VDPConfig
(Windows Version)
User's Manual

V1.2.2

Foreword

General

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

Safety Instructions

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

Signal Words	Meaning
 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.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.2.3	1. Add VTS tab in "2.8 Project Configuration", update the operations of "2.3 Initializing Devices."	September 2019
V1.2.2	2. Move the content of "configuring device" to the Project Configuration as "2.8.2 Maintenance". 3. Modify the SIP template. 4. Delete the VT system function of the Project Configuration.	September 5, 2018
V1.2.1	1. Add "Privacy Protection Notice". 2. Update "About the Manual".	May 3, 2018
V1.2.0	1. Add "Project Configuration". 2. Add "Configuring Alarm" and "Configuring Arm/Disarm Settings".	January 15, 2018
V1.1.0	1. Add "Cybersecurity Recommendations" and "Online Upgrade". 2. Update "The Main Interface".	October 25, 2017
V1.0.2	3. Update "Basic Operations". 4. Add "Initializing Devices".	May 5, 2017
V1.0.1	Update the structure of the Basic Operations chapter.	December 1, 2016
V1.0.0	First release.	February 26, 2016

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

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

Table of Contents

Foreword ..... **I**
1 Overview **1**
1.1 General 1
1.2 The Main Interface 1
2 Basic Operations **4**
2.1 Searching Devices 4
2.2 Adding Devices 6
2.2.1 Adding One Device 6
2.2.2 Adding Multiple Devices 7
2.3 Initializing Devices 9
2.4 Modifying IP 14
2.4.1 Modifying One IP 14
2.4.2 Modifying IP in Batches 15
2.5 Configuring System Settings 16
2.5.1 Timing 16
2.5.2 Rebooting and Restoring 18
2.5.3 Modifying and Resetting Password 20
2.5.4 Configuring Alarm 28
2.5.5 Configuring Arm/Disarm Settings 31
2.6 Local Upgrade 32
2.6.1 Upgrading One Device 32
2.6.2 Upgrading Devices in Batches 34
2.7 Data Backup 35
2.7.1 Exporting data 35
2.7.2 Importing data 37
2.8 Project Configuration 39
2.8.1 Batch Configuring 39
2.8.2 Maintenance 43
2.8.3 VTS 45
Appendix 1 Cybersecurity Recommendations **48**

1 Overview

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 Interface

For the main interface of the Tool, see Figure 1-1. For details, see Table 1-1.

- After the Tool starts, it will search the devices according to the network segments setting in **Search setting**.
- After the installation, the **Current Segment Search** check box is selected by default in the **Search setting** during the first login.

Figure 1-1 Main interface

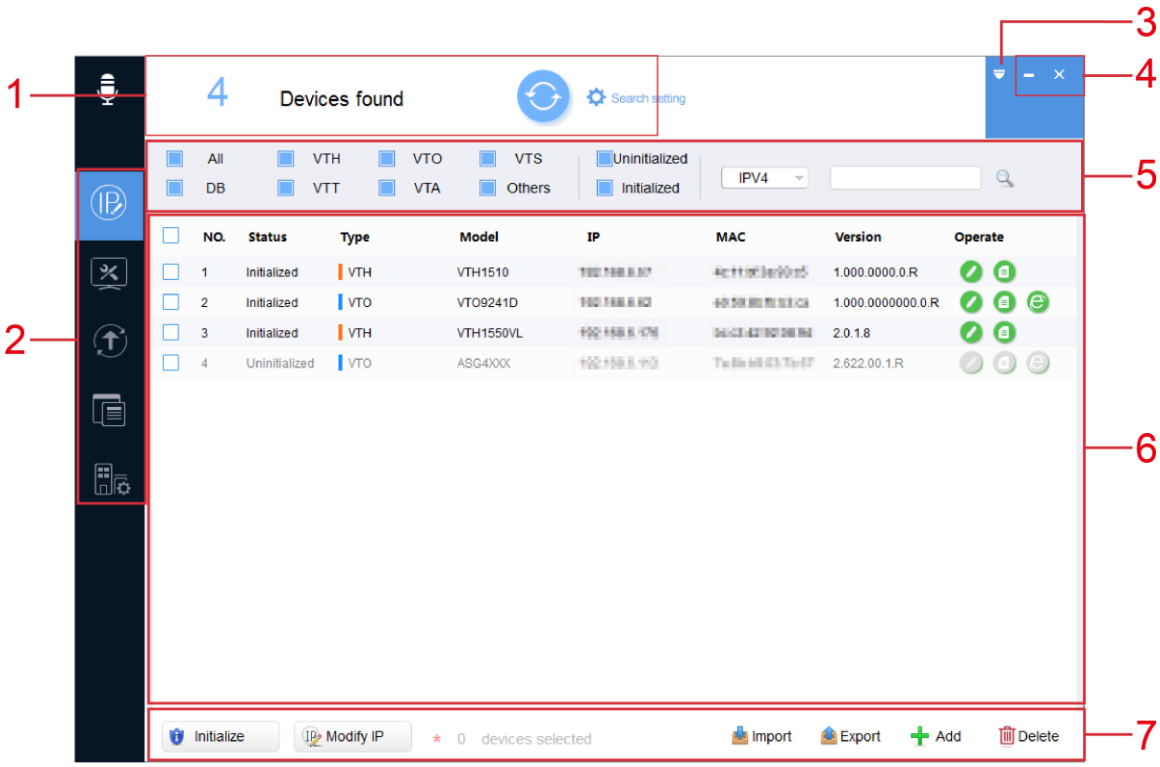
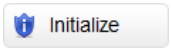
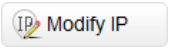
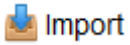
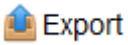
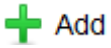
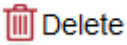


Table 1-1 Main interface description

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	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, reset password and alarm configuration. ● 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	Provides access to check the **Help** file and software version, and set update timeout and network timeout

No.	Function	Description
4	Window Control Button	• Click  to minimize the software. • Click  to exit the software.
5	Filtering	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	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 the web login interface.  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 or more devices and click  to initialize the select devices. • Batch IP modification: Select devices and click  to modify the IP address of the select devices. • Device import: Click  to import one or multiple devices through template. • Device details export: Select one or more devices and click  to import the device details. • Device addition: Click  to add one or more devices manually. • Device deleting from the list: Select one or more devices and click  to delete the select devices.

2 Basic Operations

2.1 Searching Devices

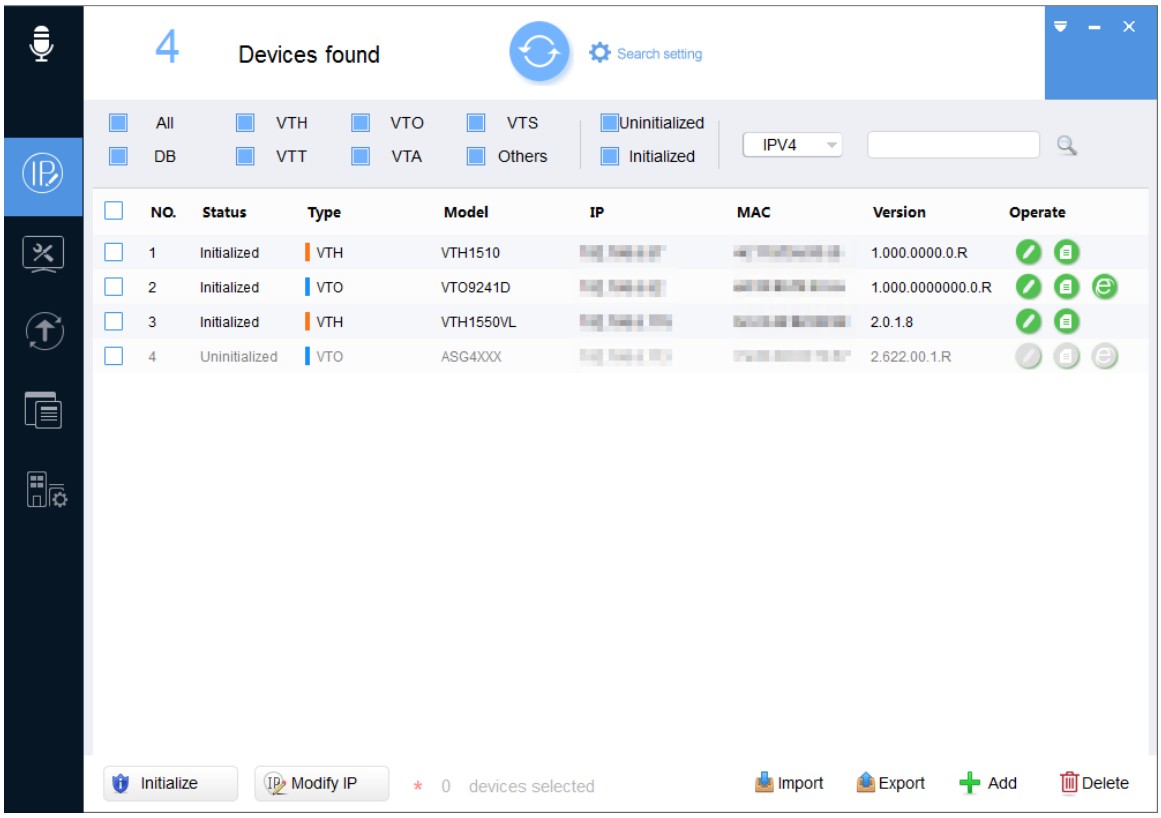
You can search the devices through setting the current segment or other segment.

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.

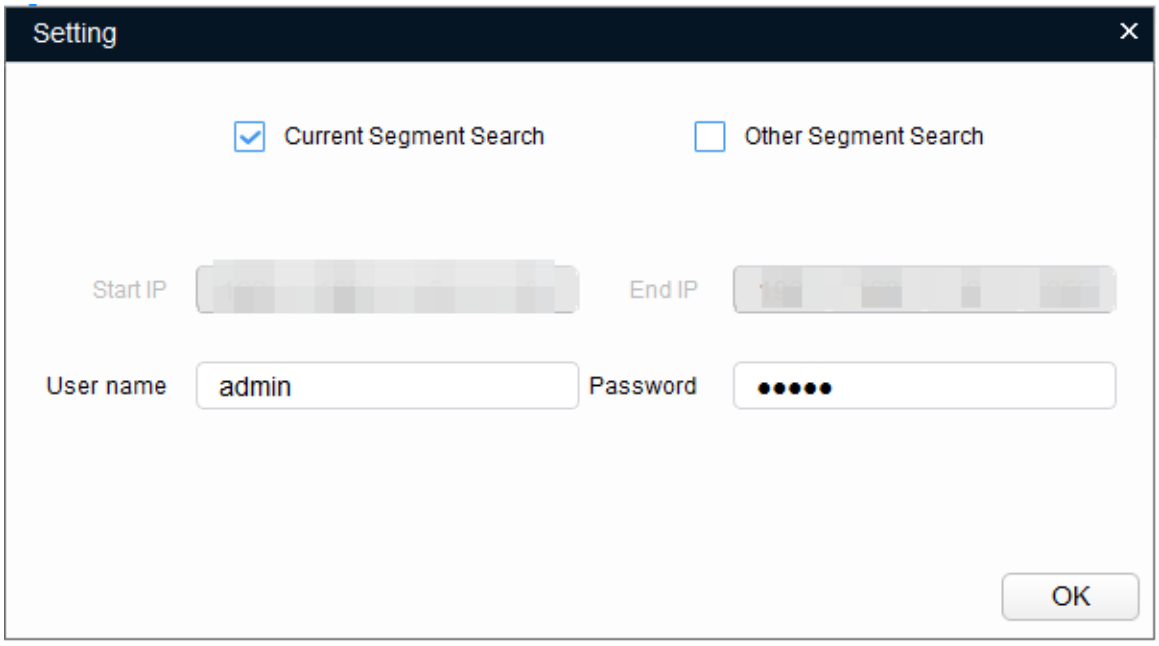
Figure 2-1 Modify IP (1)



Step 2 Click Search setting.

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

Figure 2-2 Setting



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.

- 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 username 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 interface.

- 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.

Make sure that 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.

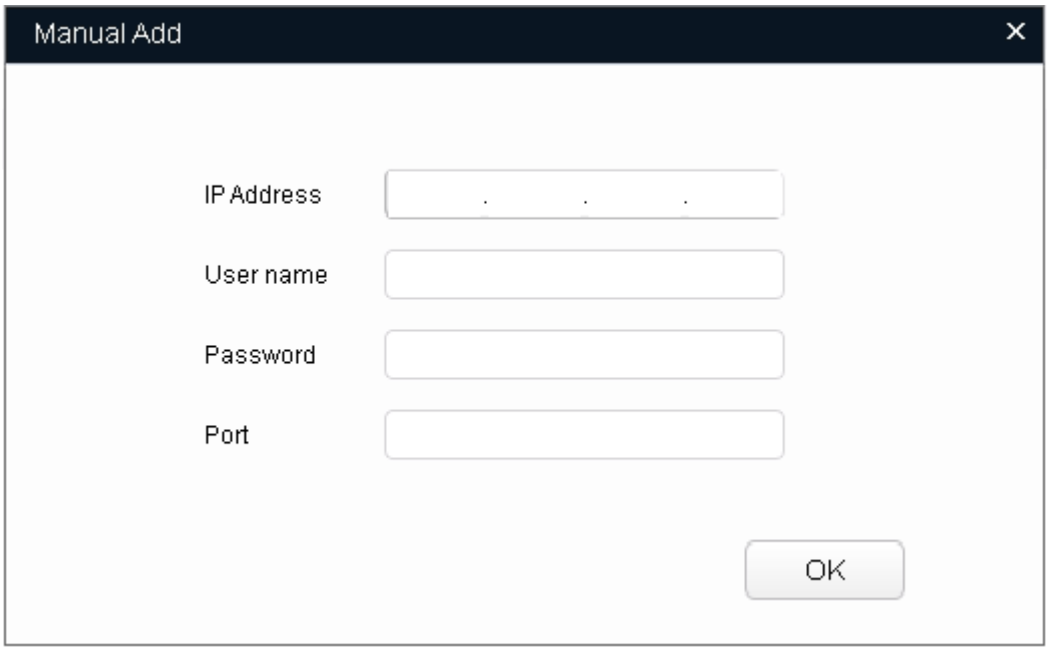
Step 1 Click .

The **Modify IP** interface is displayed.

Step 2 Click Add.

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

Figure 2-3 Manual add



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

Table 2-1 Manual add description

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.

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.

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.

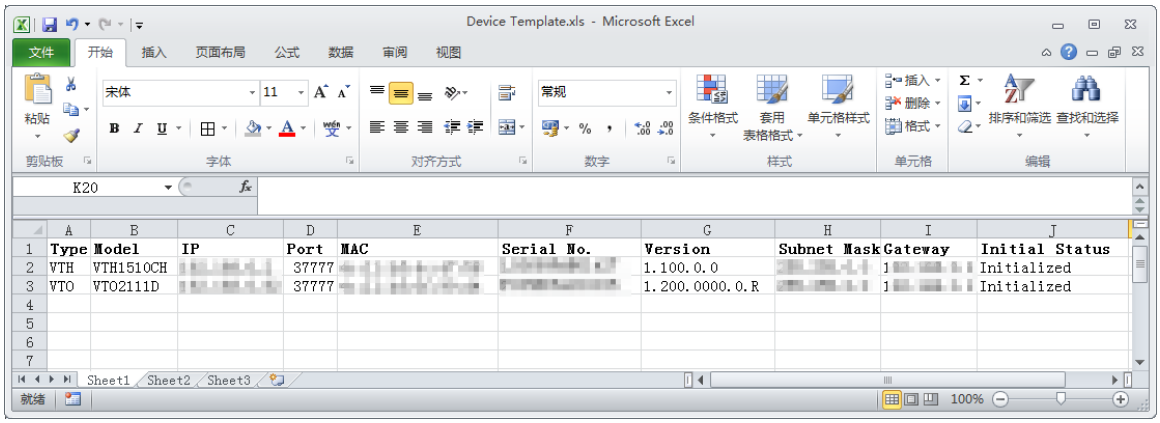
Step 5 Click **OK**.

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.

- 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**.

Figure 2-4 Device template



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

Table 2-2 Device template description

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.

Step 3 Save and close the template.

2.2.2.3 Importing Devices

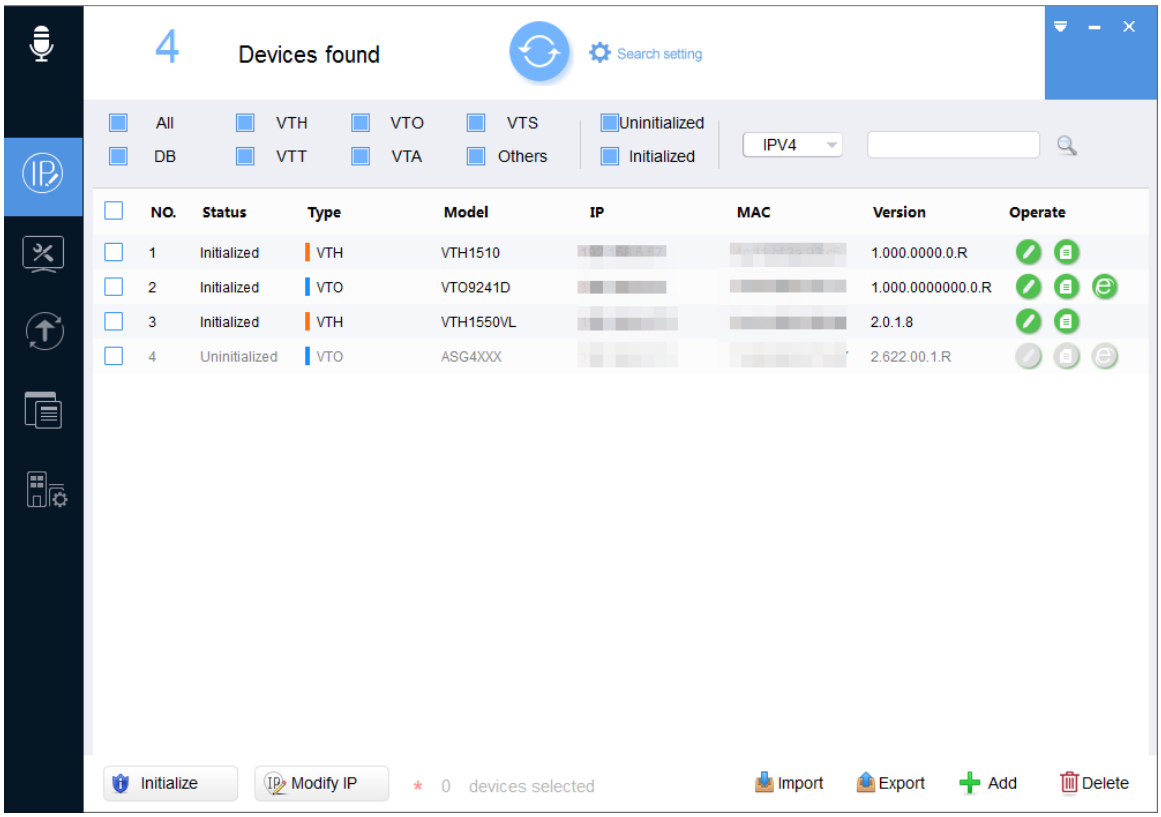
You can import the filled template to add device.

