VDPConfig (Windows Version)

User's Manual

V1.2.4

Foreword

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

Revision History

Version	Revision Content	Release Time
V1.2.4	1. Update "Initializing Devices". 2. Add notice of "Local Upgrade." 3. Add "Single Ponit."	March 2020
V1.2.3	1. Add VTS function in "Project Configutation." 2. Update the operations of "Initializing Devices."	September 2019
V1.2.2	1. Move the content of "configuring device" to the Project Configuration as "Maintaince". 2. Modify the SIP template. 3. Delete the VT system function of the Project Configuration.	September 2018
V1.2.1	1. Add "Privacy Protection Notice". 2. Update "About the Manual".	May 2018
V1.2.0	1. Add "Project Configuration". 2. Add "Configuring Alarm" and "Configuring Arm/Disarm Settings".	January 2018
V1.1.0	1. Add "Cybersecurity Recommendations" and "Online Upgrade". 2. Update "The Main Interface".	October 2017

Version	Revision Content	Release Time
V1.0.2	1. Update "Basic Operations". 2. Add "Initializing Devices".	May 2017
V1.0.1	Update the structure of the Basic Operations chapter.	December 2016
V1.0.0	First release.	February 2016

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 jurisdictions. For detailed information, refer to 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, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and 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 occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

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

You can use the Tool to configure and maintain 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 locally.
- Quickly configure VTO, VTH and IPC under the same unit and configure corresponding matching relationship.

1.2 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

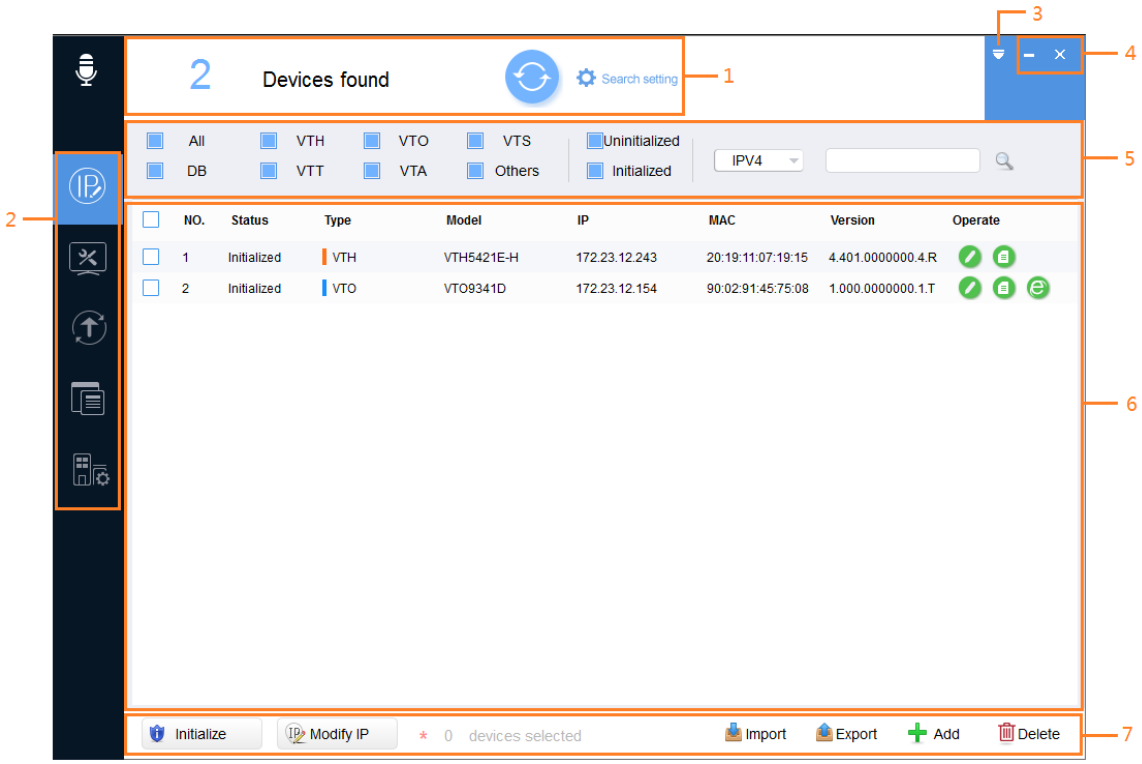
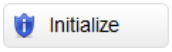
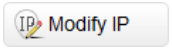
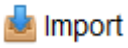
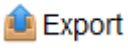
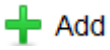


Table 1-1 Main interface parameters

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**, **System Settings**, **Upgrade**, **Template Setup** and **Project Configuration**. • : Modify IP for one device or multiple devices. • : Set device system time, reboot device, restore device, modify password, reset password and alarm configuration. • : Upgrade local devices individually or in batches. • : Manage and apply the template. The template includes the information such as encoding and video configuration information. • : 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 button	You can do the following operations. • Initialize device: Select one or more devices and click  to initialize the select devices. • Modify IP addresses in batches: Select devices and click  to modify the IP address of the select devices. • Import device: Click  to import one or multiple devices through template. • Export device: Select one or more devices and click  to export the device details. • Add device: Click  to add one or more devices manually. • Delete device from the list: Select one or more devices and click  to delete the selected devices.

2 Basic Operations

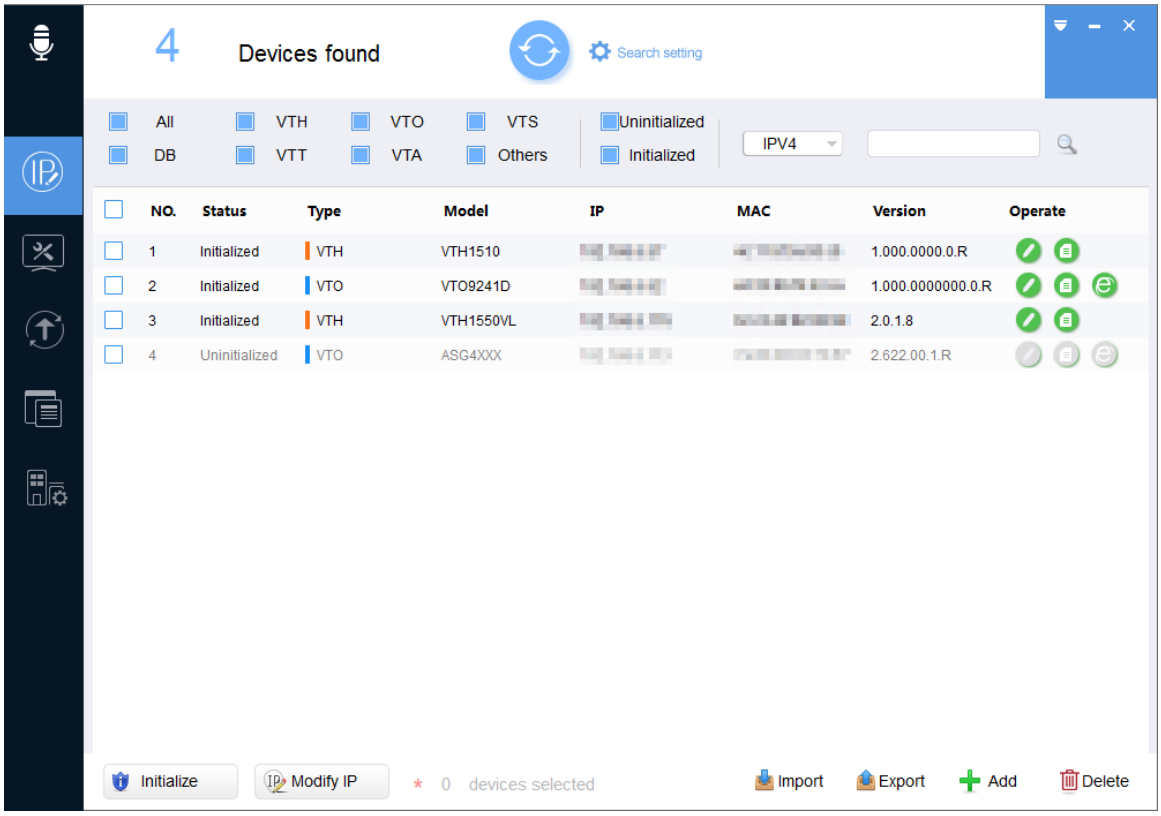
2.1 Searching Devices

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.

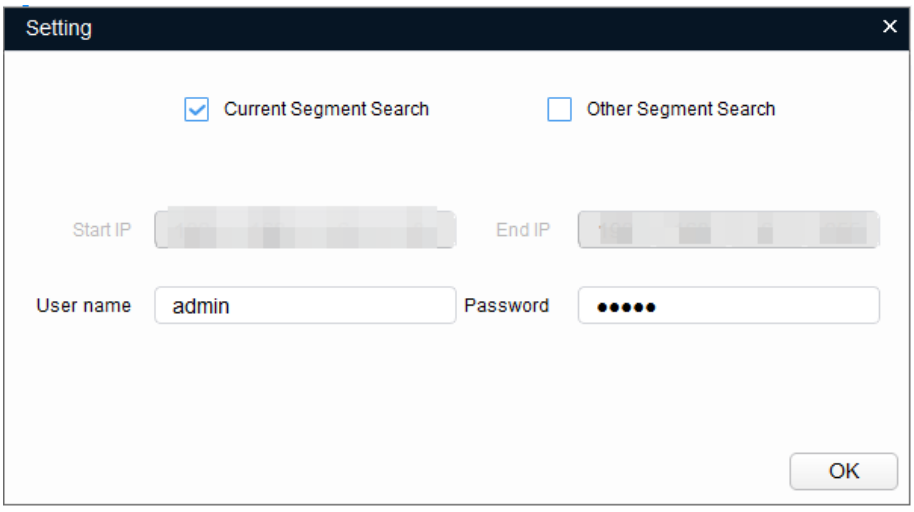
Step 1 Click .

Figure 2-1 Modify IP



Step 2 Click Search setting.

Figure 2-2 Setting



Step 3 Select the searching way.

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

- If you select both the **Current Segment Search** check box and the **Other Segment Search** check box, the system searches devices under the both conditions.
- The username and the password are the ones used to log in to 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 connected between the device and the PC which is 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  .

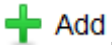
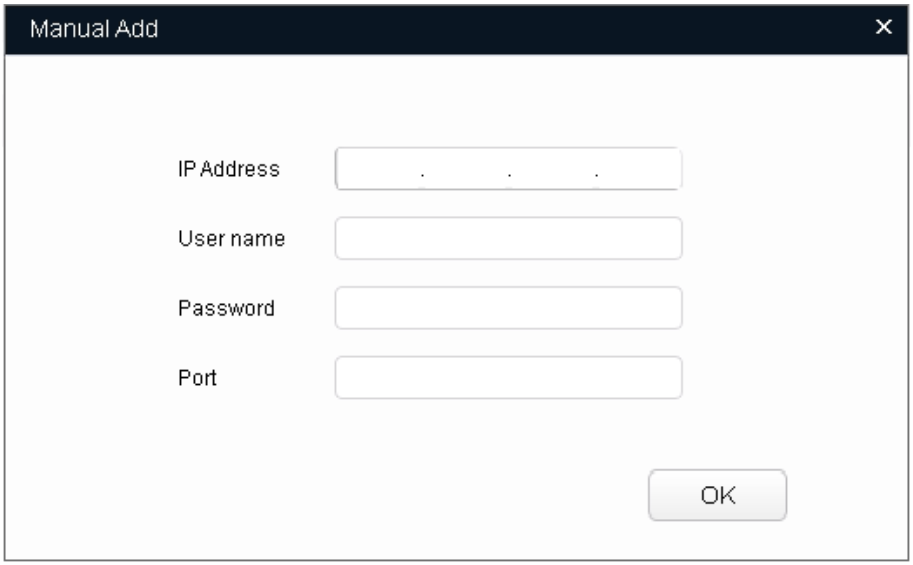
Step 2 Click  .

Figure 2-3 Manual add



Step 3 Set the device parameters.

Table 2-1 Manual add parameters

Parameter	Description
IP Address	The IP address of the device.
User name	The username 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 searching devices or importing the template.

- Add devices through searching if you know the network segment where the device is located. For details, see "2.1 Searching Devices" and "2.2.2.1 Adding by Searching."
- If you have the template data of the device, add the devices through importing the template. For details, see "2.2.2.2 Adding by Template."

2.2.2.1 Adding by Searching

You can add multiple devices through searching the current segment or other segment. For details, see "2.1 Searching Devices."

2.2.2.2 Adding by Template

You can add multiple devices through importing the template.

Make sure that your PC is installed with Microsoft Excel.

2.2.2.2.1 Accessing to the Template

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

Step 1 Click .

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

Step 3 Select the save path, enter the file name in the **File name** box, and then click **Save**.
The system starts exporting the device details. After the exporting is completed, a success notice is displayed.

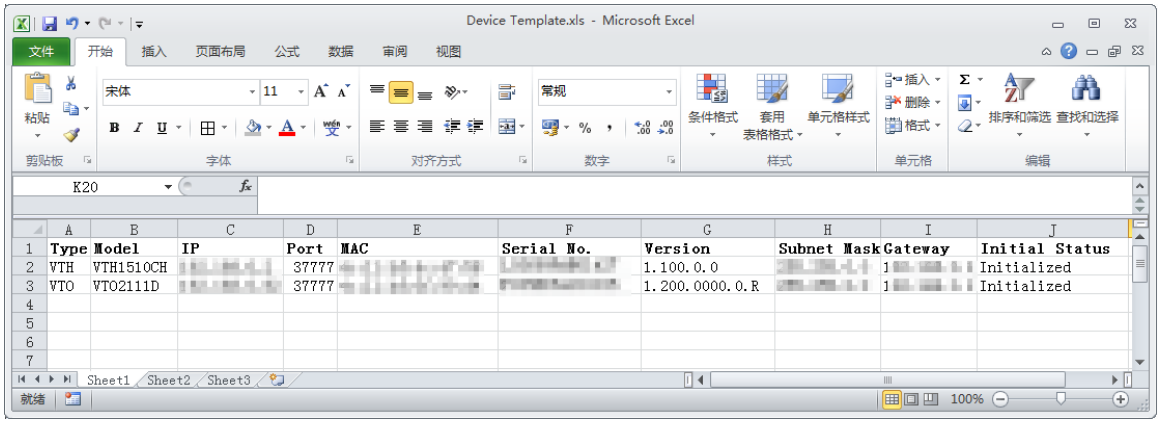
Step 4 Click **OK** to complete exporting.
You can check the exported device details in the save path.

