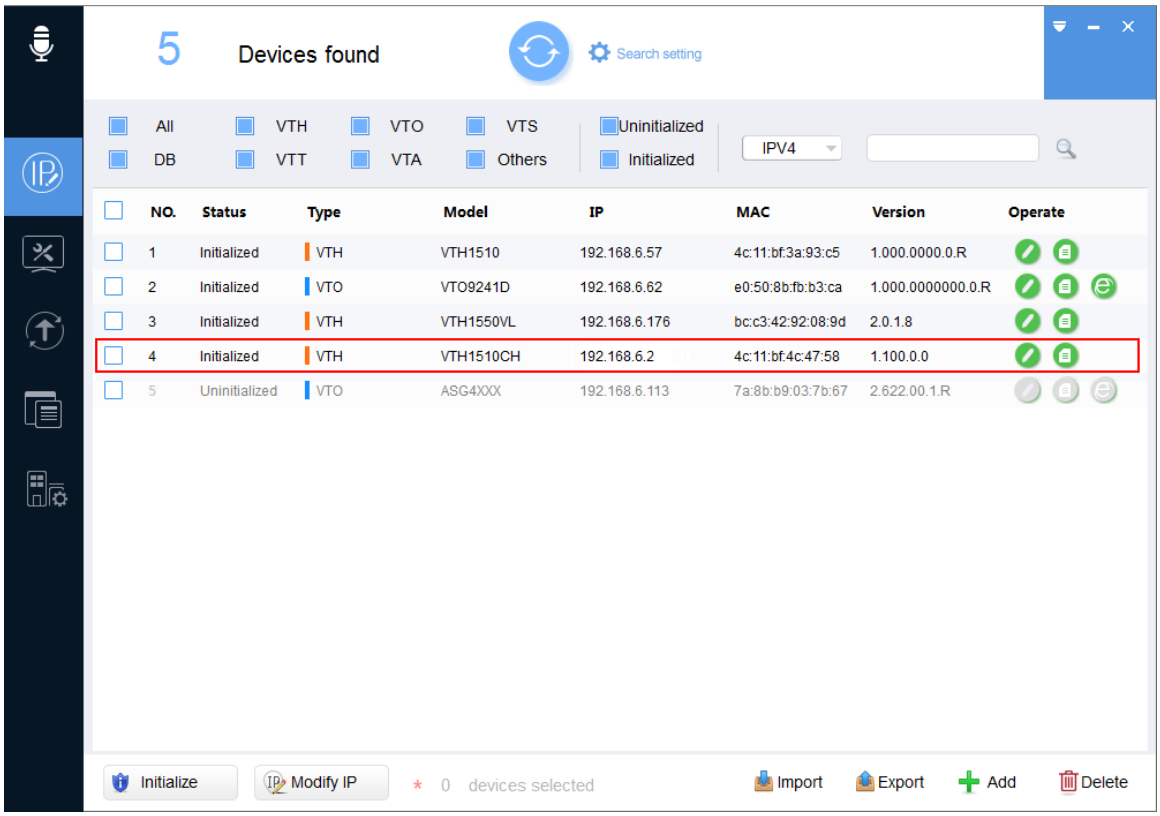


Figure 2-6

2.3 Initializing Devices

You can initialize one or multiple devices.

NOTE

- Not all models support this function.
- The initializing operation can only be performed to the devices within the same local area network.
- You cannot operate the uninitialized devices that are shown in gray background. And the uninitialized devices do not appear in other interfaces of the Tool.

Step 1 Click .

The **Modify IP** interface is displayed. See Figure 2-7.

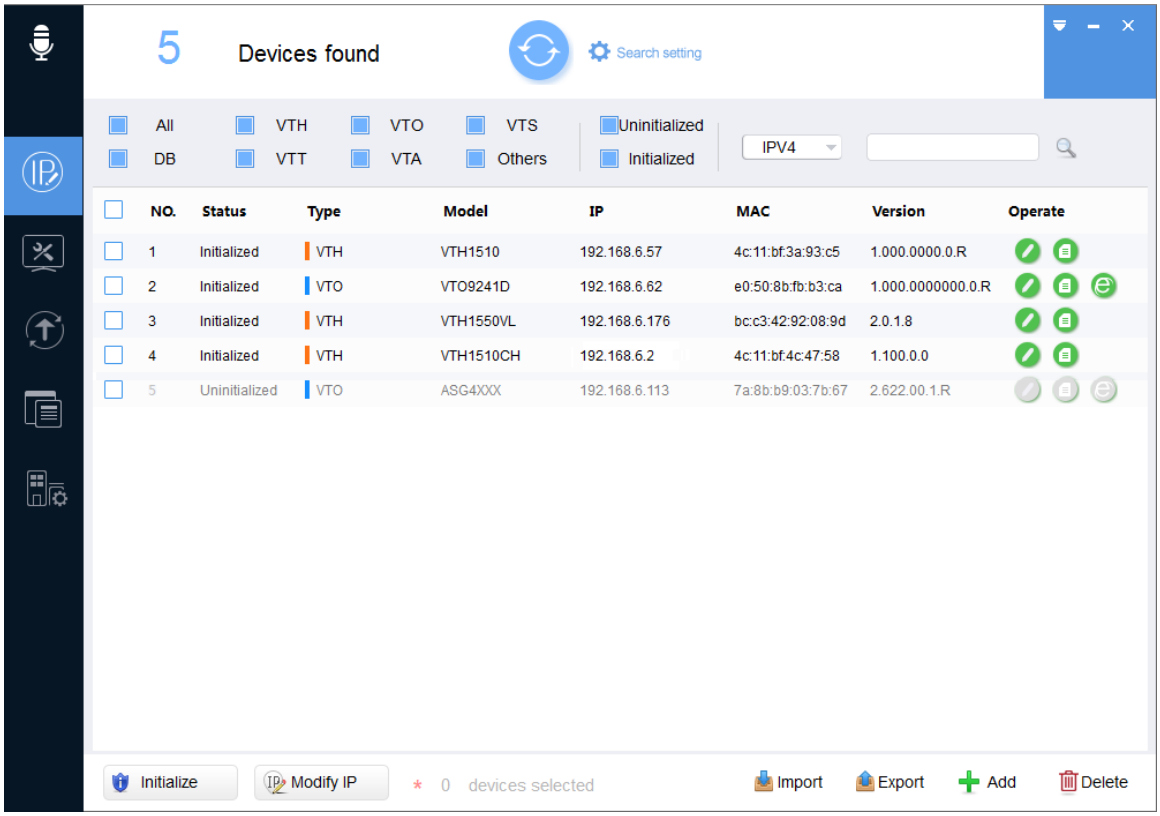


Figure 2-7

Step 2 Select an uninitialized device.

Step 3 Click Initialize.

The **Device initialization** interface is displayed. See Figure 2-8.

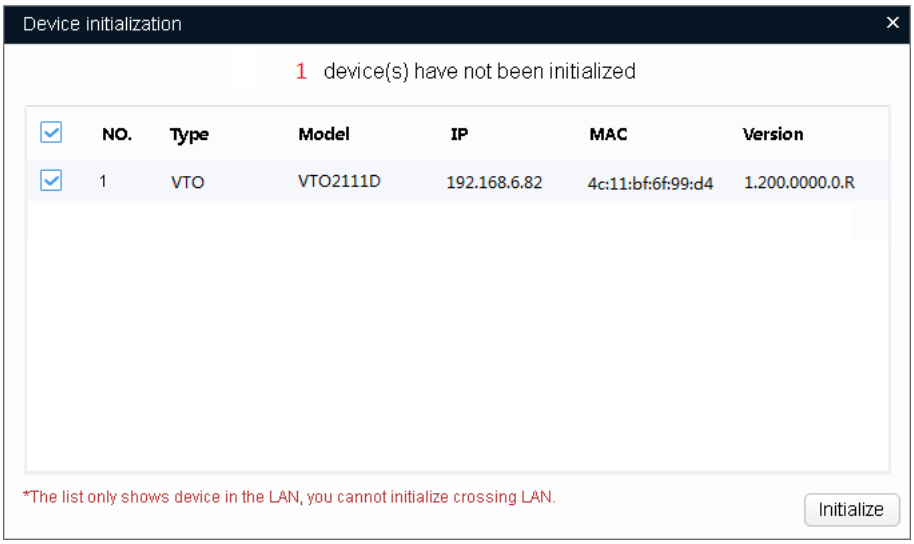


Figure 2-8

Step 4 Select the device, and then click **Initialize**.

The **Device initialization** interface is displayed. See Figure 2-9.

NOTE

- The user interface might be different dependent on the model you purchased. If there is inconsistency between the Manual and the actual product, the actual product shall govern.
- If you do not provide the reserve information for password reset, you can reset the password only through XML file.

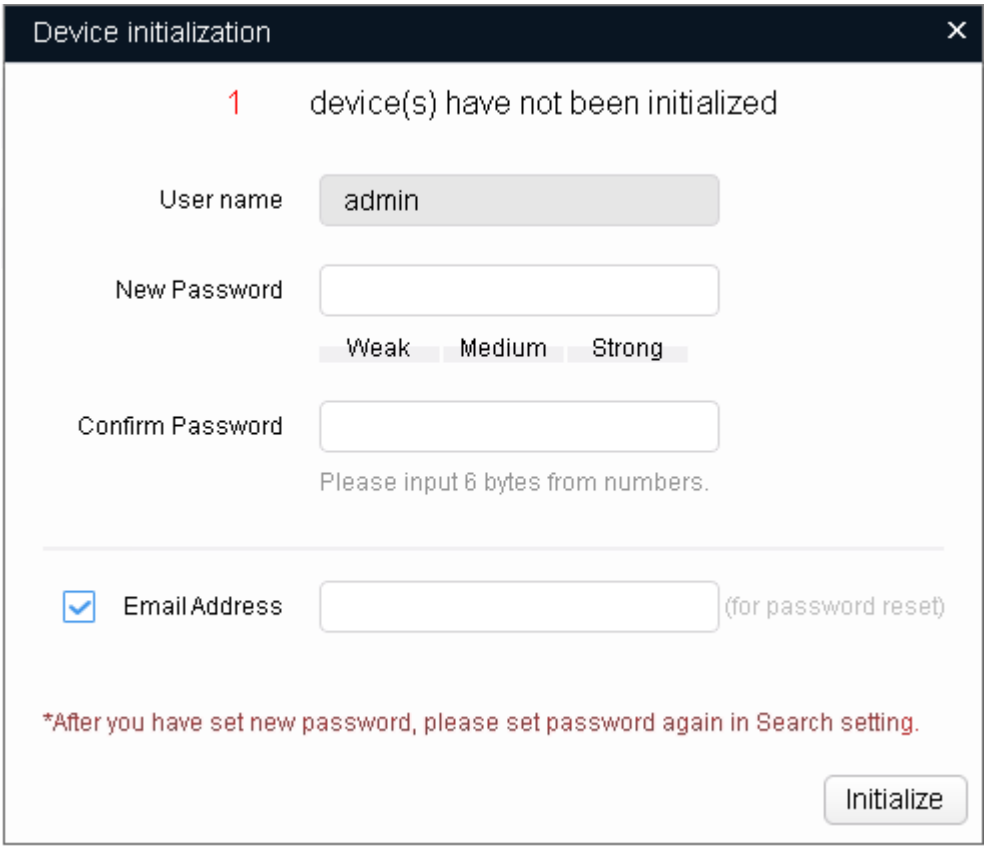


Figure 2-9

Step 5 Set the initialization parameters for the device. See Table 2-3.

Parameter	Description
User name	By default, the user name is **admin**.
New Password	There are two setting rules for new password dependent on the devices, and please following the instructions on the interface to set the new password. ● The new password can be set from 8 characters through 32 characters and contain at least two types from number, letter and special characters (excluding "'", '"', ";", ":" and "&"). ● The new password can only be set as six numbers. NOTE After setting the new password, please enter the new password in the **Search setting**.
Confirm Password	Confirm the new password.
Email Address	Selected by default. The email address will be used for password reset.

Table 2-3

Step 6 Click **Initialize**.

The **Device initialization** interface is displayed. See Figure 2-10.

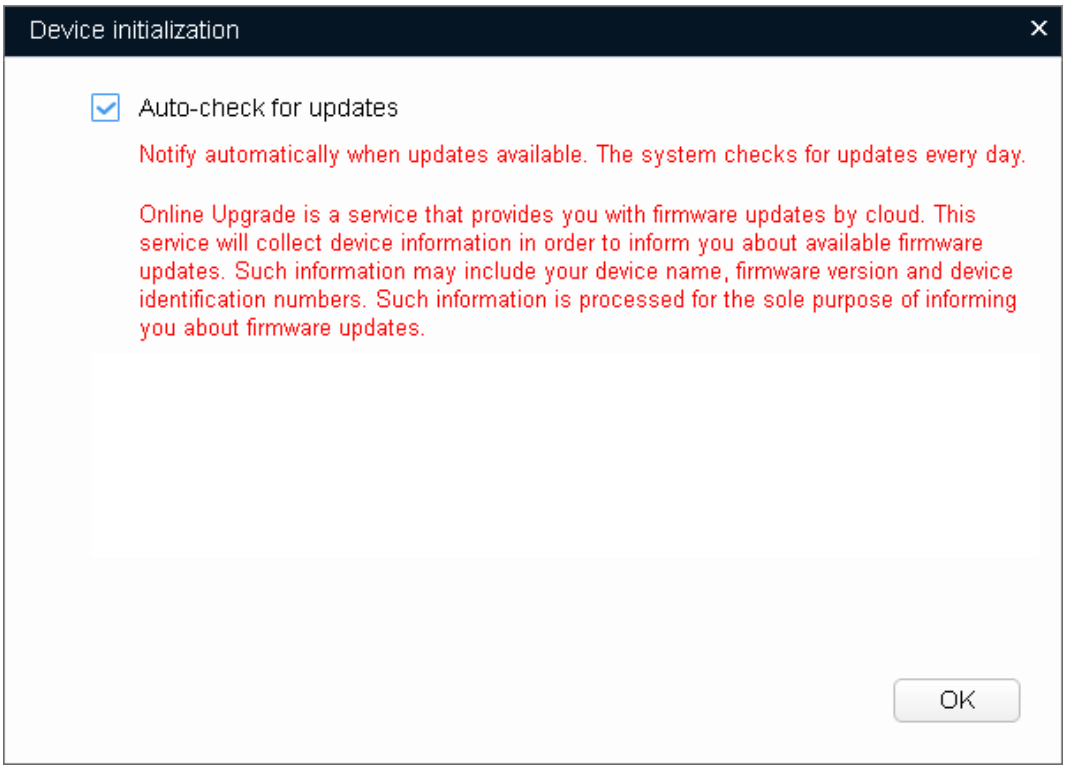


Figure 2-10

Step 7 Select the **Auto-check for updates** check box.

Step 8 Click **OK** to start initializing the device.

The **Initialization** interface is displayed after initializing is completed. See Figure 2-11.

You can click the success icon ( ) or click the failure icon ( ) for the details.

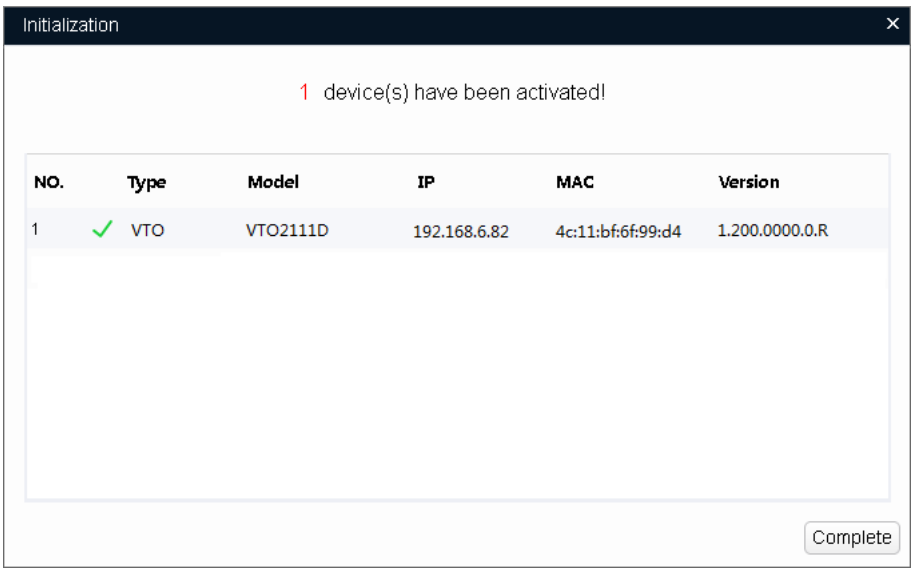


Figure 2-11

Step 9 Click **Complete**.

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

2.4 Modifying IP

You can modify IP for one or multiple devices according to the actual situation.

- When the devices quantity is small or their login passwords are different, you can modify one IP at a time.
- When the devices quantity is big and they share the same login password, you can modify IP in batches.

2.4.1 Modifying One IP

You can choose this procedure for modifying one IP.

Step 1 Click .

The **Modify IP** interface is displayed. See Figure 2-12.

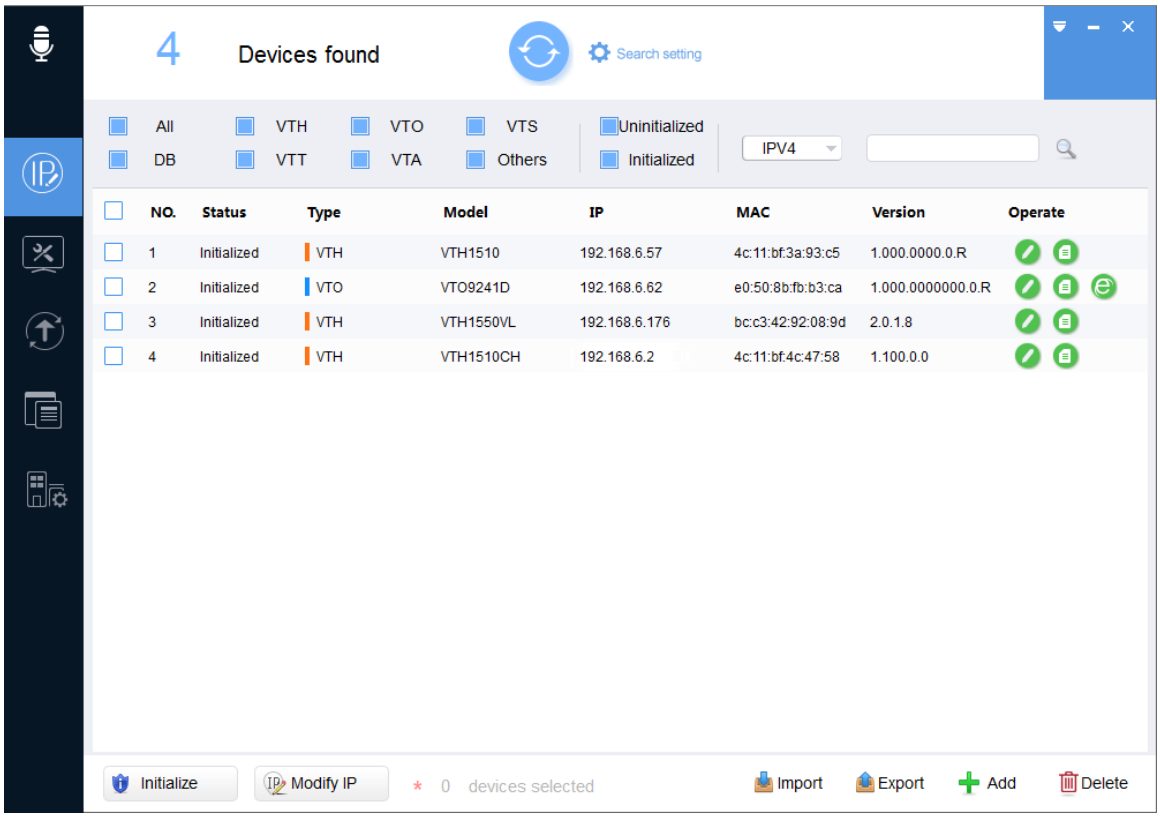


Figure 2-12

Step 2 Click the **IP Modification** button ( ) of the device that you want to modify IP.

The **Modify IP Address** dialog box is displayed. See Figure 2-13.

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

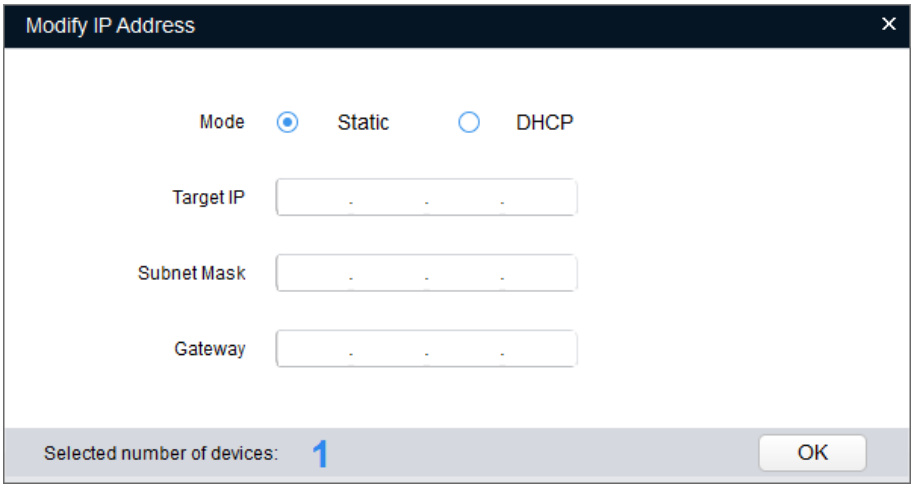


Figure 2-13

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

- 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.
- 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.

NOTE

The VTO does not support DHCP mode.

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

2.4.2 Modifying IP in Batches

You can choose this procedure for modifying IP for multiple devices at a time.

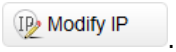
Step 1 Click  .

The **Modify IP** interface is displayed.

Step 2 Select the devices you want to modify IP.

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

Step 3 Click 

.

The **Modify IP Address** dialog box is displayed. See Figure 2-14.