Close the template file before importing.

Step 1 Click .

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

Figure 2-5 Modify IP (2)



Step 2 Click Import.

The **Open** dialog box is displayed.

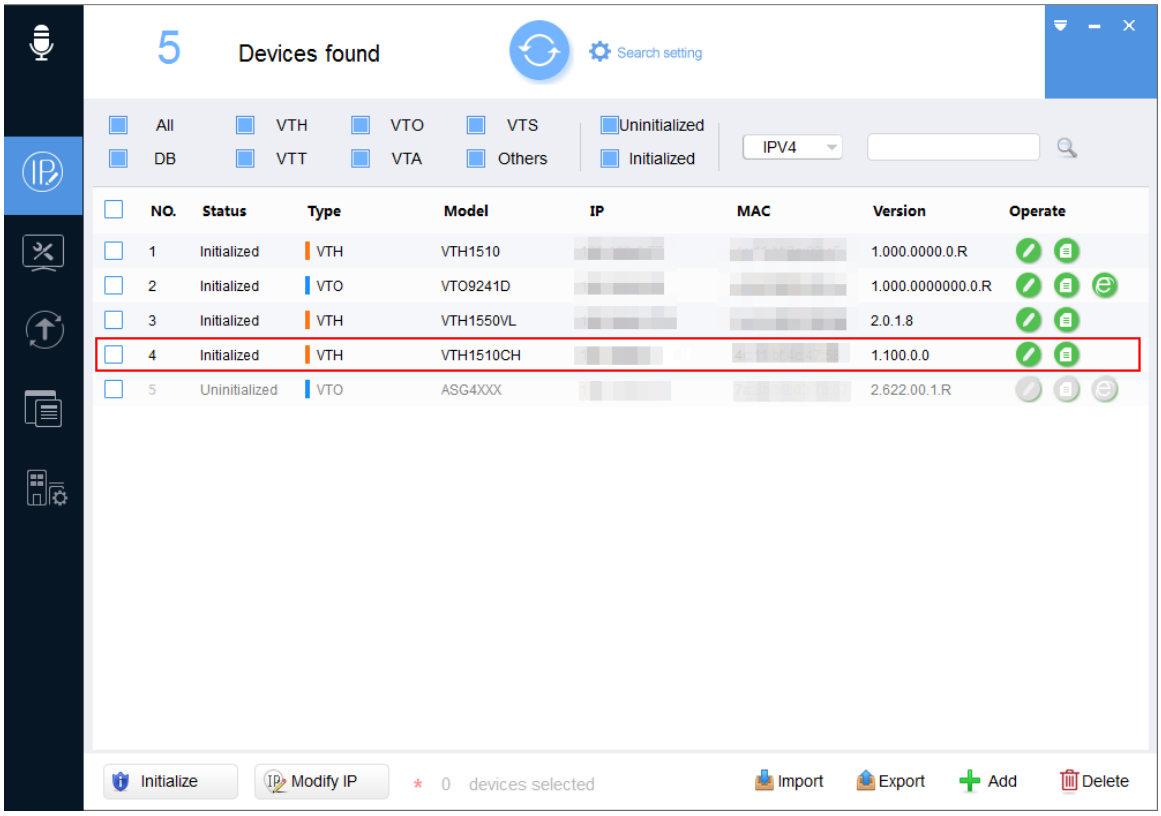
Step 3 Select the template, and then click **Open**.

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 Imported devices



2.3 Initializing Devices

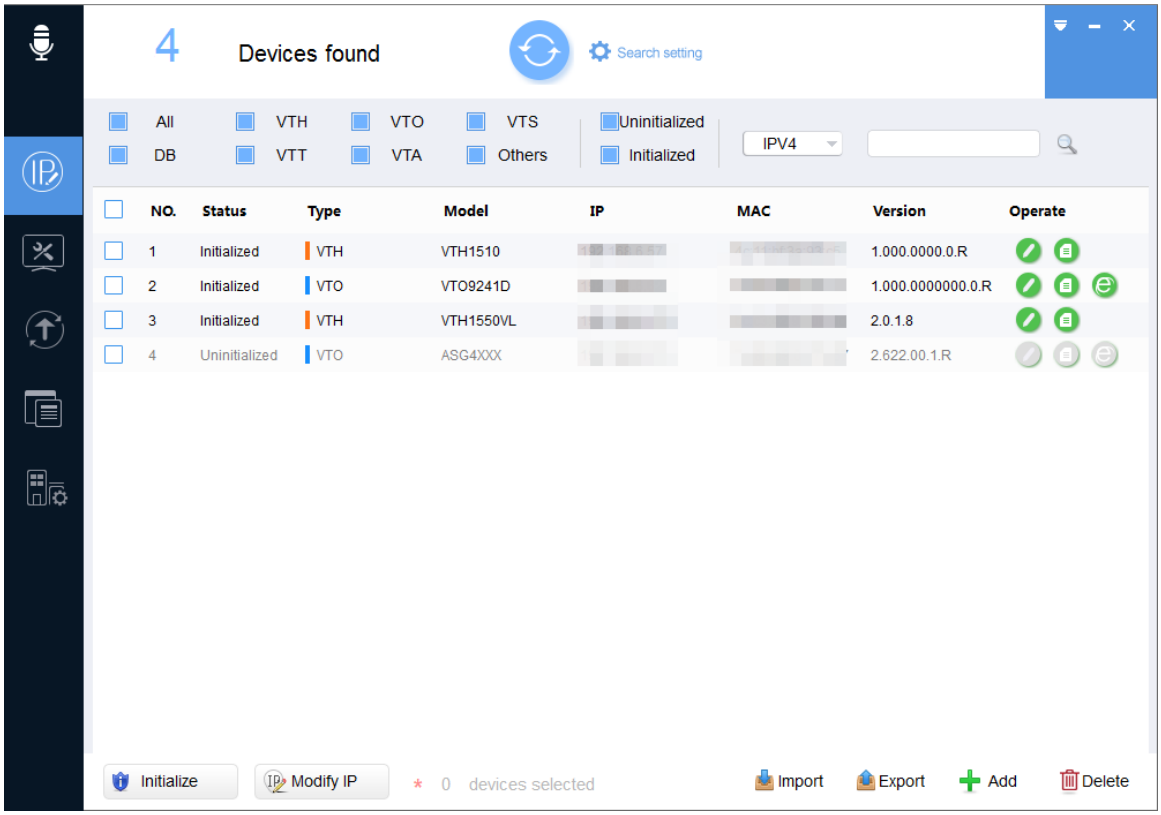
You can initialize one or multiple devices.

- 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 Modify IP (3)

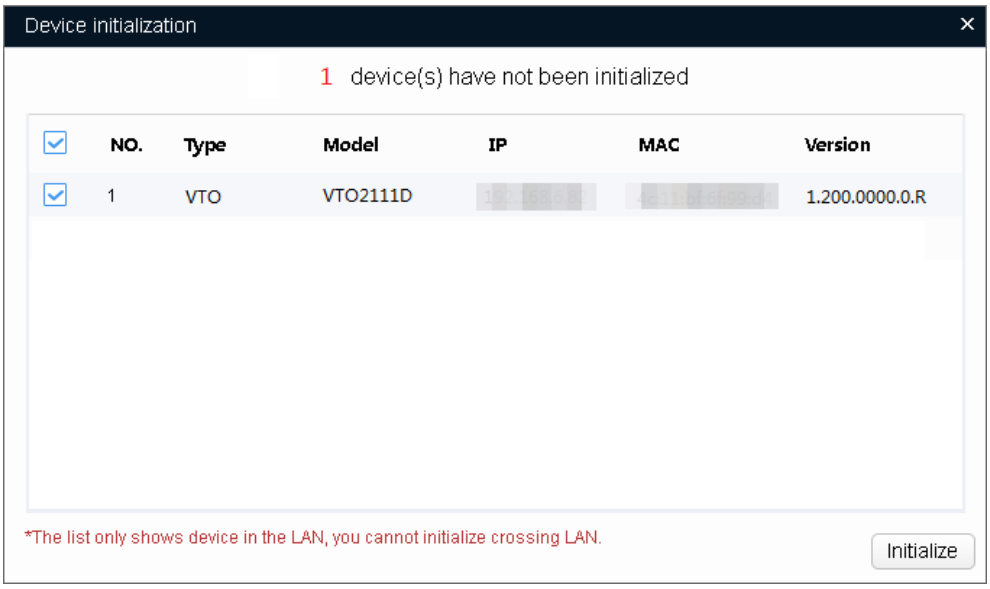


Step 2 Select an uninitialized device.

Step 3 Click Initialize.

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

Figure 2-8 Device initialization (1)

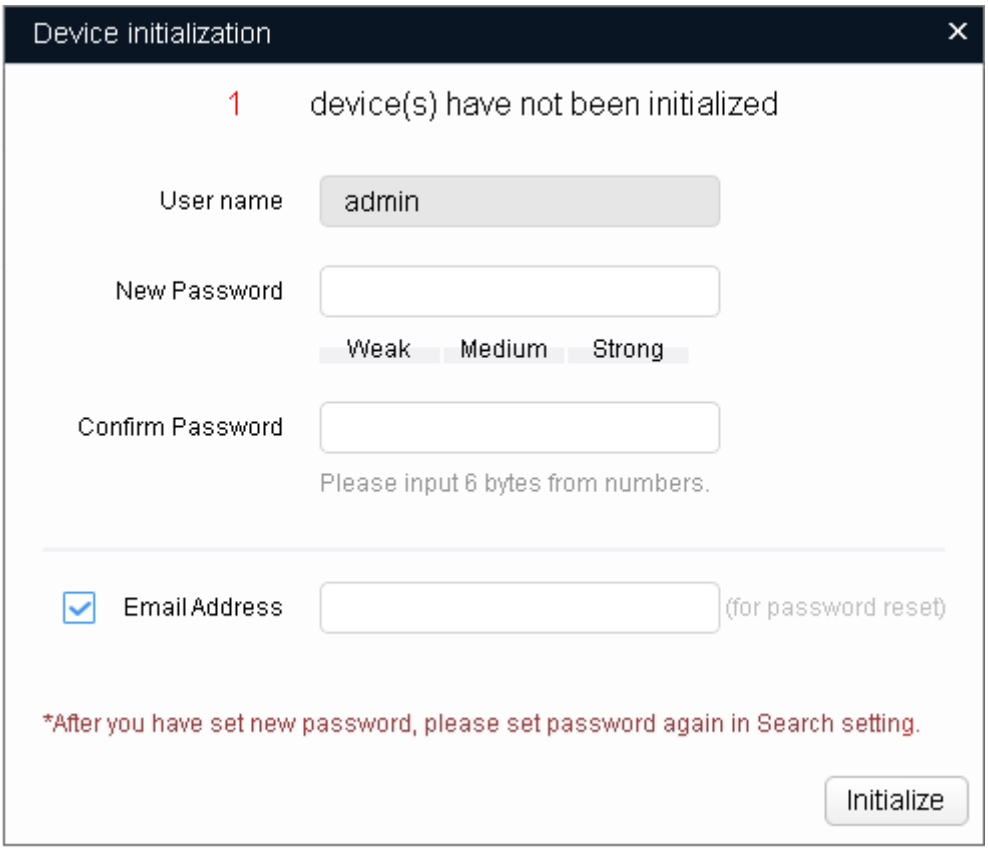


Step 4 Select the device, and then click **Initialize**.

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

- The interface might be different, 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.

Figure 2-9 Device initialization (2)



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

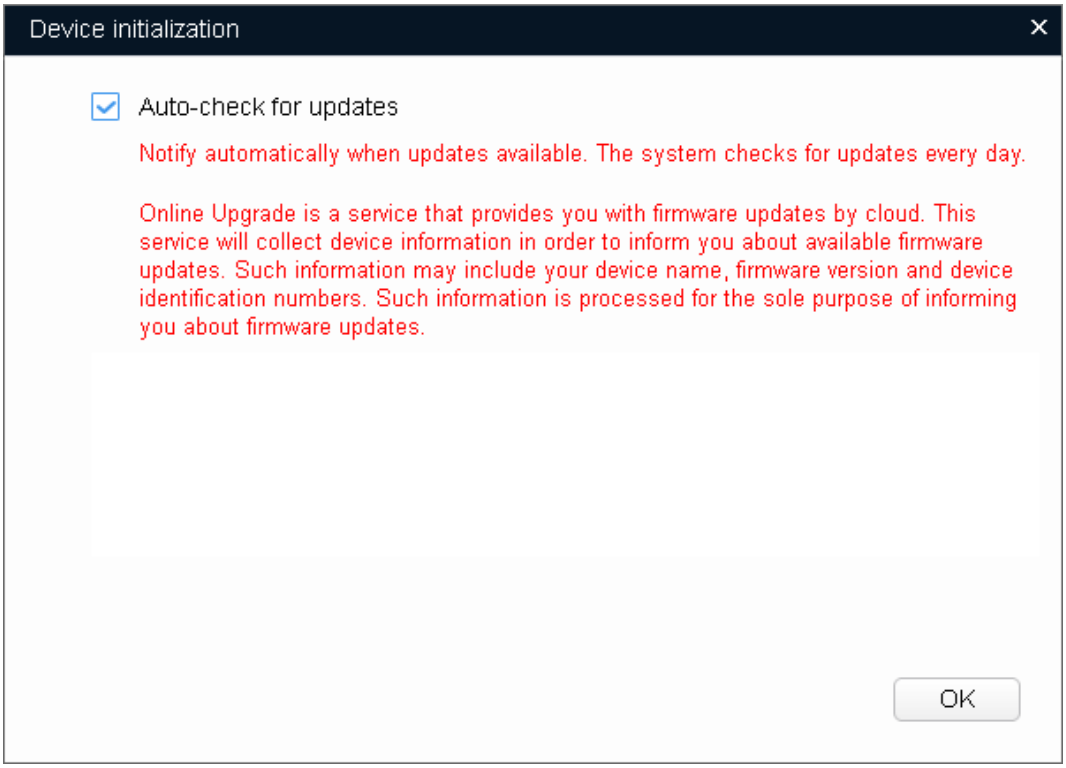
Table 2-3 Initialization parameters

Parameter	Description
User name	The user name is **admin** by default.
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 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 ' " ; : &). ● The new password can only be set as six numbers. After setting the new password, 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.

Step 6 Click **Initialize**.

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

Figure 2-10 Device initialization (3)



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

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

The **Initialization** interface is displayed. See Figure 2-11 and Figure 2-12.

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

Figure 2-11 Initializing multiple devices

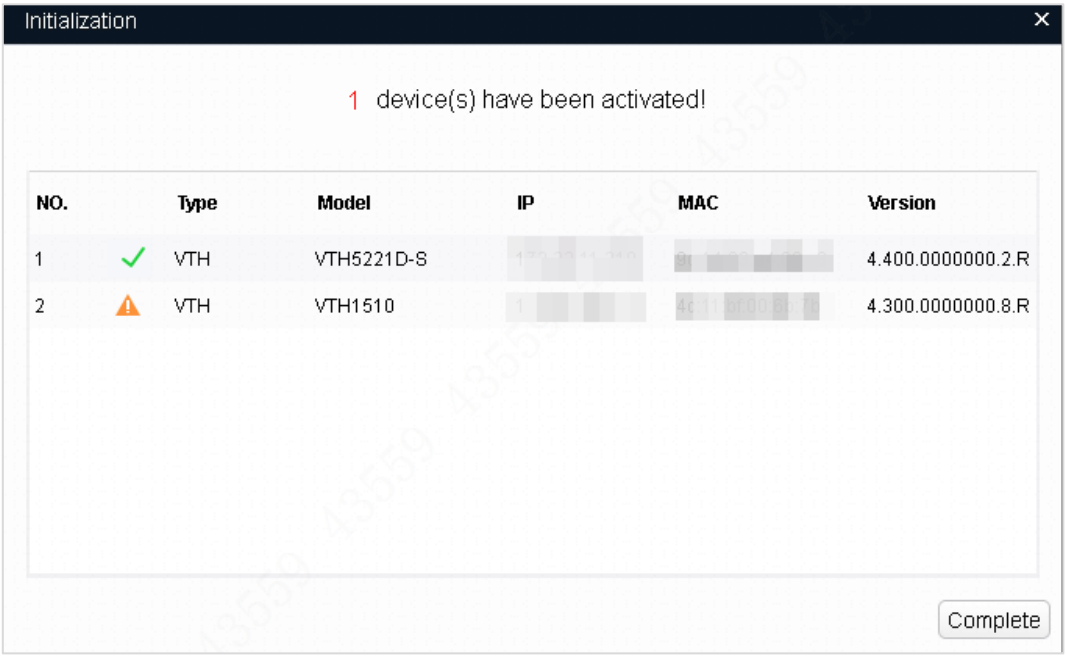
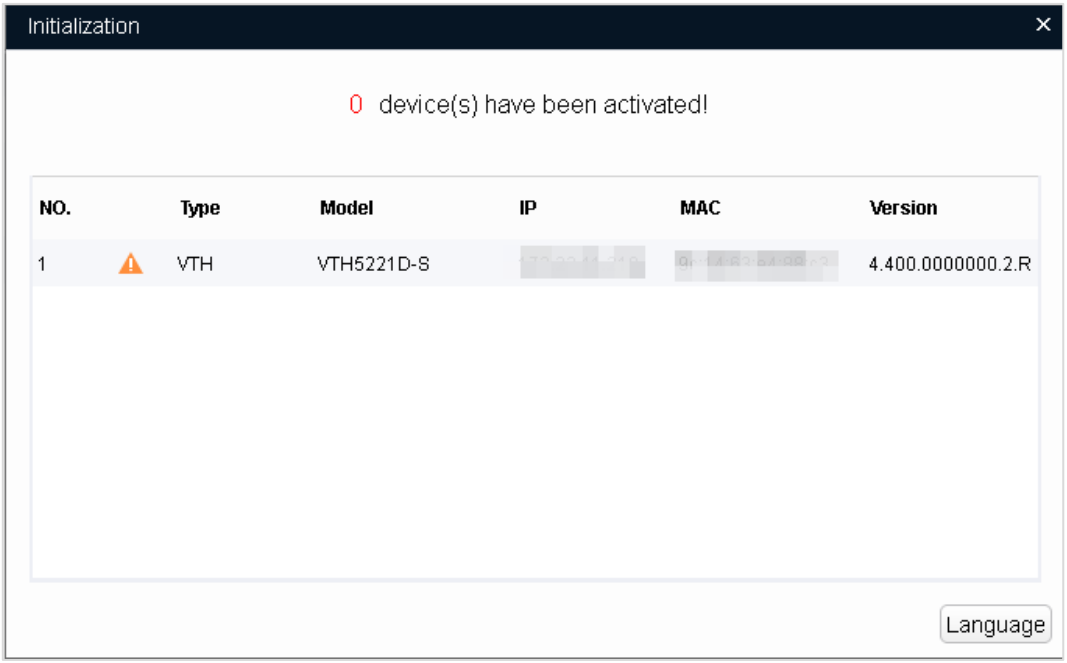


Figure 2-12 Initializing one device

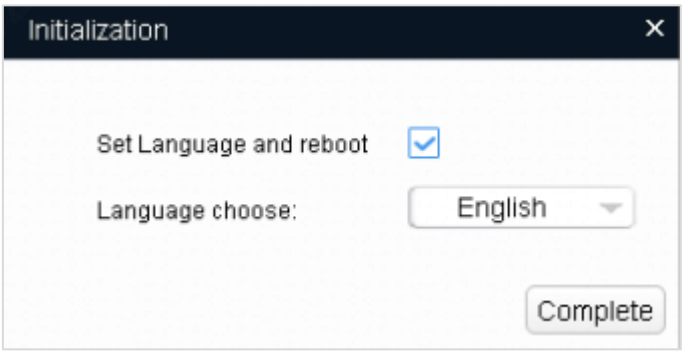


Step 9 Initialize device.