2.2.2.2.2 Filling in the Template

Step 1 Find the template in the save path, and then open it.

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

Figure 2-4 Device template



Step 2 Enter the device parameters.

Table 2-2 Device template parameters

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

Step 3 Save and close the template.

2.2.2.2.3 Importing Devices

You can import the filled template to add device.

⚠

Close the template file before importing.

Step 1 Click .

Step 2 Click Import.

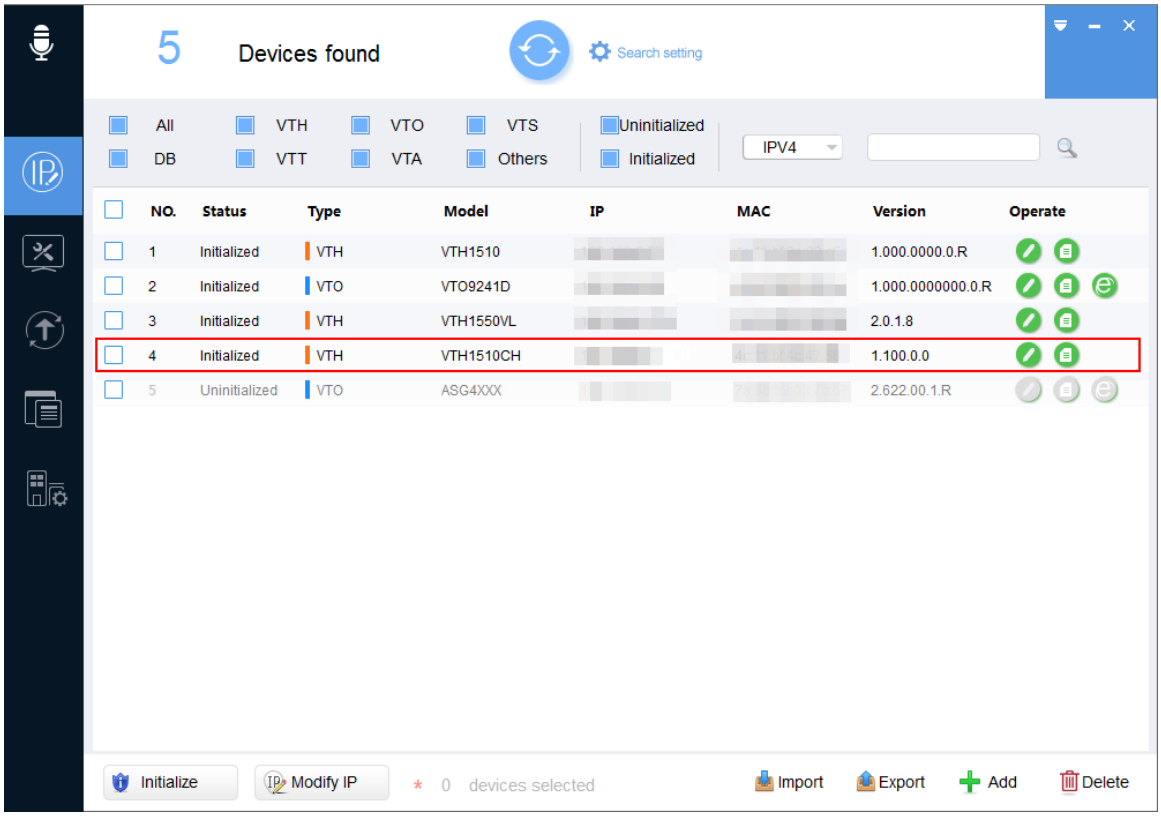
Step 3 Select the template, and then click **Open**.

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

Step 4 Click **OK**.

The newly imported devices appear in the device list.

Figure 2-5 Imported devices



2.3 Initializing Devices

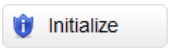
You can initialize one or multiple devices.

📖

- This function is available on select models.
- Only devices within the same local area network can be initialized at the same time.
- 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.

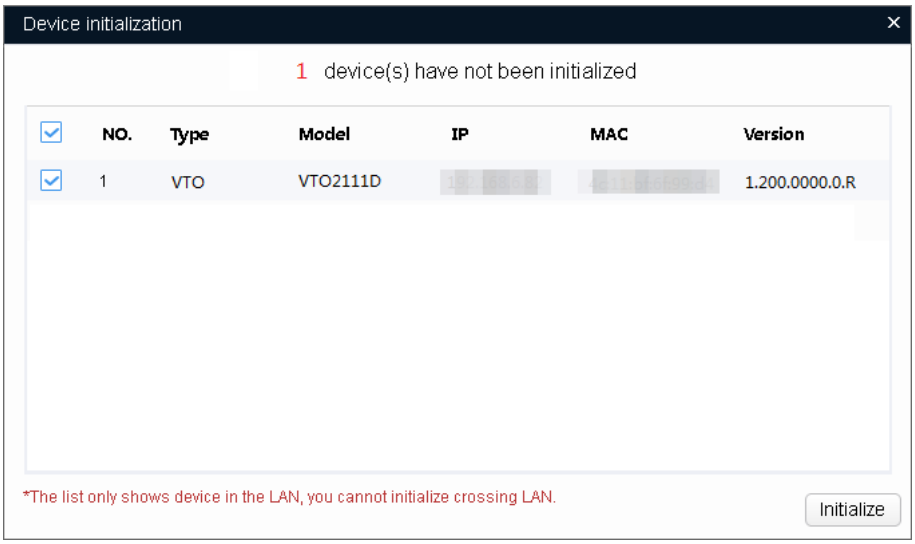
Step 1 Click  .

Step 2 Select an uninitialized device.

Step 3 Click 

.

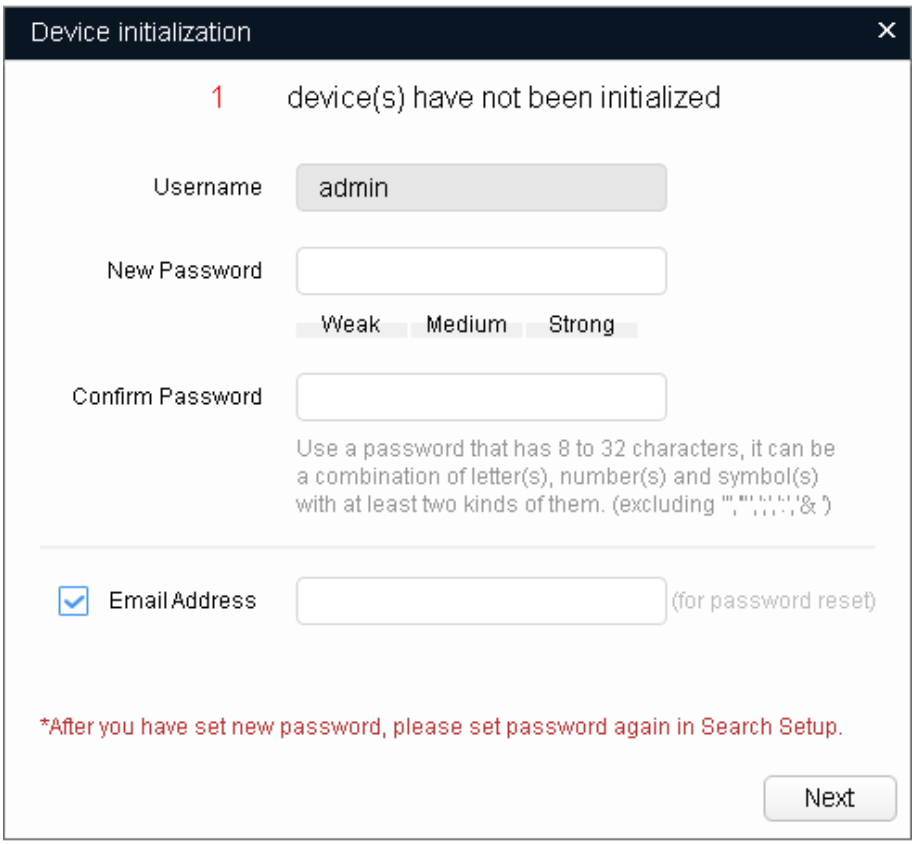
Figure 2-6 Device initialization (1)



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

- 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 2-7 Device initialization (2)



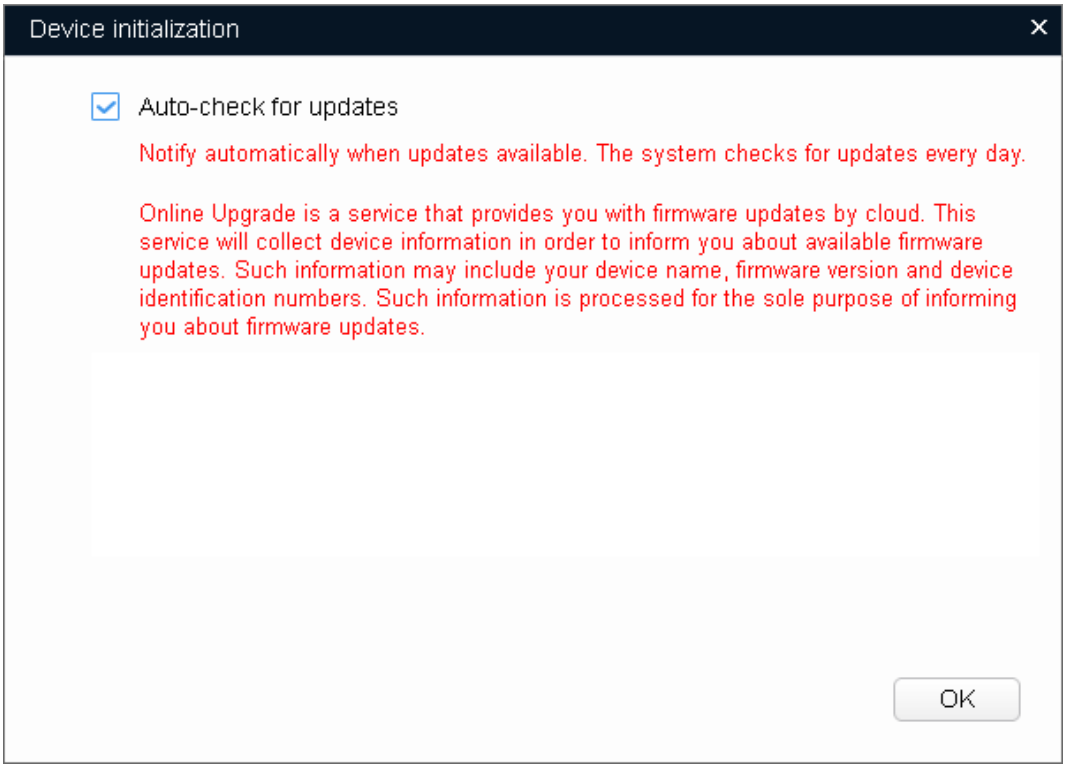
Step 5 Set the initialization parameters for the device.

Table 2-3 Initialization parameters

Parameter	Description
User name	The username is **admin** by default.
New Password	Enter the new password. There is an indication for the strength of the new password. The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &). There are two setting rules for new password dependent on the devices. Follow the instructions on the interface to set the new password. After setting the new password, set the password again 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**.

Figure 2-8 Device initialization (3)

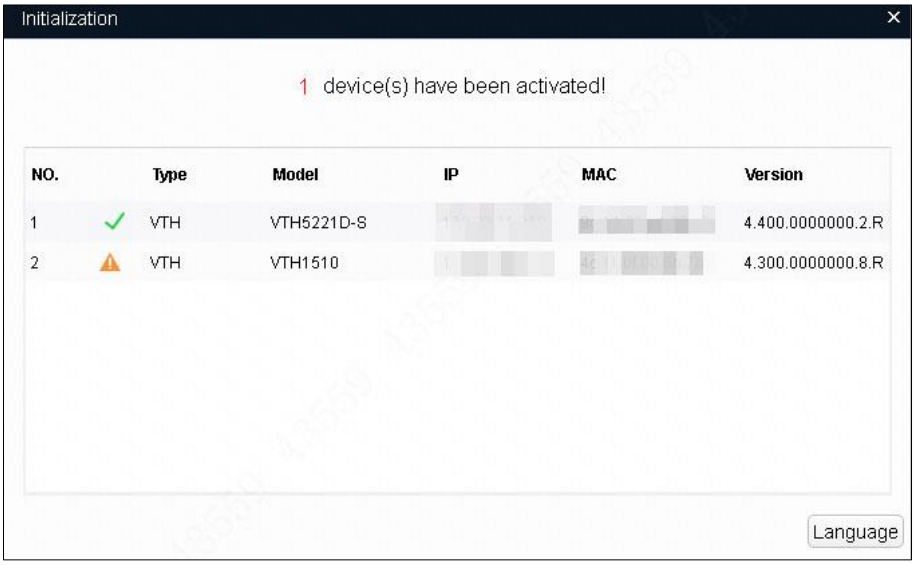


Step 7 Select the **Auto-check for updates** check box.

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

After initialization, you can click the success icon ( ) or click the failure icon ( ) for the details.

Figure 2-9 Initializing devices

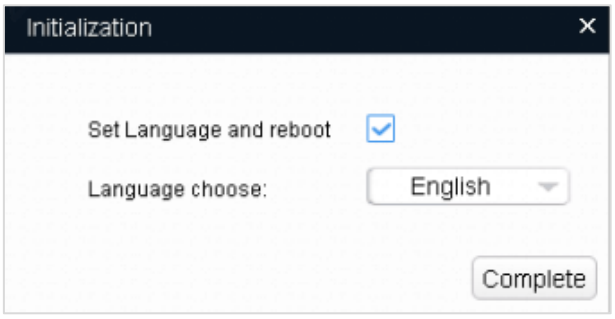


Step 9 Set language for the initialized device.

- Only some device models support setting language when initializing; otherwise, devices might fail to initialize.
- Ensure and select the supported languages of devices; otherwise, devices might fail to initialize.
- It is recommended to initialize the same model devices at one time.