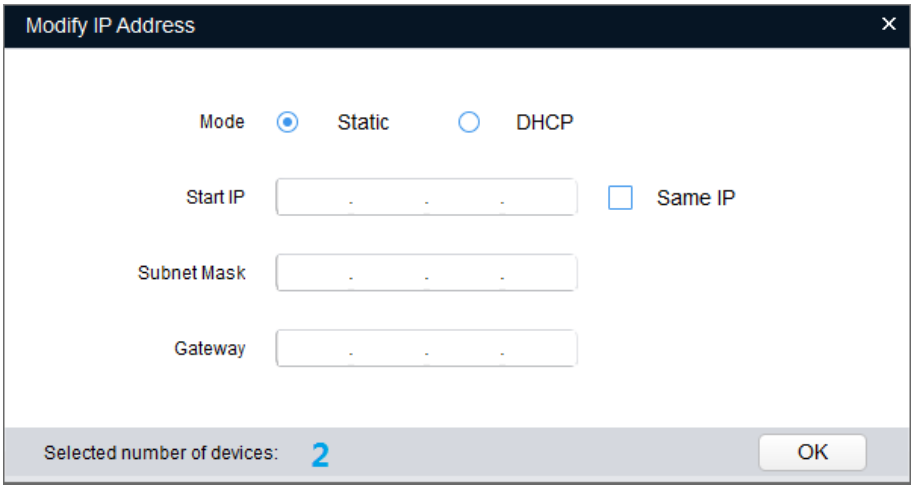


Figure 2-14

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

- 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.
- 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.

NOTE

The VTO does not support DHCP mode.

NOTE

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

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

2.5 Configuring System Settings

You can configure the settings for system time, reboot, restore, password modification and reset.

Click  to enter the system configuration interface.

2.5.1 Timing

You can calibrate the device time through configuration.

Step 1 On the system configuration interface, click the **Timing** tab.

The **Timing** interface is displayed. See Figure 2-15.

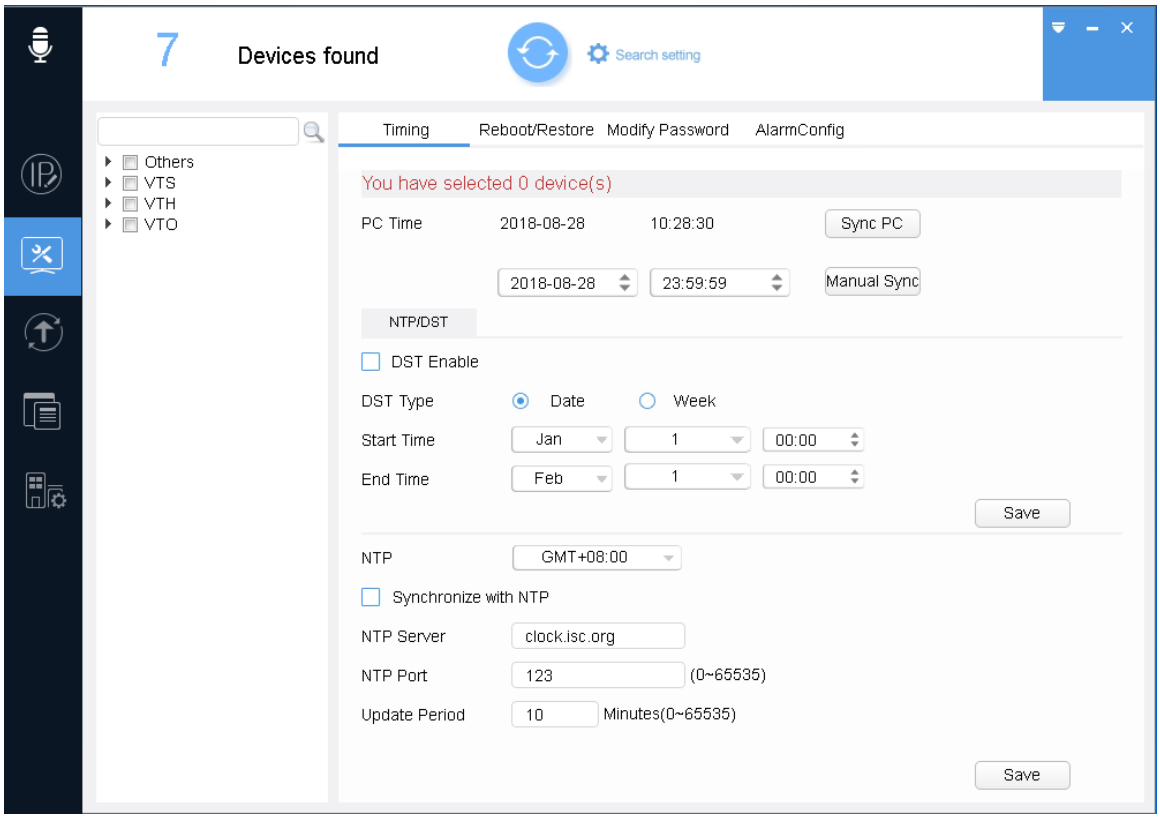


Figure 2-15

Step 2 Click ▸ next to the device type.

The device list is displayed.

Step 3 Select one or multiple devices.

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching 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 the **Synchronize with NTP** check box and set the parameters. See Table 2-4. Then click **Save**.

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

Table 2-4

Step 5 (Optional) Select the **DST Enable** (Daylight Saving Time) check box and set the parameters. See Table 2-5. Then click **Save**.

NOTE

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

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

Table 2-5

2.5.2 Rebooting and Restoring

2.5.2.1 Rebooting

You can set the time to automatically reboot device and manually reboot device.

CAUTION

Rebooting will interrupt the business. Please stop other operations before rebooting device.

Step 1 On the system configuration interface, click the **Reboot/Restore** tab.

The **Reboot/Restore** interface is displayed. See Figure 2-16.

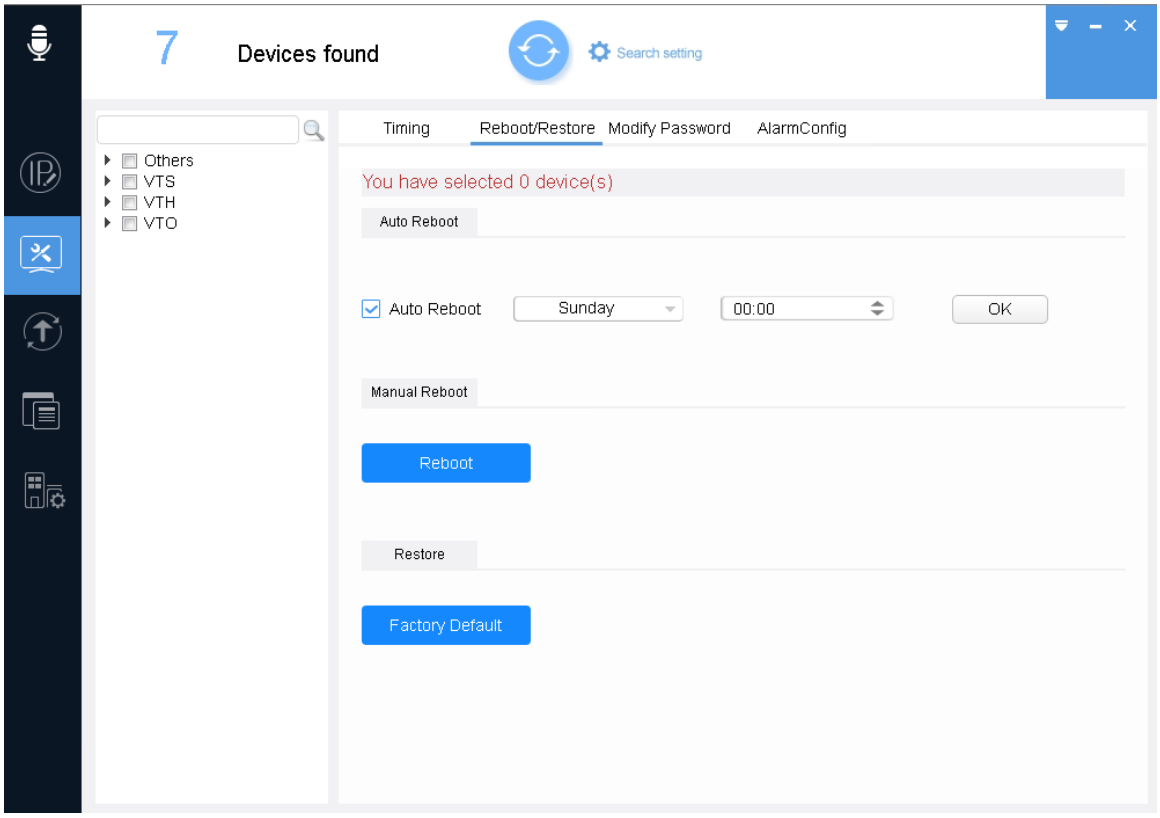


Figure 2-16

Step 2 Click ▸ next to the device type.

The device list is displayed.

Step 3 Select one or multiple devices.

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

Step 4 Select the reboot type for the device according to the actual situation.

- Auto reboot: In the **Auto Reboot** area, select the **Auto Reboot** check box, set the time according to the actual situation, and then click **OK**. The device will reboot at the set time.
- Manual reboot: In the **Manual Reboot** area, click **Reboot** to reboot device immediately.

2.5.2.2 Restoring

You can restore the factory settings to clear configurations and account files.

NOTE

Not all devices support clearing network configurations and account files. For some devices, it only supports restoring NTP and DST settings.

Step 1 On the system configuration interface, click the **Reboot/Restore** tab.

The **Reboot/Restore** interface is displayed. See Figure 2-17.

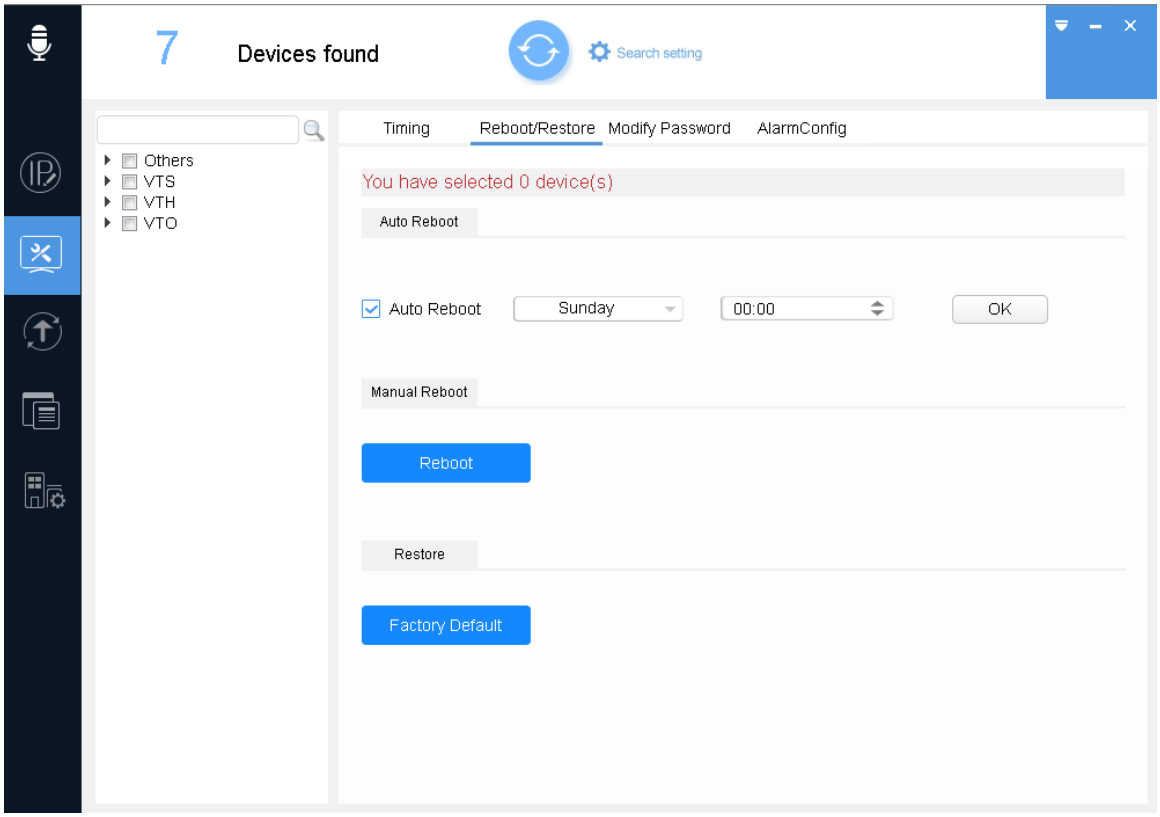


Figure 2-17

Step 2 Click ▶ next to the device type.

The device list is displayed.

Step 3 Select one or multiple devices.

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

Step 4 Click **Factory Default** to start restoring.

After restoring is completed, the result is displayed. See Figure 2-18.

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

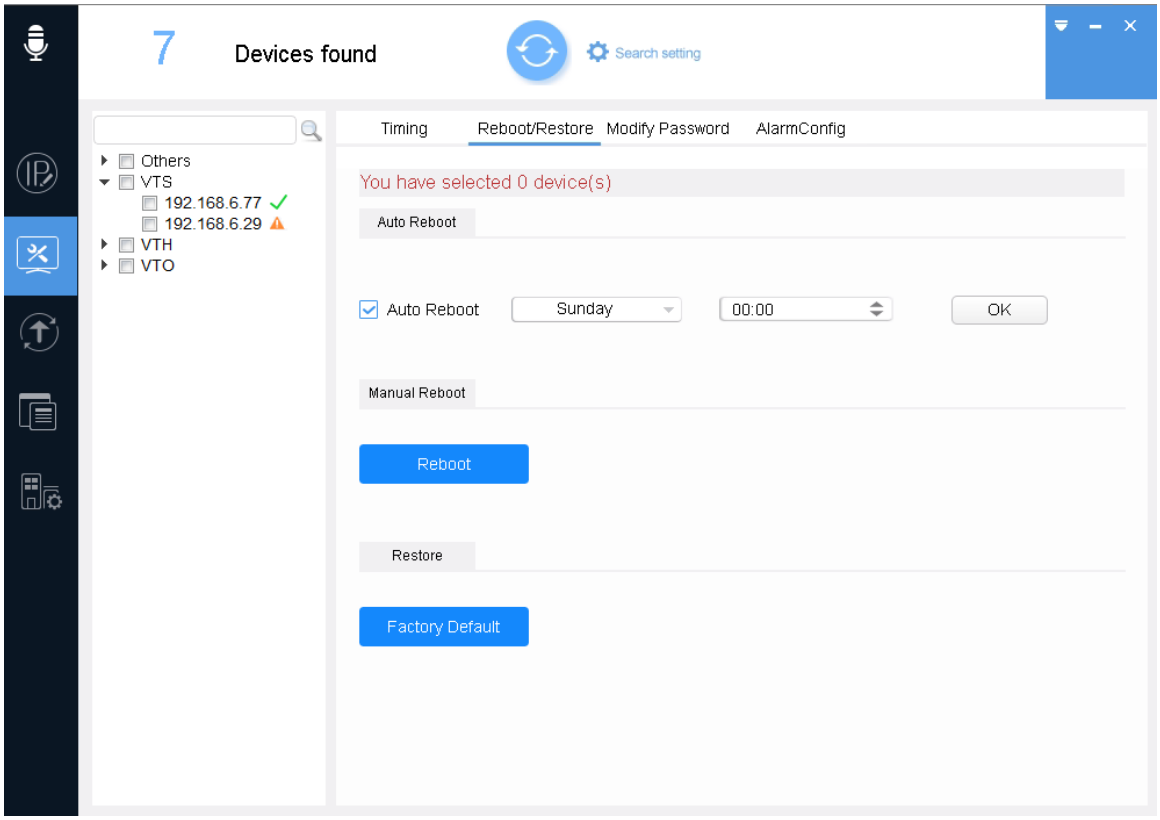


Figure 2-18

2.5.3 Modifying and Reset Password

2.5.3.1 Modifying Password

You can modify the device login password.

Step 1 On the system configuration interface, click the **Modify Password** tab.

The **Modify Password** interface is displayed. See Figure 2-19.

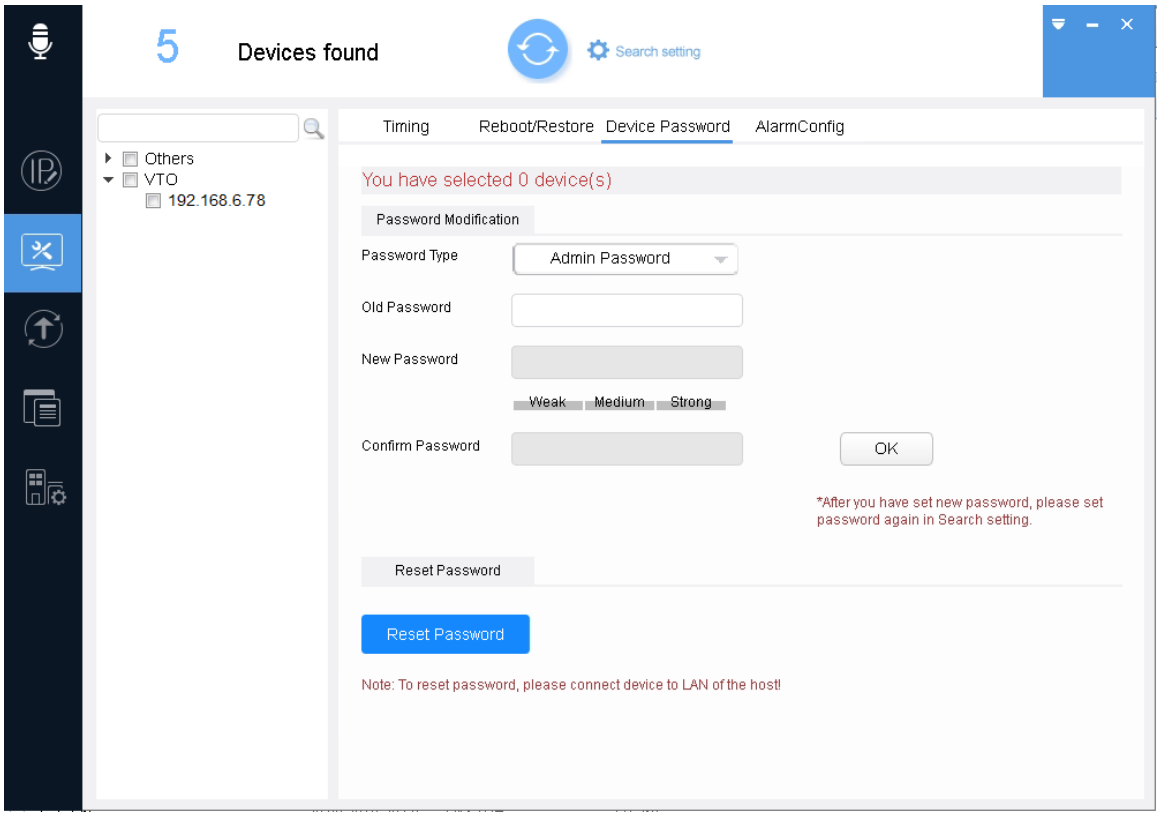


Figure 2-19

Step 2 Click ▸ next to the device type.

The device list is displayed.

Step 3 Select one or multiple devices.

NOTE

- If you select multiple devices, their login passwords must be the same.
- If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

Step 4 In the **Password Type** list, select **Admin Password** or **User Password**.

NOTE

- Only VTH supports modifying **User Password**.
- If you modify the passwords for multiple devices including VTH, there are two situations:
  - ◇ If you select the **User Password**, you can only modify password of VTH.
  - ◇ If you select the **Admin Password**, you can modify the passwords for all selected devices.

Step 5 Enter the old password, and then click **OK**.

The password setting rules is displayed. See Figure 2-20.

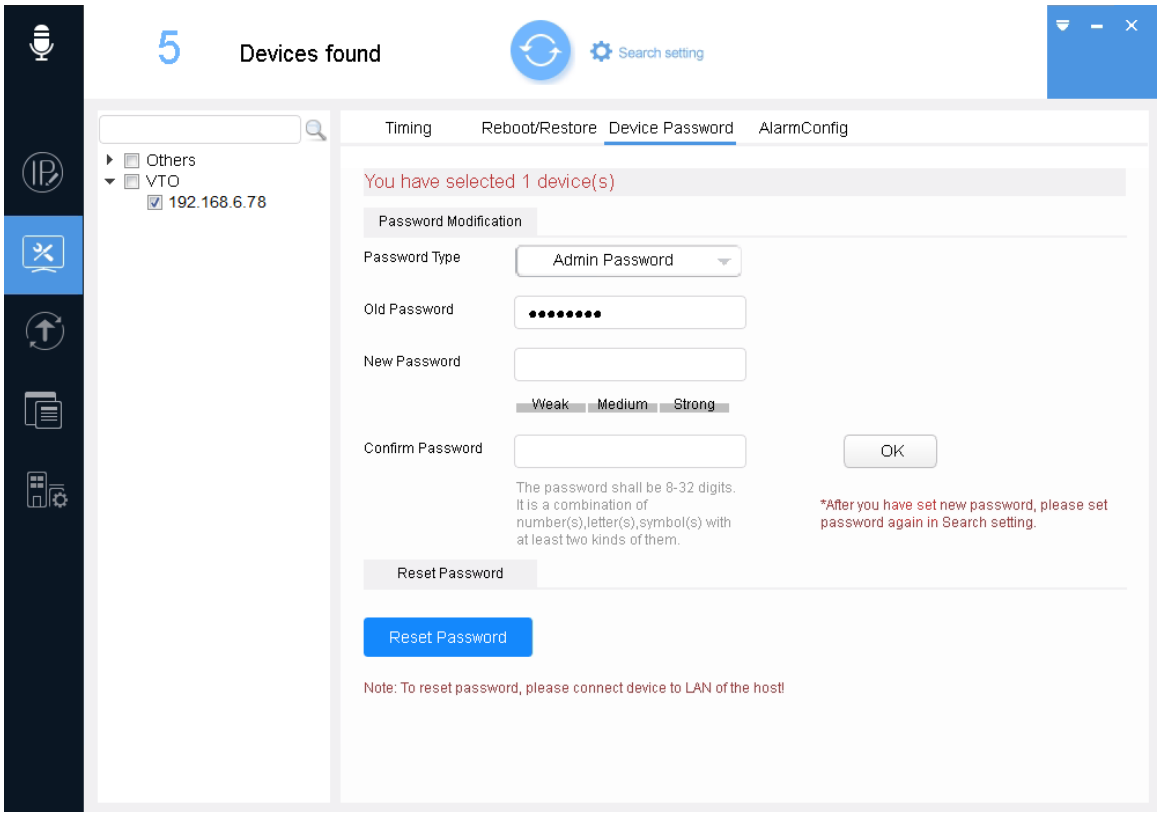


Figure 2-20

Step 6 Enter the new password and confirm password.