- Initialize multiple devices.
  Click **Complete** to complete the 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 in other interfaces of the Tool.
- Initialize one device.

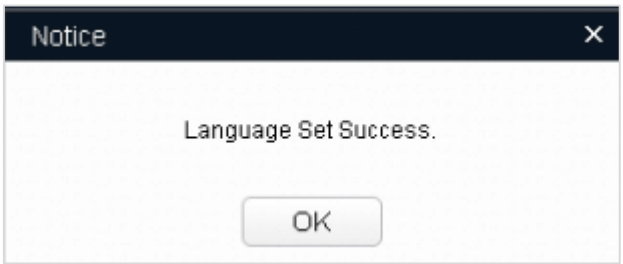
1) Click **Language**. And the language selection interface is displayed. See Figure 2-13. Select the language from the **Language choose** list.

Figure 2-13 Language selection



2) Click **Complete**. The **Notice** dialog box is displayed. See Figure 2-14.

Figure 2-14 Notice



3) Click **OK** to complete the 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 in other interfaces of the Tool.

2.4 Modifying IP

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

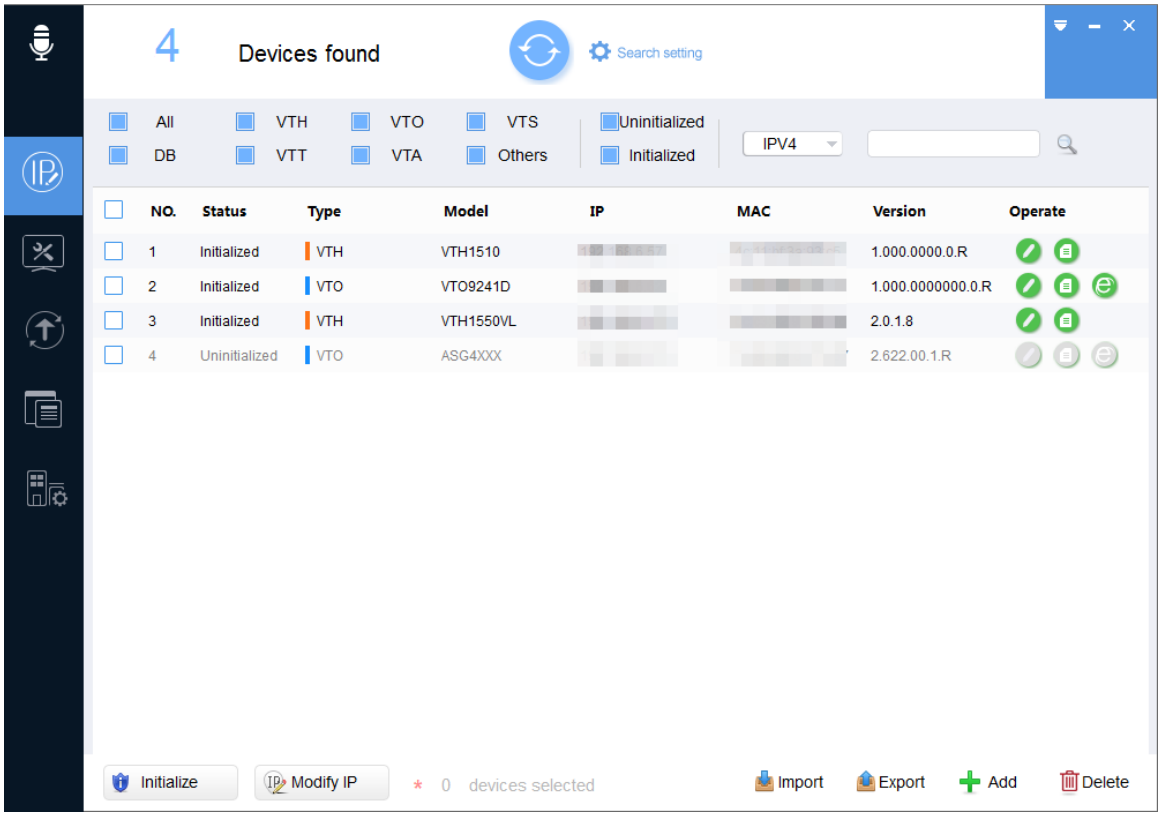
- When the devices quantity is small or their login passwords are different, you can modify one IP at a time.
- When the devices quantity is big and they share the same login password, you can modify IP in batches.

2.4.1 Modifying One IP

Step 1 Click  .

The **Modify IP** interface is displayed. See Figure 2-15.

Figure 2-15 Modify IP (4)

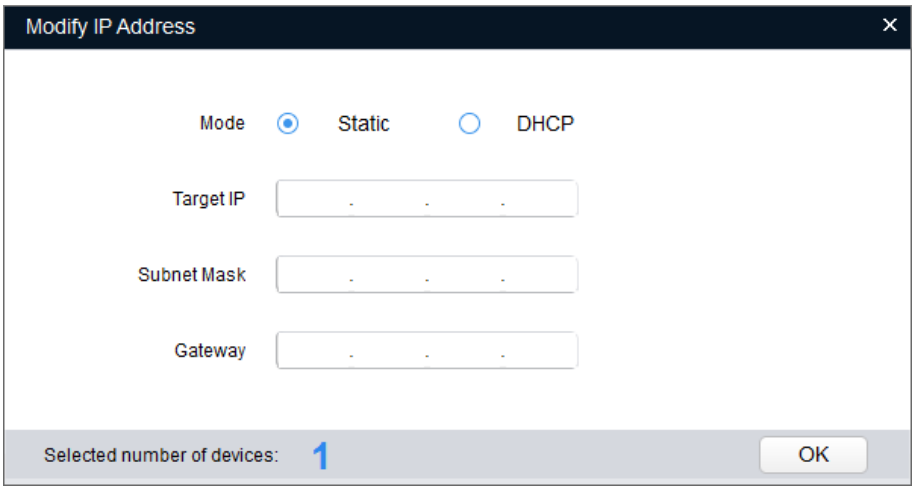


Step 2 Click the **IP Modification** button () of the device that you want to modify IP.

The **Modify IP Address** dialog box is displayed. See Figure 2-16.

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 2-16 Modify IP address (1)



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.

The VTO does not support DHCP mode.

Step 4 Click **OK**.

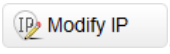
2.4.2 Modifying IP in Batches

Step 1 Click  .

The **Modify IP** interface is displayed.

Step 2 Select the devices you want to modify IP.

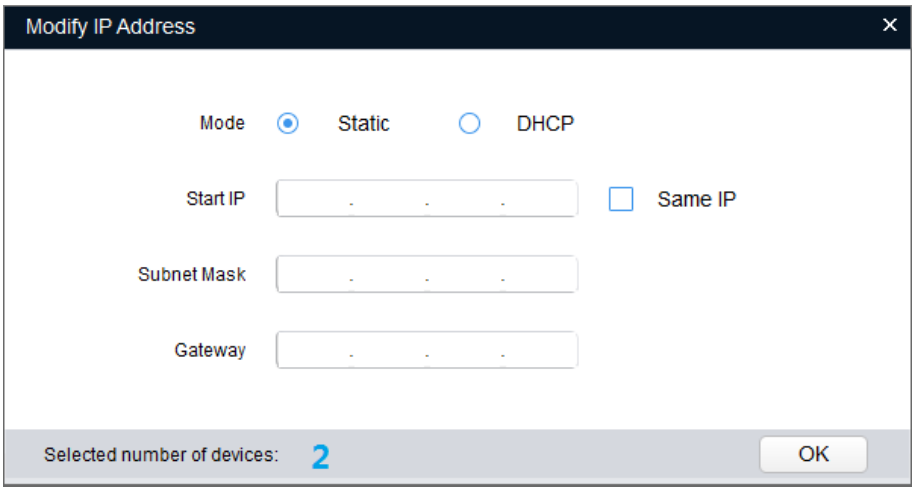
If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

Step 3 Click 

.

The **Modify IP Address** dialog box is displayed. See Figure 2-17.

Figure 2-17 Modify IP address (1)



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.

The VTO does not support DHCP mode.

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.

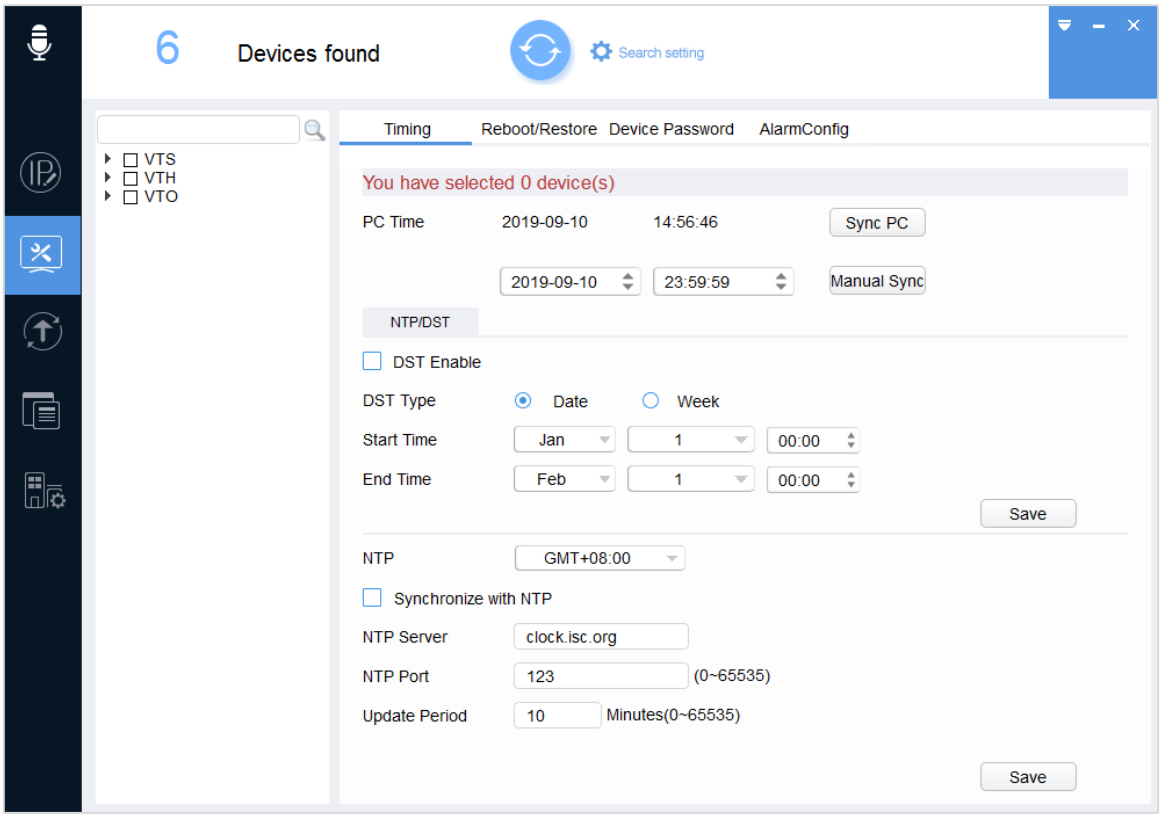
2.5.1 Timing

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 2-18.

Figure 2-18 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, 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**.

Table 2-4 NTP sync

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

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

Table 2-5 DTS

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	

2.5.2 Rebooting and Restoring

2.5.2.1 Rebooting

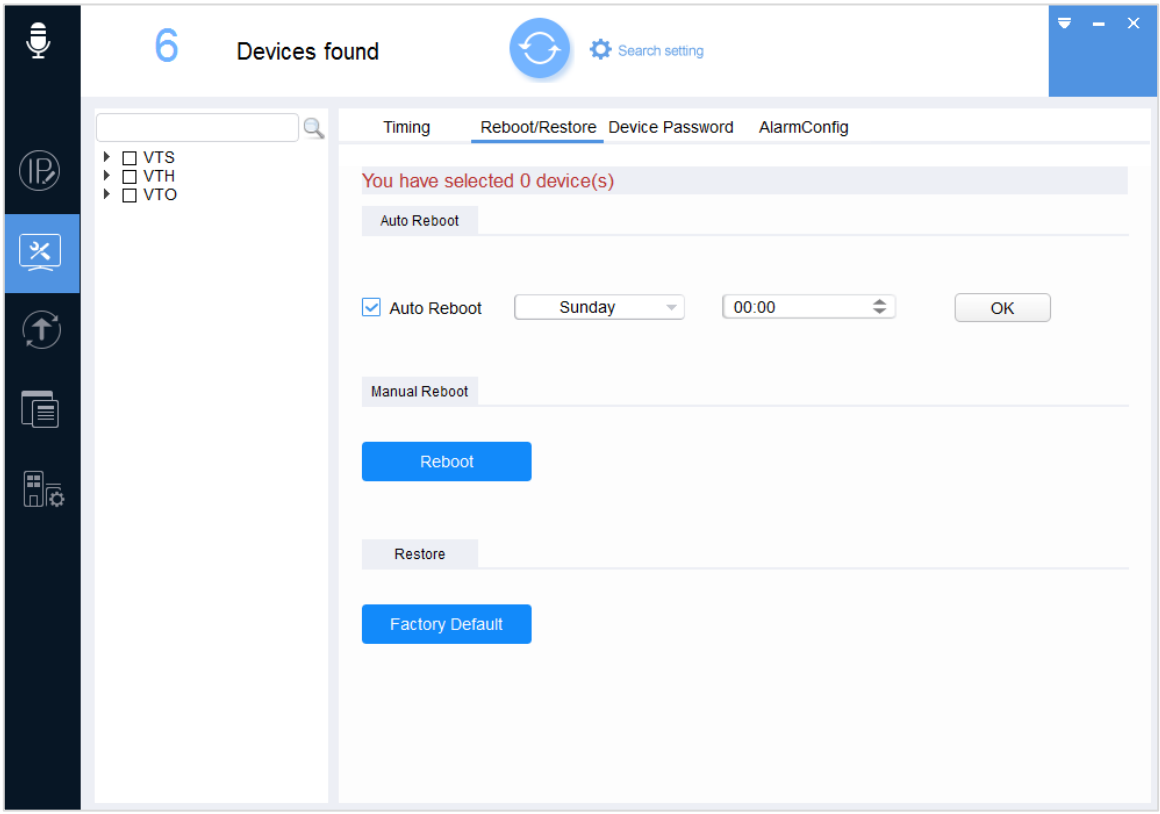
You can set the time to automatically reboot device and manually reboot device.

Rebooting will interrupt the business. Stop other operations before rebooting device.

Step 1 On the **System Settings** interface, click the **Reboot/Restore** tab.

The **Reboot/Restore** interface is displayed. See Figure 2-19.

Figure 2-19 Reboot/Restore (1)



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, 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

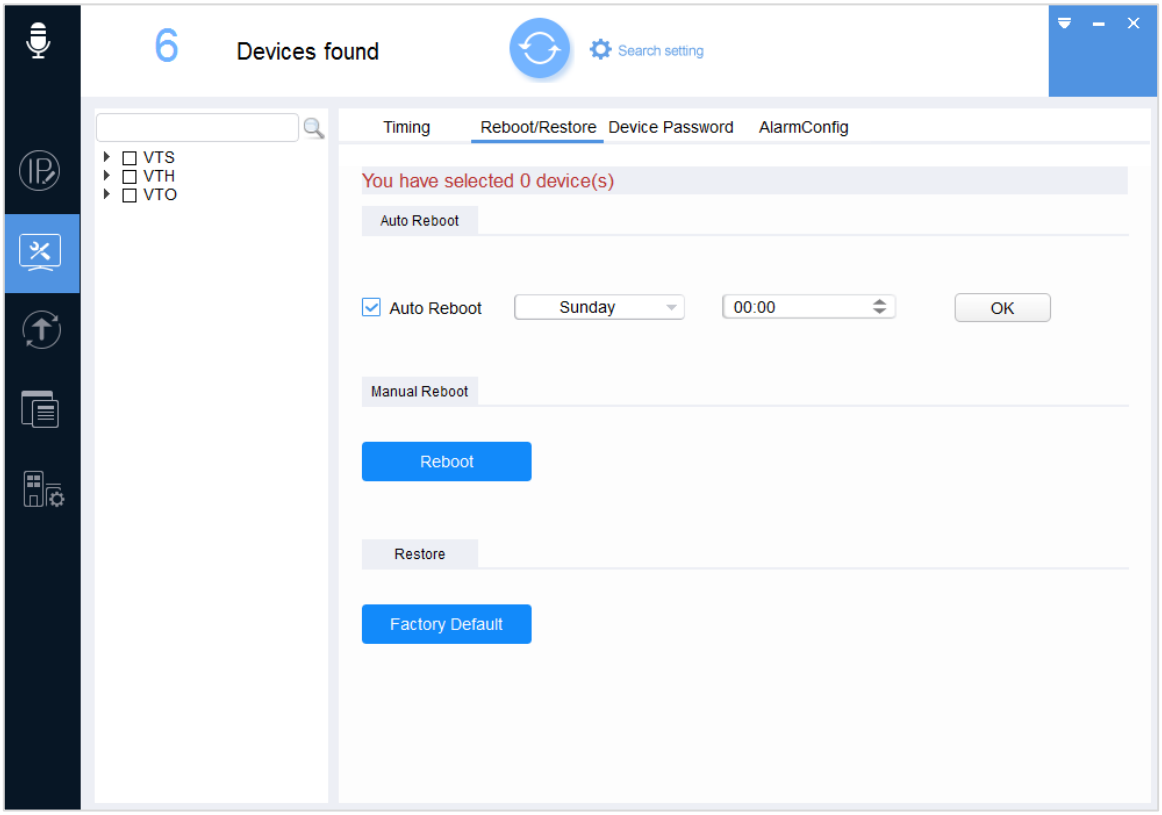
You can restore the factory settings to clear configurations and account files.

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 Settings** interface, click the **Reboot/Restore** tab.

The **Reboot/Restore** interface is displayed. See Figure 2-20.