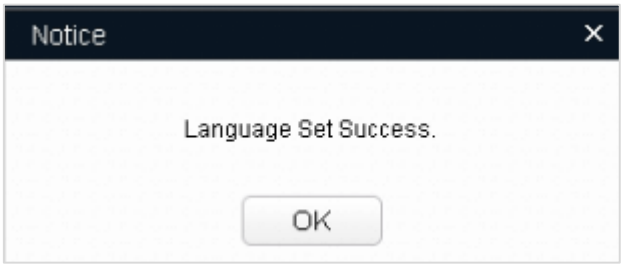
1) Click **Language**.
2) Select the needed language from the **Language choose** list.

Figure 2-10 Language selection



3) Click **Complete**. The **Notice** interface is displayed.

Figure 2-11 Notice



4) Click **OK** to complete the initialization.
After initialization, 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.

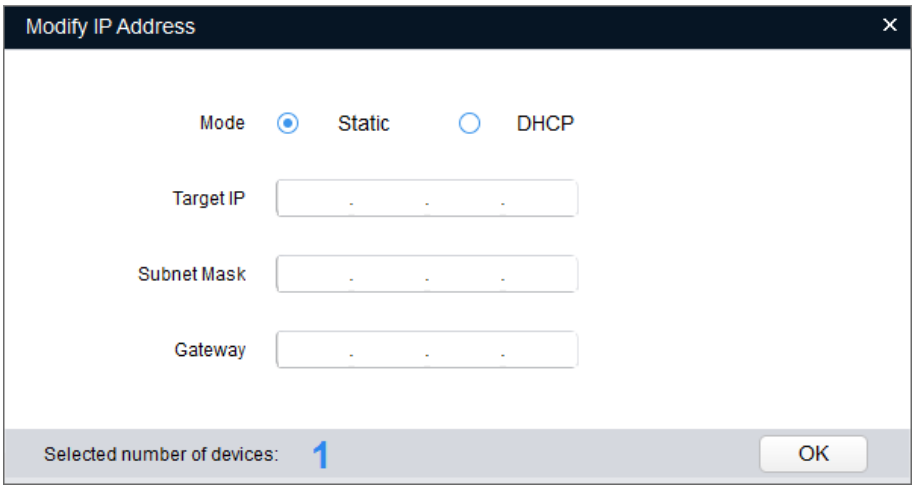
2.4.1 Modifying One IP

Step 1 Click .

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

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 2-12 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 manually 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** to complete modification.

2.4.2 Modifying IP in Batches

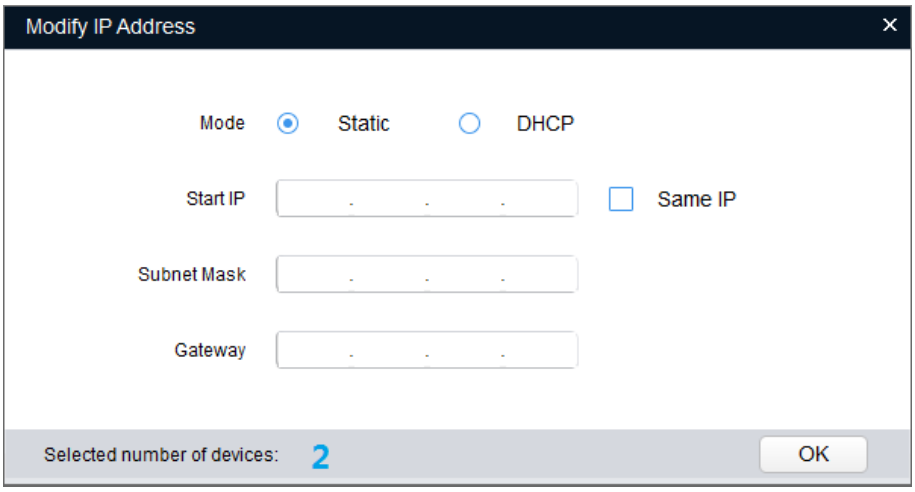
Step 1 Click .

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 Modify IP.

Figure 2-13 Modify IP address (2)



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

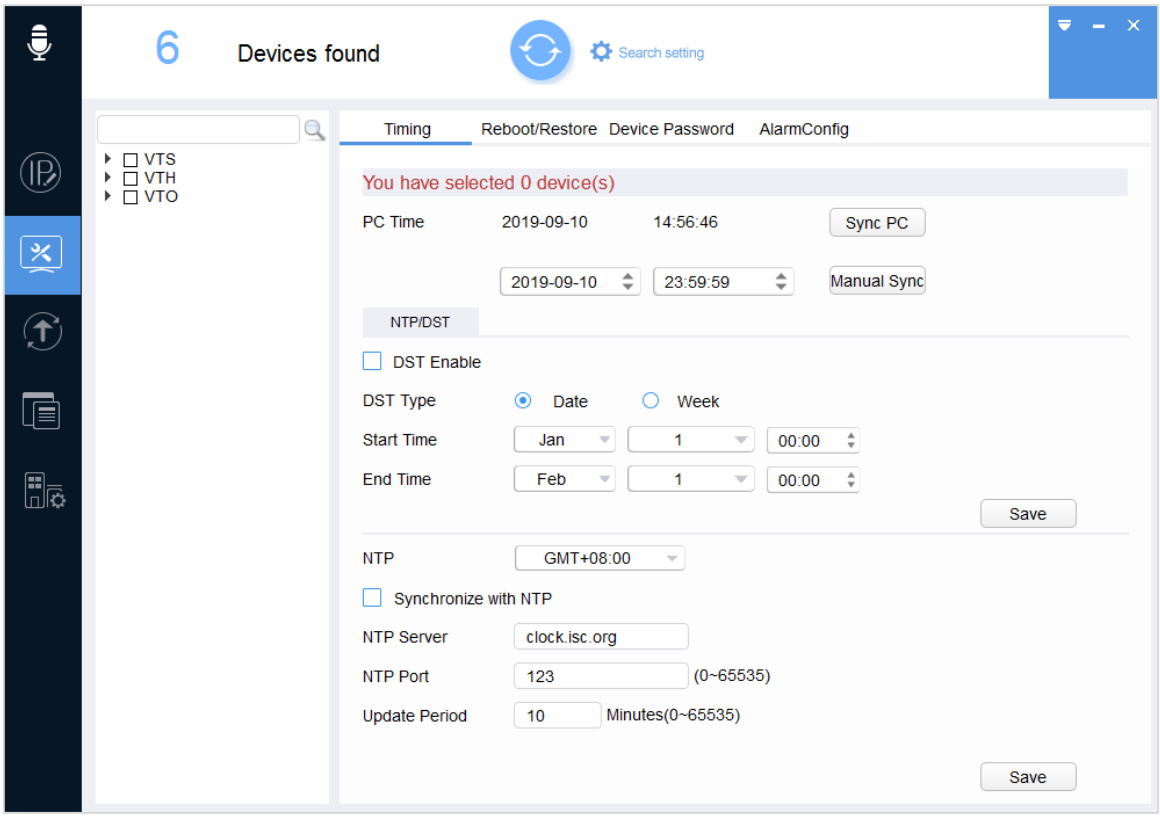
You can configure the settings for system time, reboot, restore, password modification and password resetting.

2.5.1 Timing

You can calibrate the device time through configuration.

Step 1 Click and click **Time** tab.

Figure 2-14 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. 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. 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

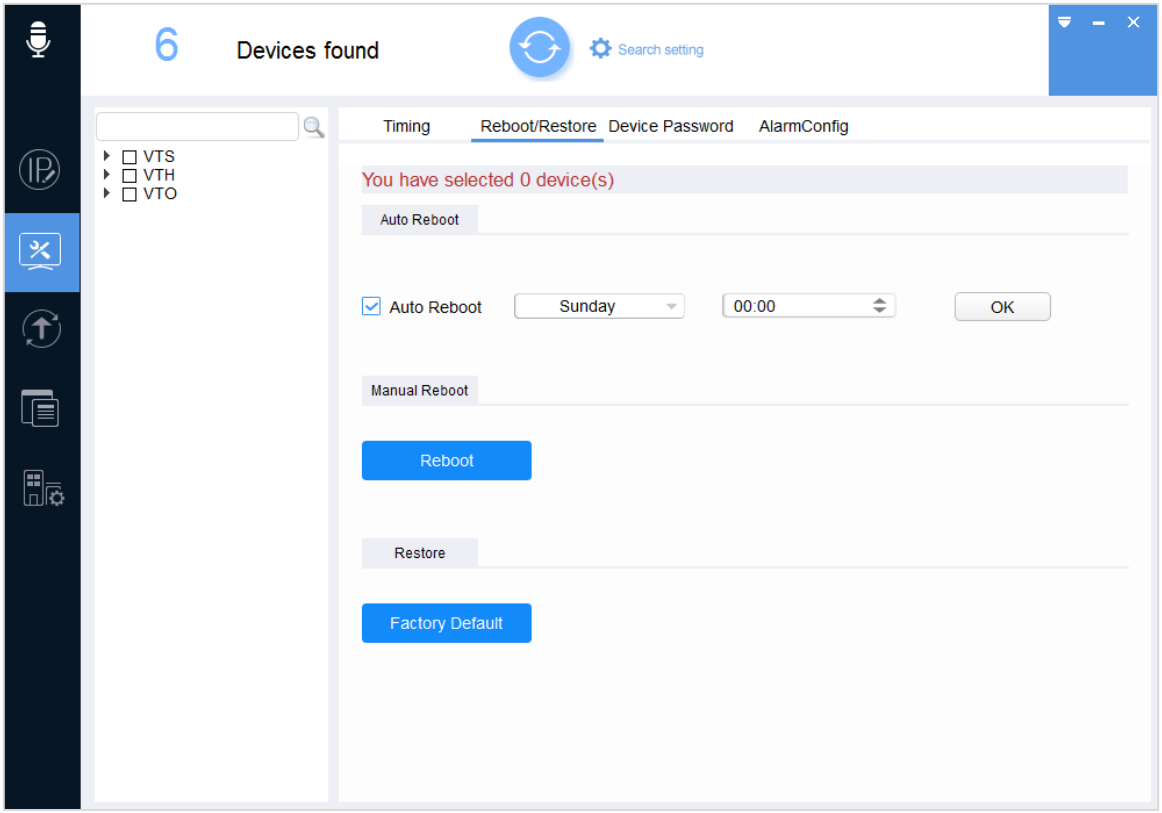
2.5.2.1 Rebooting

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 Click  and click **Reboot/Restore** tab.

Figure 2-15 Reboot/Restore



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

2.5.2.2 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 Click  and click **Reboot/Restore** tab.

Step 2 Click ▸ next to the device type.

The device list is displayed.

Step 3 Select one or multiple devices.

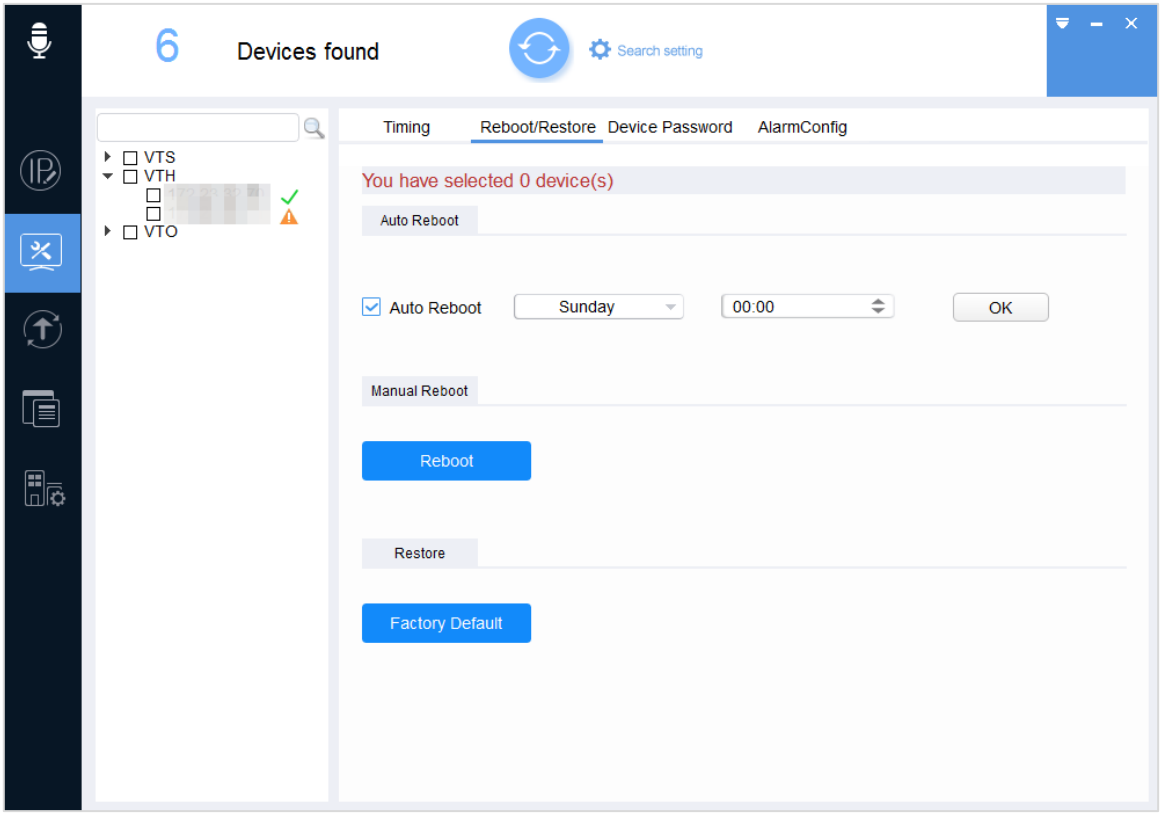
If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

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

After restoring is completed, the result is displayed.