There are two setting rules for new password depending on the devices, and please following the instructions on the interface to set the new password.

- The new password can be set from 8 characters through 32 characters and contain at least two types from number, letter and special characters (excluding"'", """, ";", ":" and "&").
- The new password can only be set as six numbers.

NOTE

- Not all devices support the above password rules. The actual interface shall govern.
- After setting the new password, when you search the devices by **Search setting**, use the new password to login the device.

Step 7 Click **OK** to complete modification.

NOTE

- 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.
- If the default password of admin has been changed, it might not be able to change to the default password again depending on the device.

2.5.3.2 Resetting Password

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

NOTE

- The password resetting operation can only be performed to the devices within the same 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.

2.5.3.2.1 Using the QR Code

You can reset the password by scanning the QR code. This procedure can only reset one device at a time.

Step 1 On the system configuration interface, click the **Modify Password** tab.

The **Modify Password** interface is displayed. See Figure 2-21.

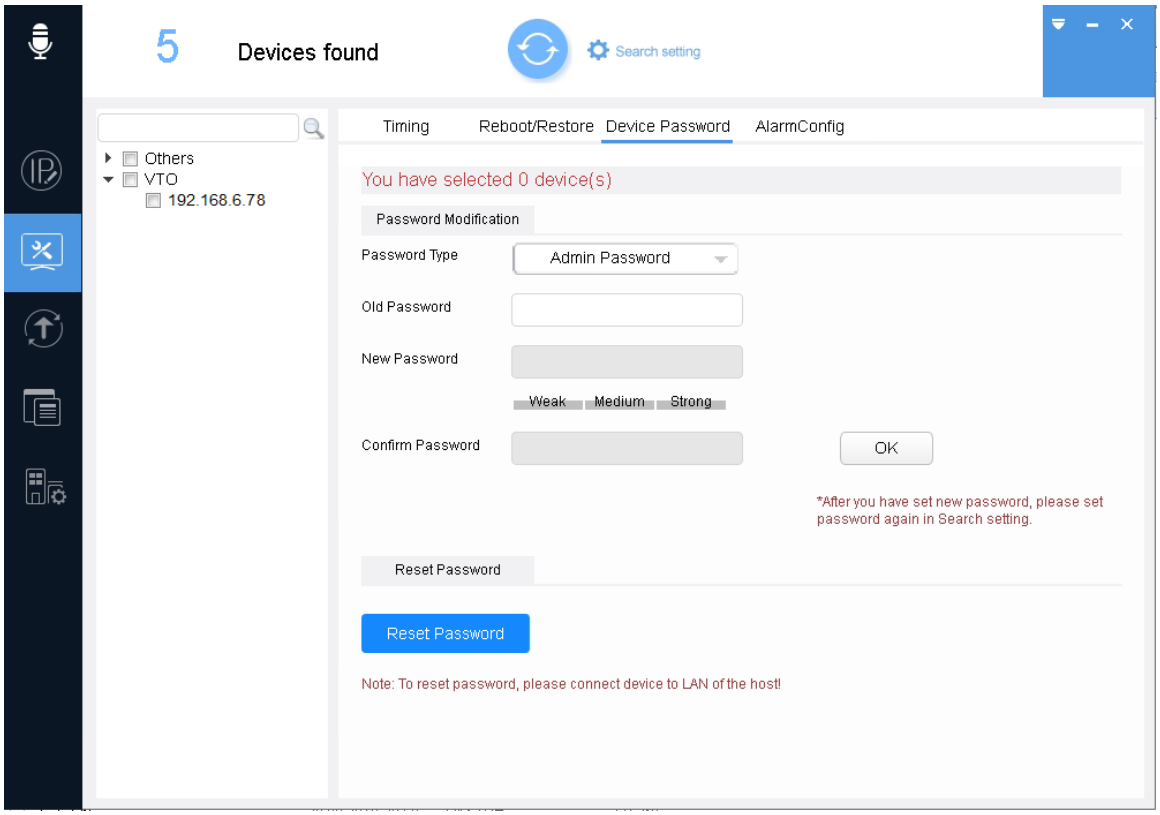


Figure 2-21

Step 2 Click ▶ next to the device type.

The device list is displayed.

Step 3 Select the device that needs to reset the password.

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

Step 4 Click **Reset Password**.

- If the device does not support this function, a **Notice** dialog box is displayed.
- If the device supports this function, the **Reset Password** interface is displayed. See Figure 2-22.

NOTE

The user interface might be different dependent on the model you purchased. If there is inconsistency between the Manual and the actual product, the actual product shall govern.

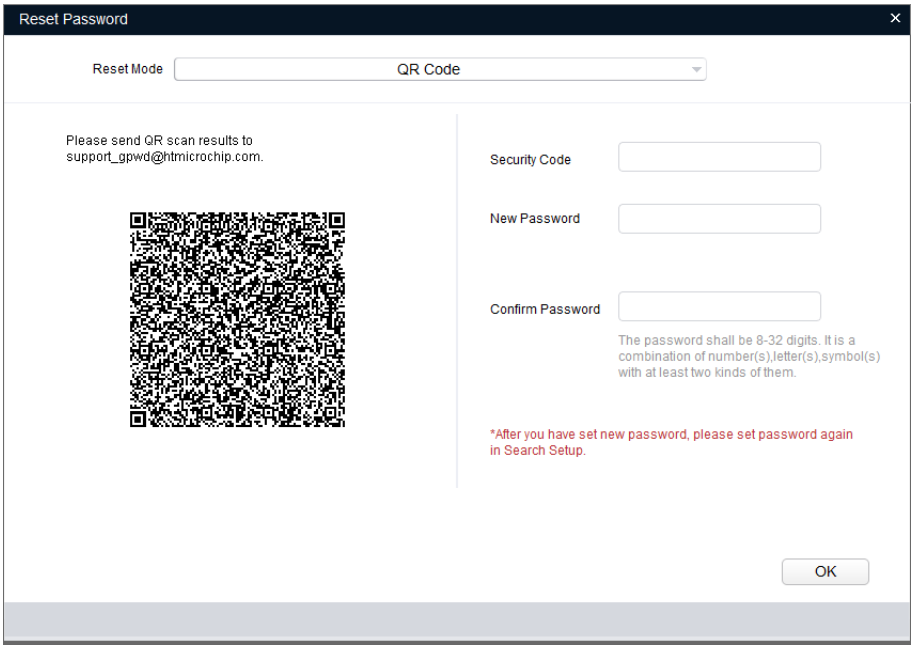


Figure 2-22

Step 5 In the **Reset Mode** list, select **QR Code**.

Step 6 Obtain the security code according to the instructions on the interface.

CAUTION

After you receive the security code, please use it to reset the password within 24 hours; otherwise the security code will become invalid.

Step 7 Enter the security code, new password, and confirm password.

There are two setting rules for new password dependent on the devices, and please follow the instructions on the interface to set the new password.

- The new password can be set from 8 characters through 32 characters and contain at least two types from number, letter and special characters (excluding"'", """, ";", ":" and "&").
- The new password can only be set as six numbers.

NOTE

After setting the new password, please enter the new password in the **Search setting**.

Step 8 Click **OK** to start resetting the password.

After resetting is completed, the result is displayed. See Figure 2-23.

You can click the success icon ( ) or click the failure icon ( ) for the details.

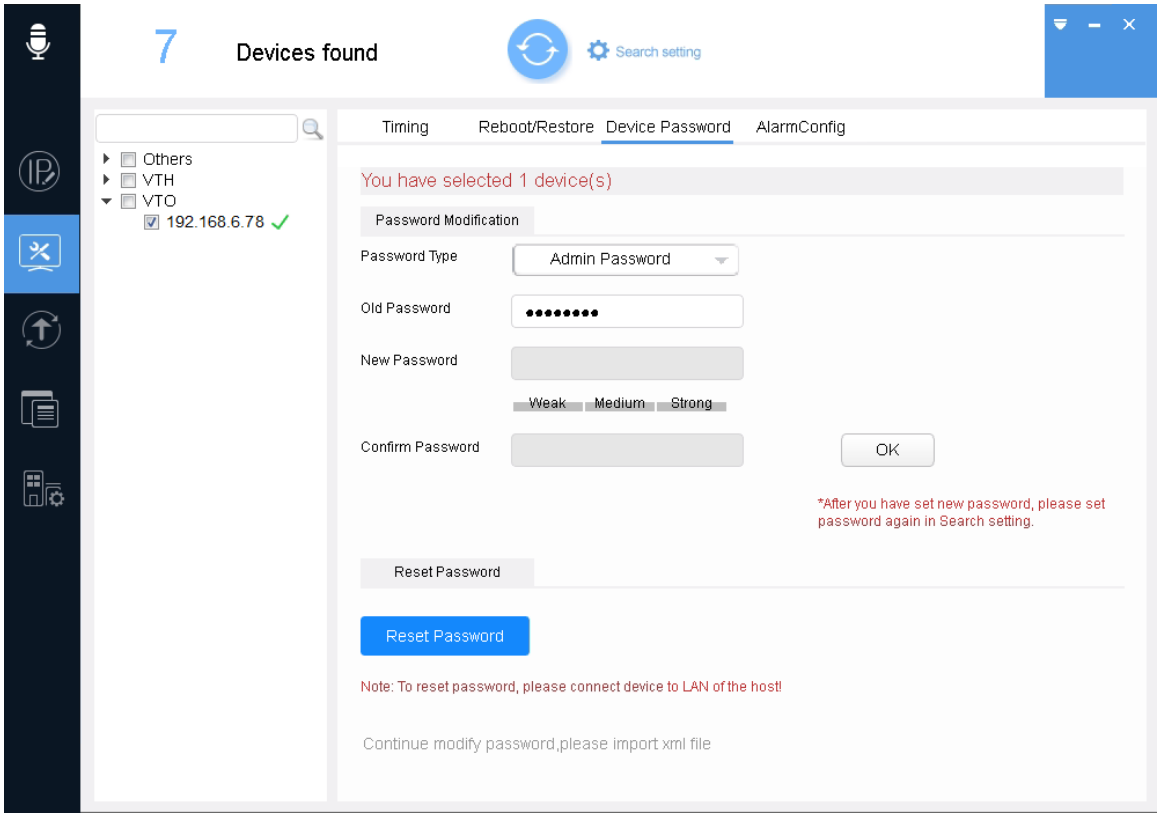


Figure 2-23

2.5.3.2.2 Using the XML File

You can also reset the password by XML file for one device at a time.

Step 1 On the system configuration interface, click the **Reset Password** tab.

The **Reset Password** interface is displayed. See Figure 2-24.

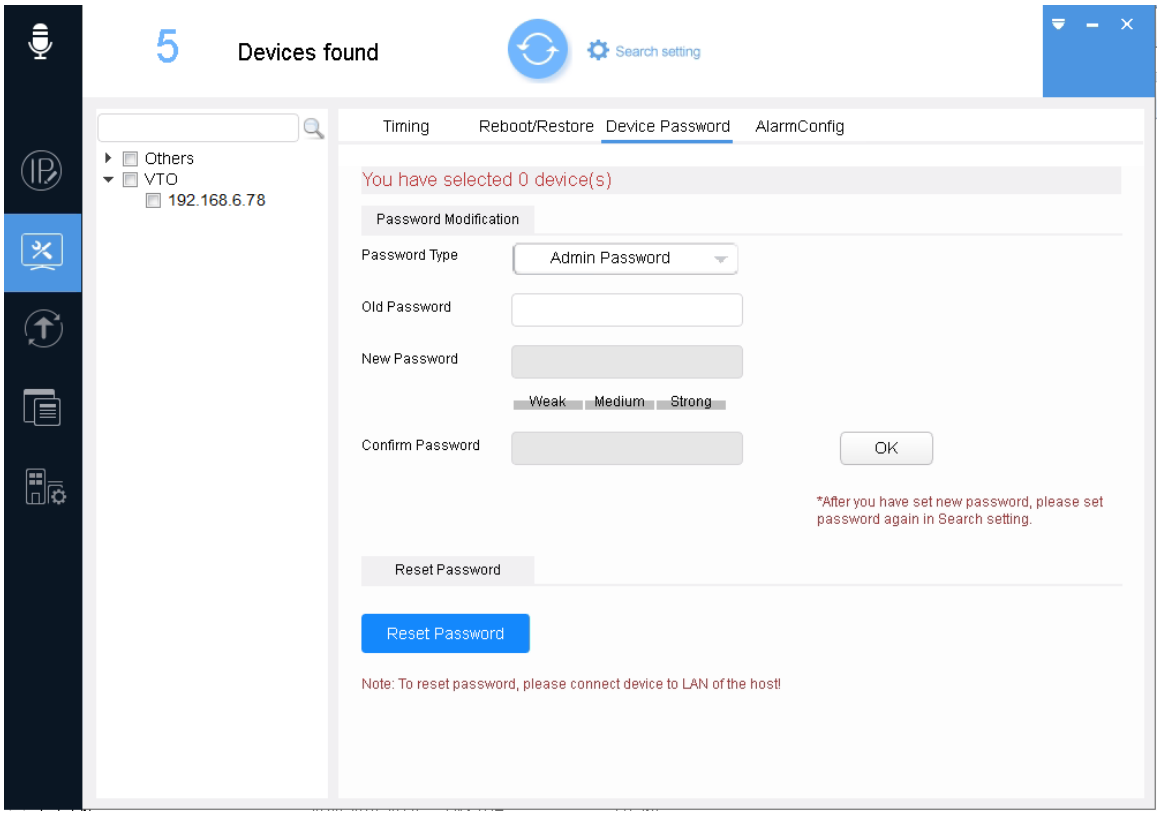


Figure 2-24

Step 2 Click ▶ next to the device type.

The device list is displayed.

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

Step 3 Select one or multiple devices, and then click **Reset Password**.

- If the device does not support this function, a **Notice** dialog box is displayed.
- If the device supports this function, the **Reset Password** interface is displayed. See Figure 2-25.

NOTE

- The user interface might be different dependent on the model you purchased. If there is inconsistency between the Manual and the actual product, the actual product shall govern.
- When reset passwords for multiple devices, the Tool resets all devices based on the password reset mode of the first selected device.

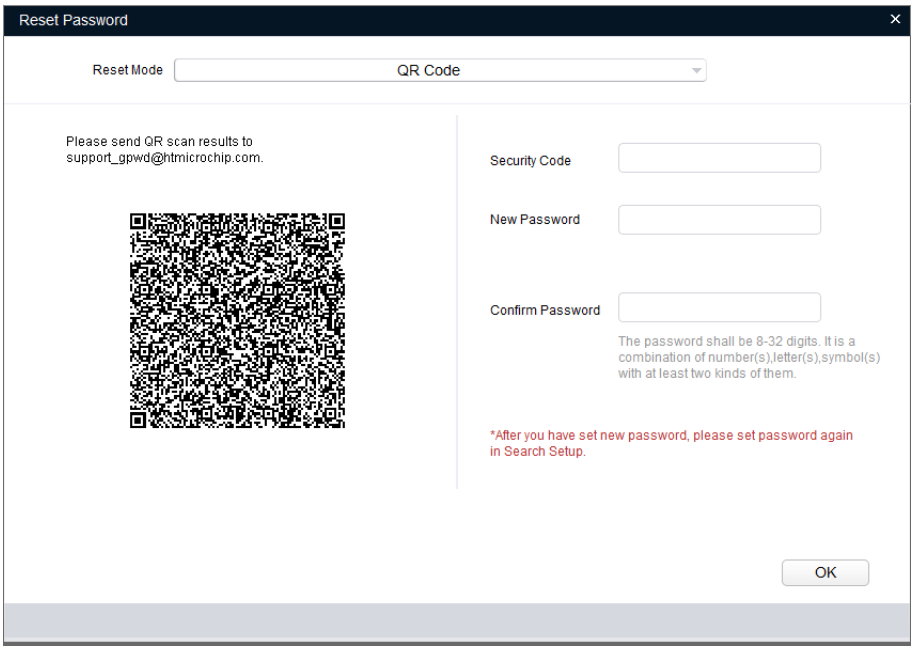


Figure 2-25

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

The **Reset Password-Export XML** interface is displayed. See Figure 2-26.

NOTE

The user interface might be different dependent on the model you purchased. If there is inconsistency between the Manual and the actual product, the actual product shall govern.

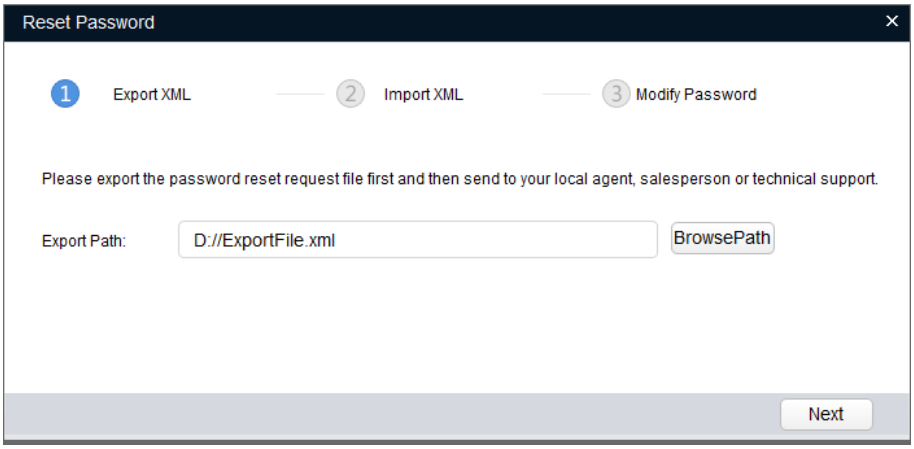


Figure 2-26

Step 5 Export XML.

1) Click **BrowsePath** 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 **Reset Password-Import XML** interface is displayed.

Step 6 Obtain the **result.xml** file.

Find the **ExportFile.xml** under the save path and send it as an attachment to the designated mailbox indicated on the interface. In a few minutes, you will receive a **result.xml** file as an attachment and save it properly.

Step 7 Import XML.

NOTE

If the **Reset Password-Import XML** interface is closed, click **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 2-27.

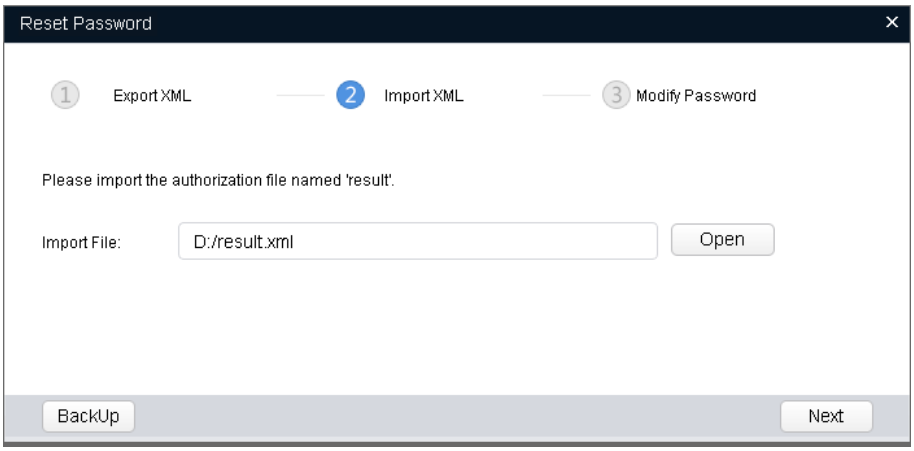


Figure 2-27

2) Click **Next** to start importing.
   After the importing is completed, the **Reset Password-Modify Password** interface is displayed. See Figure 2-28.

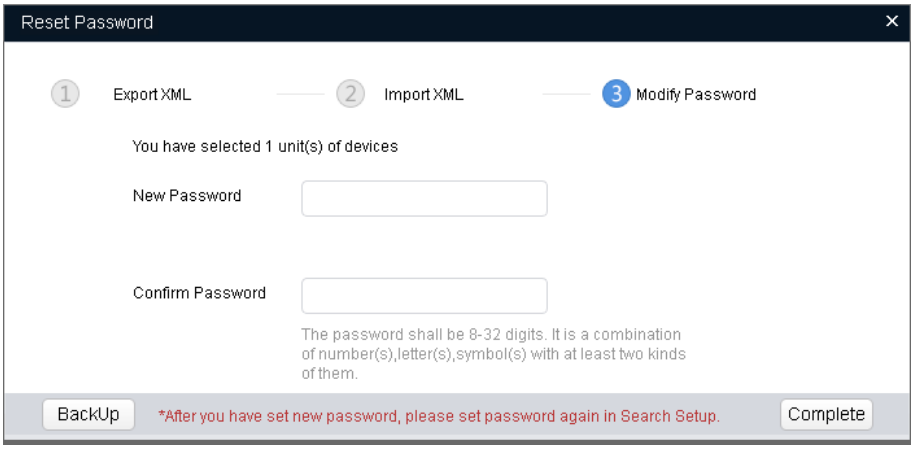


Figure 2-28

Step 8 Modify Password.

Enter the new password and confirm password. There are two setting rules for new password dependent on the devices, and please following the instructions on the interface to set the new password.

- The new password can be set from 8 characters through 32 characters and contain at least two types from number, letter and special characters (excluding"'", """, ";", ":" and "&").
- The new password can only be set as four numbers.

NOTE

After setting the new password, when you search the devices by **Search setting**, use the new password to login the device.

Step 9 Click **Complete** to starting resetting the password.

After operation is completed, the result is displayed. See Figure 2-29.

You can click the success icon ( ) or click the failure icon ( ) for the details.