Figure 2-20 Reboot/Restore (2)



Step 2 Click ▸ next to the device type.

The device list is displayed.

Step 3 Select one or multiple devices.

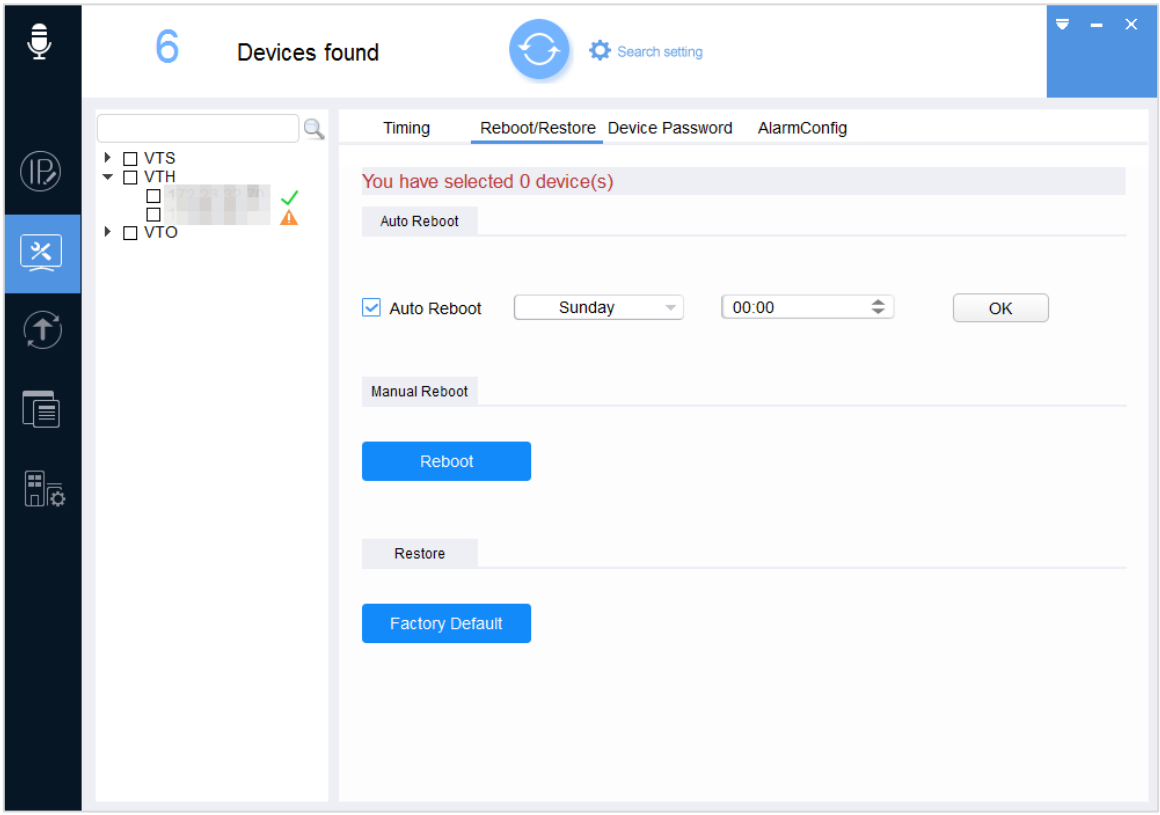
If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

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

After restoring is completed, the result is displayed. See Figure 2-21.

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

Figure 2-21 Restoring result



2.5.3 Modifying and Resetting Password

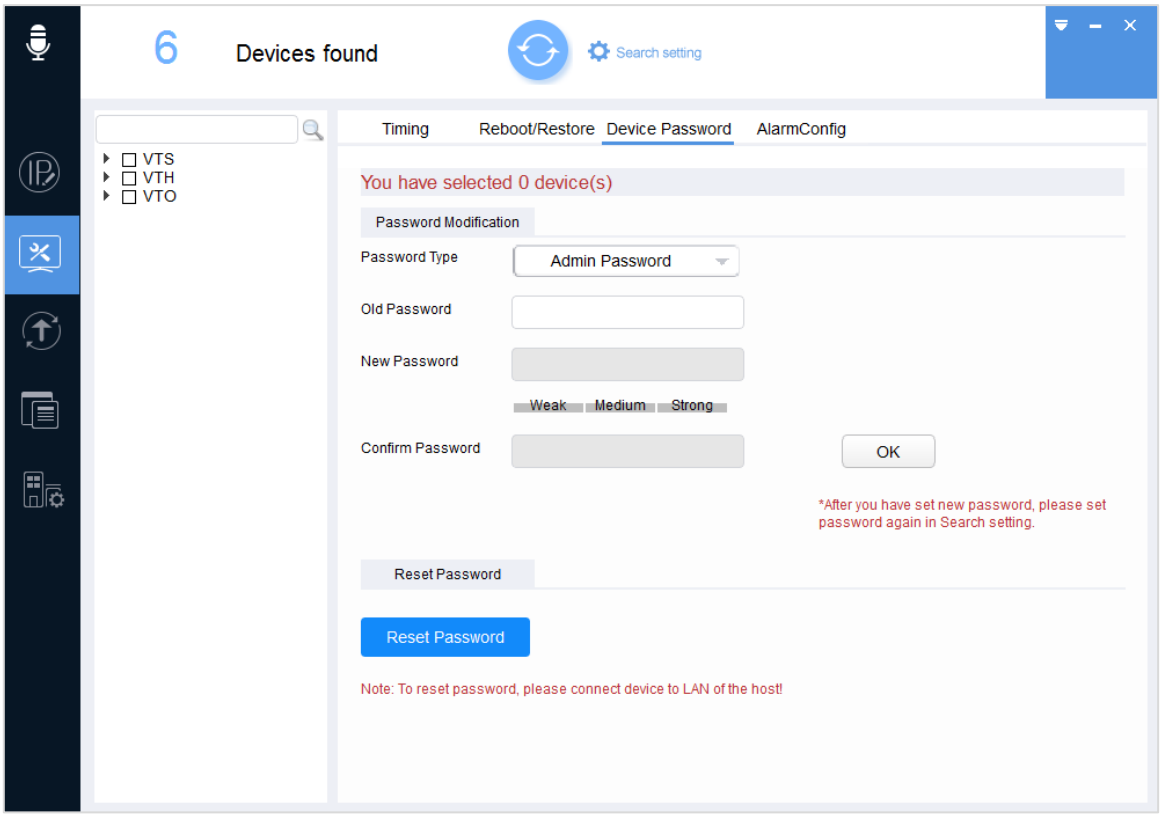
2.5.3.1 Modifying Password

You can modify the device login password.

Step 1 On the **System Settings** interface, click the **Device Password** tab.

The **Device Password** interface is displayed. See Figure 2-22.

Figure 2-22 Device password (1)



Step 2 Click ▸ next to the device type.

The device list is displayed.

Step 3 Select one or multiple devices.

- 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."

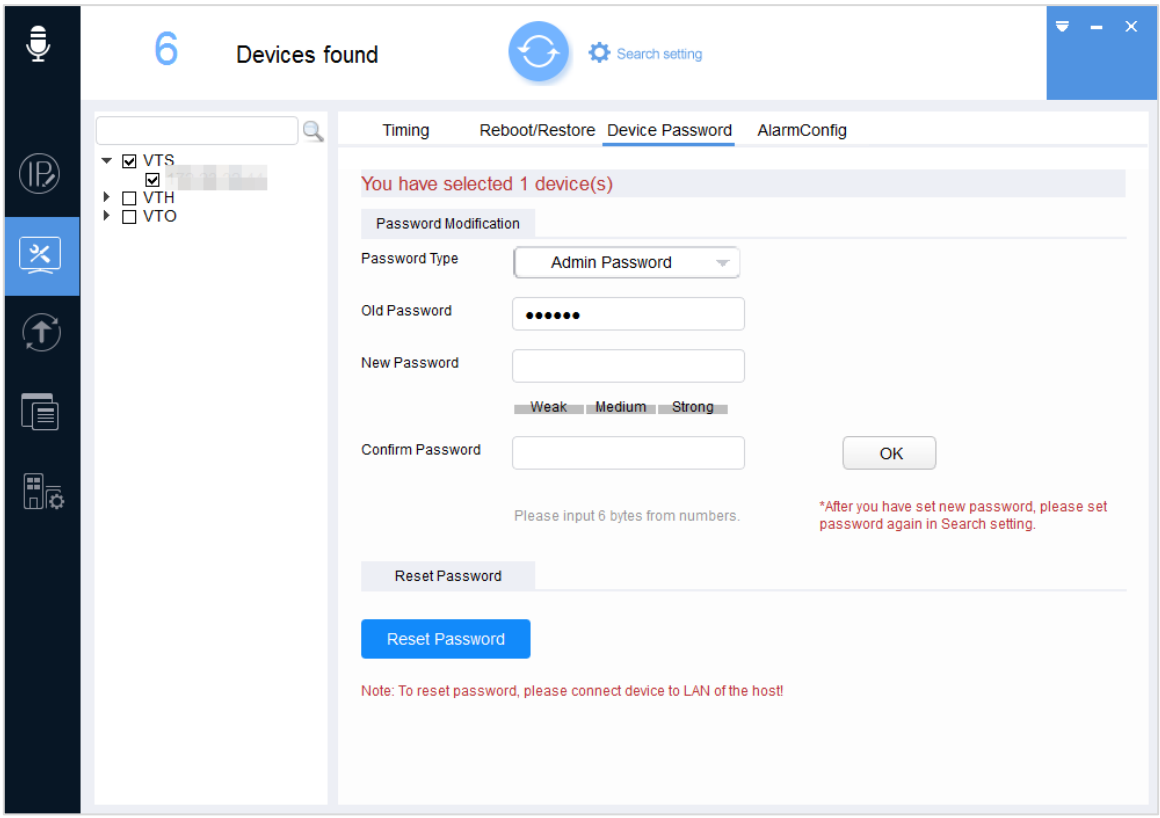
Step 4 In the **Password Type** list, select **Admin Password** or **User Password**.

- 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 are displayed. See Figure 2-23.

Figure 2-23 Password setting rules



Step 6 Enter the new password and confirm password.

There are two setting rules for new password depending on the devices, and follow the instructions on the interface to set 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 ' " ; : &).
- The new password can only be set as six numbers.

- Not all devices support the above password rules, and the actual interface shall prevail.
- After setting the new password, enter the new password to login the device when you search the devices.

Step 7 Click **OK**.

- 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 admin password been changed, it might not be changed to the default password again.

2.5.3.2 Resetting Password

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

- The password resetting operation can only be performed to the devices within the same local area network.
- If you did not enter the reserve information for password reset during device initialization, you can reset the password only through XML file.

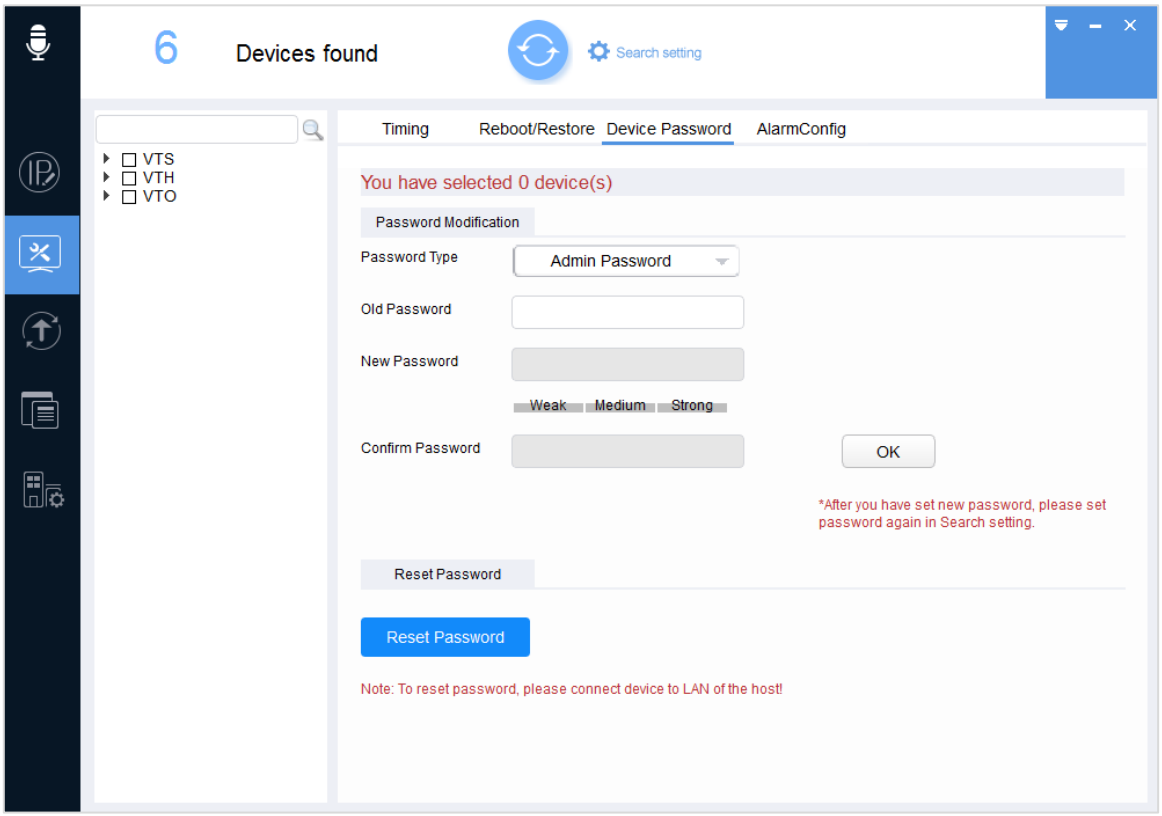
2.5.3.2.1 Using the QR Code

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 Settings** interface, click the **Device Password** tab.

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

Figure 2-24 Device password (2)



Step 2 Click ▸ next to the device type.

The device list is displayed.

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

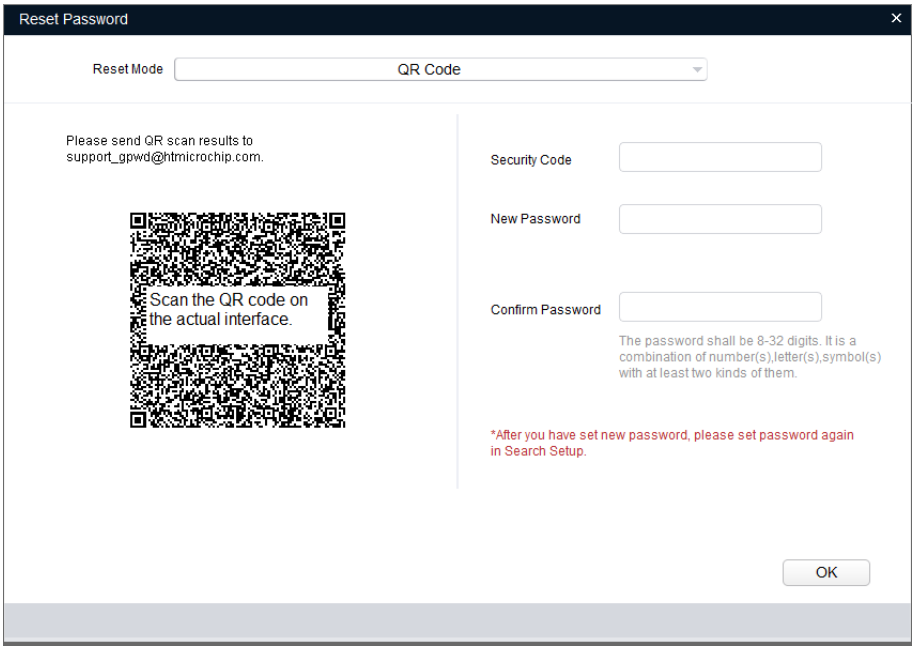
If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

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 2-25.

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 prevail.

Figure 2-25 Reset password (QR code)



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

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

After you get the security code, 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 follow the instructions on the interface to set 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 ' " ; : &).
- The new password can only be set as six numbers.

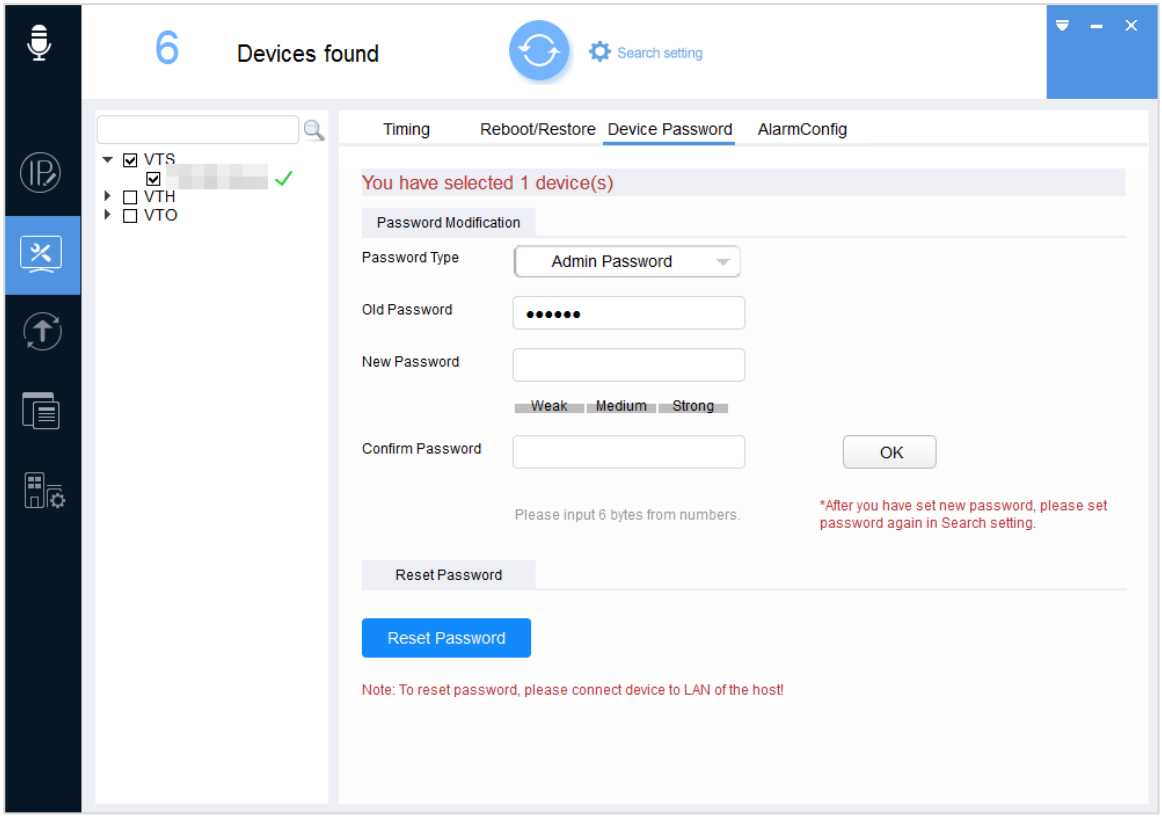
After setting the new password, enter the new password to log in to the device when you search the devices

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

After resetting is completed, the result is displayed. See Figure 2-26.