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

Figure 2-16 Restoring result



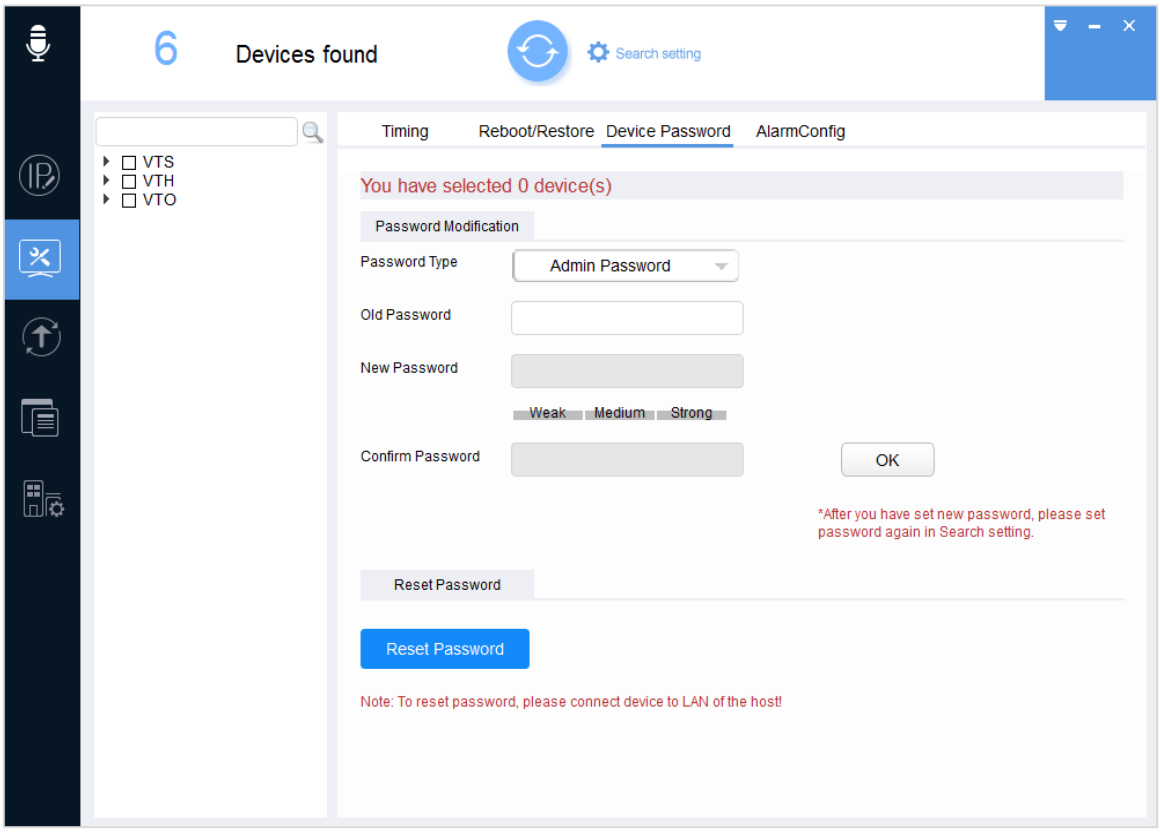
2.5.3 Modifying and Resetting Password

2.5.3.1 Modifying Password

You can modify the device login password.

Step 1 Click  and click **Device Password** tab.

Figure 2-17 Device password



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 Set the password parameters.

Table 2-6 Password parameters

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

- Not all devices support the above password rules, and the actual interface shall prevail.
- After setting the new password is completed, reset the password in **Search setting** interface.
- If the new password is the same with the old password, a **Notice** dialog box is displayed after clicking **OK**. Then you need to click **OK** to go back and reset the new password.

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

2.5.3.2 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 Click  and click **Device Password** tab.

Step 2 Click ▸ next to the device type.

The device list is displayed.

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

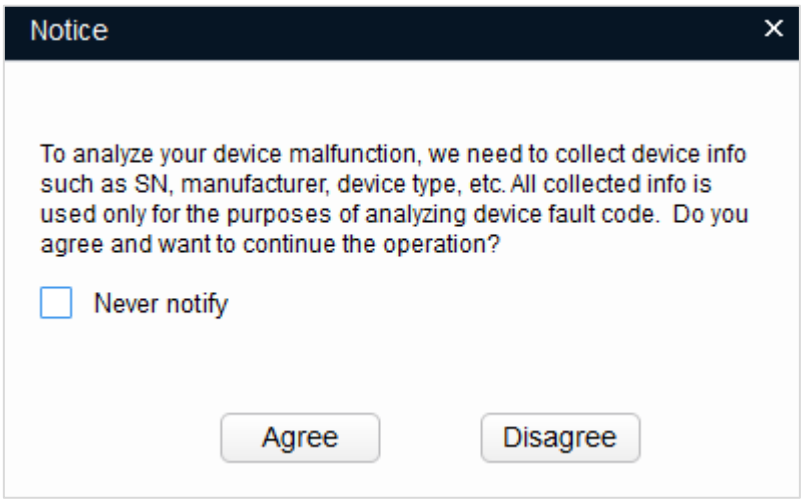
If the device is not in the device list, search again. For the details about how to search devices, see "2.1 Searching Devices."

Step 4 Click **Reset Password**.

A **Notice** box will be displayed.

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

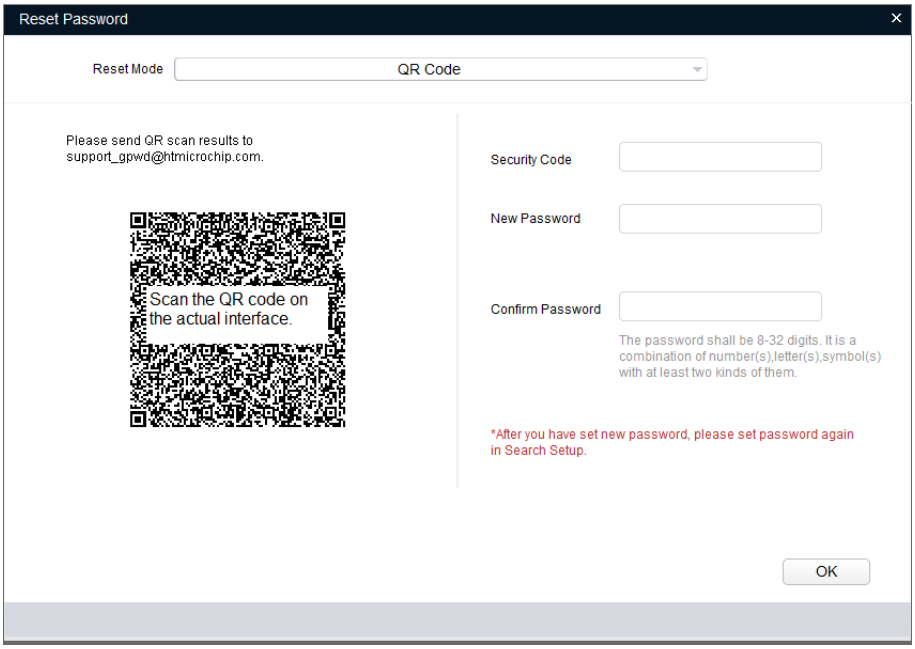
Figure 2-18 Notice of password reset



Step 5 Click **Agree**.

The **Reset Password** interface is displayed.

Figure 2-19 Reset password (QR code)



Step 6 Under **Reset Mode**, select **QR code**.

Step 7 Perform operations according to the instructions on the interface to obtain the security code.

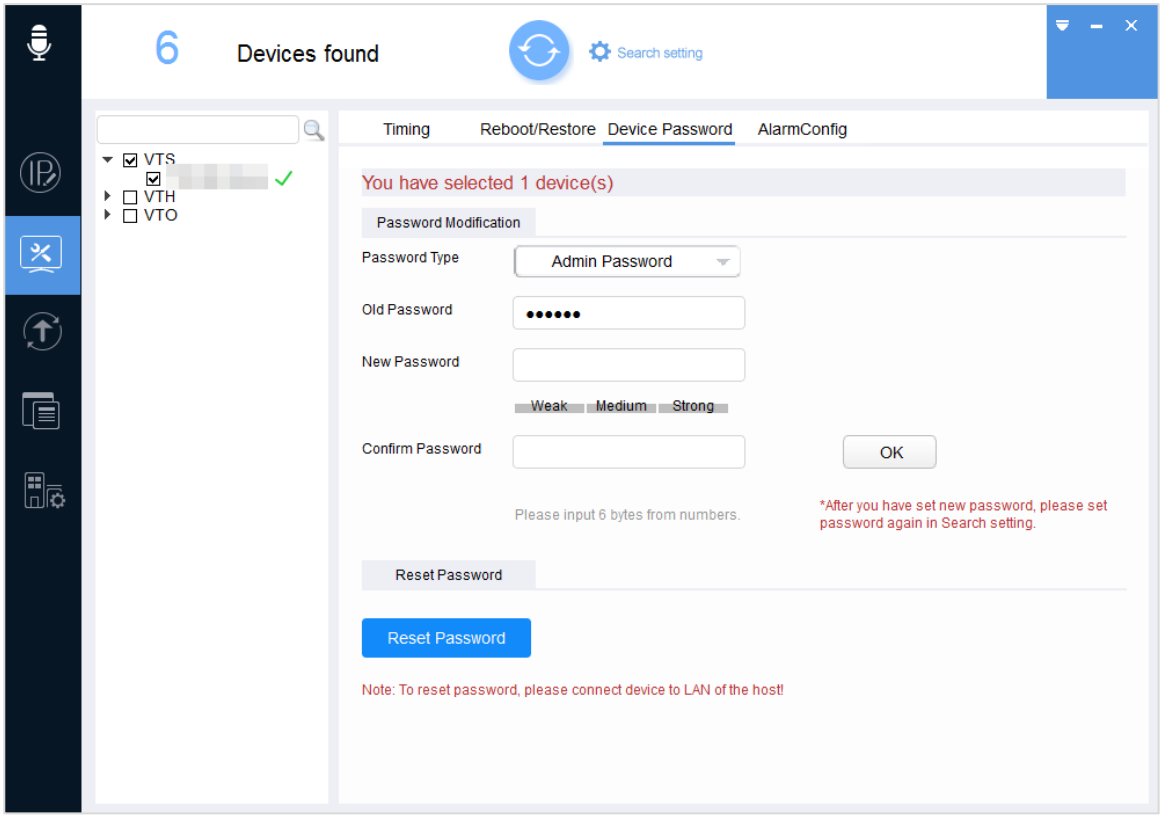
Step 8 Enter old password, new password, and confirm password.

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

Step 9 Click **OK** to start resetting the password.

The result is displayed next to the device after restoring is completed. Click the success icon (✓) or click the failure icon (⚠) for the details.

Figure 2-20 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 Click  and click **Device Password** tab.

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.

(Optional) A **Notice** box will be displayed.

(Optional) Click **Agree**.

The **Reset Password** interface is displayed.

- The interface might vary with different models, and the actual product shall prevail.
- For some devices only support resetting password by XML file, skip the **Notice** of step 4.
- When reset passwords for multiple devices, the Tool resets all devices based on the password reset mode of the first selected device.

Figure 2-21 Notice of password reset (2)

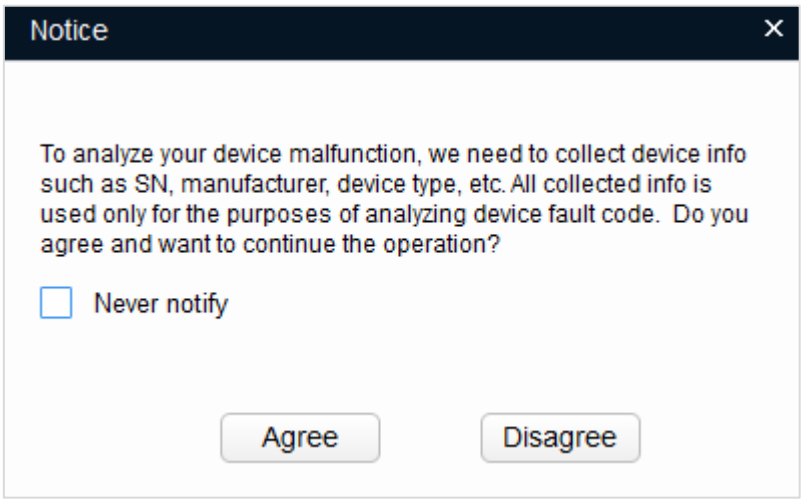
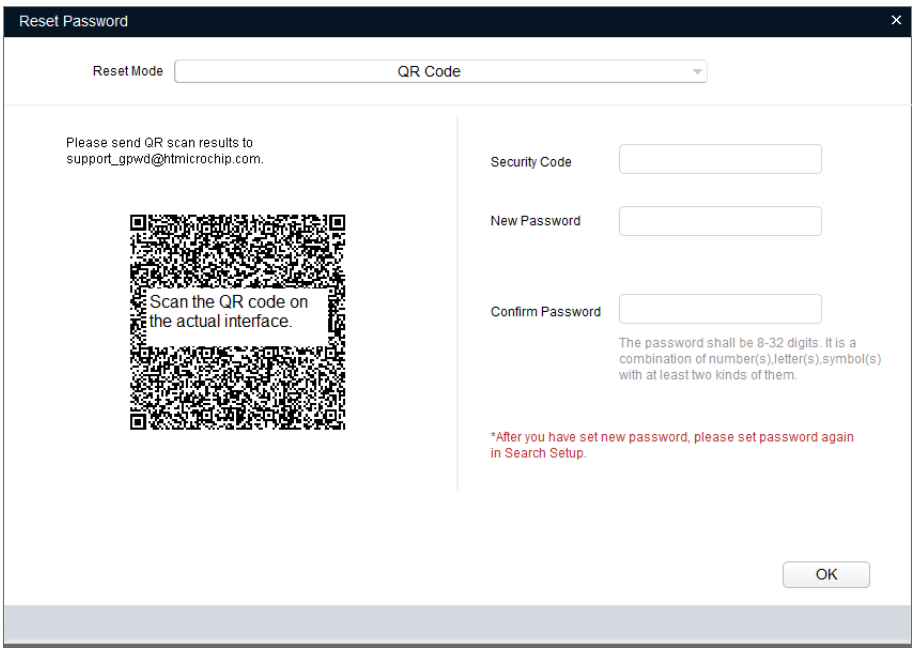


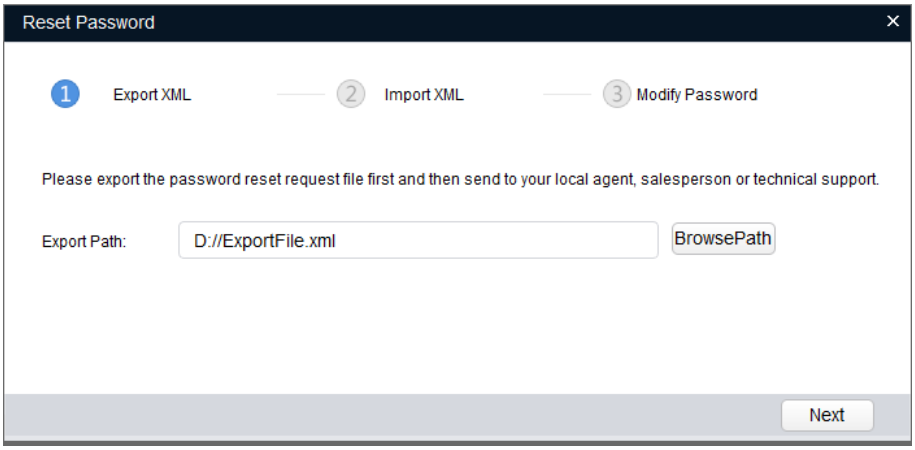
Figure 2-22 Reset password



Step 5 Under **Reset Mode**, select **XML File**.