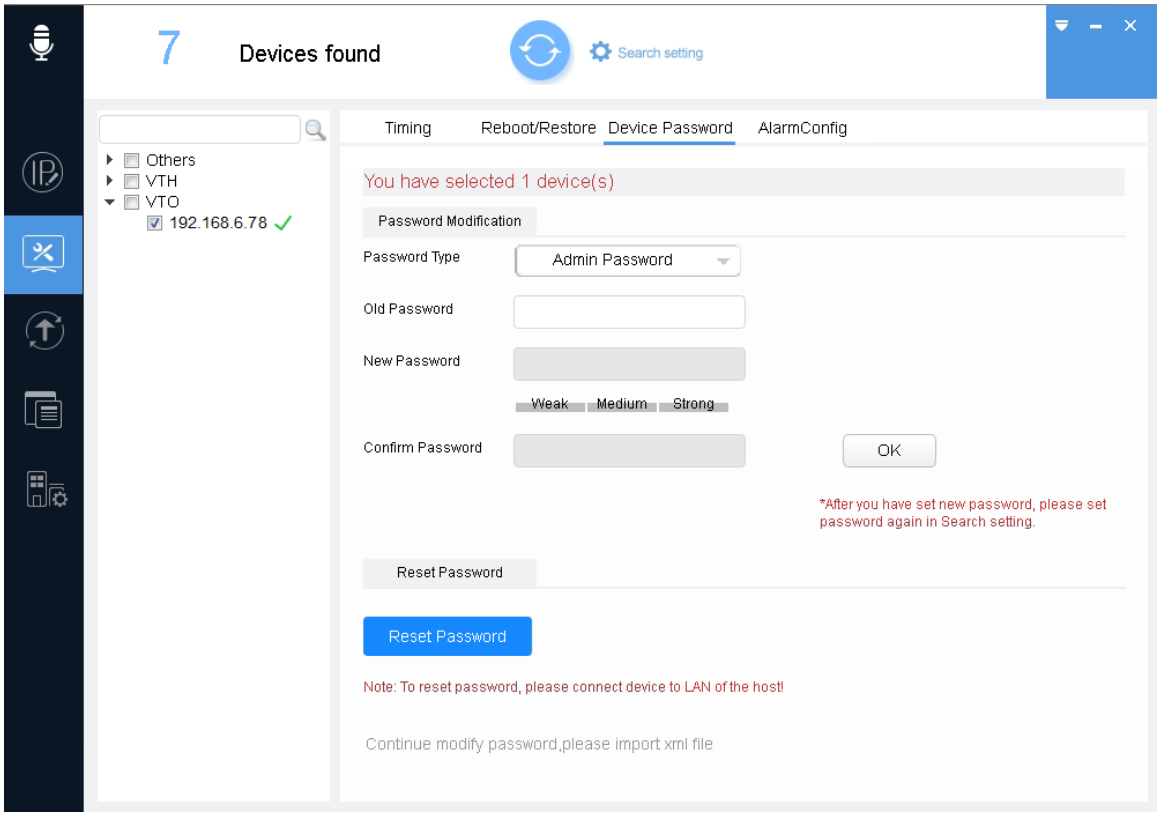


Figure 2-29

2.5.4 Configuring Alarm

You can set the alarm information of protection area and set the effectiveness of protection area in the alarm mode.

NOTE

Only VTH supports this function.

Step 1 On the system configuration interface, click the **AlarmConfig** tab.

The **AlarmConfig** interface is displayed. See Figure 2-30.

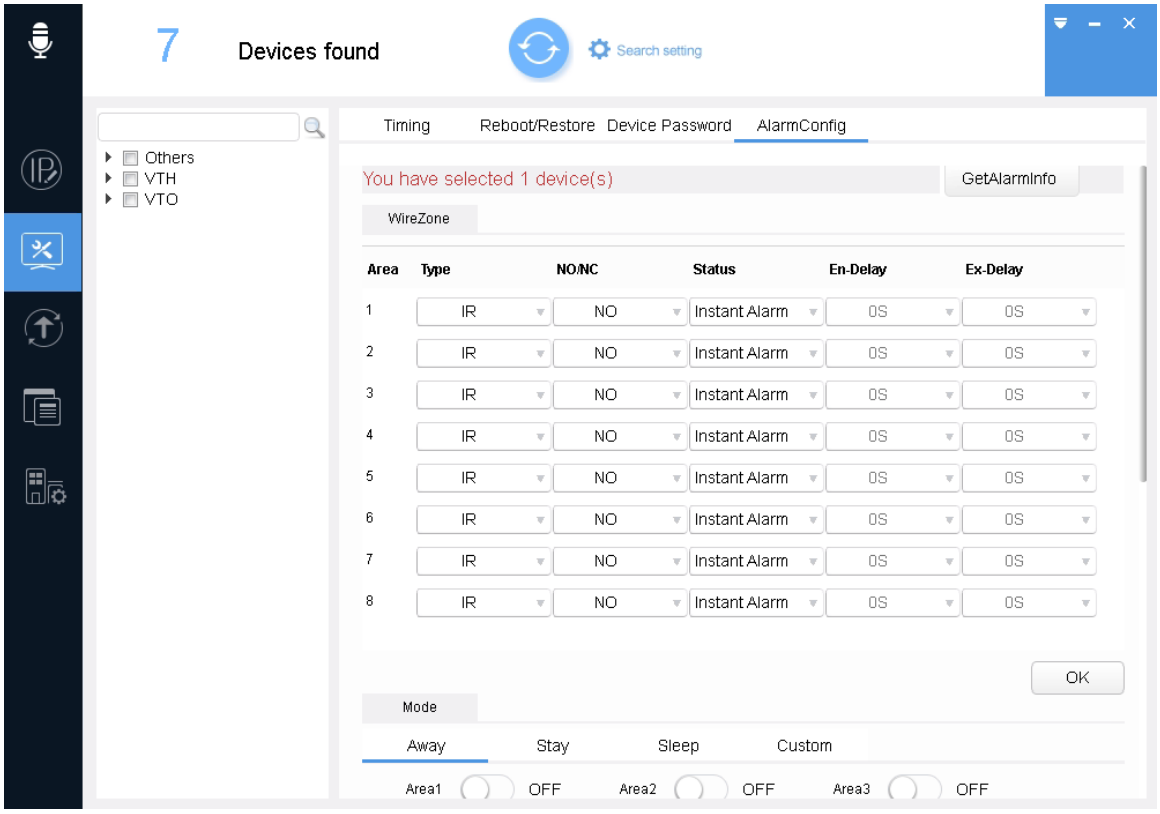


Figure 2-30

Step 2 Click ▸ next to the device type.

The device list is displayed.

Step 3 Select one device.

NOTE

- Only support to select one device at a time.
- If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

Step 4 Access the alarm information settings.

1) Click **GetAlarmInfo**.
   The **Notice** dialog box is displayed.
2) Click **OK**.

◇ If succeeded, the success icon (✓) appears next to the device, and the alarm information and the mode information are displayed. See Figure 2-31.

◇ If failed, the failure icon (⚠) appears next to the device. You can click ⚠ for the details.

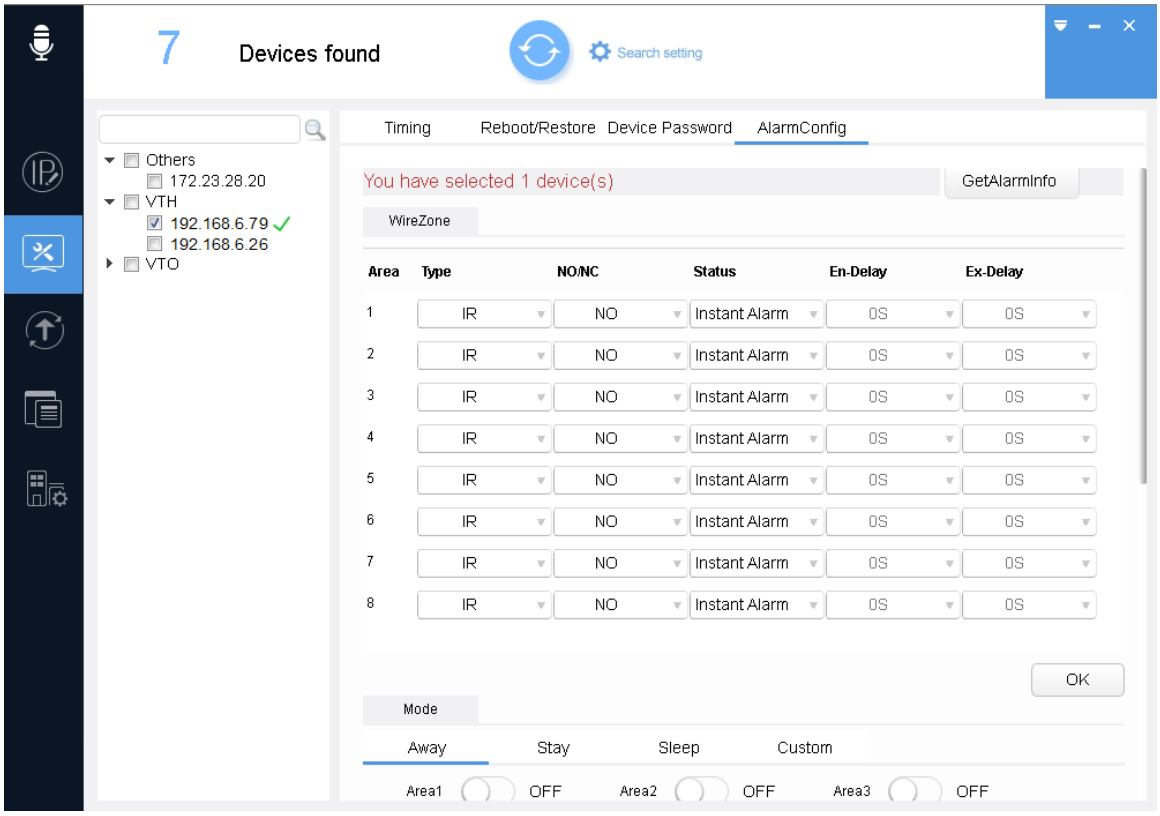


Figure 2-31

Step 5 Set the alarm information of protection area.

1) In the **WireZone** area, configuring the alarm information. See Table 2-6.

Parameter	Description
Area	The serial number of protection area. There are six protection areas in total.
Type	Alarm types, including IR, Gas Sensor, Smoke Sensor, Urgency Btn, Door Sensor, Stolen Alarm, Perimeter, and Doorbell. NOTE Only the sixth protection area supports Doorbell.
NO/NC	Alarm triggering mode of the protection areas. ● When selecting **NO**, high level indicates alarm input and low level indicates no alarm input. ● When selecting **NC**, low level indicates alarm input and high level indicates no alarm input.
Status	Includes Instant Alarm, Delay Alarm, Bypass and Remove. ● Instant Alarm: The device triggers alarm immediately if there is an alarm input. ● Delay Alarm: If there is an alarm input, the device triggers the alarm after the seconds configured in the **En-Delay** list. ● Bypass: After being set to **Bypass**, the protection area is invalid in armed mode and is valid in disarmed mode. ● Remove: Even if there is an alarm input, the device will not trigger the alarm.
En-Delay	To use this function, in the **Status** list, select **Delay Alarm**. If there is an alarm input, the device triggers the alarm after the seconds configured in the **En-Delay** list.

Parameter	Description
Ex-Delay	To use this function, in the **Status** list, select **Delay Alarm**. The protection area will be activated after the seconds configured in the **Ex-Delay** list.

Table 2-6

2) In the **WireZone** area, click **OK**.

Step 6 Set the effectiveness of protection area in armed mode.

1) In the **Mode** area, click the **Stay**, **Away**, **Sleep** or **Custom** tab.
2) Enable the protection area according to the actual situation.
3) In the **Mode** area, click **OK**.

NOTE

- After clicking **OK**, the setting of protection area effectiveness is only valid in the selected alarm mode. If you want to set the effectiveness of protection area in another alarm mode, please perform Step 6 again.
- You need to enable the alarm mode to make the configuration effective. For the details about how to enable the alarm mode, see "2.5.5.1 Configuring Arm Settings."

2.5.5 Configuring Arm/Disarm Settings

You can enable or disable the alarm mode.

NOTE

Only VTH supports this function.

2.5.5.1 Configuring Arm Settings

You can enable the alarm mode, and the alarm will be triggered if it meets the alarm conditions.

Step 1 On the system configuration interface, click the **AlarmConfig** tab.

The **AlarmConfig** interface is displayed. See Figure 2-32.

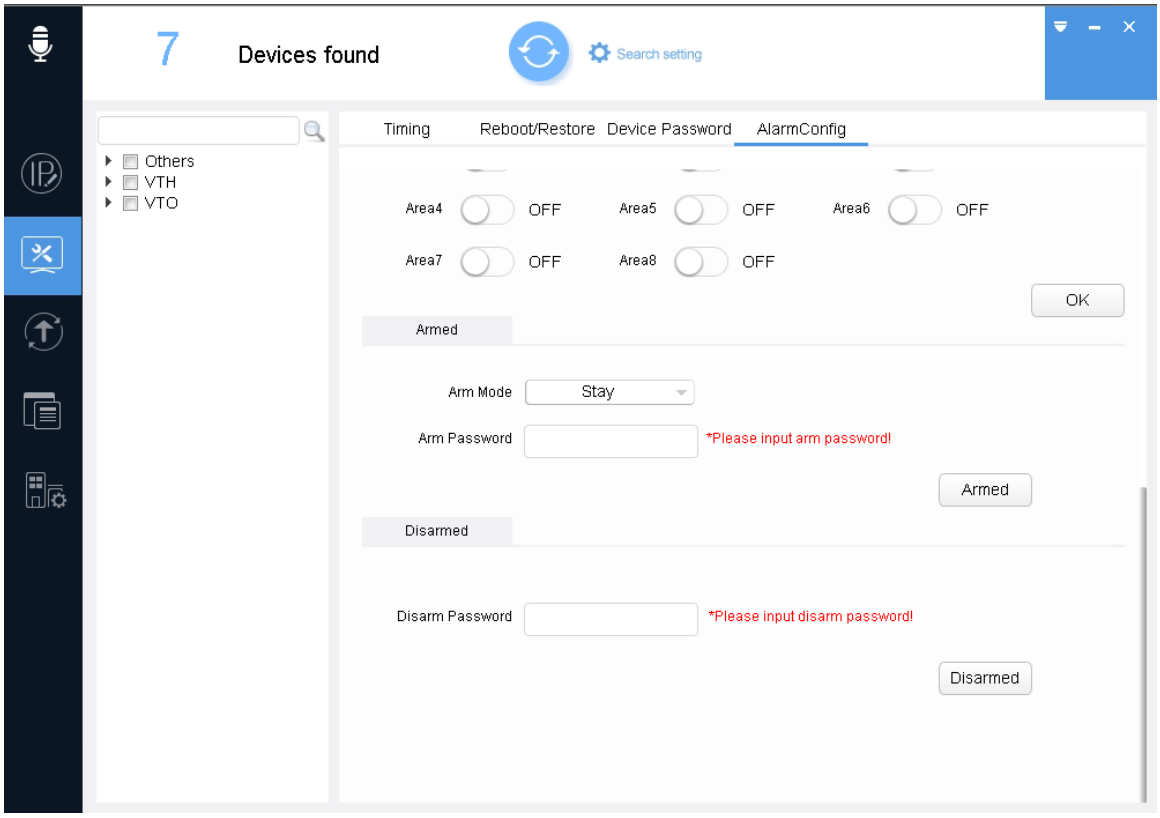


Figure 2-32

Step 2 Click ▸ next to the device type.

The device list is displayed.

Step 3 Select one or multiple devices.

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

Step 4 In the **Armed** area, select **Arm Mode**, and then enter **Arm Password**.

NOTE

Enter the user password of VTH in the **Arm Password** box.

Step 5 Click **Armed**.

2.5.5.2 Configuring Disarm Settings

You can disable the alarm mode, and the alarm will not be triggered.

Step 1 On the system configuration interface, click the **AlarmConfig** tab.

The **AlarmConfig** interface is displayed. See Figure 2-33.

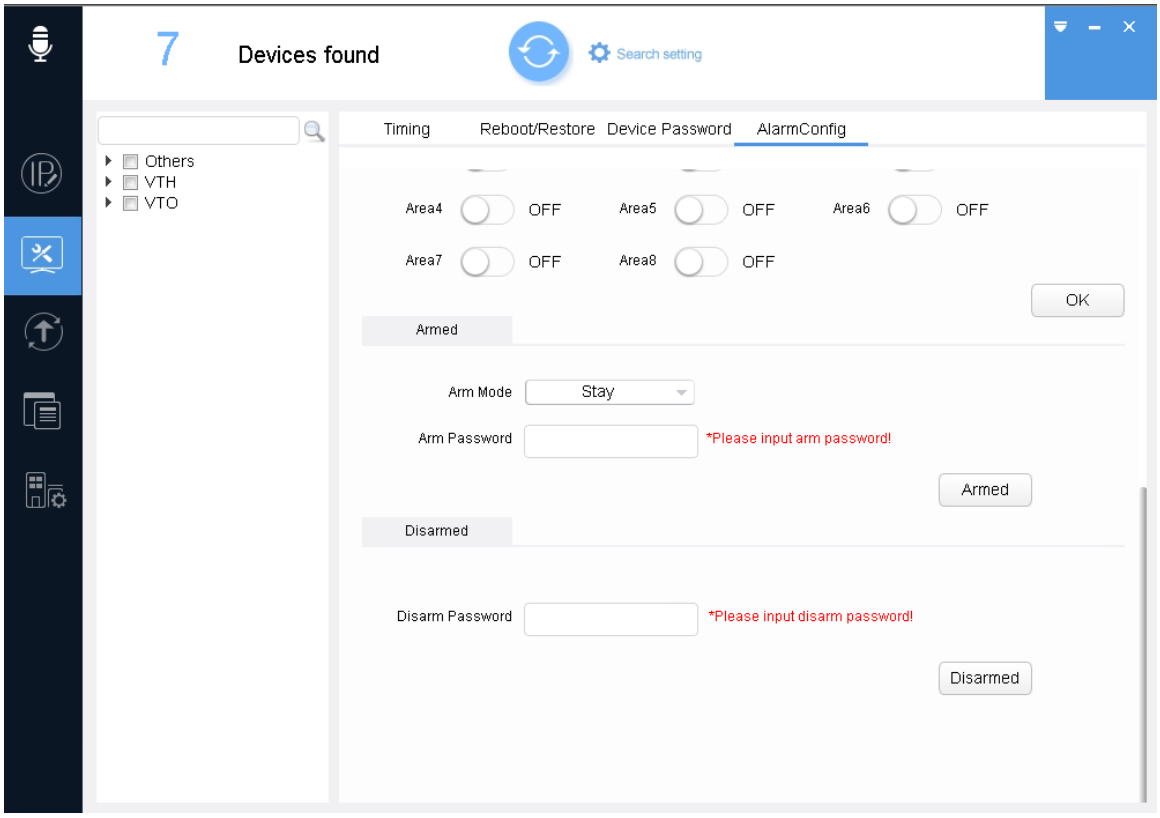


Figure 2-33

Step 2 Click ▸ next to the device type.

The device list is displayed.

Step 3 Select one or multiple device.

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

Step 4 In the **Disarmed** area, enter **Disarmed Password**.

NOTE

Enter the user password of VTH in the **Disarmed Password**.

Step 5 Click **Disarmed**.

2.6 Local Upgrade

You can upgrade one or multiple devices on the PC in which the Tool is installed.

NOTE

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 file transmission is not completed. Please upgrade the device again after the reconnection.
- If the upgrade progress exceeds 50%, the upgrade file transmission is completed and the device will be upgraded.

2.6.1 Upgrading One Device

You can choose this procedure for upgrading one device.

Step 1 Click .

The **Upgrade** interface is displayed. See Figure 2-34.

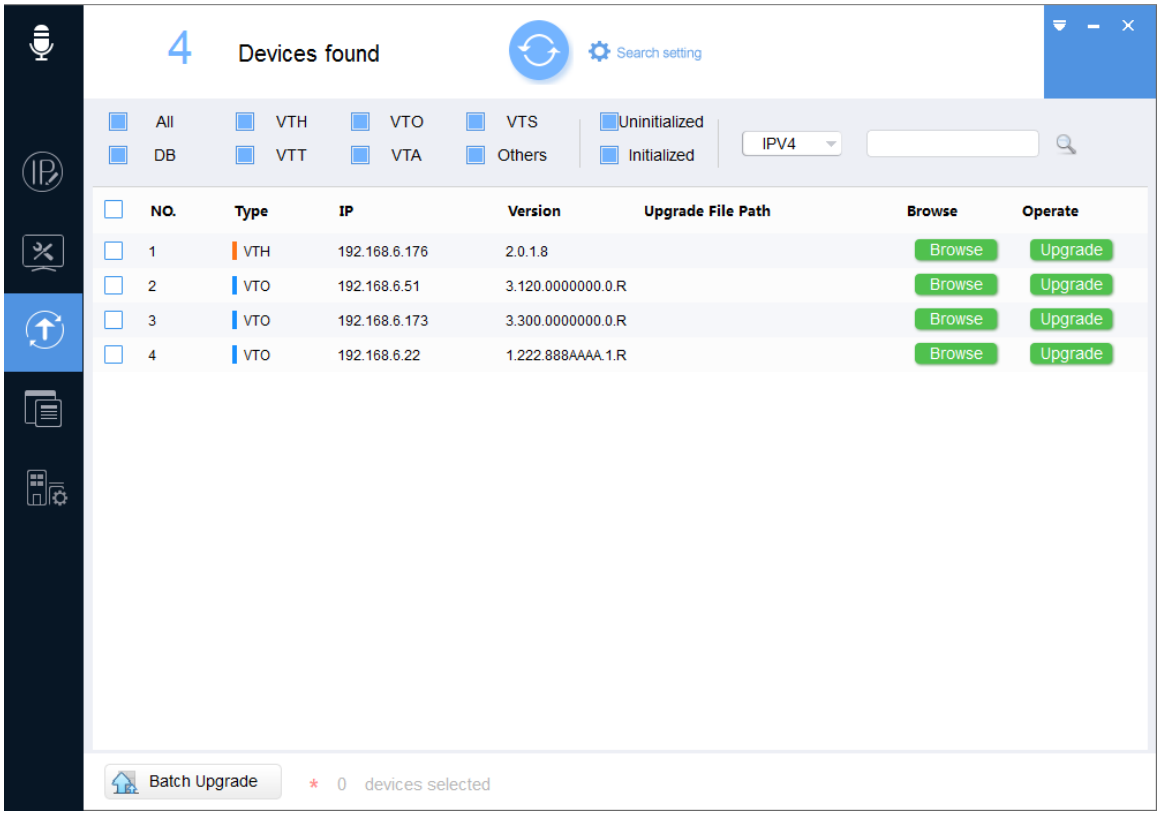


Figure 2-34

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

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

Step 3 Click **Upgrade**.