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

Figure 2-26 Password resetting result (QR code)



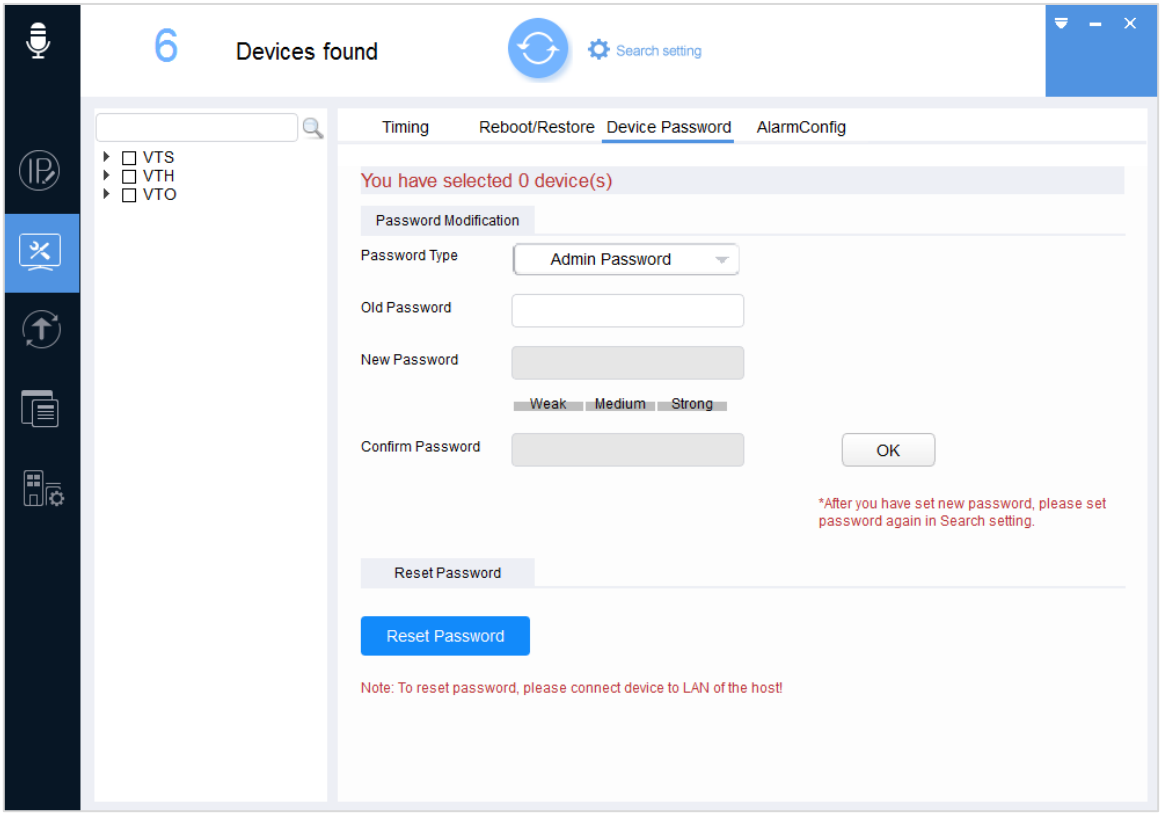
2.5.3.2.2 Using the XML File

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

Step 1 On the **System Settings** interface, click the **Device Password** tab.

The **Device Password** interface is displayed. See Figure 2-27.

Figure 2-27 Device password (3)



Step 2 Click ▸ next to the device type.

The device list is displayed.

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.

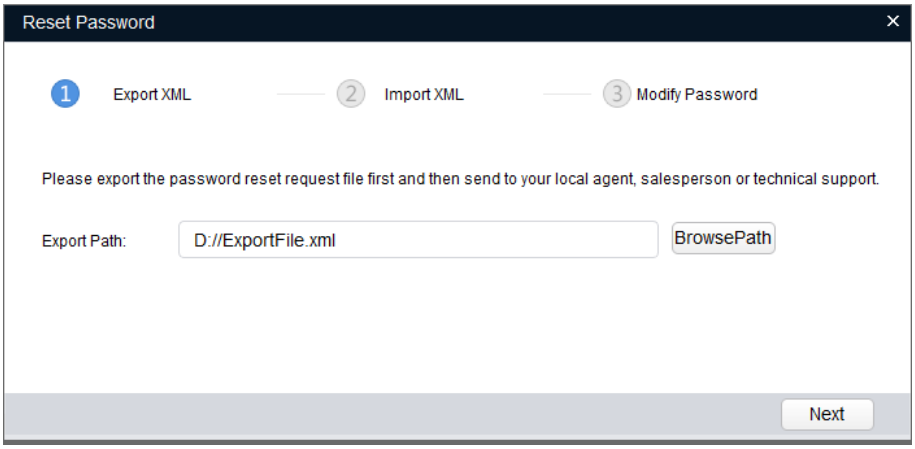
- The user interface might be different dependent on the model you purchased. If there is inconsistency between the Manual and the actual product, the actual product shall prevail.
- When reset passwords for multiple devices, the Tool resets all devices based on the password reset mode of the first selected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

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

The **Reset Password-Export XML** interface is displayed. See Figure 2-28.

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 prevail.

Figure 2-28 Reset password (Export XML)



Step 5 Export XML.

4) Click **BrowsePath** to select the save path for the exported XML file.
5) Click **Next** to start exporting.
   After the exporting is completed, a **Notice** dialog box will be displayed.
6) Click **OK**.
   After completing exporting the XML, the **Reset Password-Import XML** interface is displayed.

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

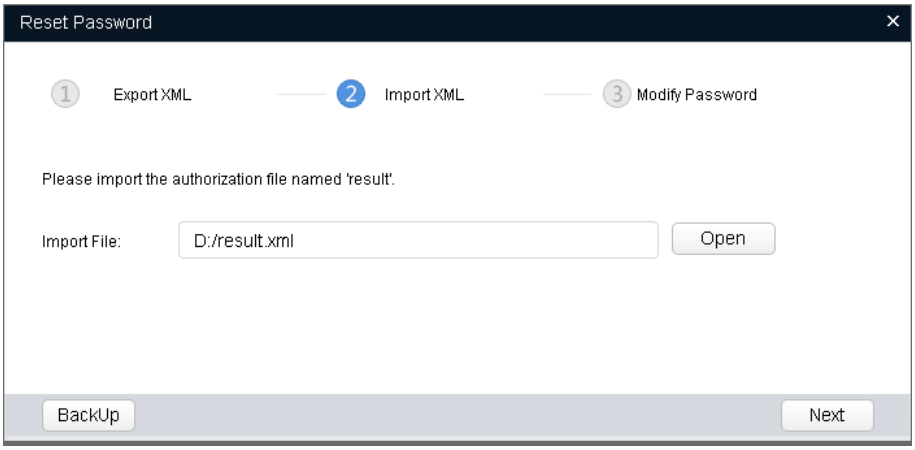
Find the **ExportFile.xml** under the save path and send it as an attachment to the designated mailbox indicated on the interface. In a few minutes, you will receive a **result.xml** file as an attachment and save it properly.

Step 7 Import XML.

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 2-29.

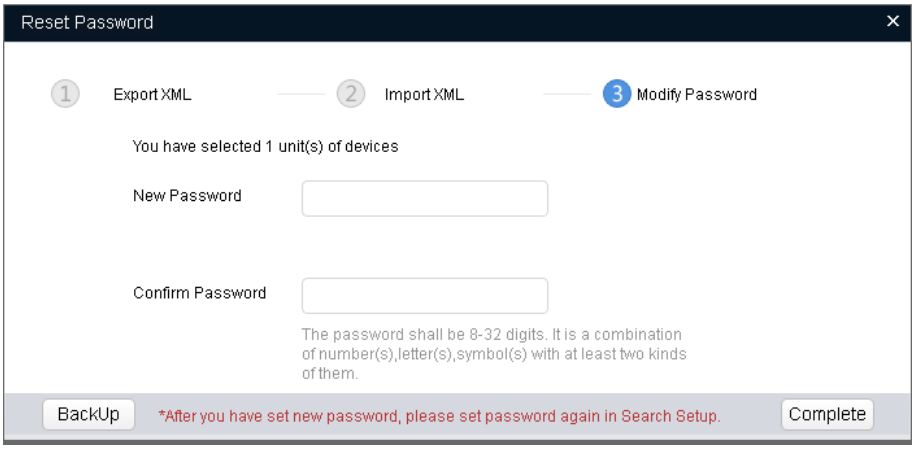
Figure 2-29 Reset password (import XML)



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

After the importing is completed, the **Reset Password-Modify Password** interface is displayed. See Figure 2-30.

Figure 2-30 Reset password (modify password)



Step 8 Modify password.

Enter the new password and confirm password. There are two setting rules for new password dependent on the devices, and follow the instructions on the interface to set 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 ' " ; : &).
- The new password can only be set as four numbers.

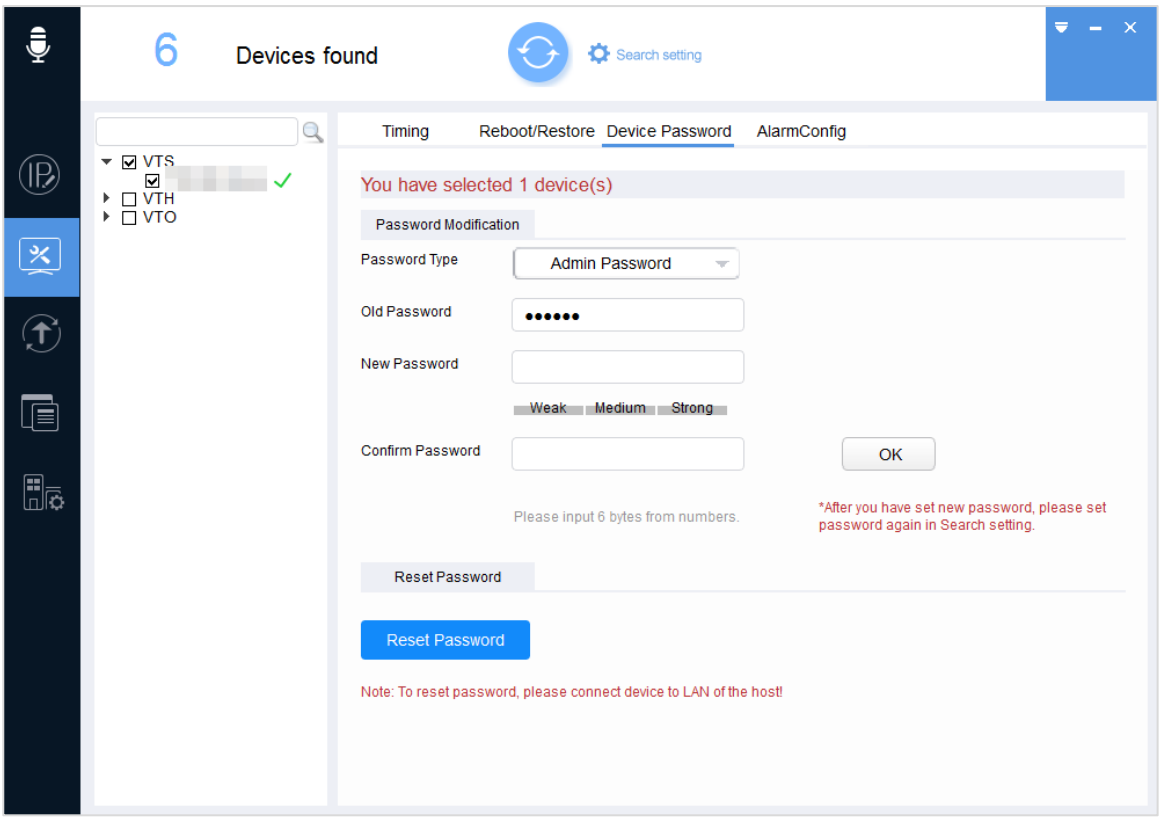
After setting the new password, when you search the devices by **Search setting**, use the new password to login the device.

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

After operation is completed, the result is displayed. See Figure 2-31.

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

Figure 2-31 Password resetting result (XML file)



2.5.4 Configuring Alarm

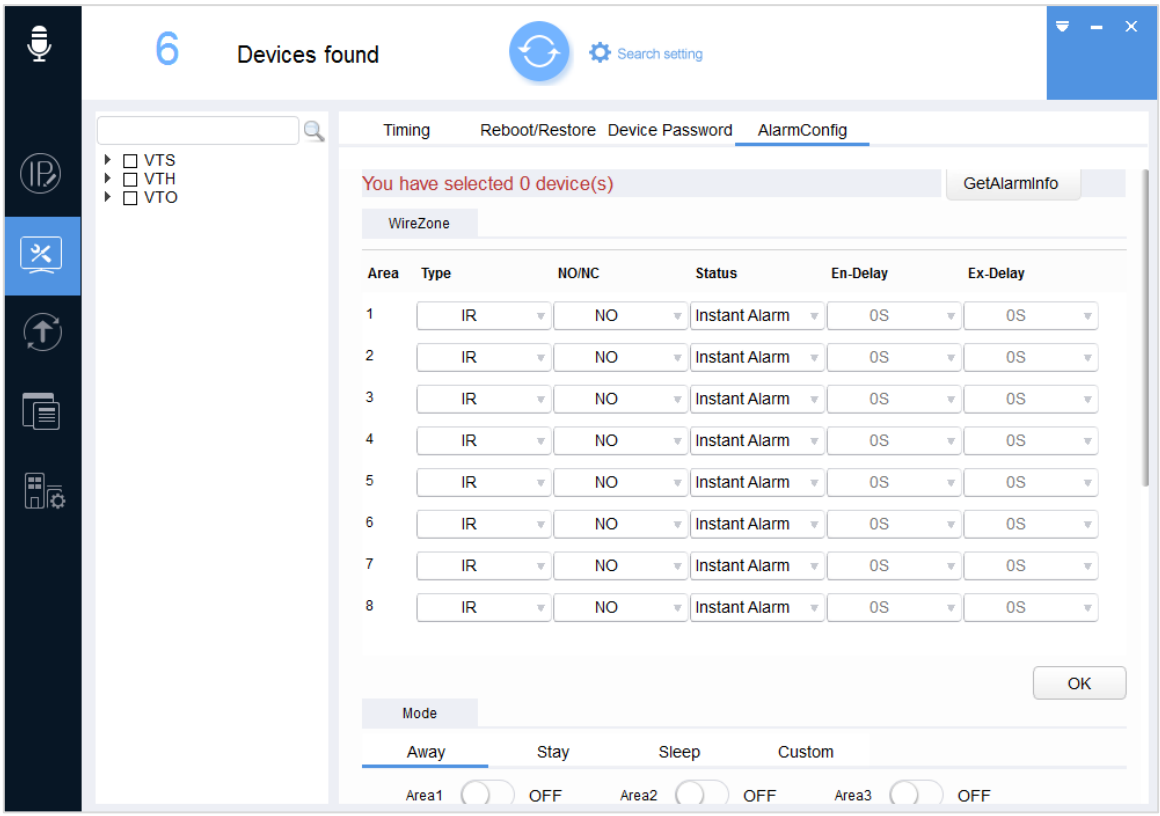
You can set the alarm information of protection area and set the effectiveness of protection area in the alarm mode.

Only VTH supports this function.

Step 1 On the **System Settings** interface, click the **AlarmConfig** tab.

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

Figure 2-32 Alarm configuration



Step 2 Click ▸ next to the device type.

The device list is displayed.

Step 3 Select one device.

- It only supports 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."

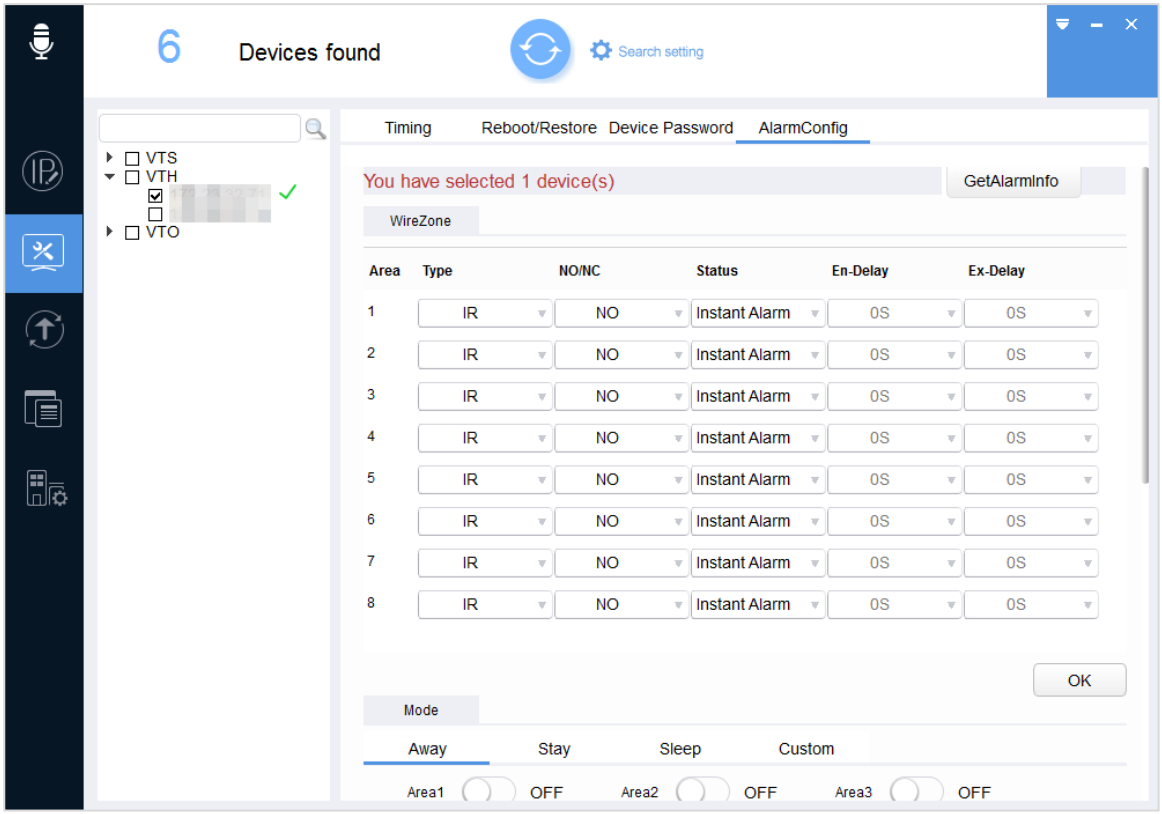
Step 4 Access the alarm information settings.

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 2-33.

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

Figure 2-33 Alarm configuration result



Step 5 Set the alarm information of protection area.

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

Table 2-6 Alarm configuration description

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. 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.