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

Figure 2-23 Reset password (Export XML)



Step 6 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** interface will be displayed.

3) Click **OK**.
After completing exporting the XML, the **Reset Password-Import XML** interface is displayed.

Step 7 Obtain the **result.xml** file.

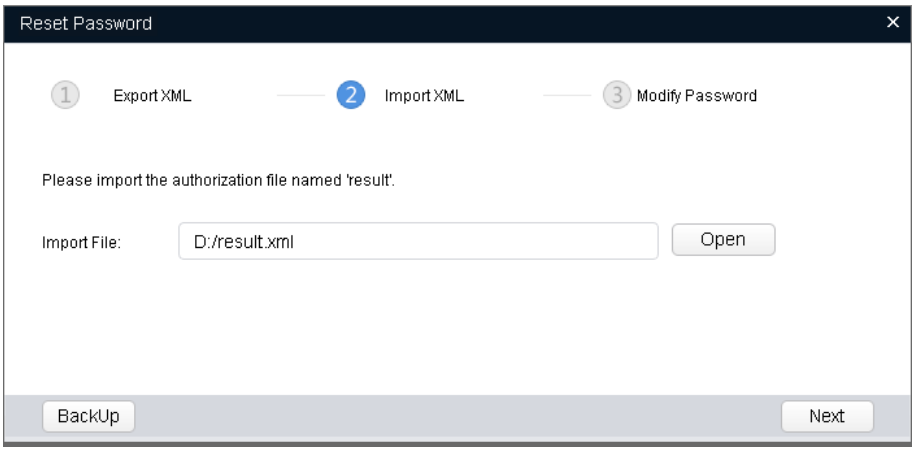
Find the **ExportFile.xml** under the save path and send it as an attachment to the designated mailbox indicated on the interface. In a few minutes, you will receive a **result.xml** file as an attachment and save it properly.

Step 8 Import XML.

If the **Reset Password-Import XML** interface is closed, click **System Settings > Reset Password**. On the **Reset Password** tab, click the note under the interface to continue the operation.

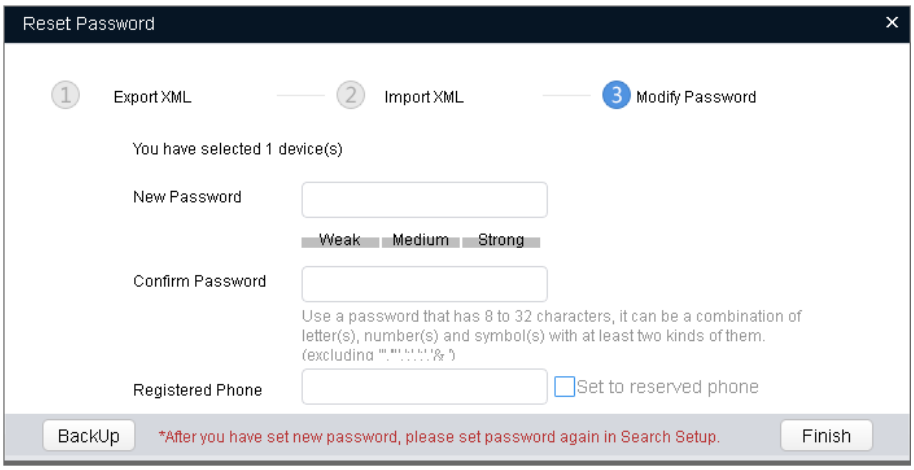
1) Click **Open** to import the **result.xml** file from the save path.

Figure 2-24 Reset password (import XML)



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

Figure 2-25 Reset password (modify password)



Step 9 Modify password.

1) Enter the new password and confirm password.

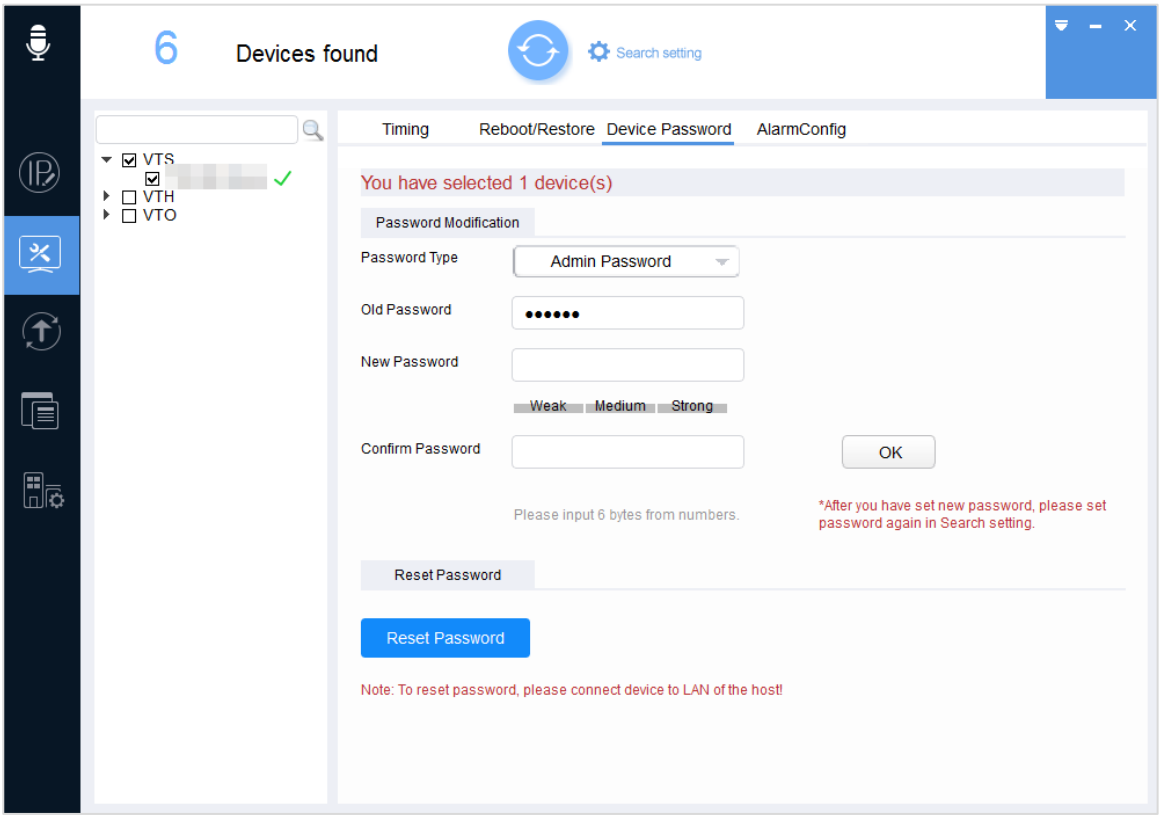
The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

2) Enter the registered phone number, and you can check the **Set to reserved phone** check box to set it as the reserved phone number.

3) Click **Finish** to start resetting the password.

The result is displayed next to the device after operation is completed. Click the success icon ( ) or click the failure icon ( ) for the details.

Figure 2-26 Password resetting result (XML file)



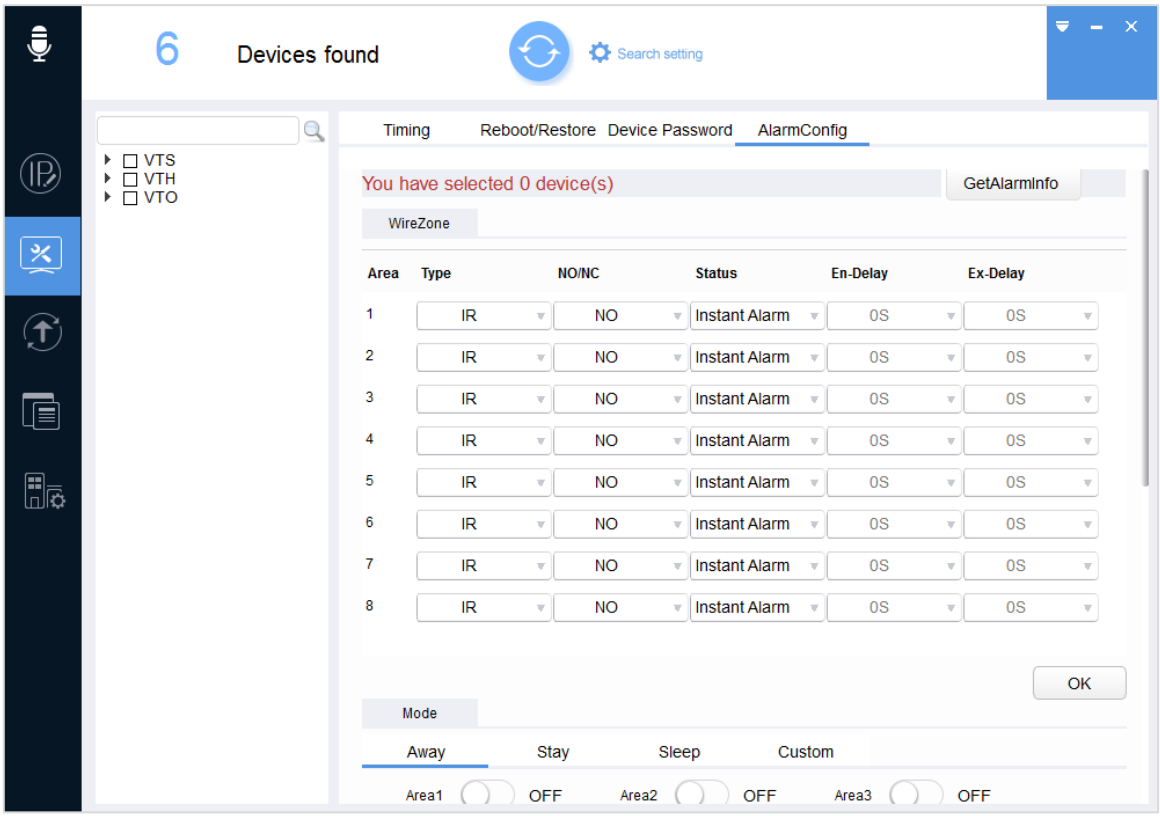
2.5.4 Configuring Alarm

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 Click  and click **AlarmConfig** tab.

Figure 2-27 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."

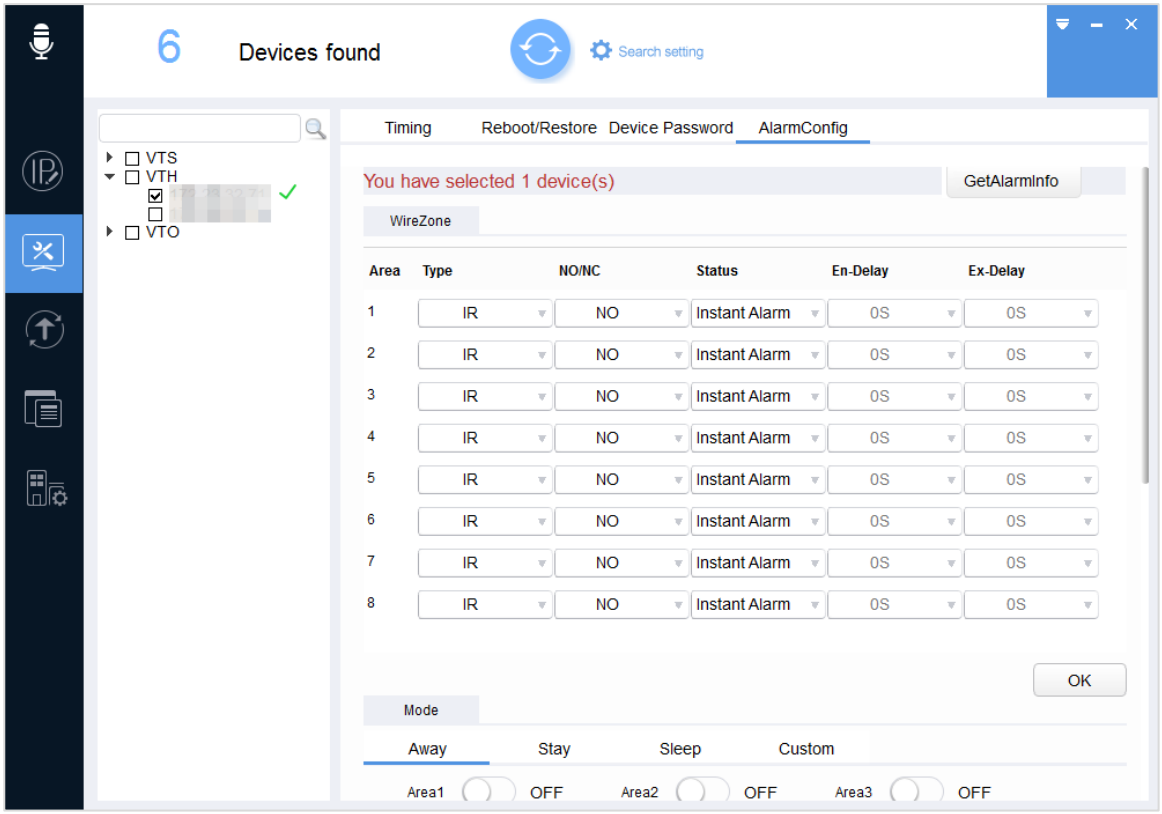
Step 4 Access the alarm information settings.

1) Click **GetAlarmInfo**.
   The **Notice** interface 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 2-28.

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

Figure 2-28 Alarm configuration result



Step 5 Set the alarm information of protection area.

1) In the **WireZone** area, configuring the alarm information.

Table 2-7 Alarm configuration description

Parameter	Description
Area	The serial number of protection area. There are 8 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. Do step 6 again to set the effectiveness of protection area in another alarm mode.
- 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 Click  and click **AlarmConfig** tab.

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 Click  and click **AlarmConfig** tab.