The Upgrade Setup interface is displayed. See Figure 2-35.

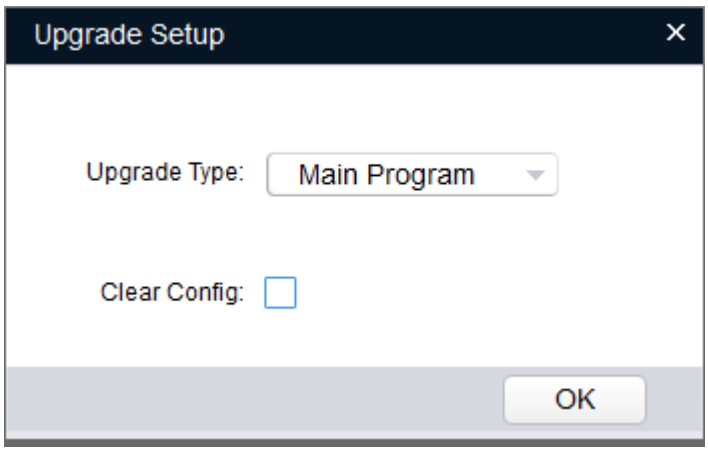


Figure 2-35

Step 4 Configure upgrade parameters.

- In the **Upgrade Type** list, select the upgrade type.
- Select the **Clear Config** check box according to the actual situation.

CAUTION

If you select the **Clear Config** check box, the Tool will restore other configurations except IP and initialization status.

Step 5 Click **OK** to start upgrading and displayed upgrade progress.

After upgrade is completed, the device reboots automatically.

2.6.2 Upgrading Devices in Batches

You can upgrade multiple devices to the same software version.

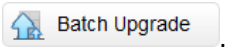
Step 1 Click  .

The **Upgrade** interface is displayed.

Step 2 Select the devices that need to be upgraded.

NOTE

- If the device is not in the device list, searching again. For the details about how to search devices, see "2.1 Searching 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. See Figure 2-36.

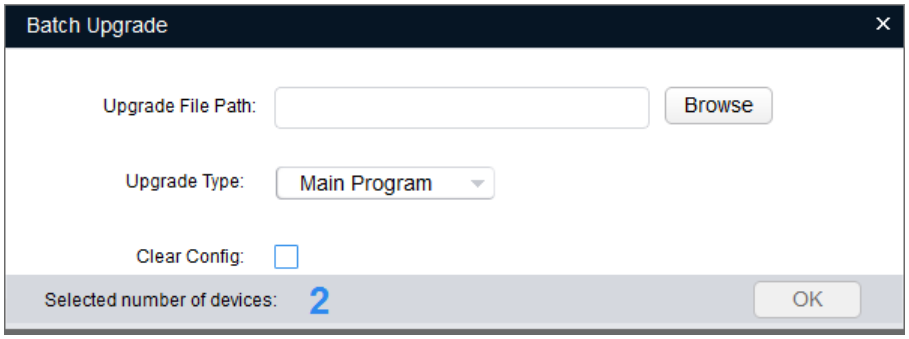


Figure 2-36

Step 4 Click **Browse** to select the upgrade file.

Step 5 Configure upgrade parameters.

- In the **Upgrade Type** list, select the upgrade type.
- Select the **Clear Config** check box according to the actual situation.

CAUTION

If you select the **Clear Config** check box, the Tool will restore other configurations except IP and initialization status.

Step 6 Click **OK** to start upgrading.

2.7 Online Upgrade

You can download upgrade package to upgrade the device.

2.7.1 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** dialog box is displayed. See Figure 2-37.

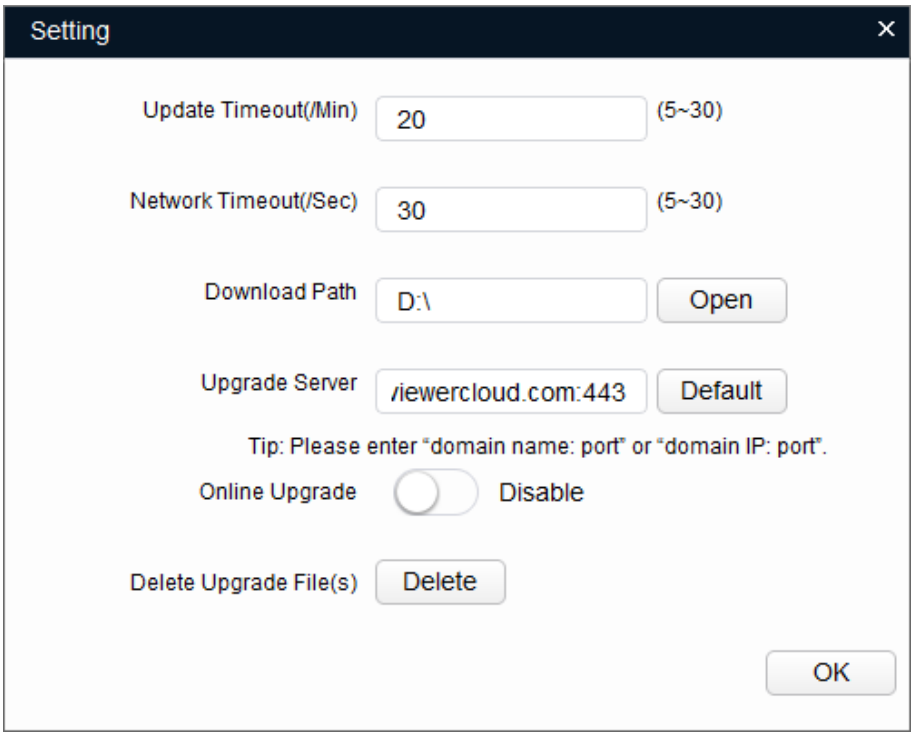


Figure 2-37

Step 2 Set the system parameters. See Table 2-7.

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 under the **Download Path**. CAUTION Please delete the unwanted upgrade files in time. Otherwise, if there is not enough disk space, it will affect download, import and export of files when performing online upgrade.

Table 2-7

Step 3 Enable **Online Upgrade**. See Figure 2-38.

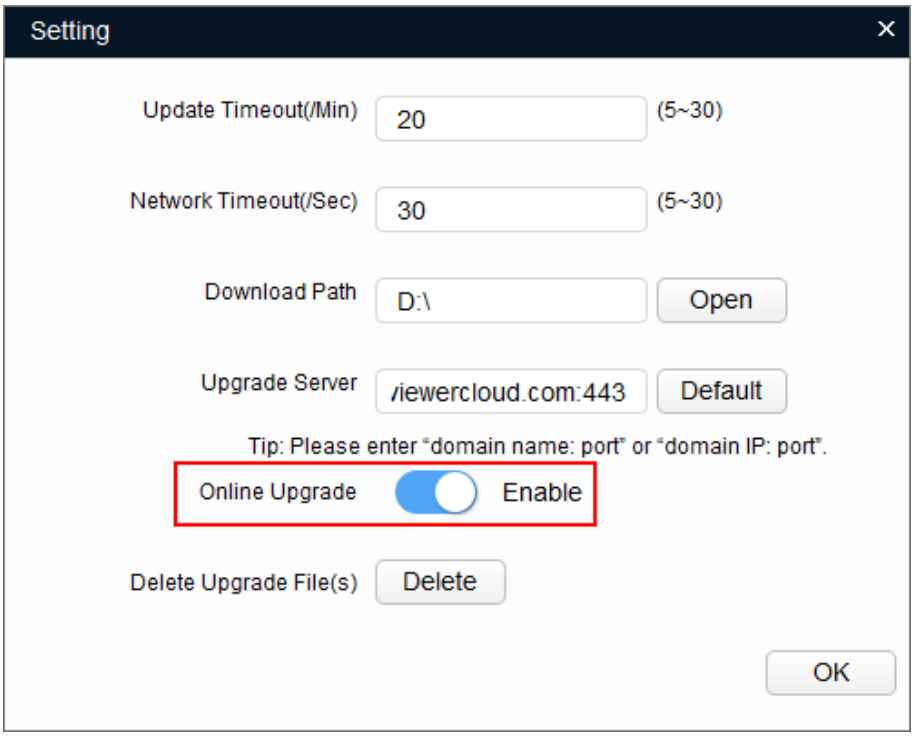


Figure 2-38

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

The online upgrade icon ( ) appears in the **Menu**. The searched devices display on the **Online upgrade** interface. See Figure 2-39.

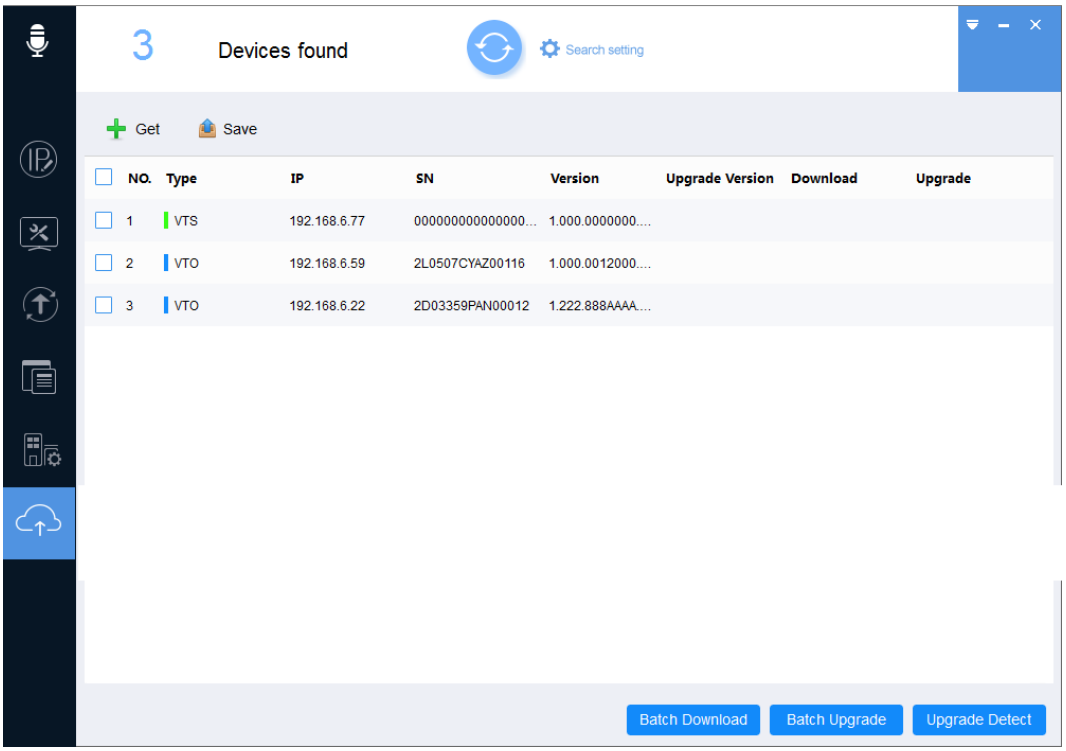


Figure 2-39

2.7.2 Performing Online Upgrade

NOTE

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** dialog box will be displayed prompting **Detecting, please wait...**

According to the network features of the PC in which the Tool is installed and the detected devices, the online upgrade operation is divided into synchronous operation and asynchronous operation. Select the upgrade method according to the actual situation.

- Synchronous operation means that you can complete the upgrade detection, upgrade package download and upgrade on the PC in which the Tool is installed. The applications are as follows:
  - ◇ The PC in which the Tool is installed and the detected devices have accessed the Internet.
  - ◇ The PC in which the Tool is installed and the detected devices are on the same LAN, and the PC has double network card that can access the Internet at the same time.
  - ◇ The PC in which the Tool is installed and the detected devices are on 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 in which the Tool is installed, and you need to migrate the data. The application is as follows:
  - ◇ The PC in which the Tool is installed and the detected devices are 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.

2.7.2.1 Performing Synchronous Operation

Step 1 Click  .

The **Online upgrade** screen is displayed. See Figure 2-40.

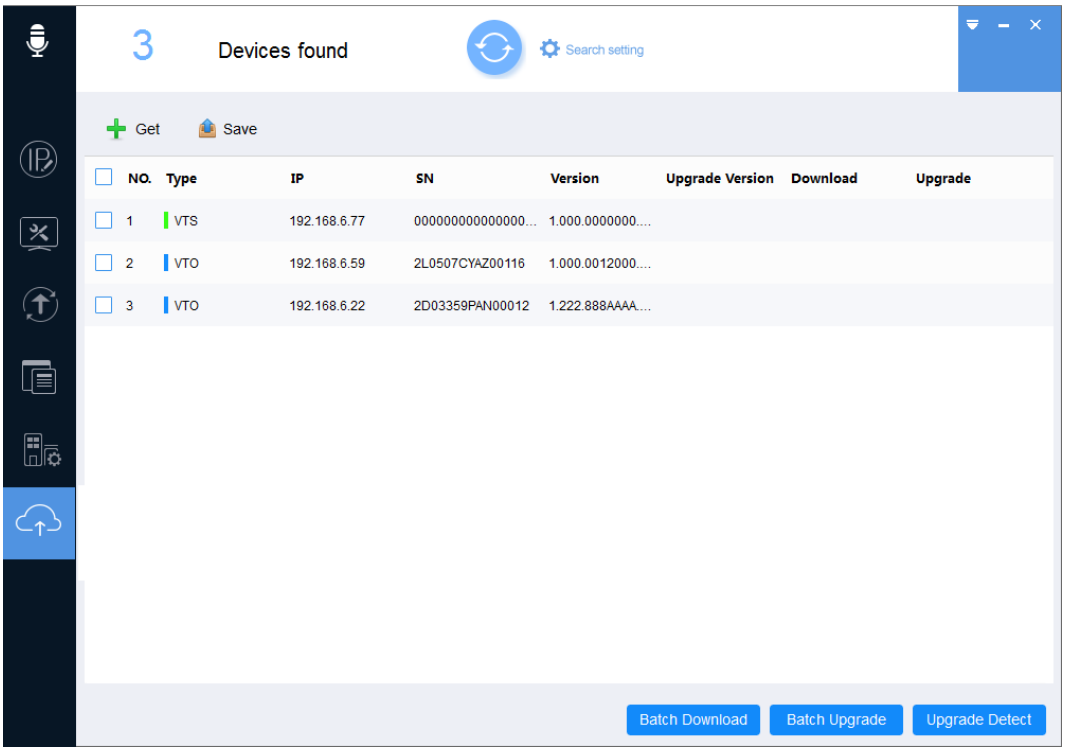


Figure 2-40

Step 2 Confirm that the PC in which the Tool is installed has connected to the Internet.

Step 3 Select one or multiple devices.

NOTE

If the device is not in the device list, perform researching again. For the details about how to search devices, see "2.1 Searching Devices."

Step 4 Click **Upgrade Detect**.

The **Download** button is displayed after the detection is completed. See Figure 2-41.

NOTE

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

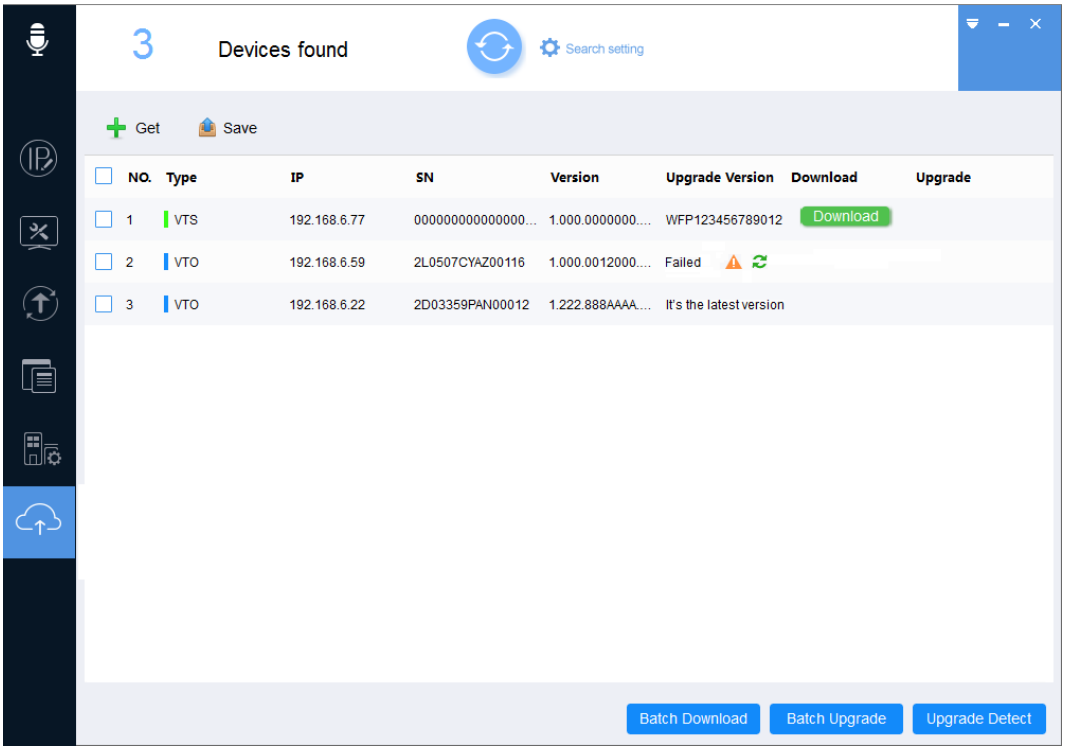


Figure 2-41

NOTE

If the detection is successful, skip Step 5.

Step 5 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**, please perform upgrade detection again.
- If the **Config Result** shows **Incorrect password**, please perform the following steps:

1) Click ↻.

The **Login** dialog box is displayed. See Figure 2-42.

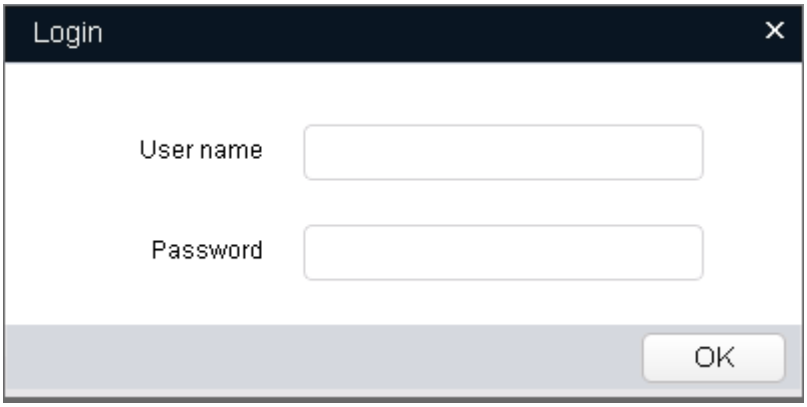


Figure 2-42

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 ⚠ for the details. If the **Config Result** still shows **Incorrect password**, please obtain the correct user name and password and repeat the above steps.

CAUTION

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

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

Step 6 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 devices with the **Download** button, and then click **Batch Download**.

The **Upgrade** button is displayed after the downloading is completed. See Figure 2-43.

NOTE

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

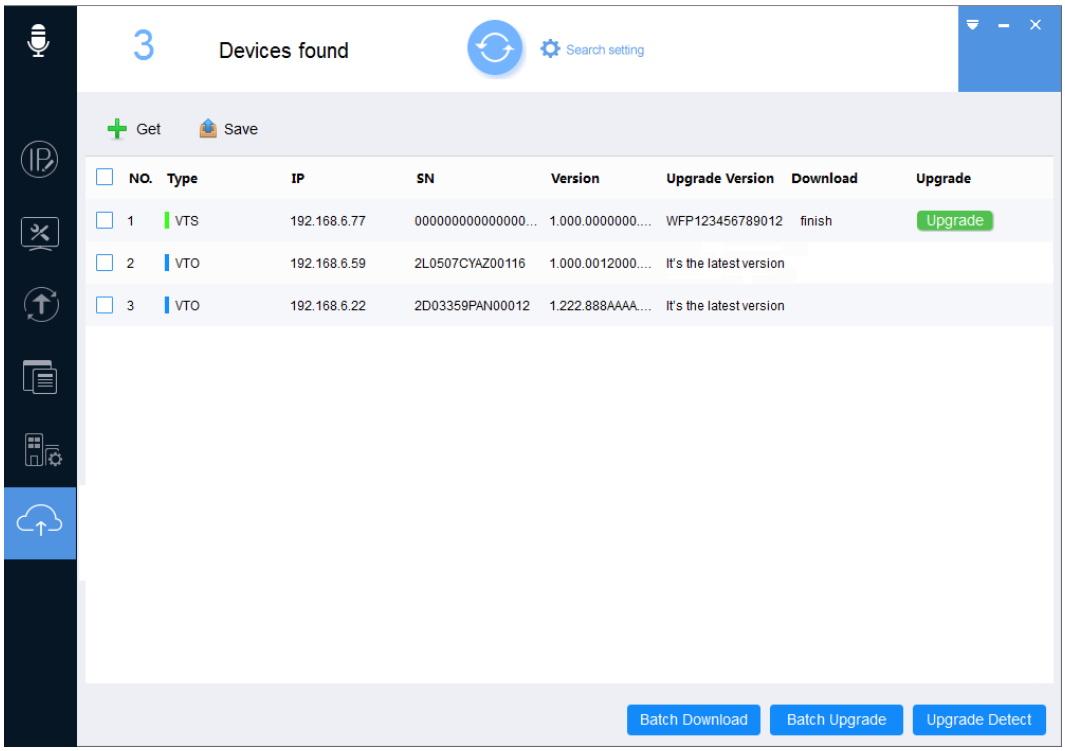


Figure 2-43

Step 7 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**.

NOTE

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 2-44.

You can click the success icon ( ) or click the failure icon ( ) for the details.