Parameter	Description
En-Delay	Select **Delay Alarm** in the **Status** list. If there is an alarm input, the device triggers the alarm after the seconds configured in the **En-Delay** list.
Ex-Delay	Select **Delay Alarm** in the **Status** list. The protection area will be activated after the seconds configured in the **Ex-Delay** list.

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**.

- 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.

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.

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, 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**.

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 2-32.

Step 2 Click ▸ next to the device type.

The device list is displayed.

Step 3 Select one or multiple device.

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**.

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.

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.

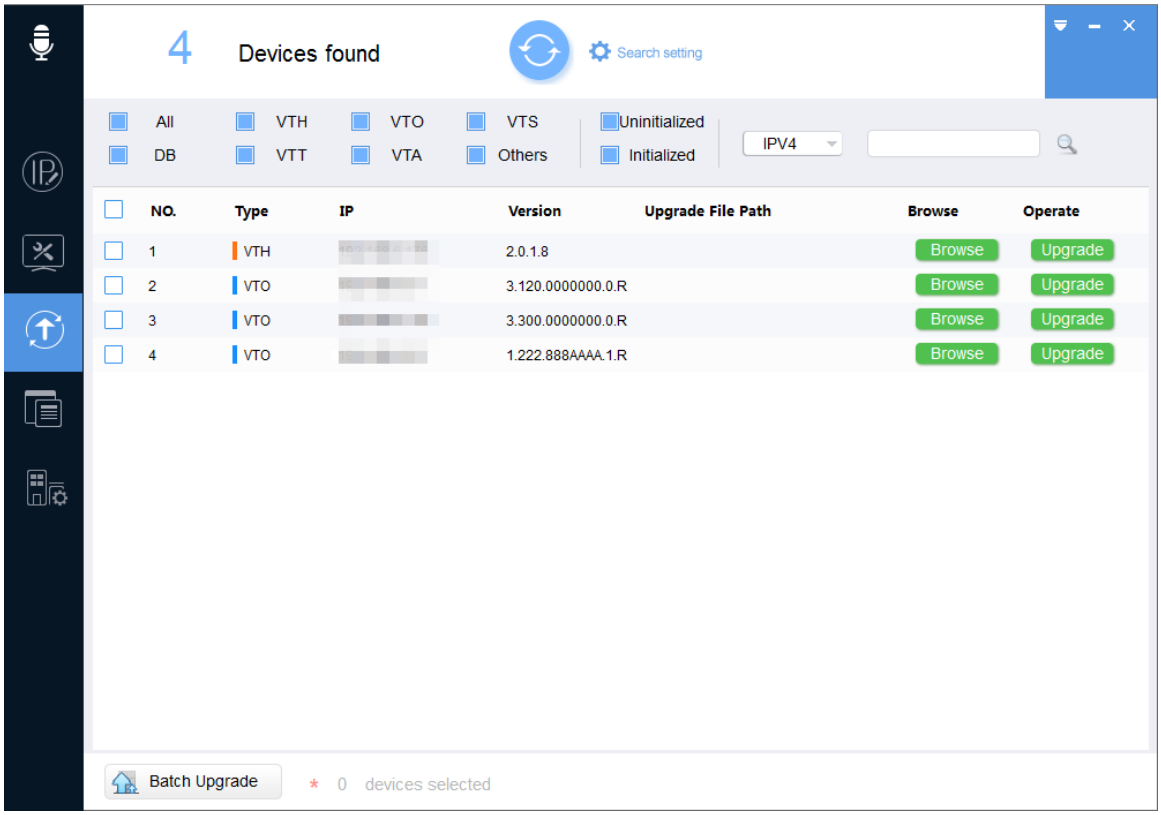
2.6.1 Upgrading One Device

You can choose this procedure for upgrading one device.

Step 1 Click .

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

Figure 2-34 Upgrade



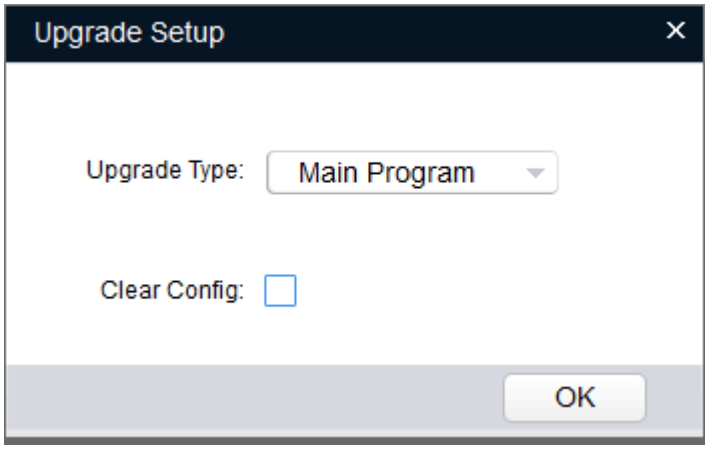
Step 2 Click **Browse** next to the device that you want to upgrade, select the upgrade file and then click **Open**.

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 Upgrade Setup



Step 4 Configure upgrade parameters.

- In the **Upgrade Type** list, select the upgrade type.
- Select the **Clear Config** check box as needed.

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.

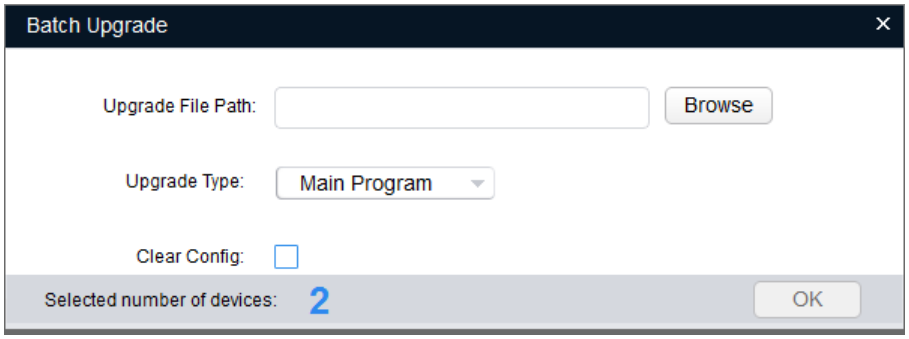
Step 2 Select the devices that need to be upgraded.

- 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 Batch Upgrade.

The **Batch Upgrade** dialog box is displayed. See Figure 2-36.

Figure 2-36 Batch Upgrade



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.

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 Data Backup

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.

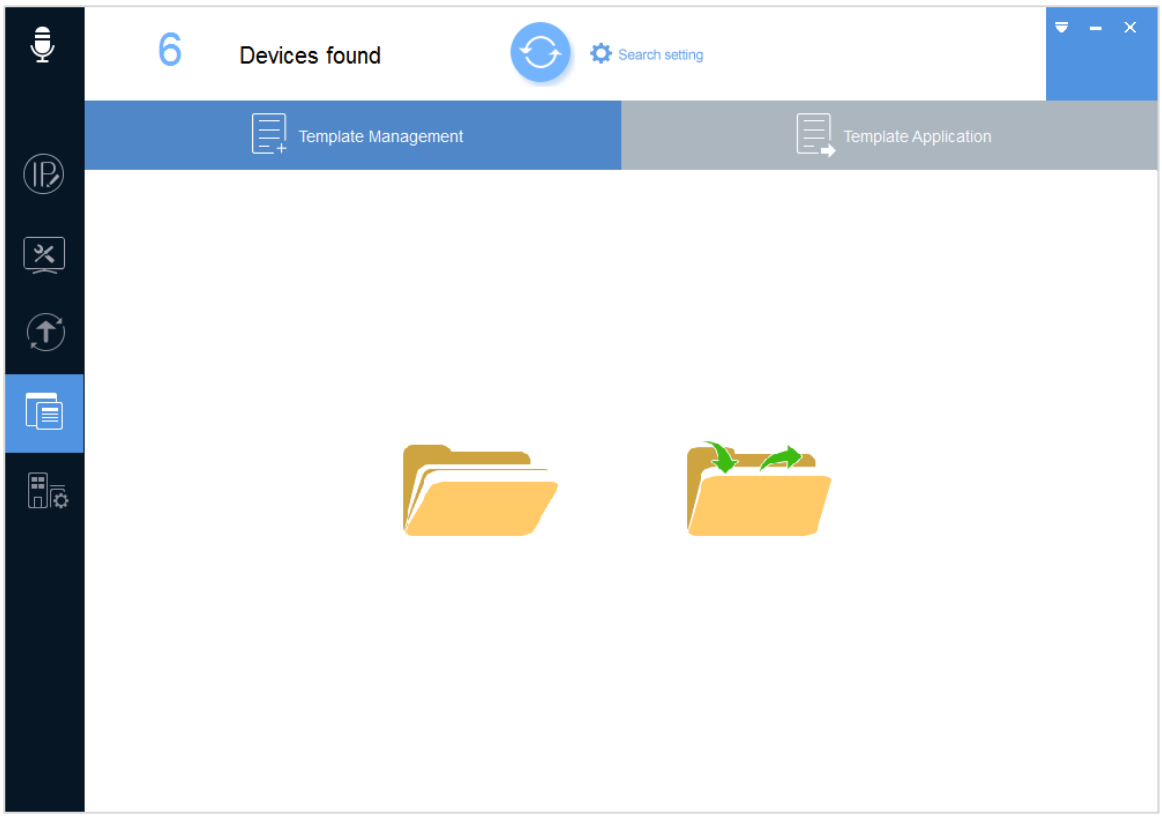
2.7.1 Exporting data

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 2-37.

Figure 2-37 Template setup

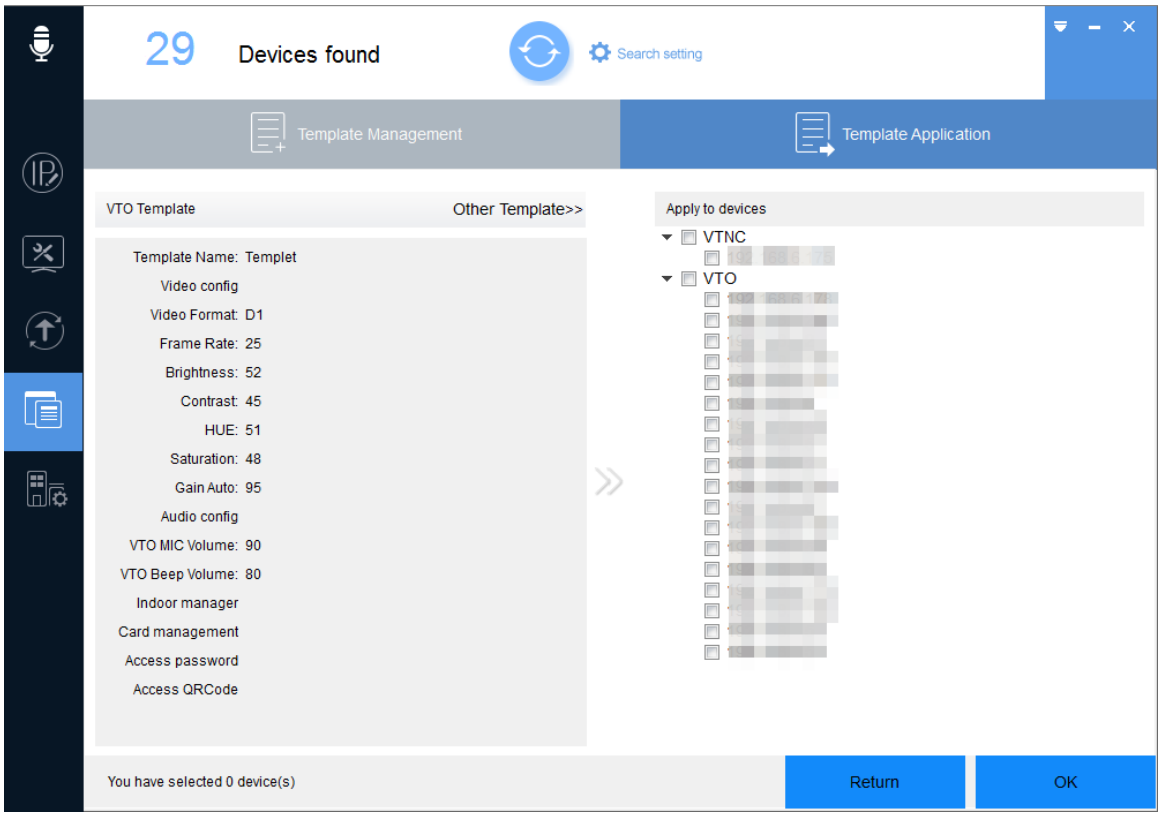


Step 2 Export the template.

1) Click .

The **Template Management** interface is displayed. See Figure 2-38.

Figure 2-38 Template management



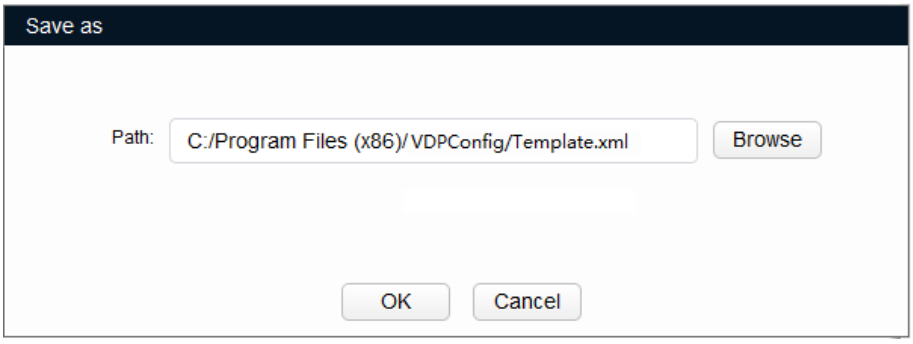
2) Click to select the device, enter the template name, for example, you can enter **Template**, and then set the information you want to export.

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 2-39.

Figure 2-39 Save as



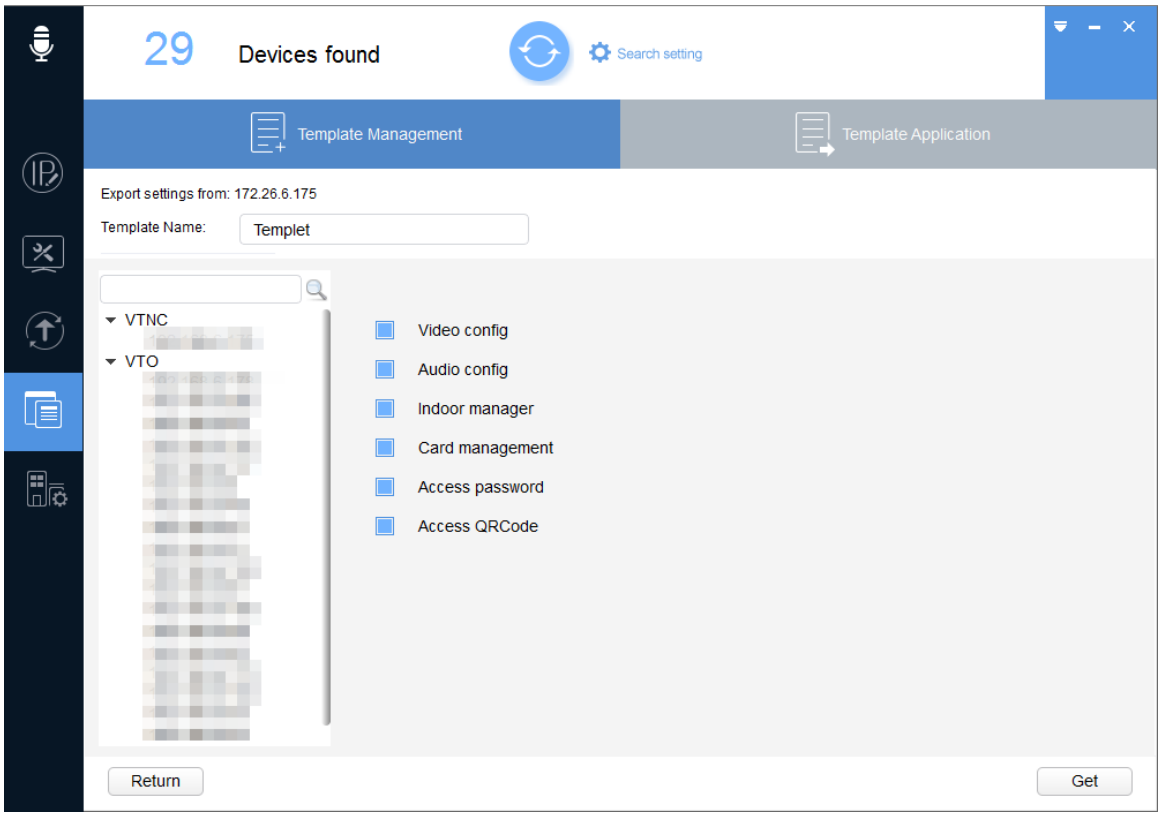
2) Click **Browse** to select the save path for the template.

3) Click **OK** to save the template.

After the exporting is completed, the **Template Application** interface is displayed. See Figure 2-40.

For details about how to apply the template, see "2.7.2 Importing data."

Figure 2-40 Template application (1)



2.7.2 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.

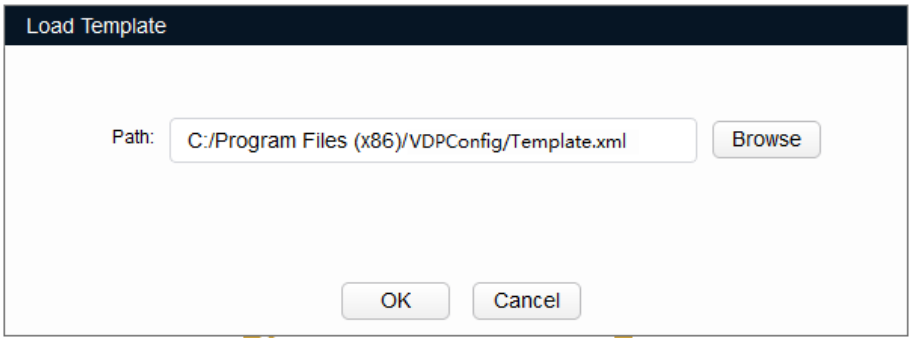
Step 2 Load the template.

1) Click .

The **Load Template** dialog box is displayed. See Figure 2-41.

Make sure the template exists, if not, see "2.7.1 Exporting data."