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 Upgrading

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

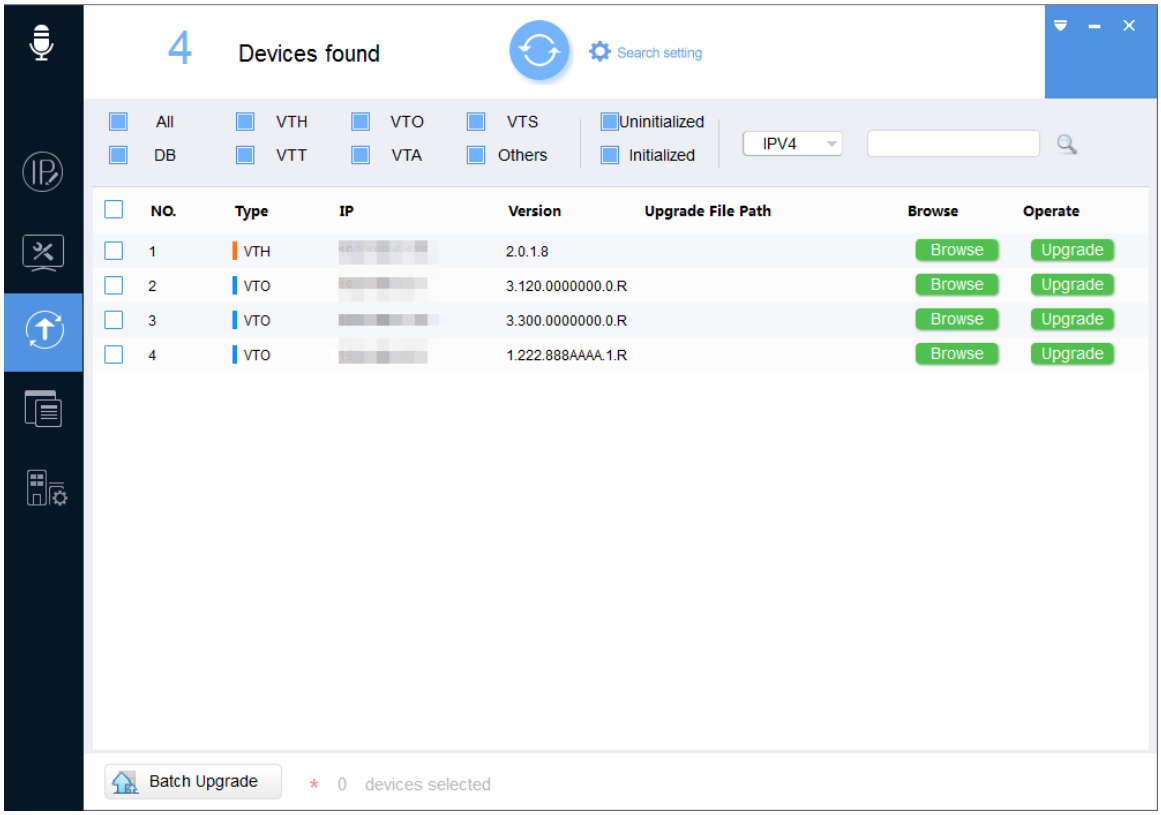
- If the device is disconnected during upgrading, the Tool will prompt the disconnection and the device might reboot.
  - ◇ If the upgrade progress does not exceed 50%, the upgrade file transmission is not completed. Please upgrade the device again after the reconnection.
  - ◇ If the upgrade progress exceeds 50%, the upgrade file transmission is completed and the device will be upgraded.
- Some Android series devices do not support upgrading from higher to lower versions, such as the VTH53X1 series; otherwise, devices will be crashed. They can only be upgraded from the lower version to the higher version.

2.6.1 Upgrading One Device

You can choose this procedure for upgrading one device.

Step 1 Click  .

Figure 2-29 Upgrade

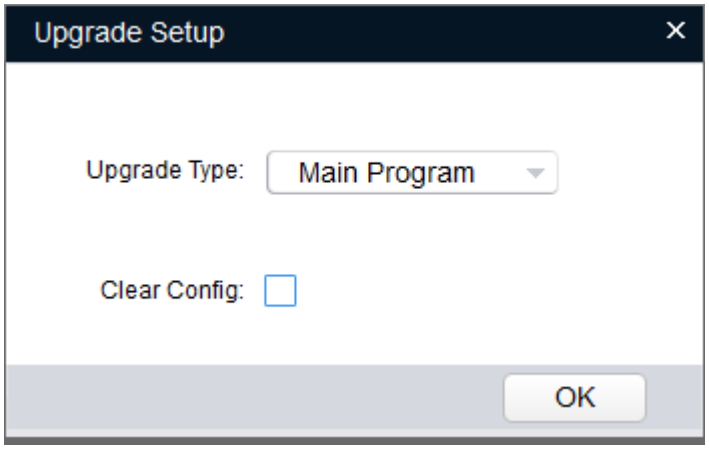


Step 2 Click **Browse** next to the device that you want to upgrade, select the upgrade file and then click **Open**.

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**.

Figure 2-30 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 device status of initialization.

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.

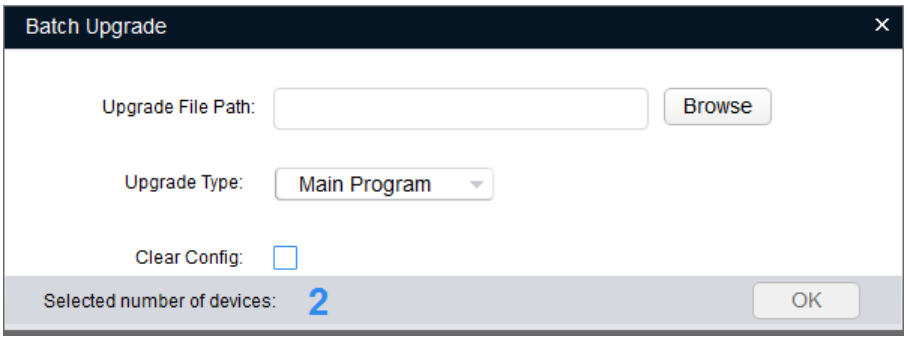
Step 1 Click .

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 that the selected devices are subject to be upgraded to the same software version.

Step 3 Click Batch Upgrade.

Figure 2-31 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 Configuring the Template

Only VTO supports this function.

You can export and import data.

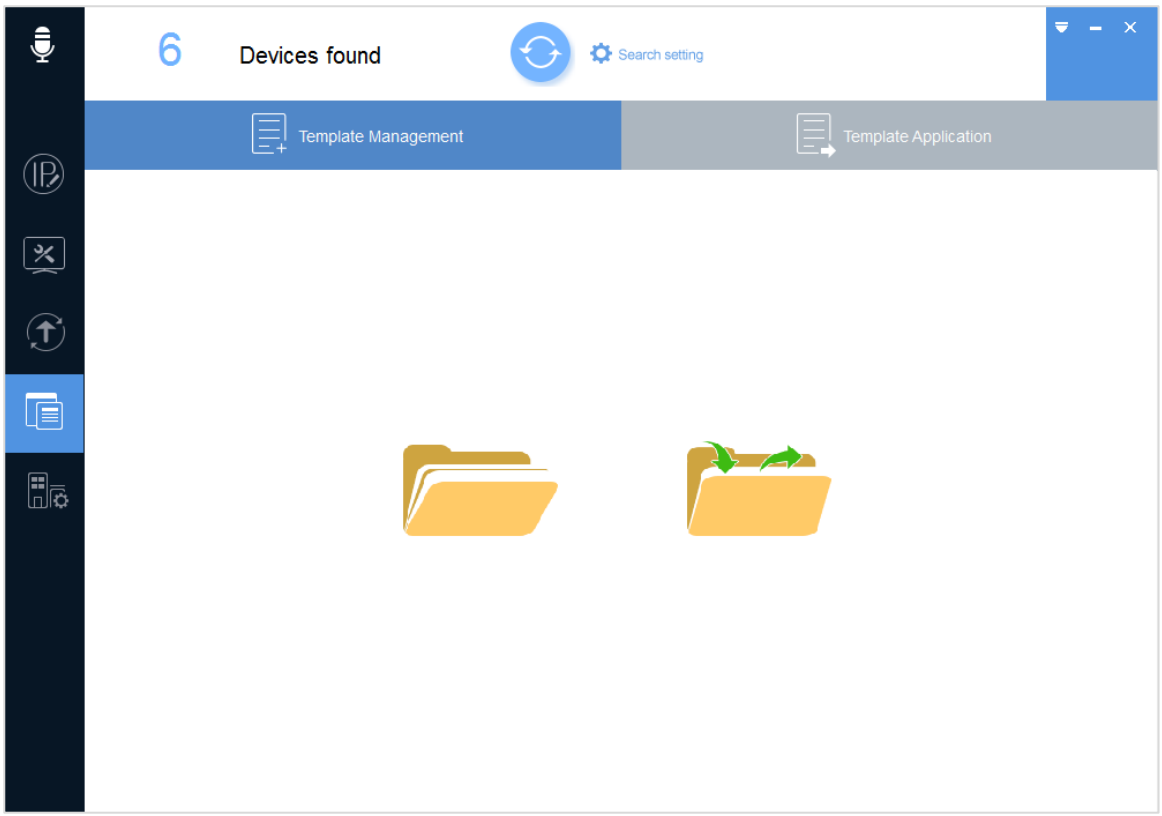
- Exporting data: Back up or save the video and audio configurations, indoor machine management, card management, access password, and access QR code for the device.
- Importing data: Restore or batch configure the video and audio parameters, indoor machine management, card management, access password,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

2.7.1 Creating a Template

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  .

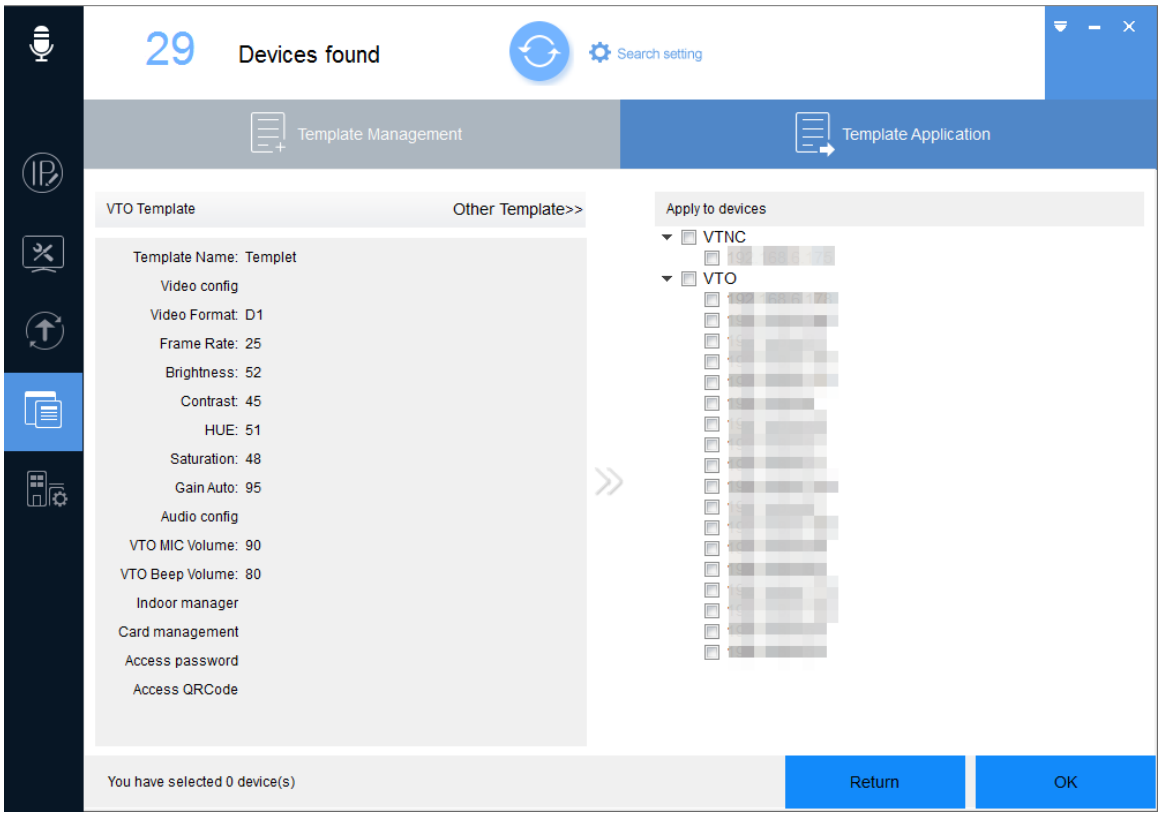
Figure 2-32 Template setup



Step 2 Export the template.

1) Click  .

Figure 2-33 Template management



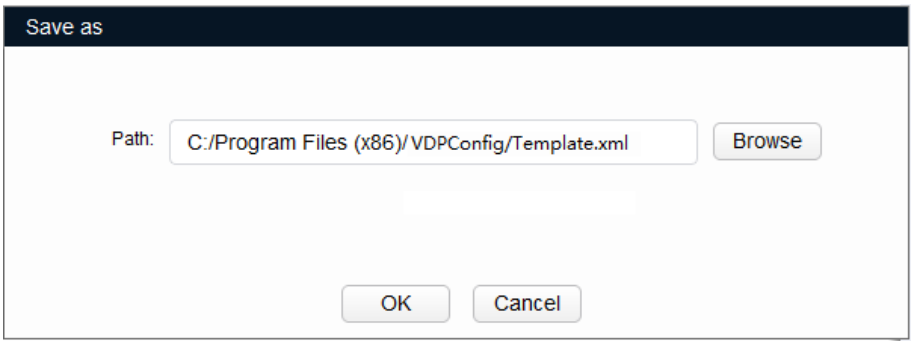
2) Select the device, and enter the template name. For example, you can enter **Template**, and then set the information that you want to export.

Step 3 Save the template.

1) Click **Get**.

The system starts obtaining the information that you want to export and indicates **get config ok!** on the interface and the **Save as** interface is displayed.