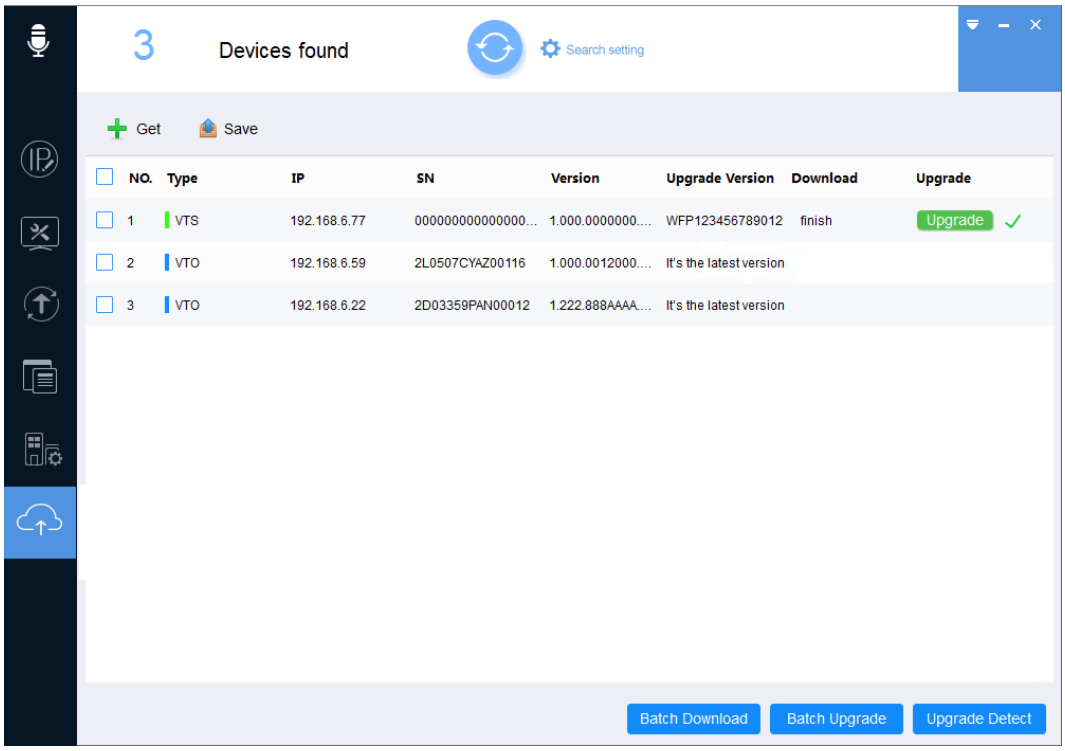


Figure 2-44

2.7.2.2 Performing Asynchronous Operation

Prerequisite:

- Asynchronous operation is applicable to the situation that PC (hereinafter referred to be "PC1") in which the Tool is installed and the detected devices are 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.

NOTE

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

Exporting PC1 Device Information

Step 1 On the Tool main user interface on PC1, click .

The **Online upgrade** screen is displayed. See Figure 2-45.

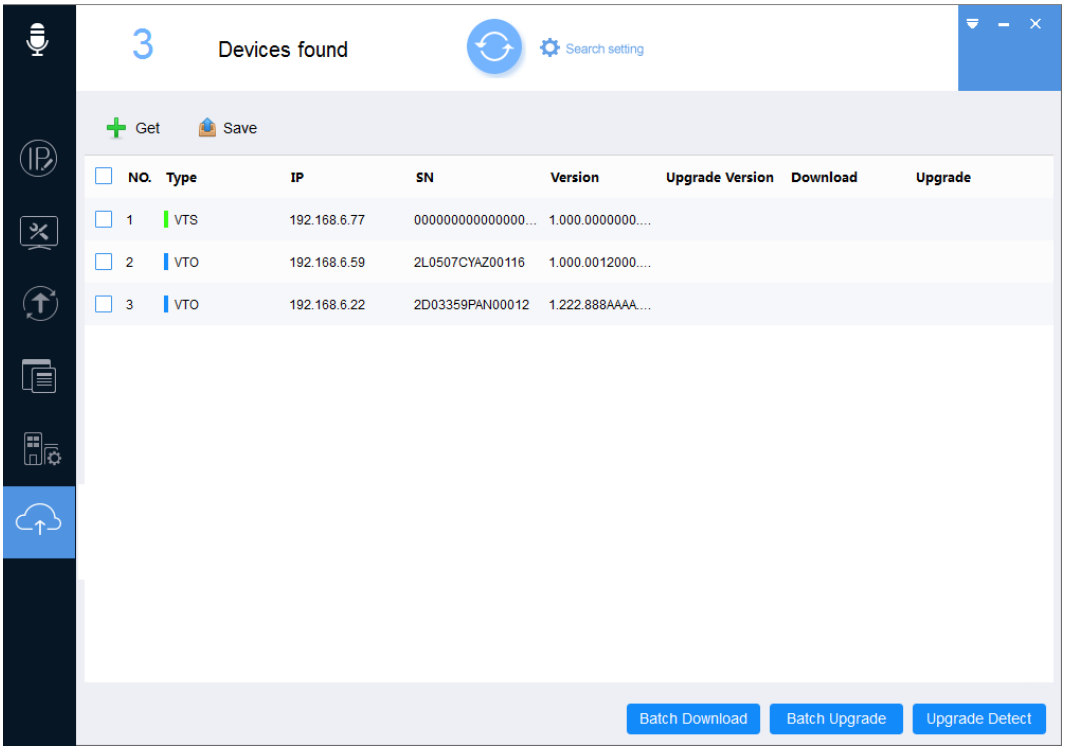


Figure 2-45

Step 2 Select one or multiple devices.

NOTE

If the device is not in the device list, perform researching again. For the details about how to search devices, see "2.1 Searching Devices."

CAUTION

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.

The detection result is displayed after the detection is completed. See Figure 2-46.

NOTE

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

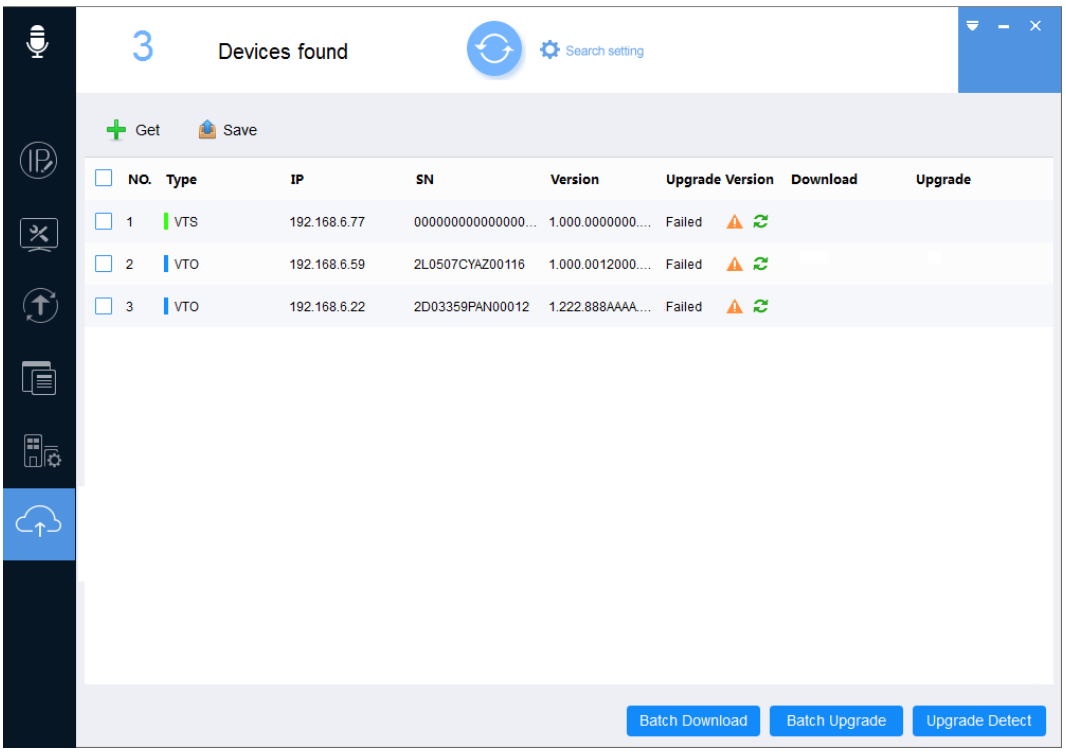


Figure 2-46

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 by going to Step 5. Otherwise, obtain the correct user name and password and repeat the above steps.

     CAUTION

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

- If the **Config Result** shows information other than previous 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**.

After the exporting is completed, the **Notice** dialog box is displayed.

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) Launch the Tool.

2) On the main user interface, click , and then select **Setting**.

The **Setting** dialog box is displayed.

3) Enable **Online Upgrade**. See Figure 2-47.

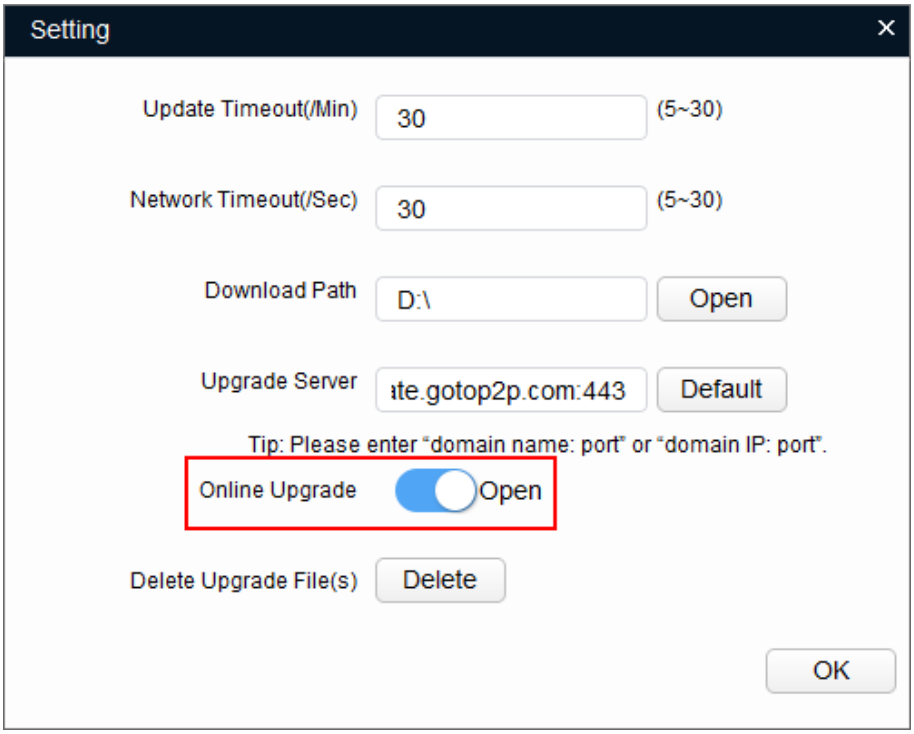


Figure 2-47

4) Click **OK**.

The **Online upgrade** screen is displayed.

5) Click Import.

The **Open** dialog box is displayed.

6) 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.

7) Click **OK** to start automatic detection.

The **Download** button is displayed after the detection is completed. See Figure 2-48.

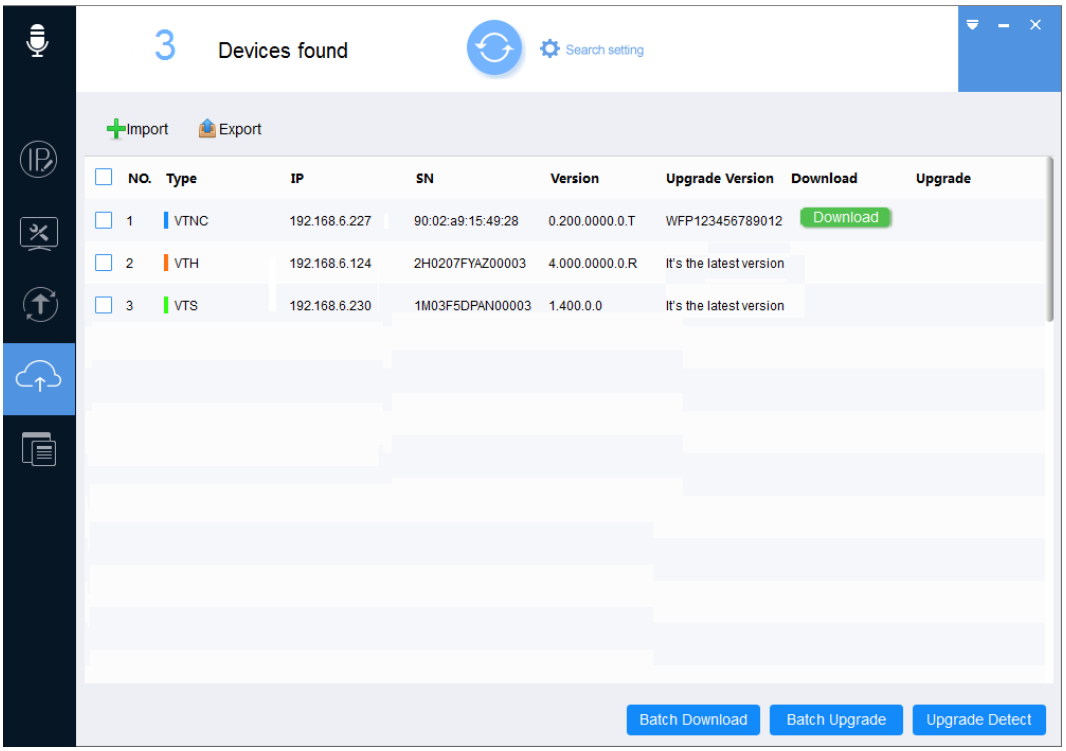


Figure 2-48

Downloading and Exporting Upgrade Package on PC2

Step 1 Select one or multiple devices on the interface shown in Figure 2-48.

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**.

The **Upgrade** button is displayed after the downloading is completed. See Figure 2-49.

NOTE

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

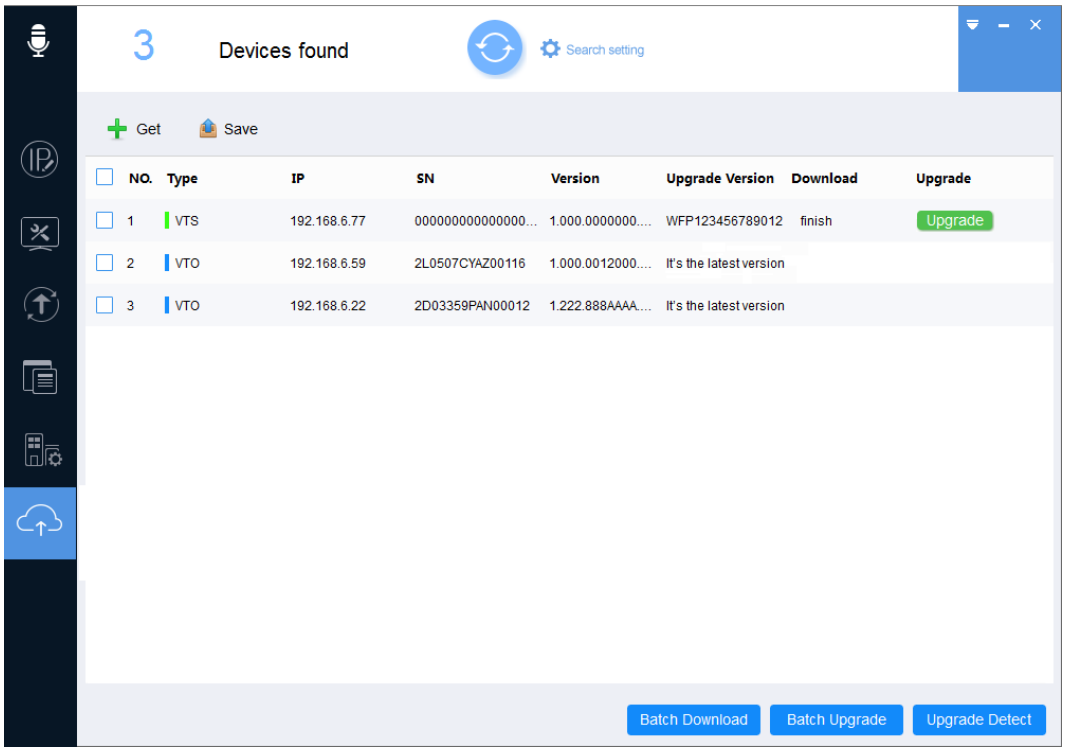


Figure 2-49

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 the **Online upgrade** interface of The Tool, click Import.

   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 2-50.

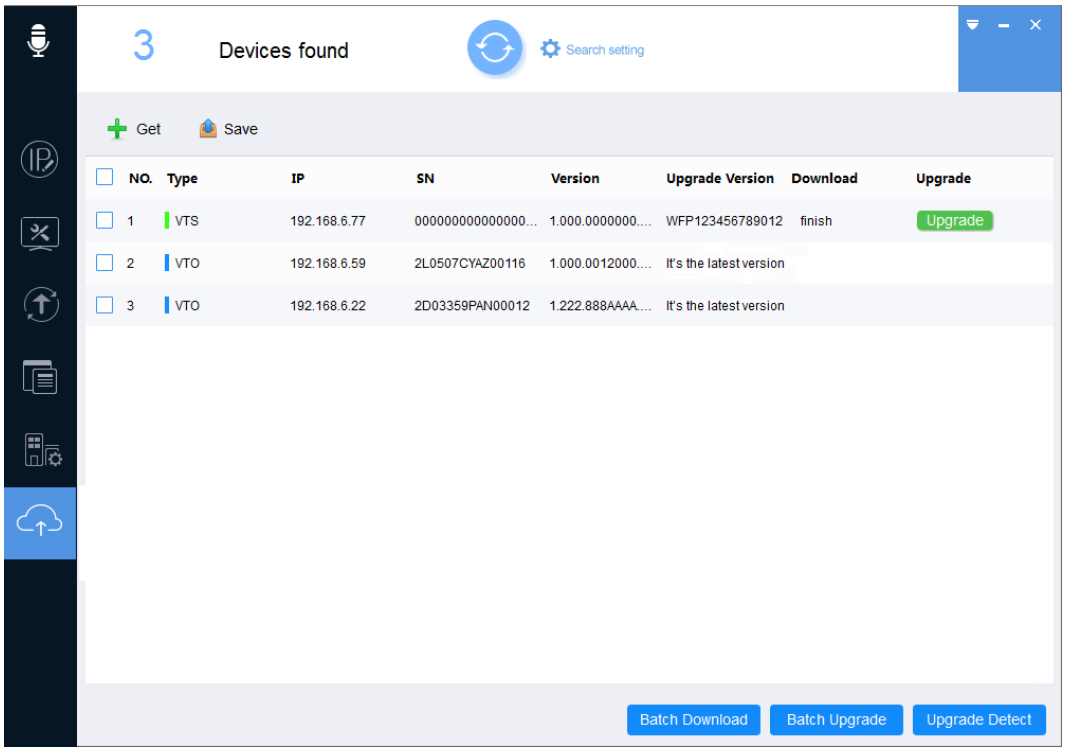


Figure 2-50

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 click **Batch Upgrade**.

NOTE

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 2-51.

You can click the success icon ( ) or click the failure icon ( ) for the details.

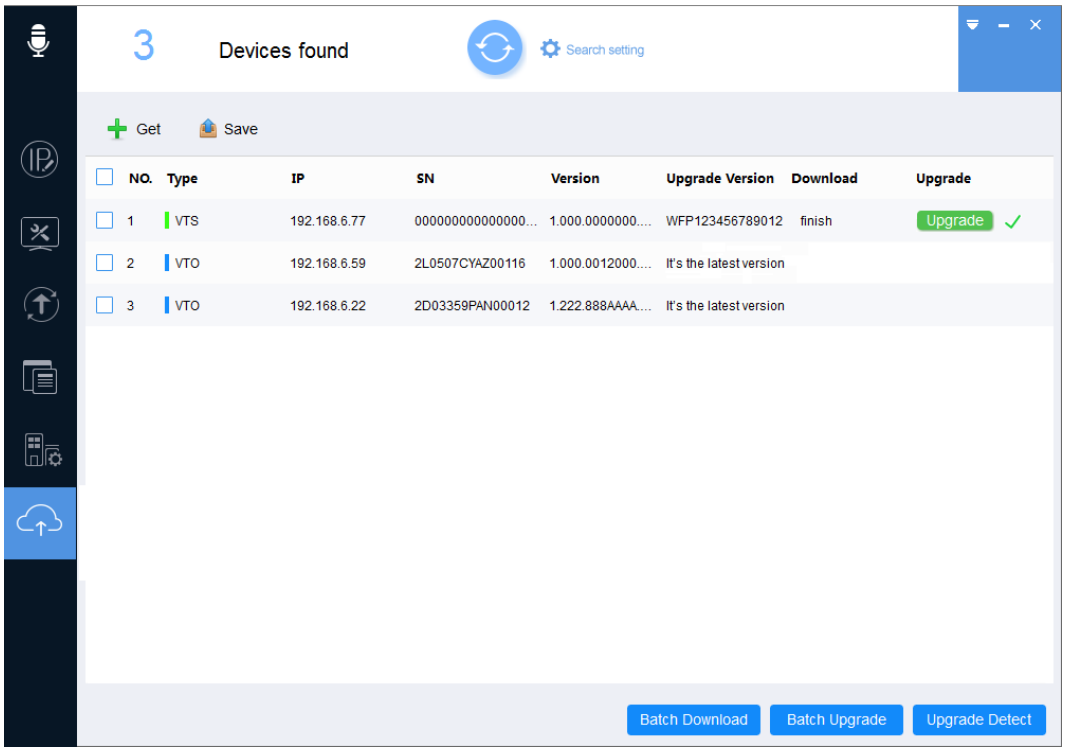


Figure 2-51

2.8 Data Backup

NOTE

Only VTO supports this function.

You can export and import data.

- Exporting data: Back up or save the video and audio configurations, indoor machine management, card management, access password, and access QR code for the device.
- Importing data: Restore or batch configure the video and audio parameters, indoor machine management, card management, access password, and access QR code for the device.

2.8.1 Exporting data

You can save or back up the video and audio parameters, indoor machine management, card management, access password, and access QR code for a device through exporting its template.