Figure 2-41 Load template

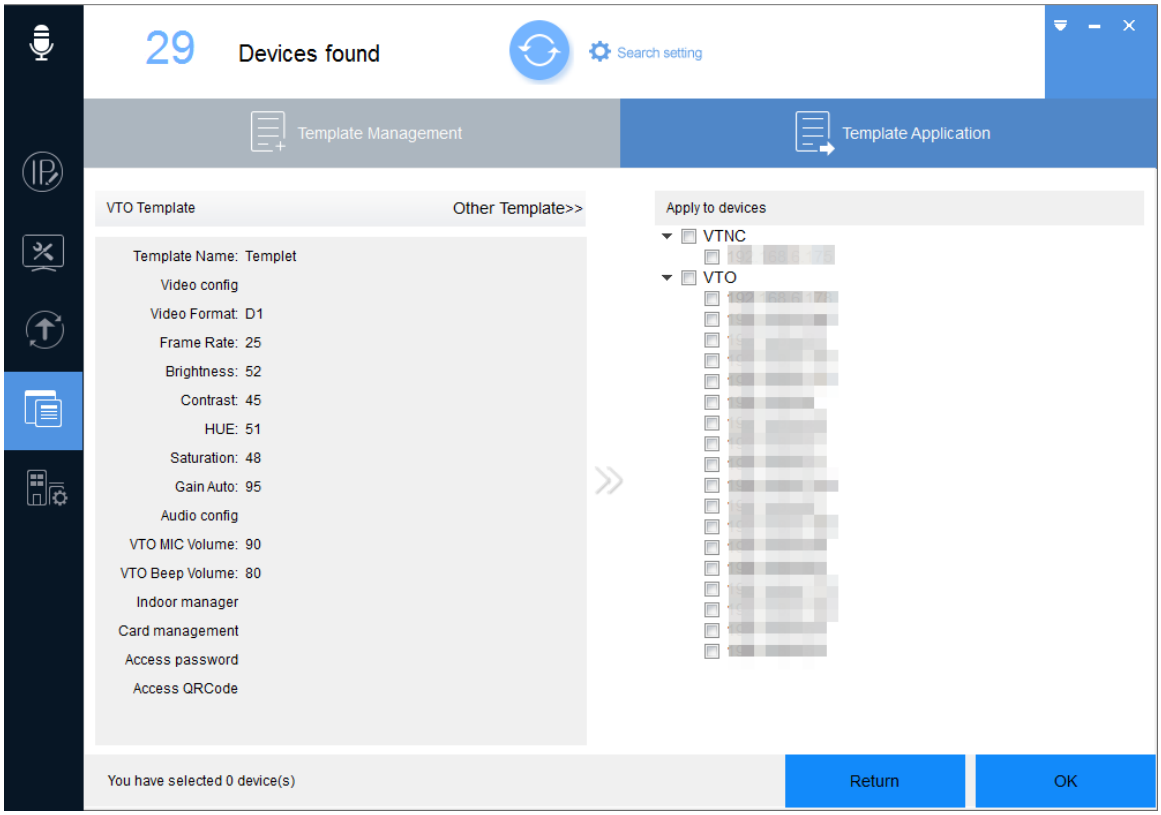


2) Click **Browse** to select the template.

3) Click **OK**.

The **Template Application** interface is displayed. See Figure 2-42.

Figure 2-42 Template application (2)



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

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

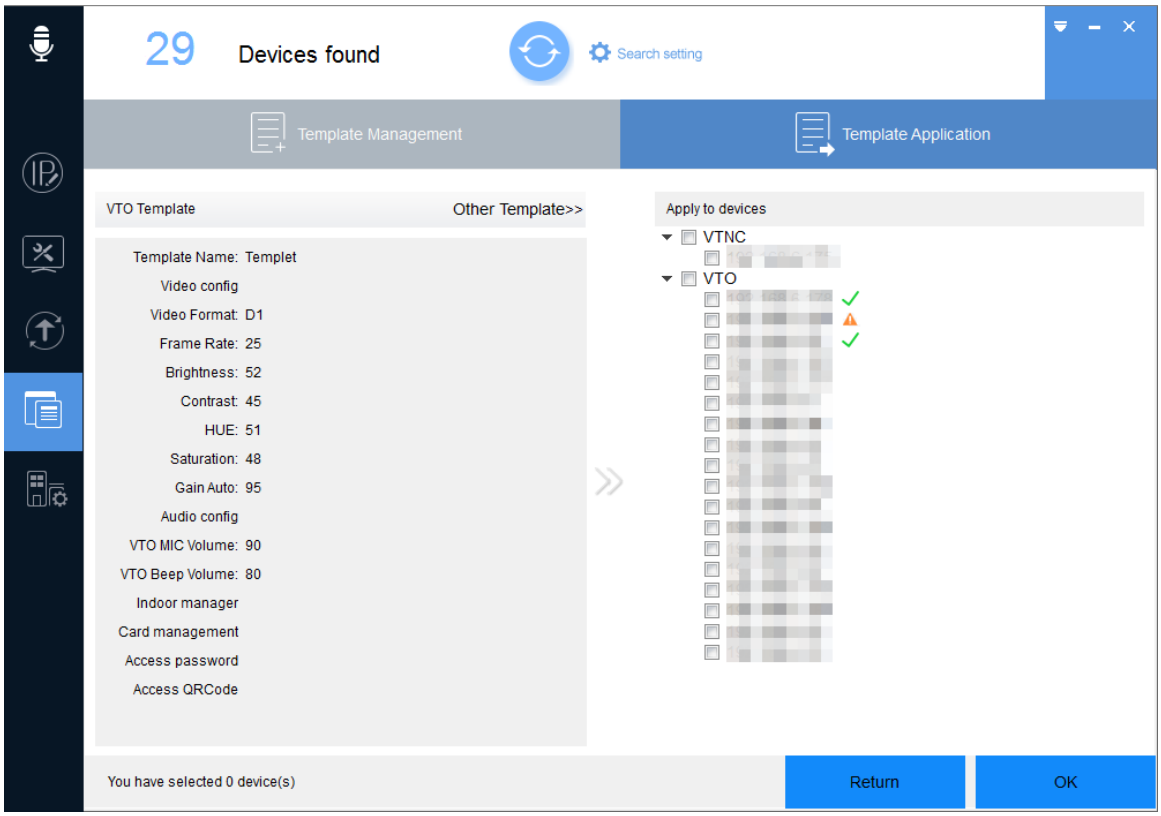
Step 4 Click **OK** to start applying the template.

After applying is completed, the result is displayed. See Figure 2-43.

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

- 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 2-43 Template application result



2.8 Project Configuration

Click  to enter the project configuration interface.

2.8.1 Batch Configuring

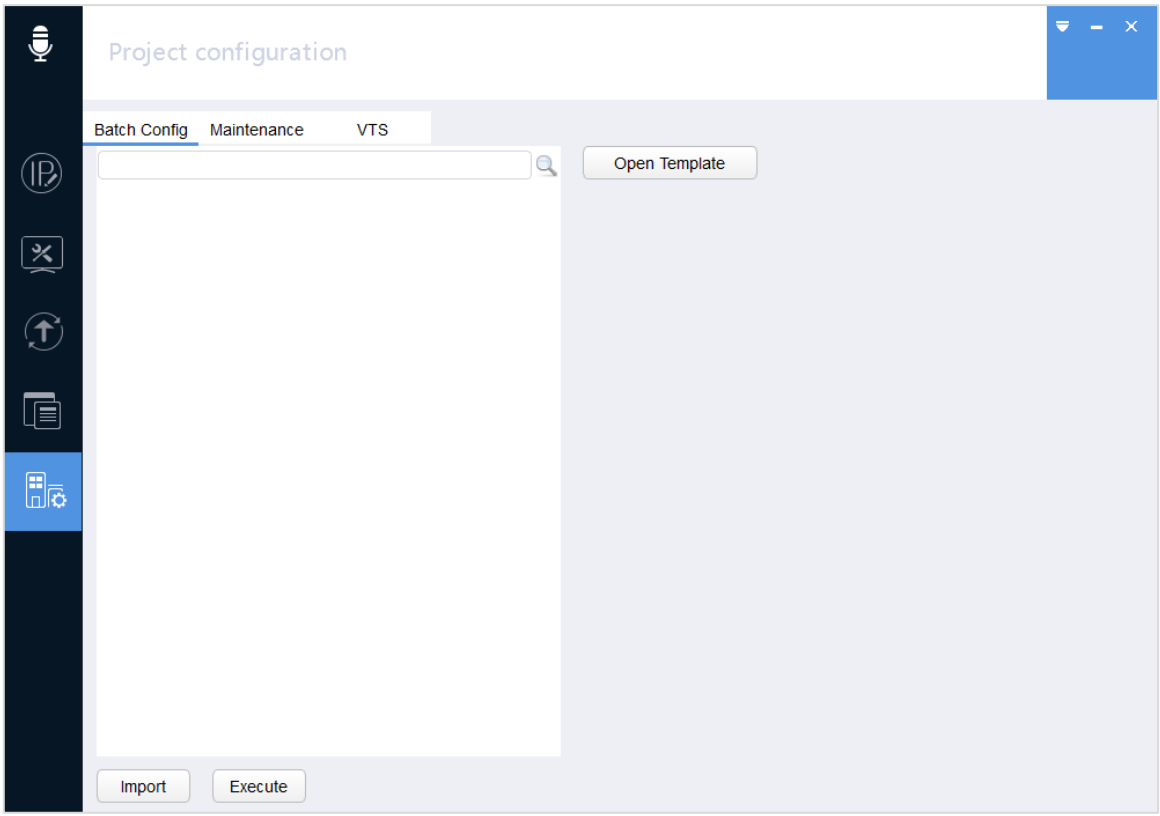
You can import and configure SIP system device.

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 2-44.

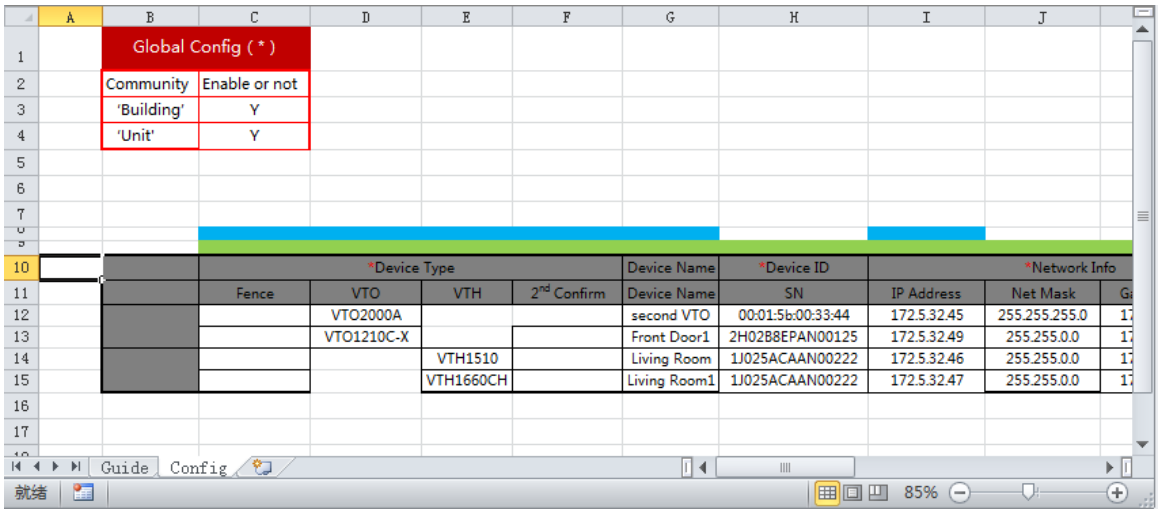
Figure 2-44 Batch Config (1)



Step 2 Click **Open Template**.

The "ProjectTemplate-New-SIP.xlsx" template is displayed. See Figure 2-45. The default sheet is **Config**.

Figure 2-45 Template



Step 3 Modify the template as needed. Click **File**, and then click **Save as**.

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.

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

Step 6 Click **Import**.

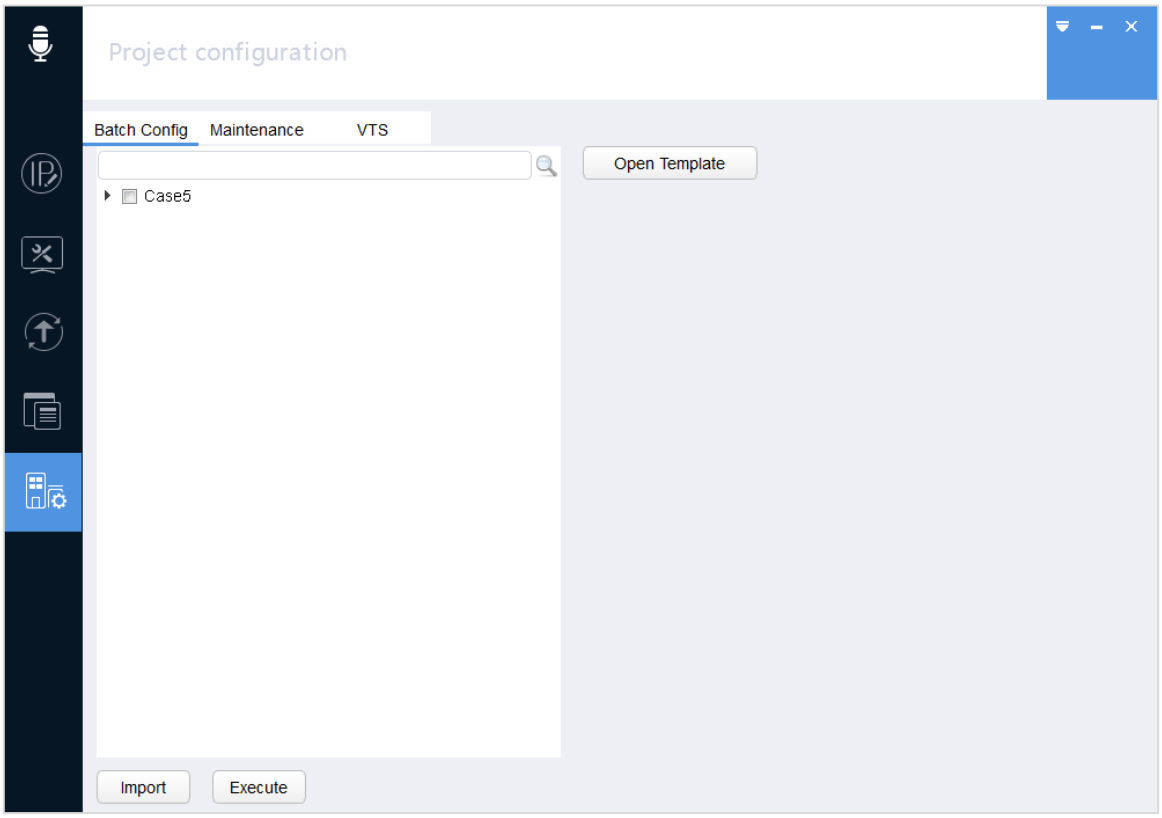
The **Open** dialog box is displayed.

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

After the importing, the **Notice** dialog box is displayed. Click **OK** and it goes back to the Batch Config interface. See Figure 2-46.

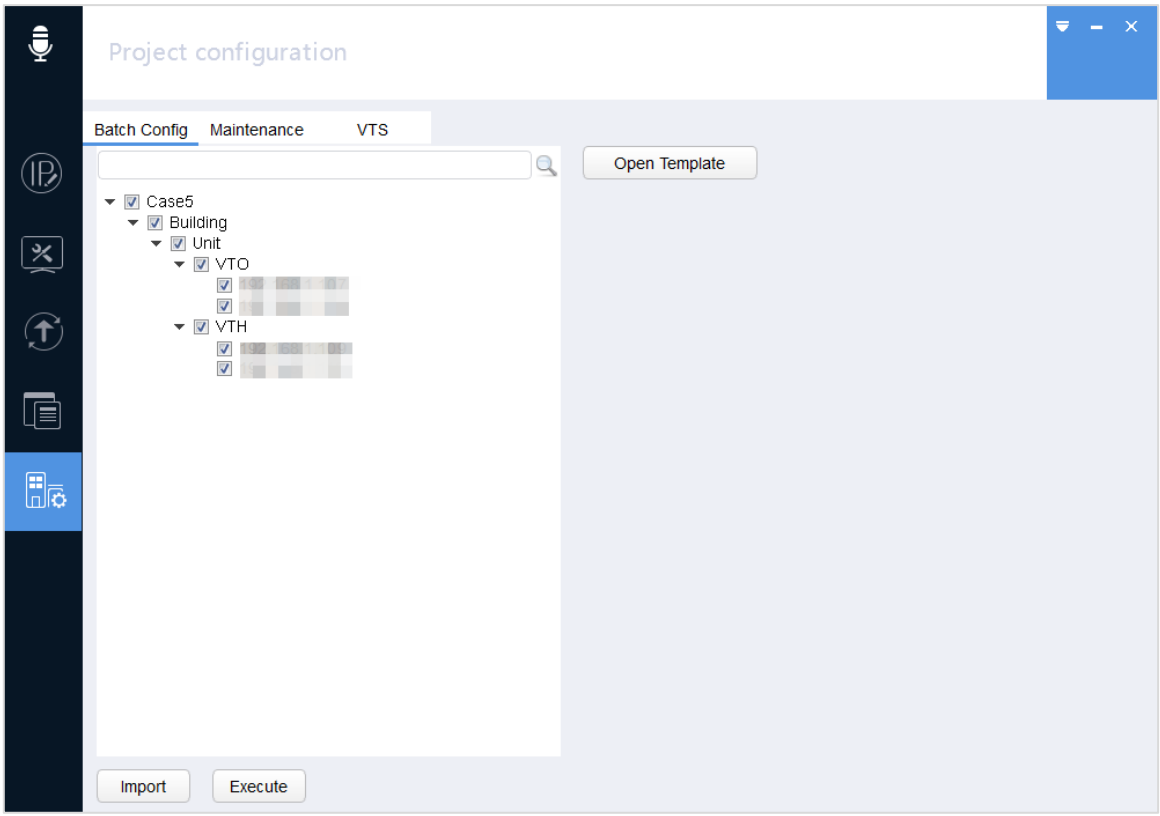
If you import two templates of different names successively, which contain device with the same SN, the latest imported template shall govern.

Figure 2-46 Batch Config (2)



Step 8 Select device. See Figure 2-47.