Figure 2-34 Save as

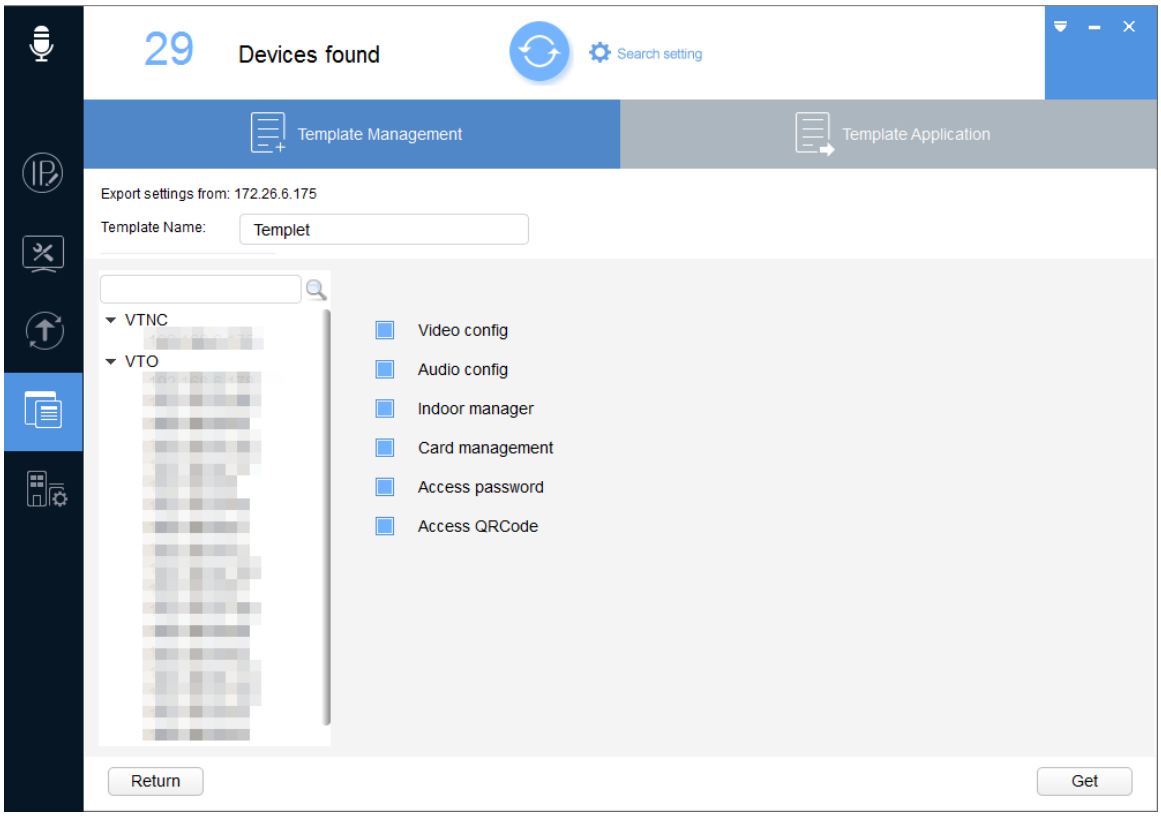


2) Click **Browse** to select the save path for the template.
3) Click **OK** to save the template.

After the exporting is completed, the **Template Application** interface is displayed.

For details about how to apply the template, see "2.7.2 Applying the Template."

Figure 2-35 Template application (1)



2.7.2 Applying the Template

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.

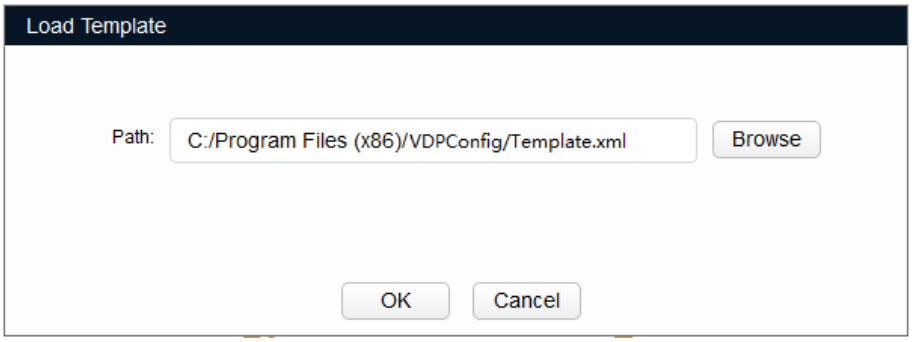
Step 1 Click .

Step 2 Load the template.

1) Click .

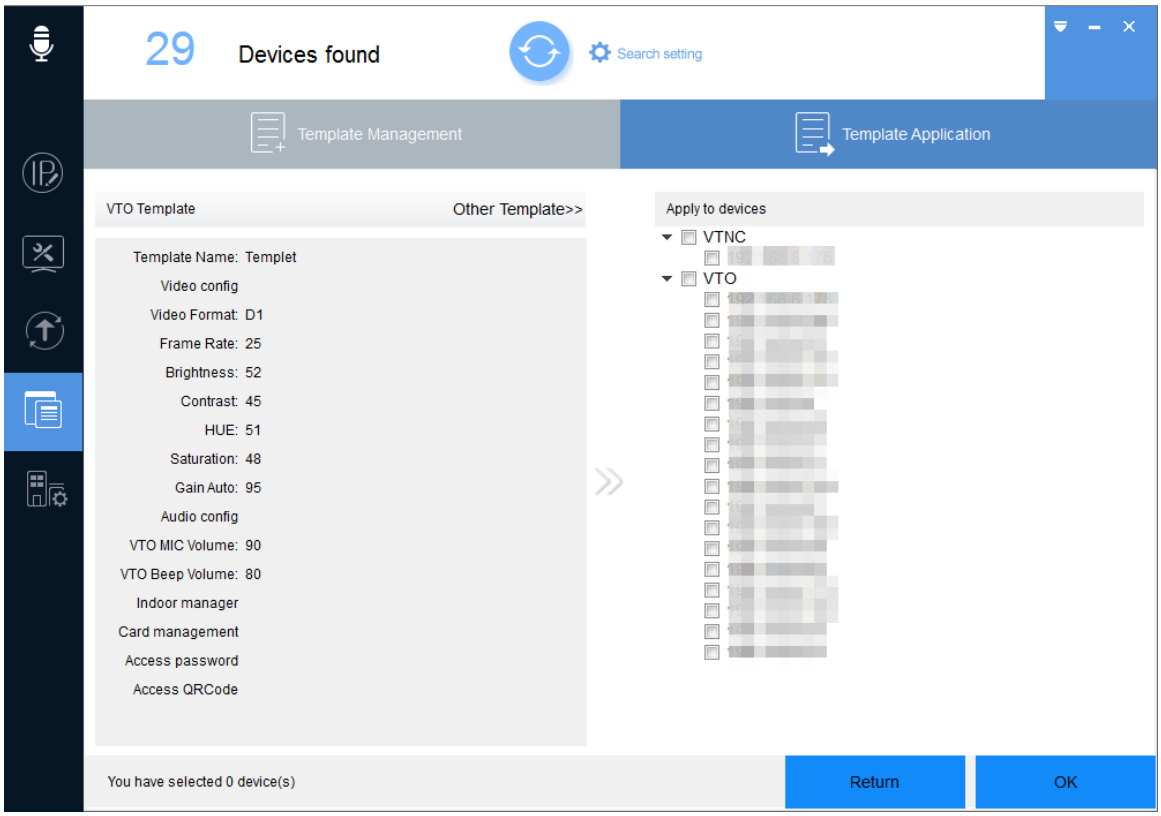
Make sure the template exists, if not, see "2.7.1 Creating a Template."

Figure 2-36 Load template



2) Click **Browse** to select the template.
3) Click **OK**.
   The **Template Application** interface is displayed.

Figure 2-37 Template application (2)



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

The **Application Template** interface is displayed.

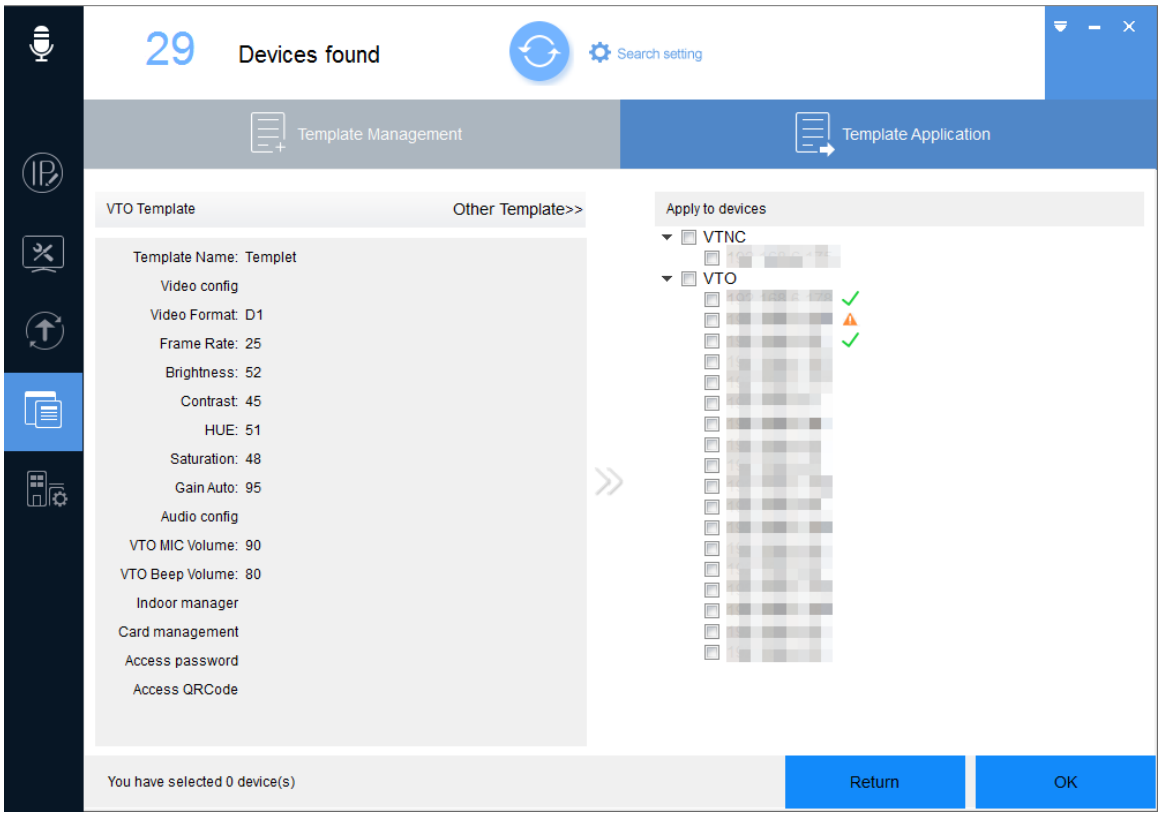
Step 4 Click **OK** to start applying the template.

After applying is completed, the result is displayed.

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 2-38 Template application result



2.8 Project Configuration

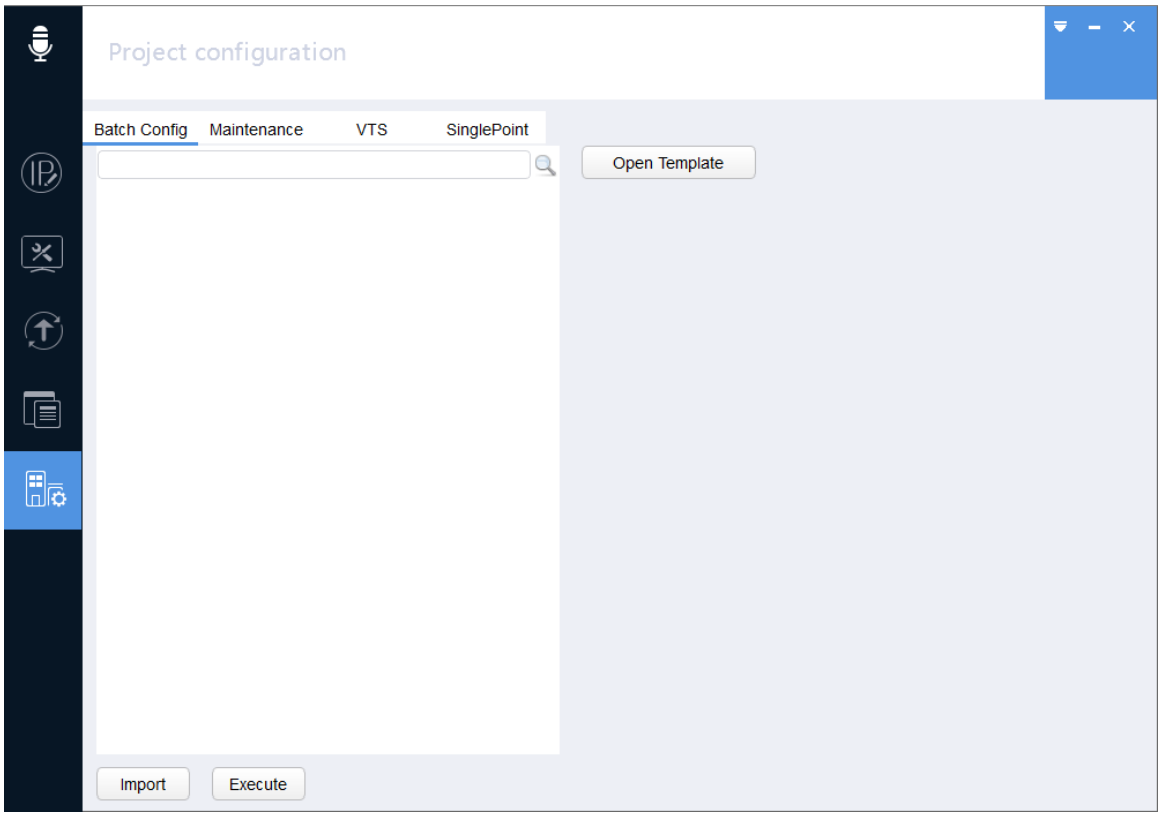
You can import devices and establish relationships between devices in LAN.

2.8.1 Configuring SIP System Device

You can import and configure SIP system device.

Step 1 Click  .

Figure 2-39 Project configuration (1)



Step 2 Click **Open Template**.