Step 1 Click .

The **Template Setup** interface is displayed. See Figure 2-52.

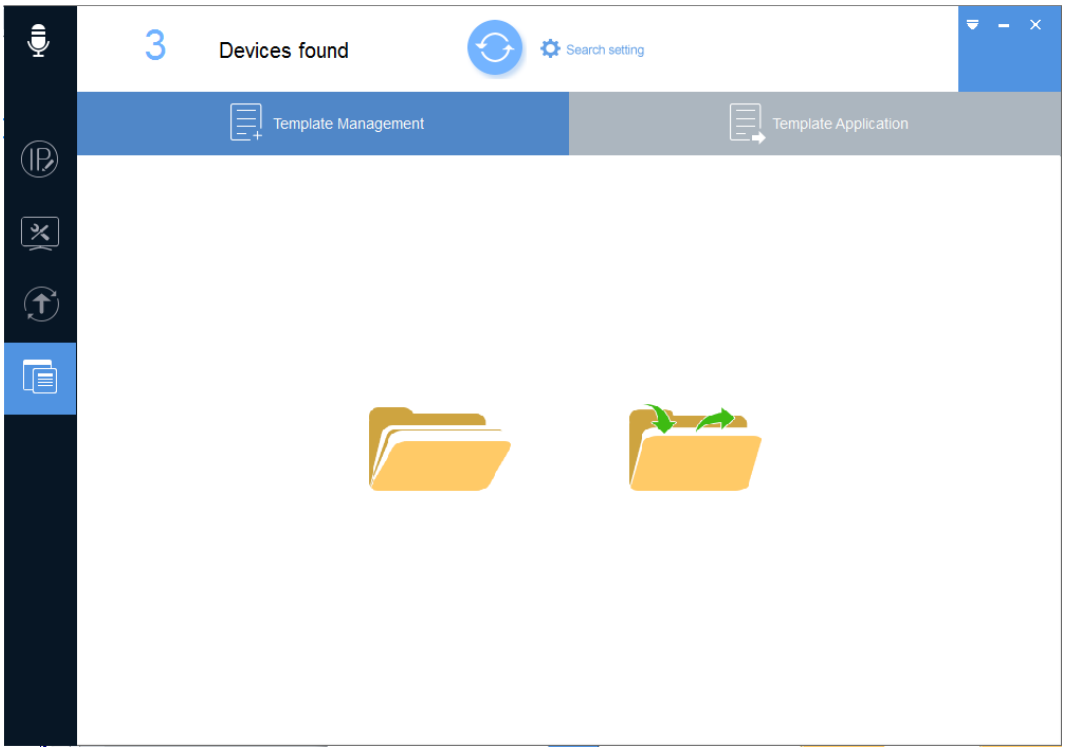


Figure 2-52

Step 2 Export the template.

1) Click  .

The **Template Management** interface is displayed. See Figure 2-53.

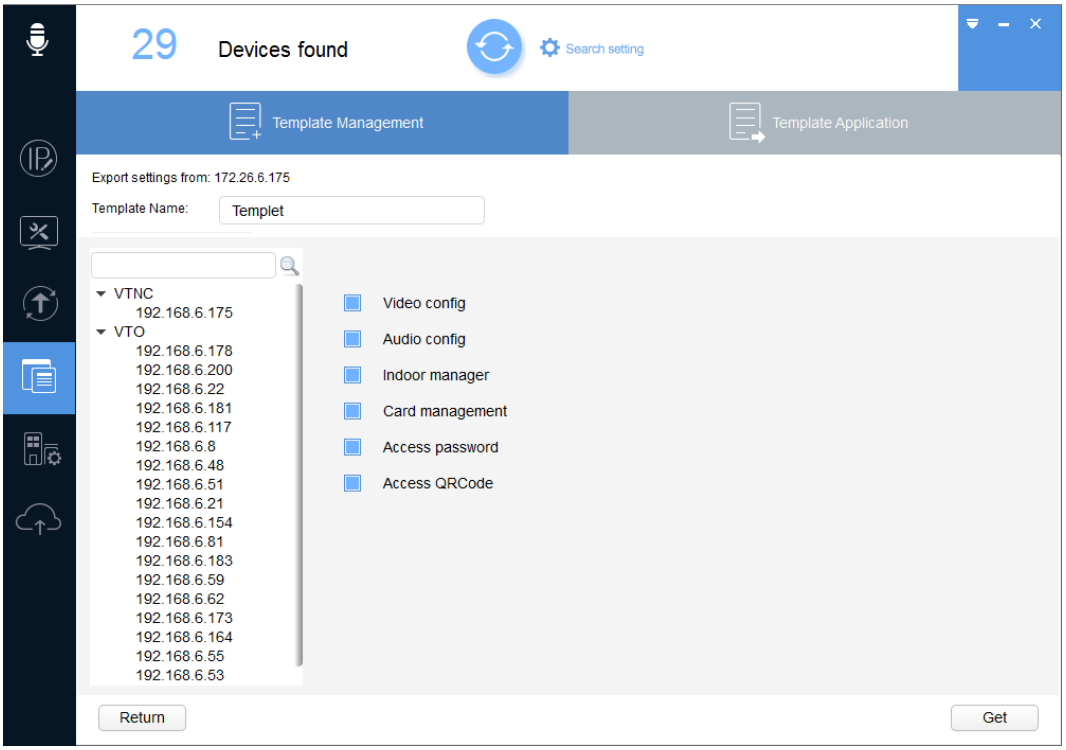


Figure 2-53

2) Click to select the device, enter the template name, for example, you can enter **Template**, and then set the information you want to export.

Step 3 Save the template.

1) Click **Get**.

The system starts obtaining the information you want to export and indicates **get config ok!** on the interface and the **Save as** dialog box is displayed. See Figure 2-54.

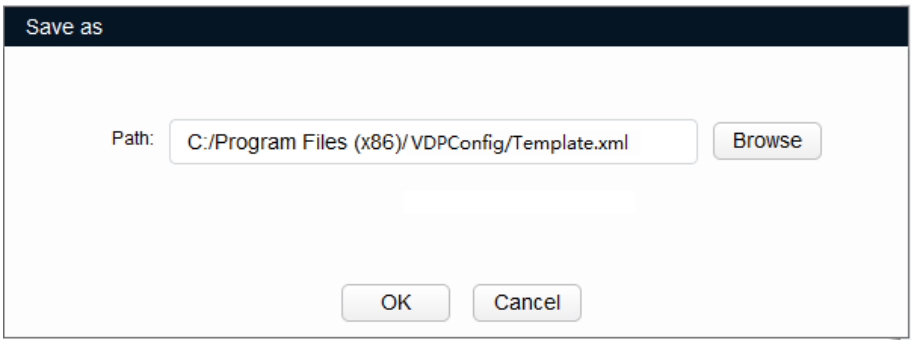


Figure 2-54

2) Click **Browse** to select the save path for the template.
3) Click **OK** to save the template.
After the exporting is completed, the **Template Application** interface is displayed. See Figure 2-55.

NOTE

For details about how to apply the template, see "2.8.2 Importing data."

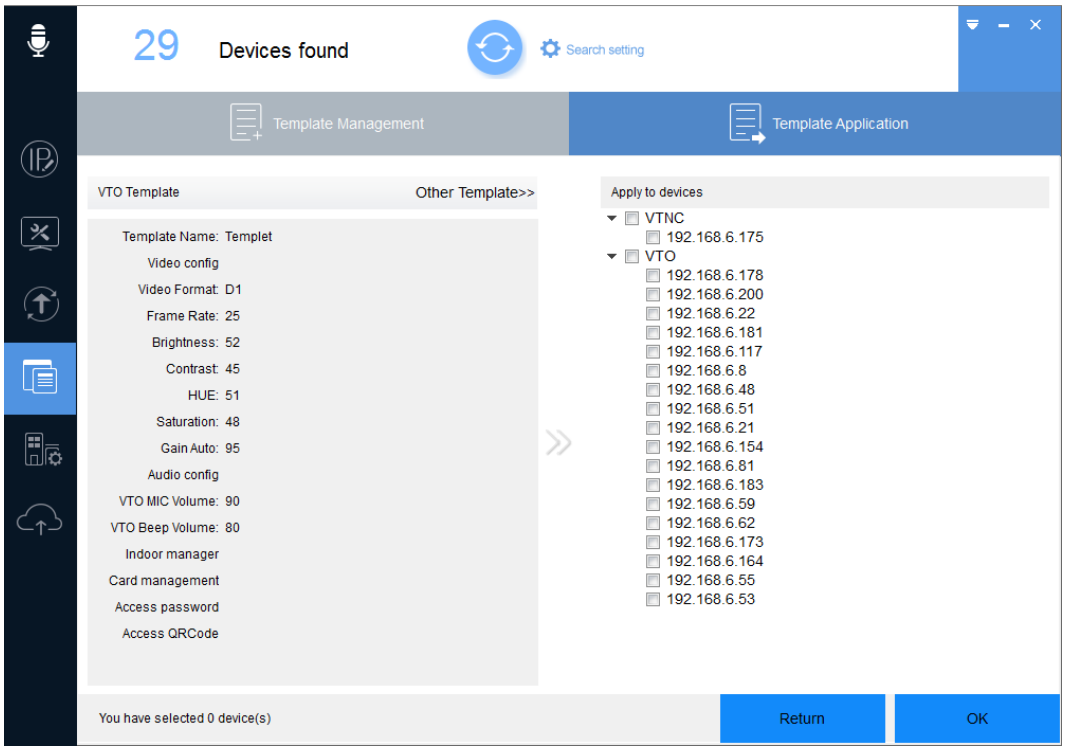


Figure 2-55

2.8.2 Importing data

You can load to apply the template to restore or batch configure video and audio parameters, indoor machine management, card management, access password, and access QR code for a device.

Step 1 Click  .

The **Template Setup** interface is displayed.

Step 2 Load the template.

1) Click  .

The **Load Template** dialog box is displayed. See Figure 2-56.

NOTE

Make sure the template exists, if not, see "2.8.1 Exporting data."

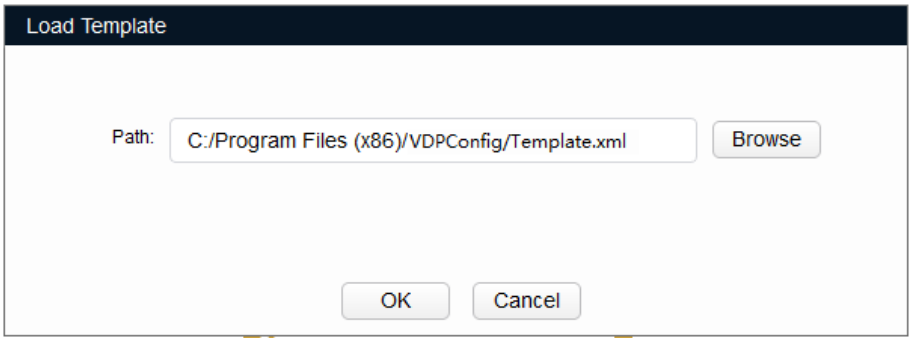


Figure 2-56

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

The **Template Application** interface is displayed. See Figure 2-57.

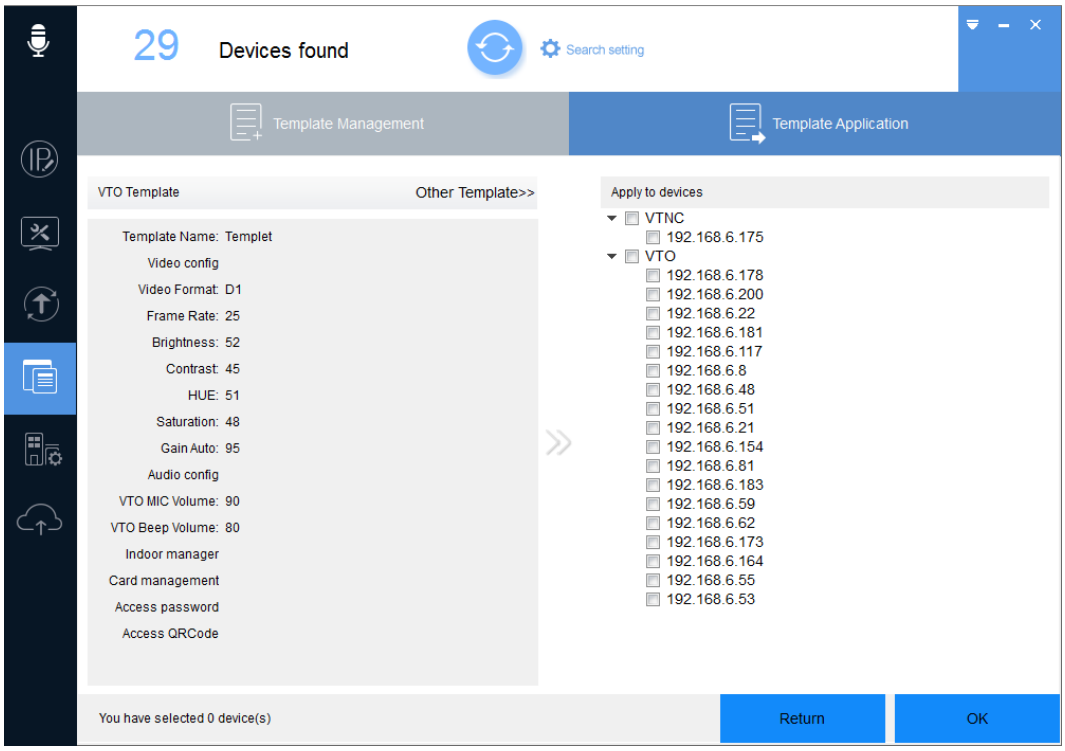


Figure 2-57

Step 3 Select one or multiple devices and then click **OK**.

The **Application Template** dialog box is displayed.

Step 4 Click **OK** to start applying the template.

After applying is completed, the result is displayed. See Figure 2-58.

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

NOTE

- Click **Other Template** to switch to other templates.

- If the device is not in the device list, searching again. For the details about how to search devices, see "2.1 Searching Devices."

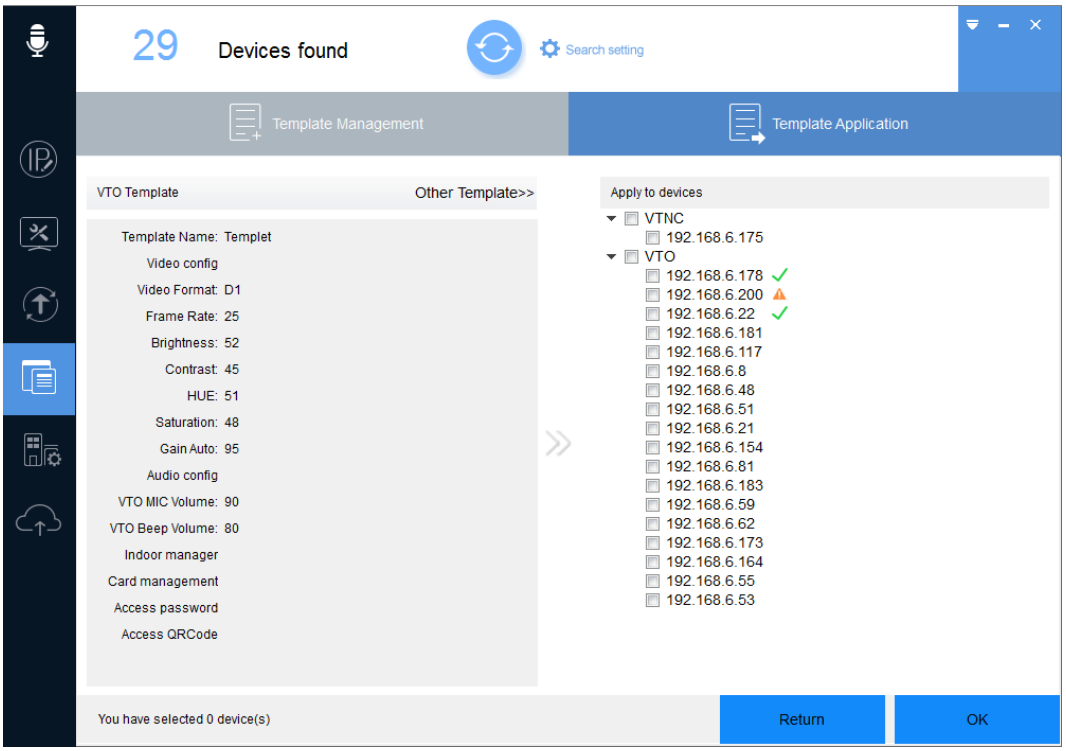


Figure 2-58

2.9 Project Configuration

Click  to enter the project configuration interface.

2.9.1 Batch Configuring

You can import and configure SIP system device.

CAUTION

Please use "Microsoft Excel" instead of "WPS Office", and the version of "Microsoft Excel" should be above "Microsoft Excel 2007".

Step 1 On the project configuration interface, click the **Batch Config** tab.

The **Batch Config** interface is displayed. See Figure 2-59.

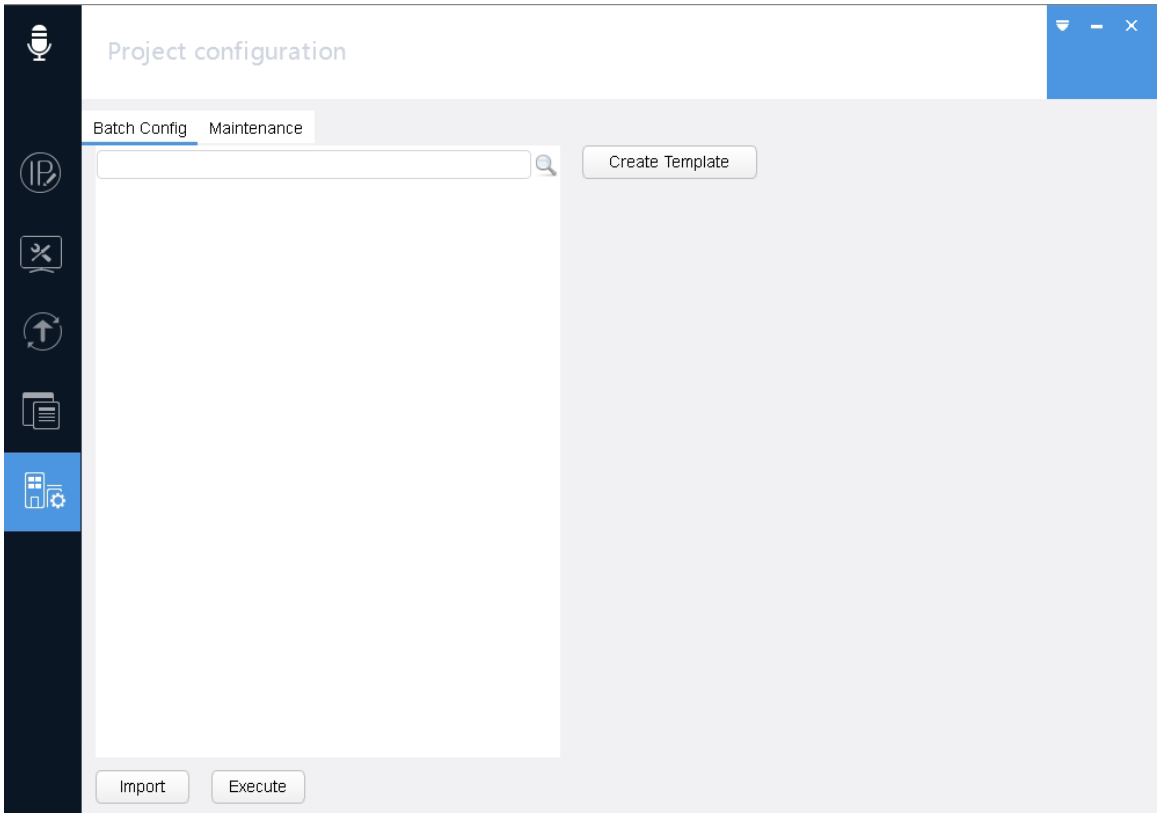
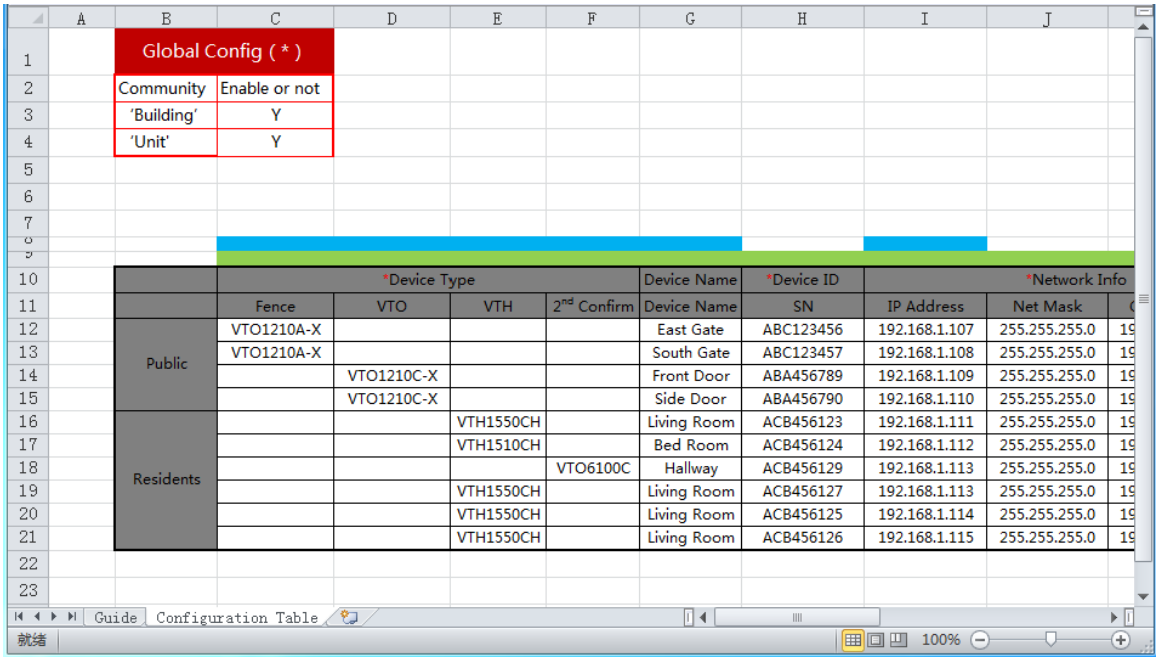


Figure 2-59

Step 2 Click **Create Template**.