Figure 2-47 Selecting device

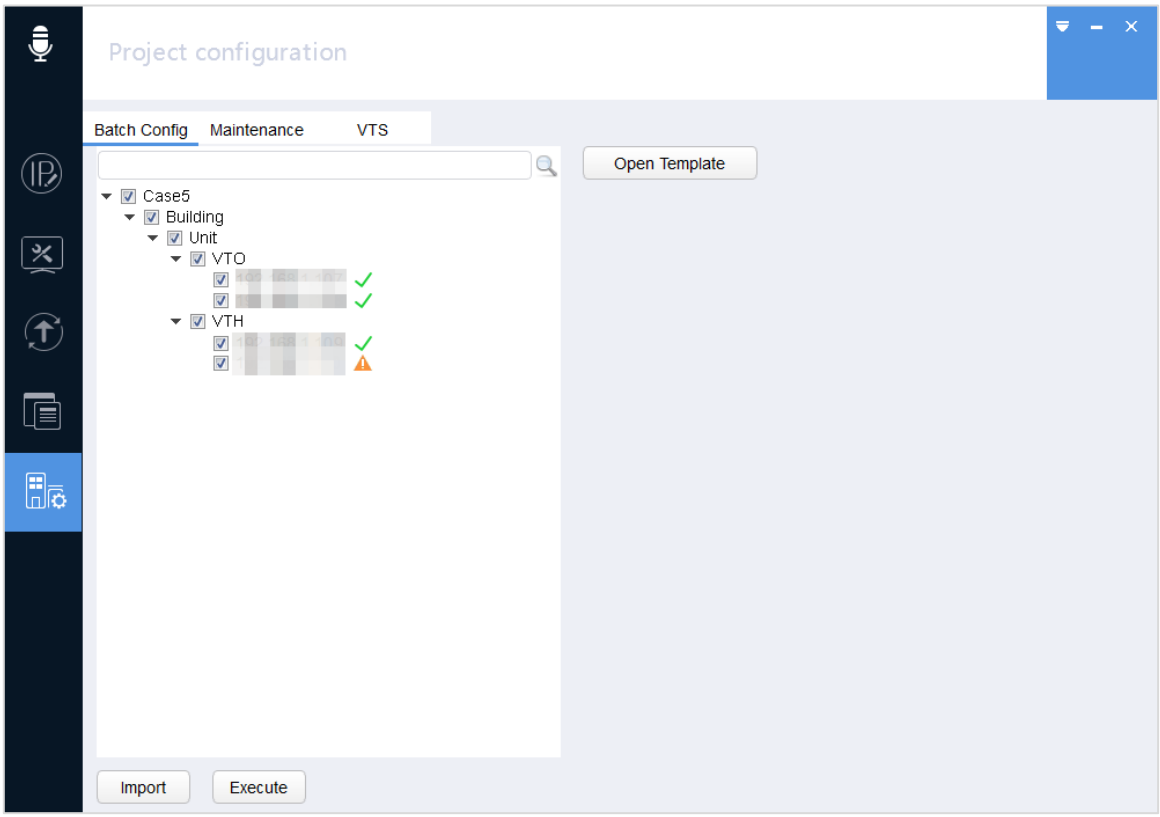


Step 9 Click **Execute**.

After the operation is completed, the result is displayed. See Figure 2-48.

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

Figure 2-48 Execute result



After the operation is completed, you can configure the device. For details, see "2.8.2 Maintenance."

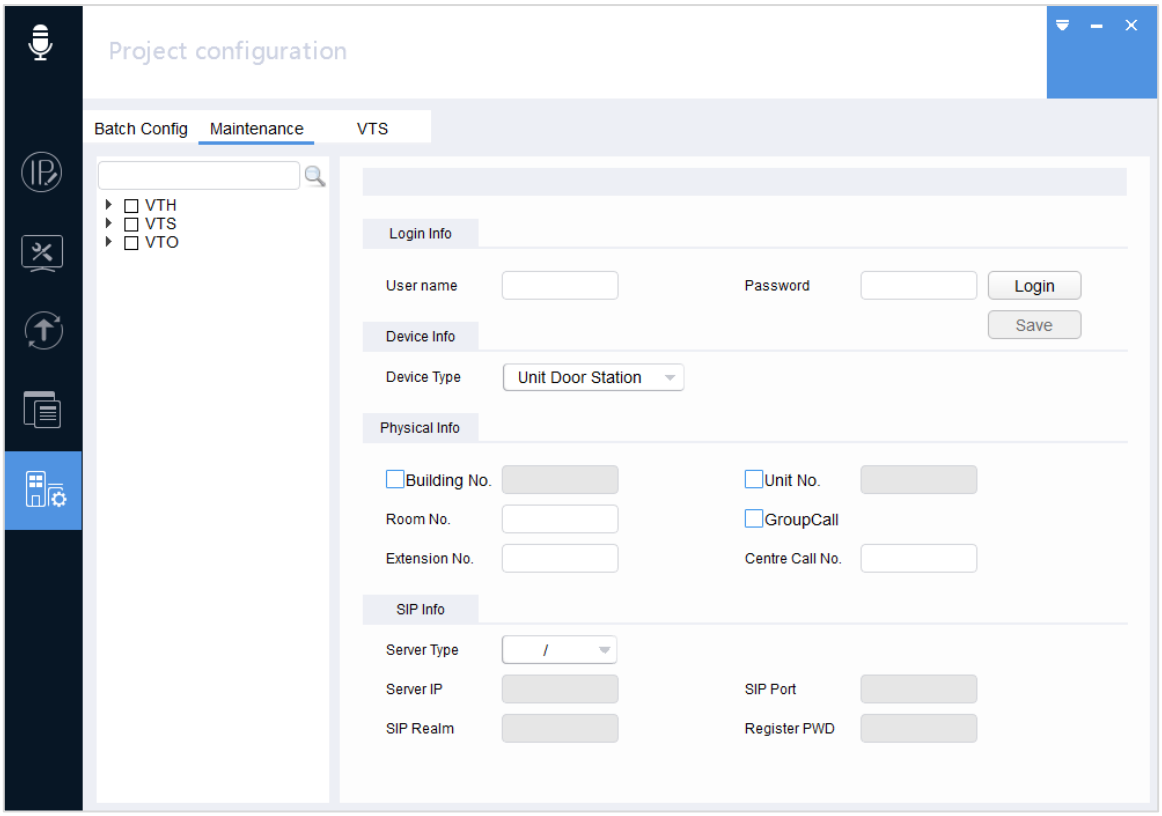
2.8.2 Maintenance

You can configure VTO and VTH on the interface. VTS is not supported.

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

The **Maintenance** interface is displayed. See Figure 2-49.

Figure 2-49 Maintenance



Step 2 Click ▸ next to the device type.

The device list is displayed.

Step 3 Select one device

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, and then click **Login**. See Figure 2-50 for VTH device and see Figure 2-51 for VTO device.

Figure 2-50 VTH

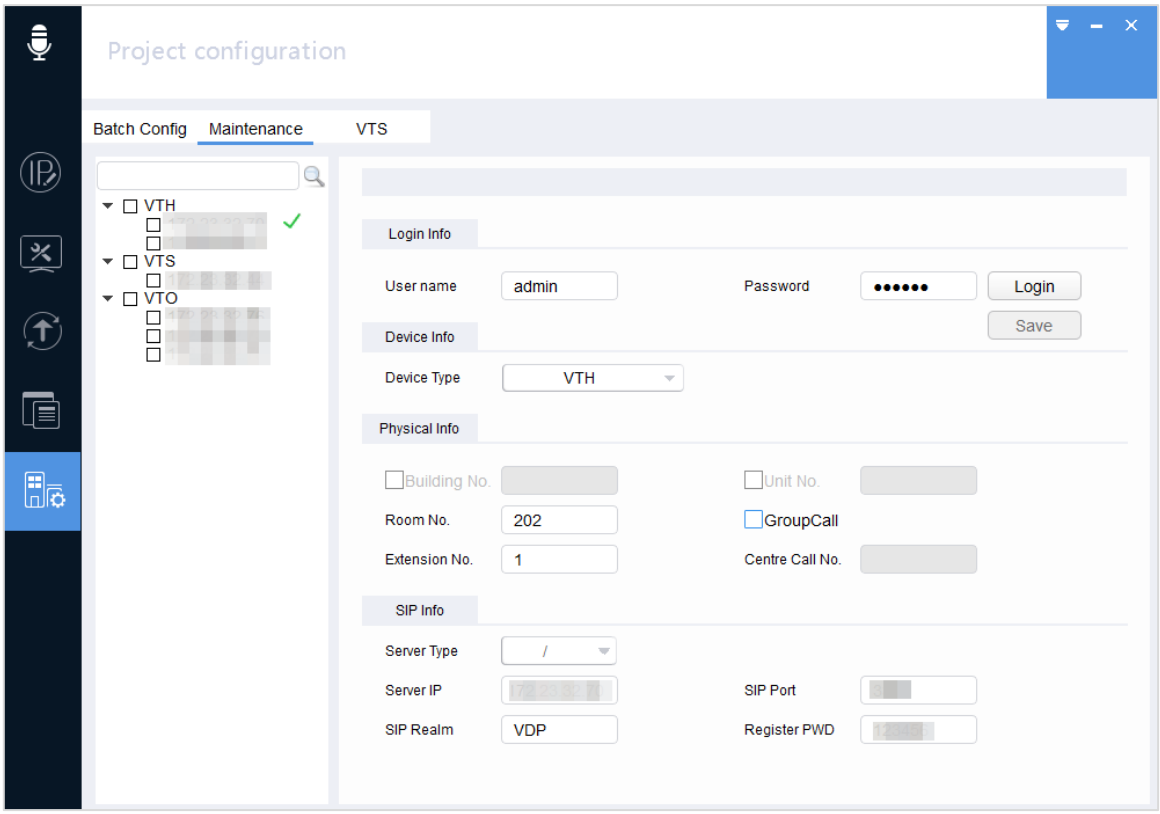
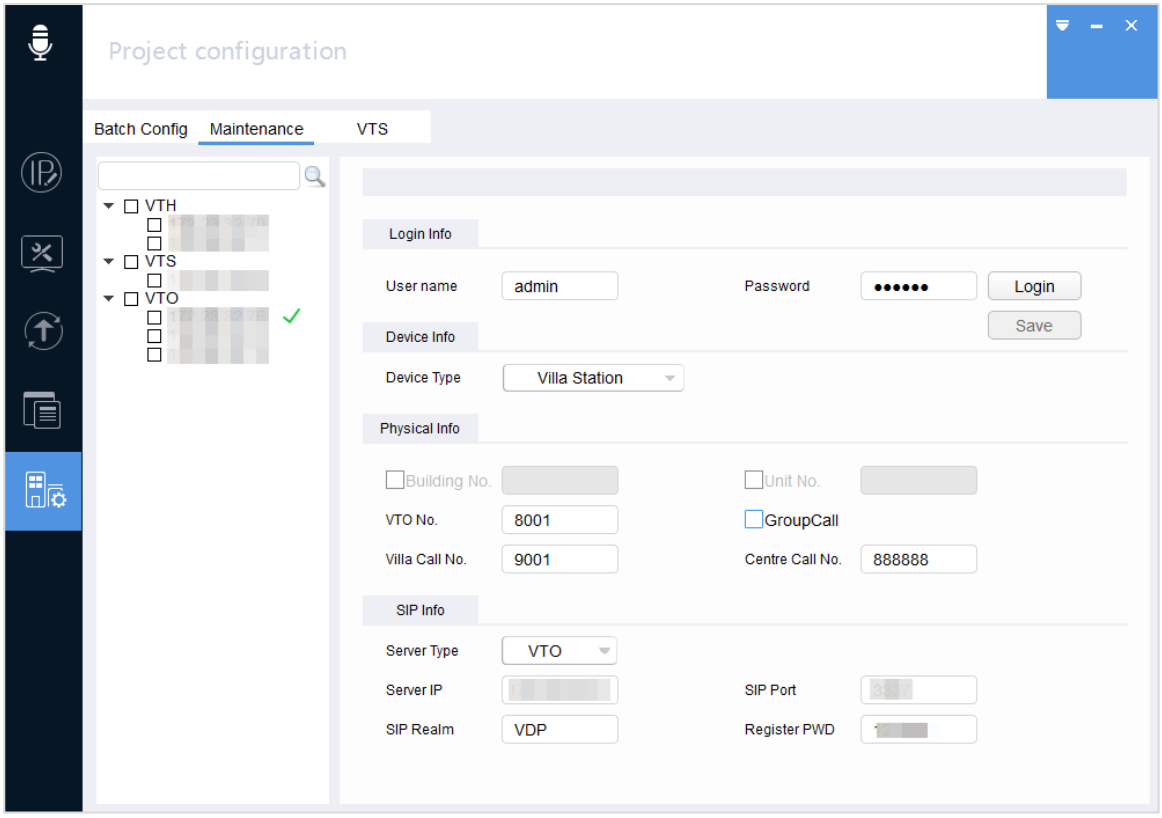


Figure 2-51 VTO



Step 5 Configure the settings. See Table 2-7.

Table 2-7 Maintenance parameters

Parameter		Description
VTH	Room No.	Enter the room number.

Parameter		Description
	Extension No.	Enter the extension number.
	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.

Step 6 Click **Save**.

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

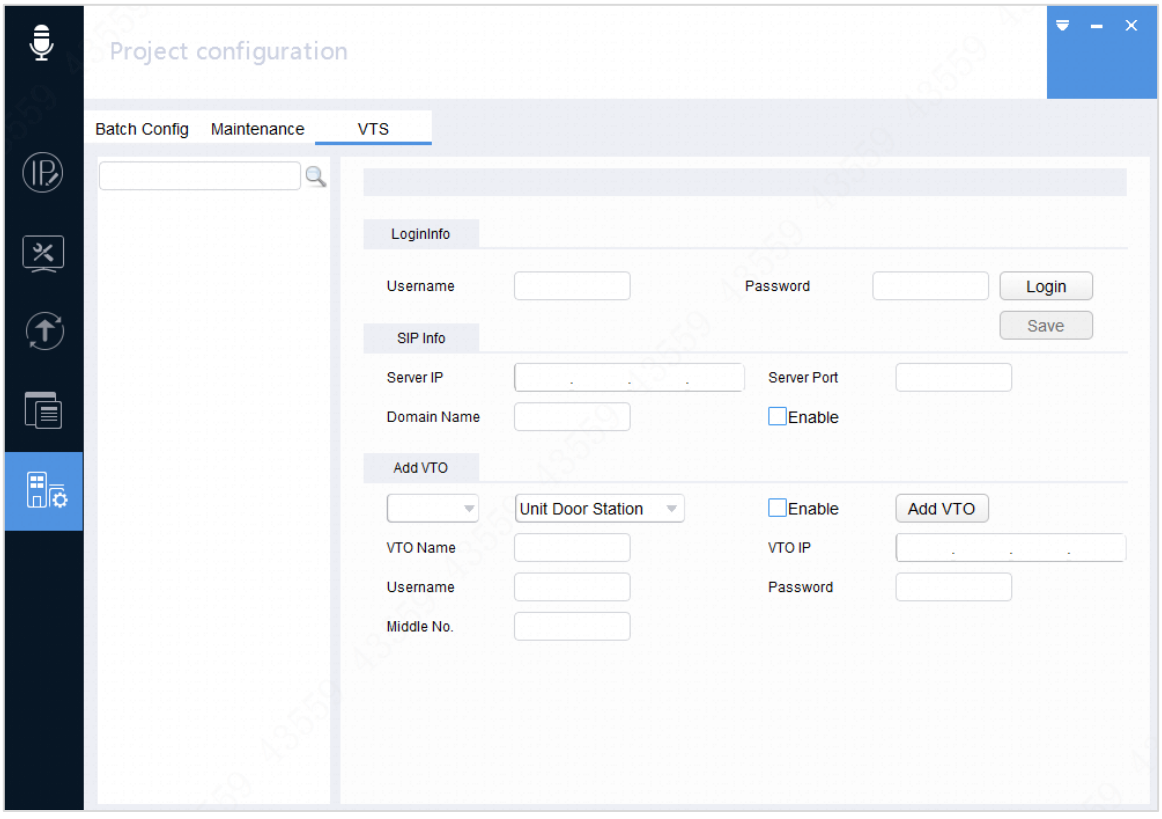
2.8.3 VTS

You can configure VTS.

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

The **VTS** interface is displayed. See Figure 2-49.

Figure 2-52 VTS (1)



Step 2 Click ▸ next to the device type.

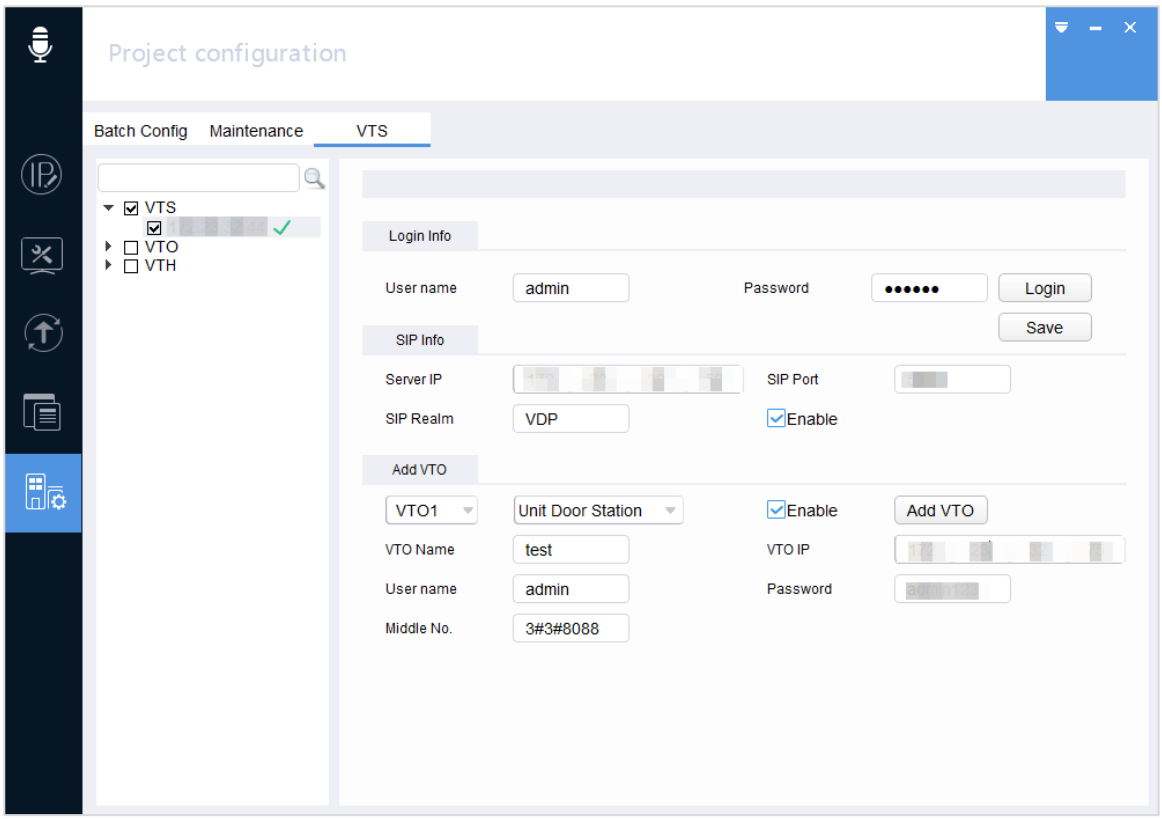
The device list is displayed.

Step 3 Select one device.

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, and then click **Login**. See Figure 2-53.

Figure 2-53 VTS (2)



Step 5 Configure SIP server. For details, see Table 2-7.

Table 2-8 SIP server parameters

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.
Enable	Select the check box to enable the server.

Step 6 Click **Add VTO** to add VTO. Select the VTO and VTO type from the corresponding drop-down list. For details, see Table 2-9.

Table 2-9 Adding VTO

Parameter	Description
VTO Name	Enter the name of VTO.
VTO IP	Enter the IP address of VTO.
User name	Enter the web login username.

Parameter	Description
Password	Enter the web login password.
Middle No.	Enter the number in the following format: Building number # Unit number # VTO number
Enable	Select the check box to enable the server.

Step 7 Click **Save**.

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

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.