The "ProjectTemplate-New-SIP.xlsx" template is displayed. See Figure 2-60. The default sheet is **Configuration Table**.



Global Config (*)

Community	Enable or not
'Building'	Y
'Unit'	Y

		*Device Type				Device Name	*Device ID	*Network Info		
		Fence	VTO	VTH	2nd Confirm	Device Name	SN	IP Address	Net Mask	
Public		VTO1210A-X				East Gate	ABC123456	192.168.1.107	255.255.255.0	19
		VTO1210A-X				South Gate	ABC123457	192.168.1.108	255.255.255.0	19
			VTO1210C-X			Front Door	ABA456789	192.168.1.109	255.255.255.0	19
			VTO1210C-X			Side Door	ABA456790	192.168.1.110	255.255.255.0	19
Residents				VTH1550CH		Living Room	ACB456123	192.168.1.111	255.255.255.0	19
				VTH1510CH		Bed Room	ACB456124	192.168.1.112	255.255.255.0	19
					VTO6100C	Hallway	ACB456129	192.168.1.113	255.255.255.0	19
				VTH1550CH		Living Room	ACB456127	192.168.1.113	255.255.255.0	19
				VTH1550CH		Living Room	ACB456125	192.168.1.114	255.255.255.0	19
				VTH1550CH		Living Room	ACB456126	192.168.1.115	255.255.255.0	19

Figure 2-60

Step 3 Click **Save**.

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

Step 4 Select the save path, enter the **File Name**, such as Case5, and then click **Save**.

Step 5 In the template, fill in the device information that you need to import.

NOTE

The information must meet the requirements of **Attention** in the **Guide** sheet.

Step 6 Click **Import**.

The **Open** dialog box is displayed.

Step 7 Select the template, and then click **Open** to import it.

After the importing, the **Notice** dialog box is displayed. See Figure 2-61.

NOTE

If you import two templates of different names successively, which contain device with the same SN, the latest imported template shall govern.

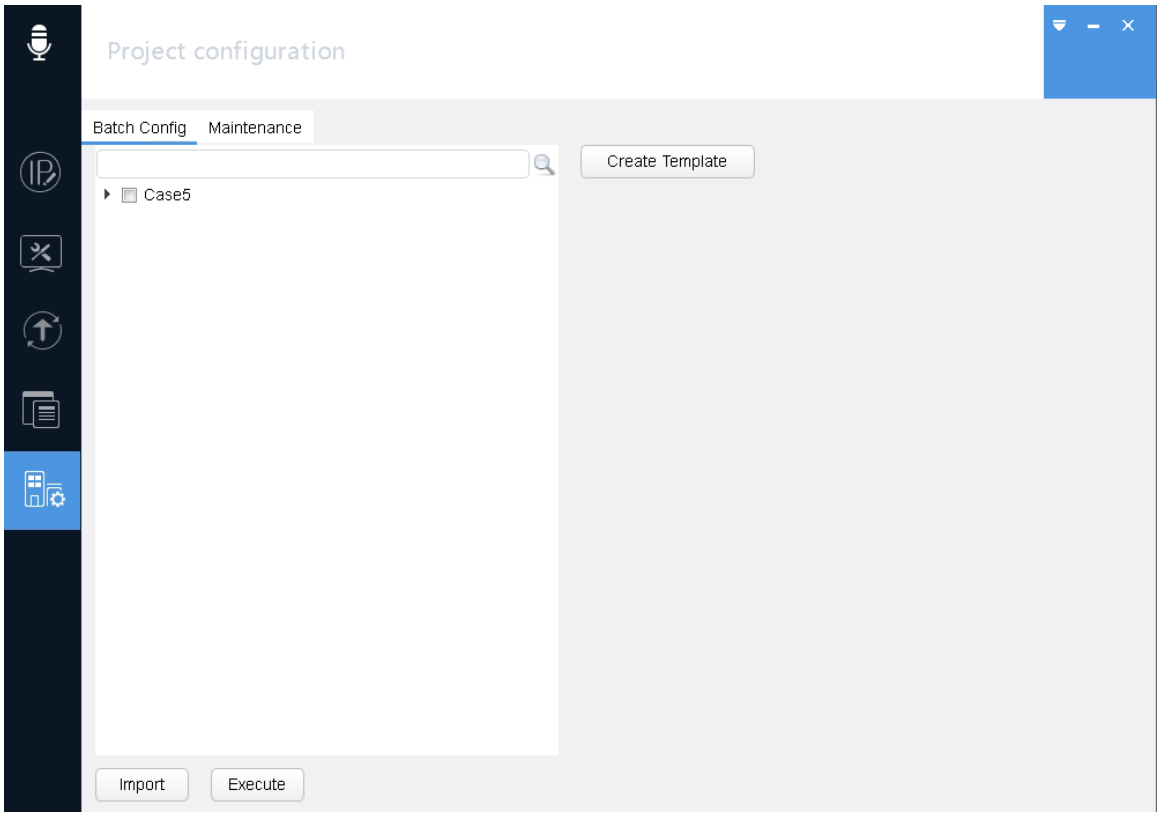


Figure 2-61

Step 8 Select device. See Figure 2-62.

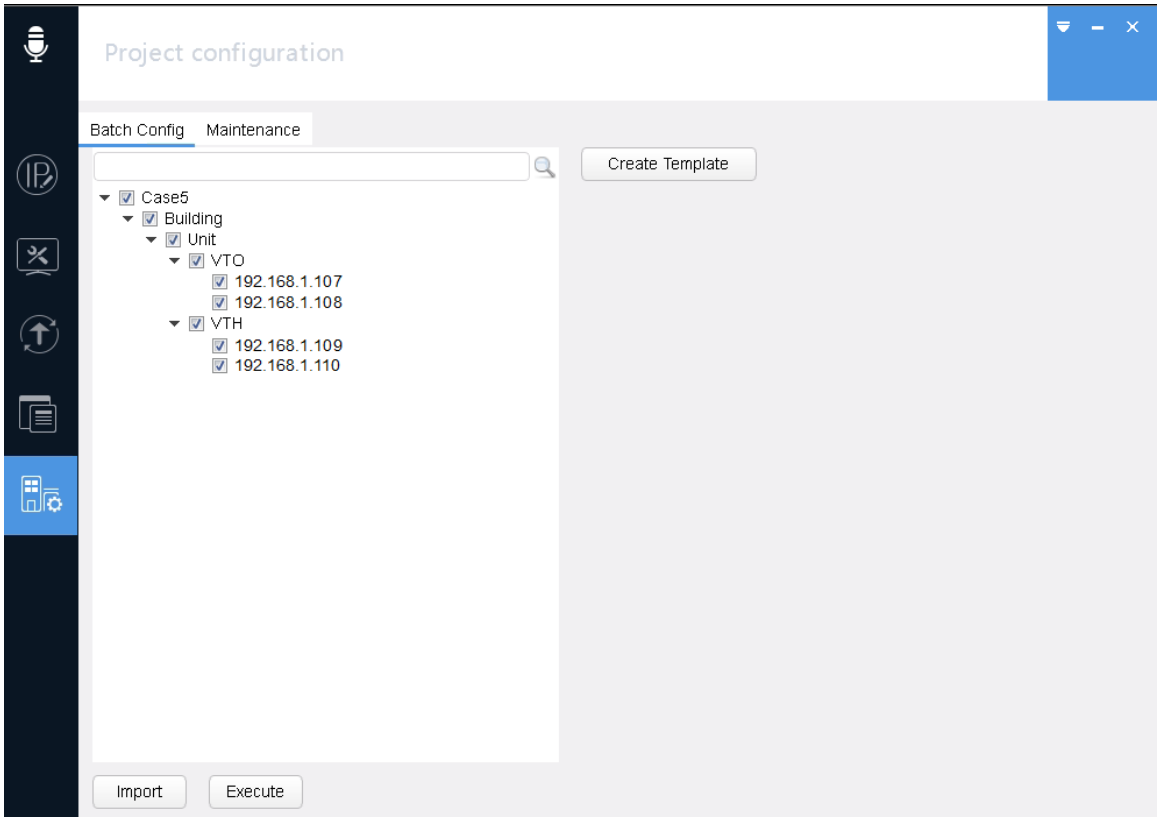


Figure 2-62

Step 9 Click **Execute**.

After the operation is completed, the result is displayed. See Figure 2-63.

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

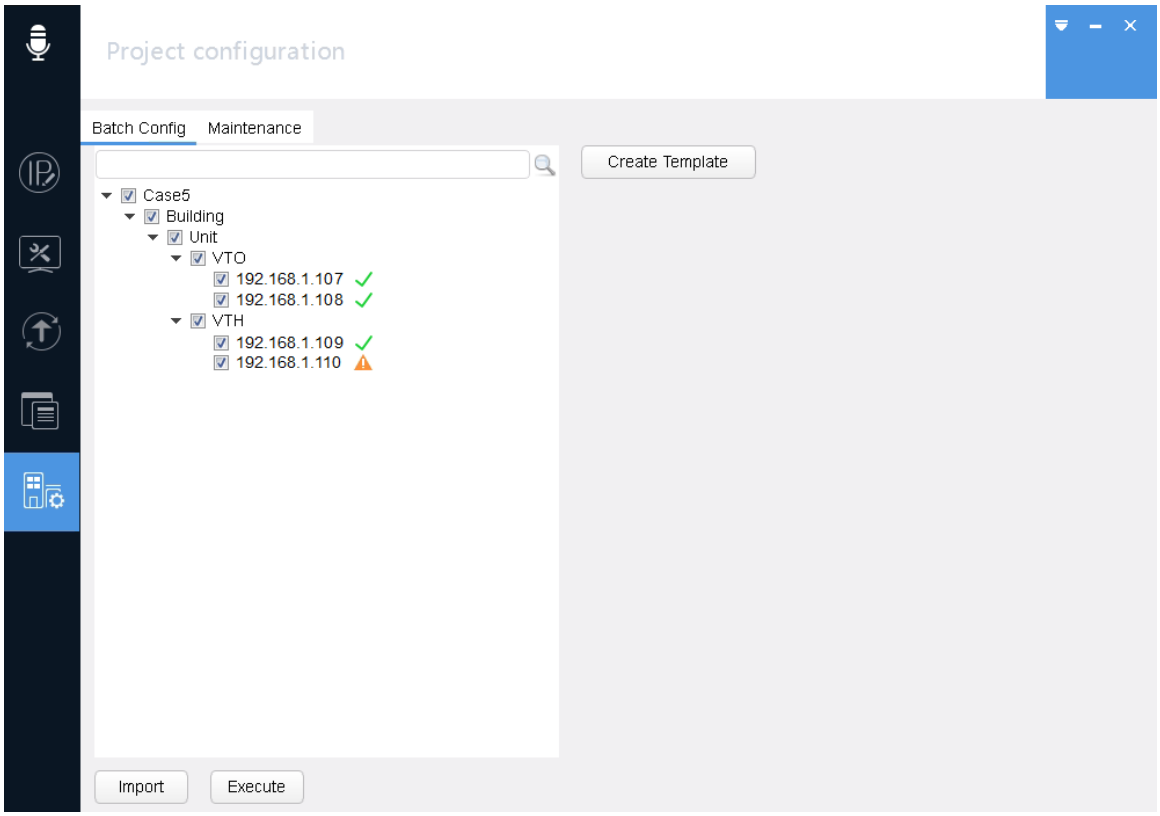


Figure 2-63

After the operation is completed, you can configure the device. For details, see "2.9.2 Maintenance."

2.9.2 Maintenance

You can configure VTO and VTH.

Step 1 On the project configuration interface, click the **Maintenance** tab.

The **Maintenance** interface is displayed, see Figure 2-64.

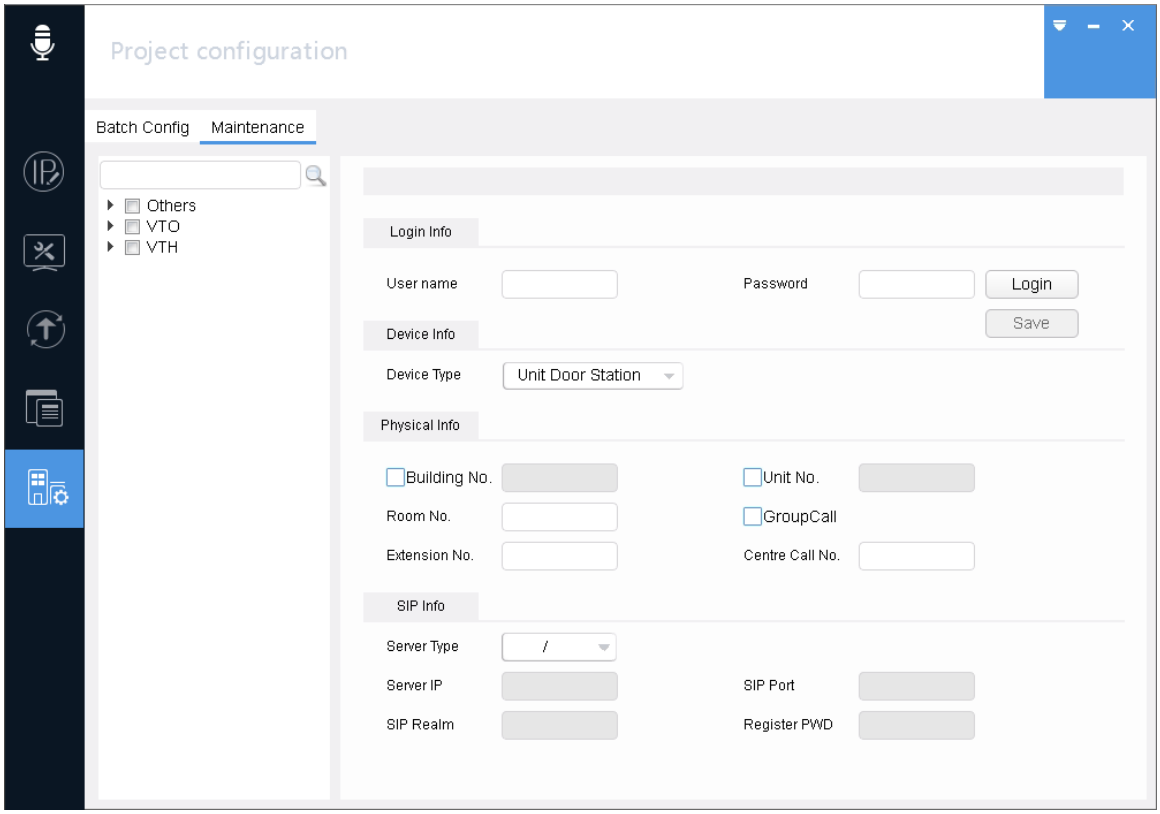


Figure 2-64

Step 2 Click ▸ next to the device type.

The device list is displayed.

Step 3 Select one or multiple devices.

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

Step 4 In the **Login Info** area, enter the device username and password, click **Login**. See Figure 2-65 for VTH device and see Figure 2-66 for VTO device.

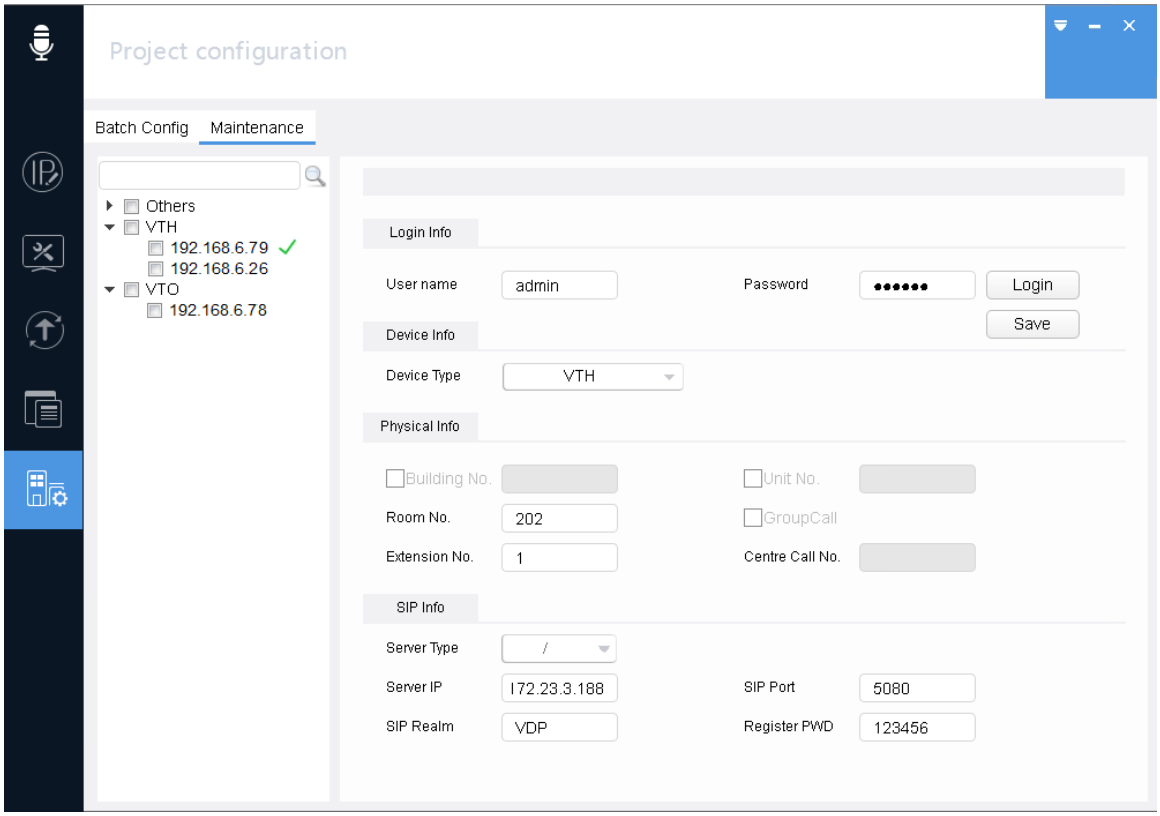


Figure 2-65

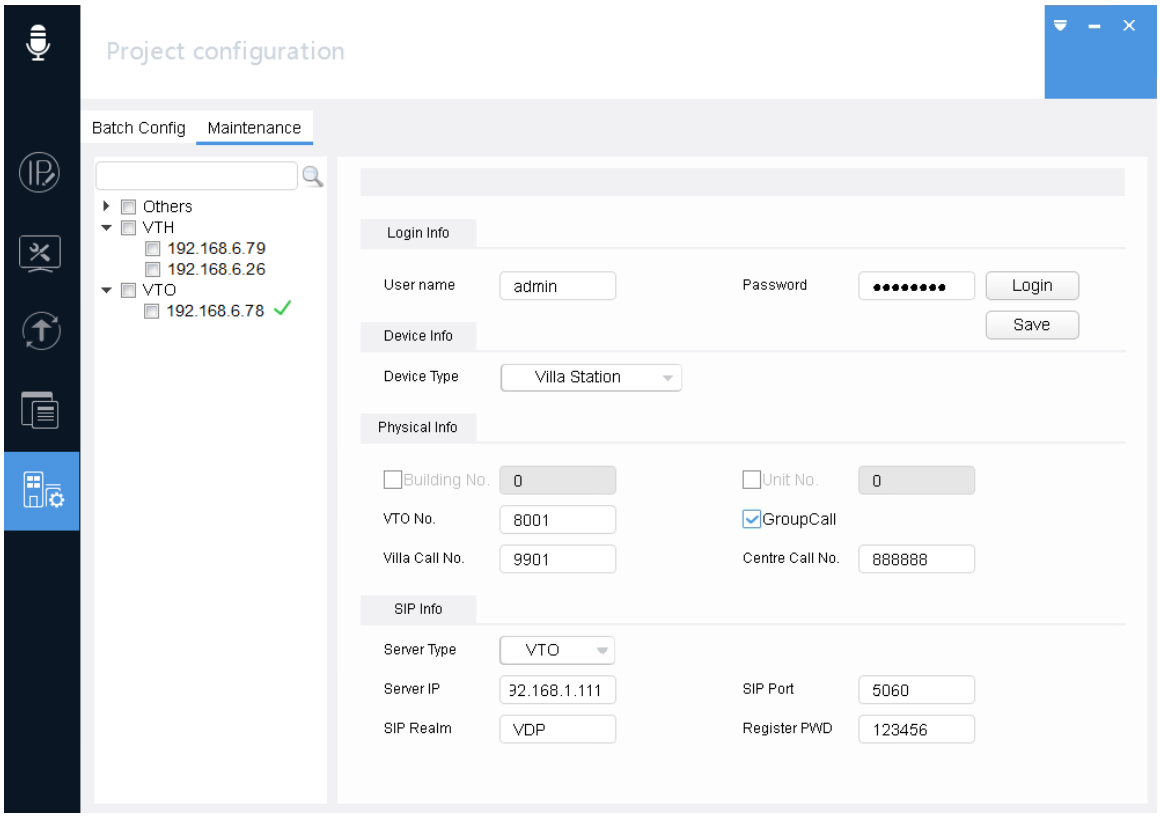


Figure 2-66

Step 5 Configure the settings. See Table 2-8.

Parameter		Description
VTH	Room No.	Enter the room number.
	Extension No.	Enter the extension number.

Parameter		Description
	Server IP	Enter the IP address of the server.
	SIP Port	Enter the port number of the SIP server.
	SIP Realm	Enter the domain name of the SIP server.
	Register PWD	Enter registration password of the SIP server.
VTO	DevType	Select the device type.
	VTO No.	Enter the VTO number.
	Group Call	When the device acts as a server, enable or disable group call function.
	Villa Call No.	Enter the villa call number.
	Center Call No.	Enter the center call number.
	Server Type	Select the server type.
	Server IP	Enter the IP address of the server.
	SIP Port	Enter the port number of the SIP server.
	SIP Realm	Enter the domain name of the SIP server.
	Register PWD	Enter registration password of the SIP server.

Table 2-8

Step 6 Click **Save** to complete the configuration.

You can click the success icon ( ) or click the failure icon ( ) for the details.