Figure 2-40 Template

	A	B	C	D	E	F	G	H	I	J
1	**Overview**									
2	This table is for VDP devices project configuration. 1) Batch configuration for devices by VDP configtool 2) Batch adding devices on Express platform									
3	**Attentions**									
4	1) SIP Port-5060 (VTO as SIP server); -5080 (Express as SIP server) 2) 2nd Confirm VTO type only exists in Express Solution. 2nd Confirm VTO device No. is VTH (Room No.) and extension range is 200-299 3) Building No. and unit No. dose not exist when VTO is SIP server 4) VTO SIP realm is necessary when VTO is server (Default: VDP); VTO SIP realm is optional when VTO is client; VTH SIP realm is optional 5) In villa system, device No. is 'VTO No. # VTH No.'. For example VTO No. is 8001 , VTH No. is 9901, device No. is 8001#9901									
5	6) Device Type: It is used to determine the device type. Obtain the first non-blank field from left to right, and it is subjected to the column number of Device Type. (For example, if you enter the device type in both VTO column and VTH column, the device type will be read as VTO.)									
6	7) Device Name: The device name, you can leave it bland, and it will not be issued.									
7	8) Device ID-SN: The device serial number. It is the unique number for tools to search for the device. You can export the number through the Export button, or the Details button ( ) in the device row.									
8	9) Network Info-IP address, net mask, and gateway, which are requested to comply to network standard.									
9	10) Login-Info: Username and project password. Click Initialize to issue the password and the port number is 37777 by default.									

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

Step 4 Select the save path, enter the **File Name**, such as "SIP template-SIP", and then click **Save**.

The file names must include "-SIP"; otherwise, the system cannot recognize and import the file.

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**.

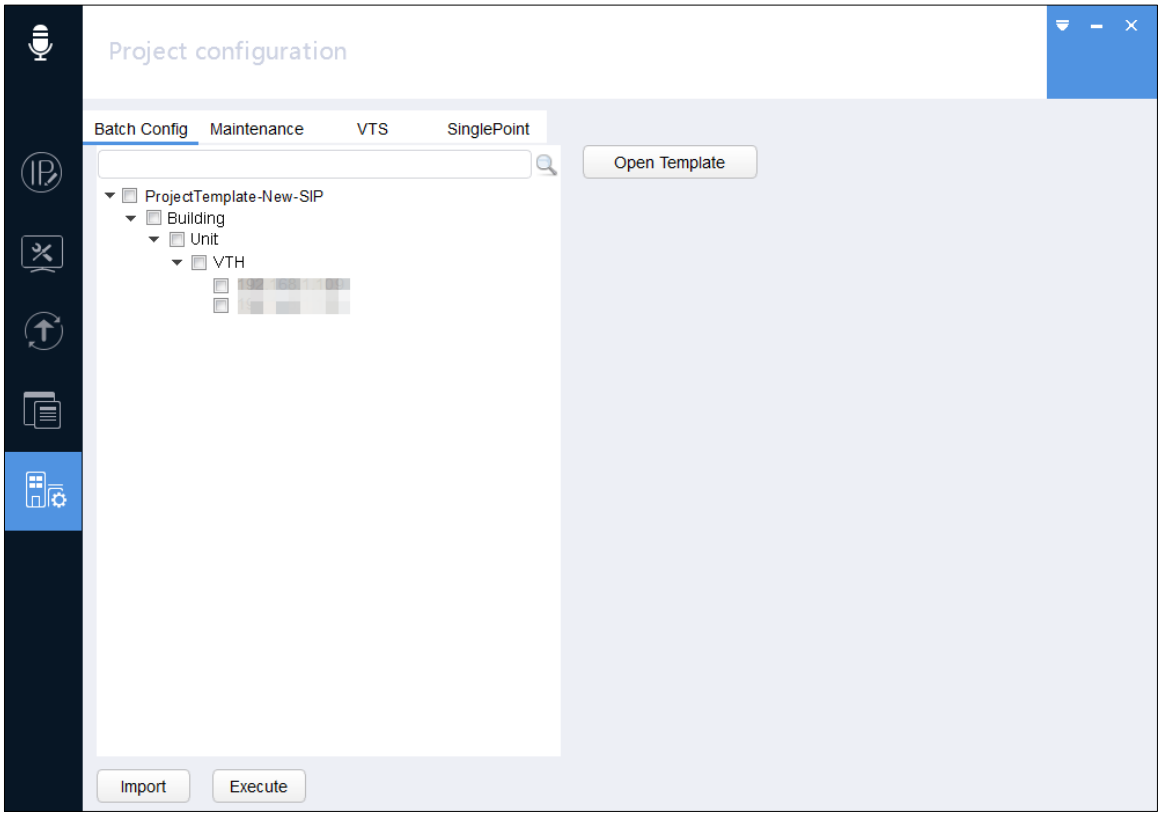
The **Open** interface is displayed.

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

After the importing, a **Notice** interface is displayed. Click **OK** and it goes back to the **Project Configuration** interface.

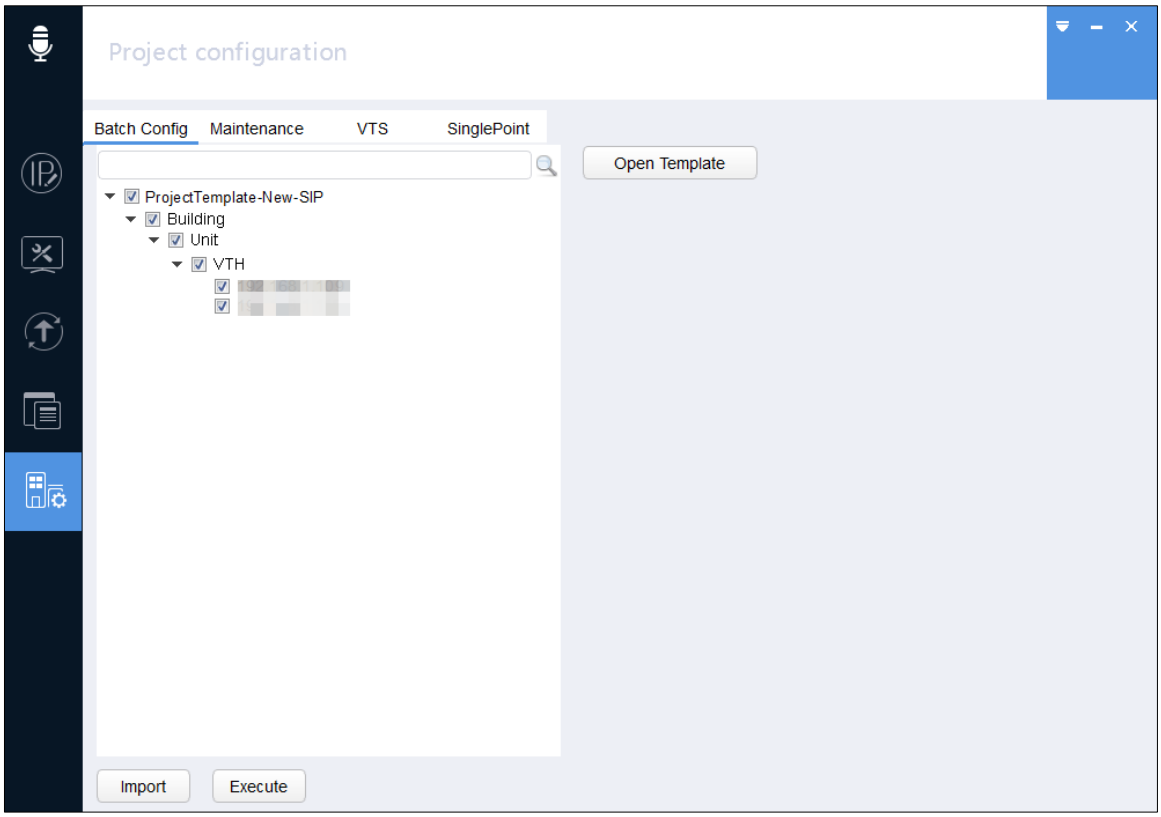
If you import two templates of different names successively, which contain device with the same SN, the latest imported template shall govern.

Figure 2-41 Project configuration (2)



Step 8 Select device.

Figure 2-42 Selecting device

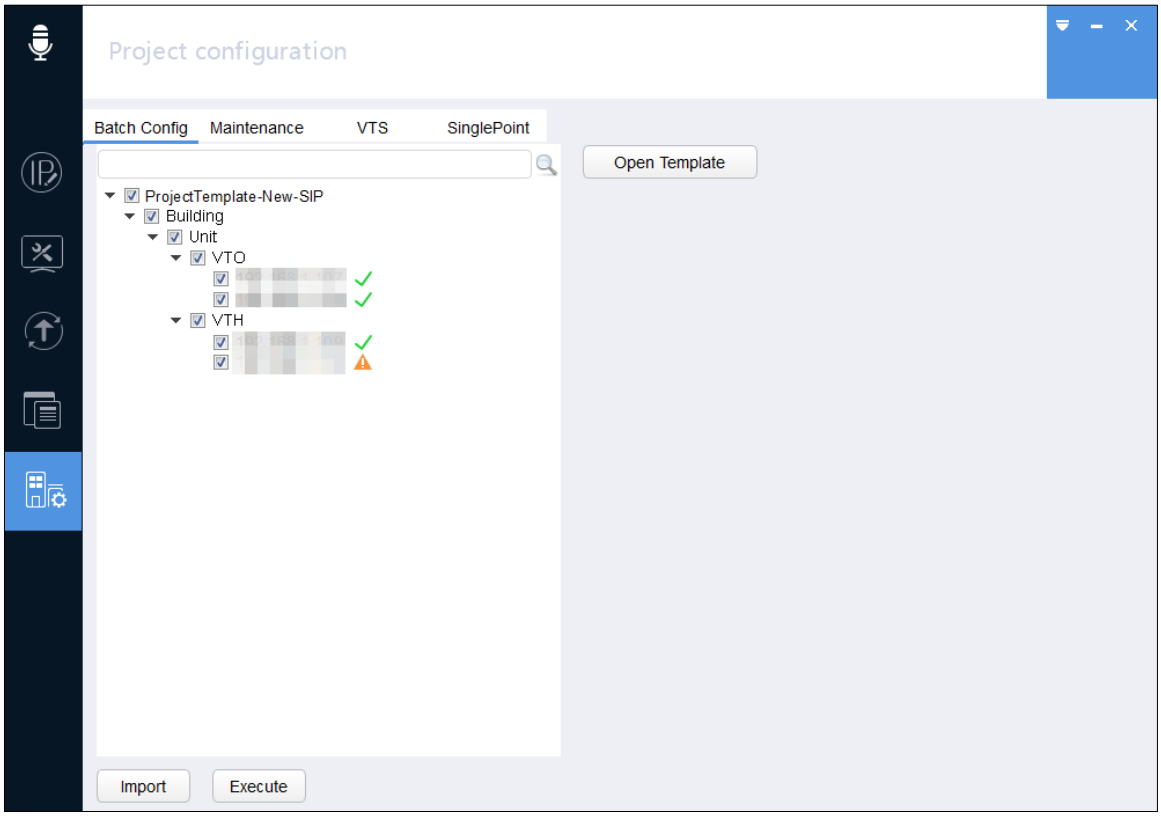


Step 9 Click **Execute**.

After the operation is completed, the result is displayed.

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

Figure 2-43 Executed result



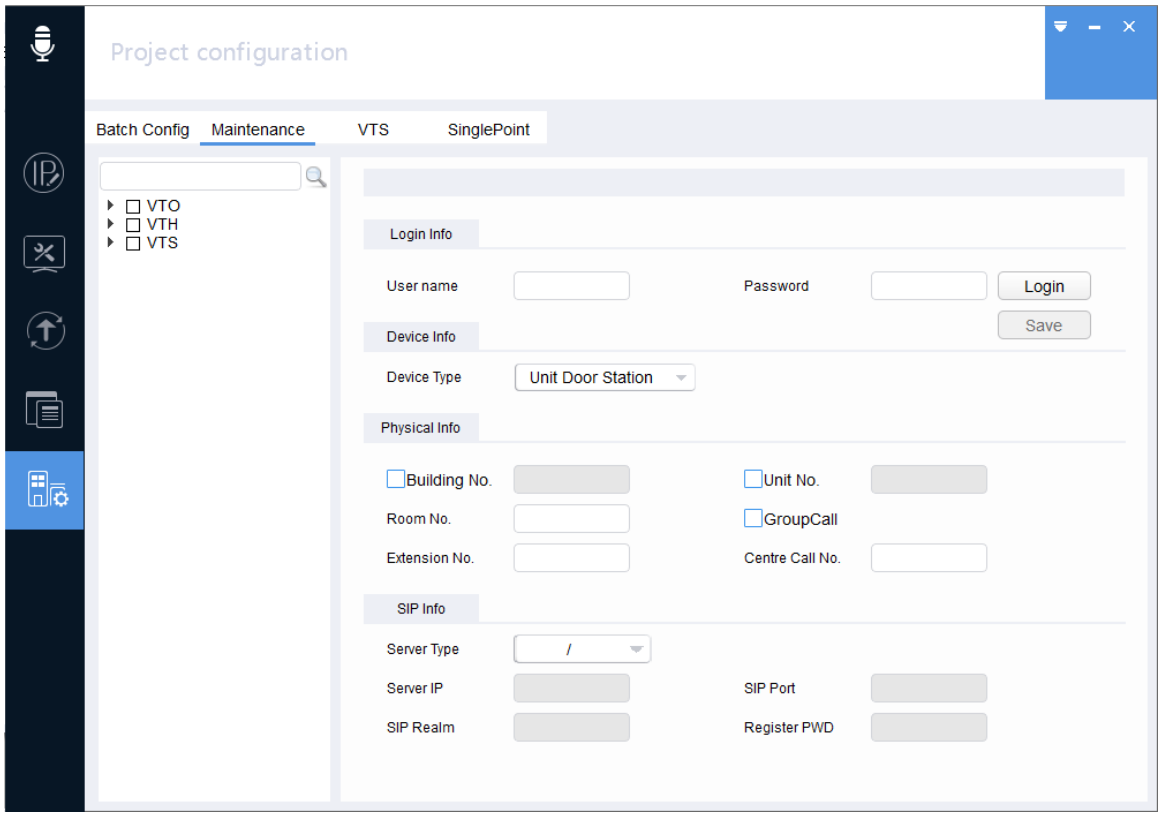
After the operation is completed, you can configure the device. For details, see "2.8.2 Configuring VTO and VTH."

2.8.2 Configuring VTO and VTH

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

Step 1 Click , and click the **Maintenance** tab.

Figure 2-44 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**.

Figure 2-45 VTH

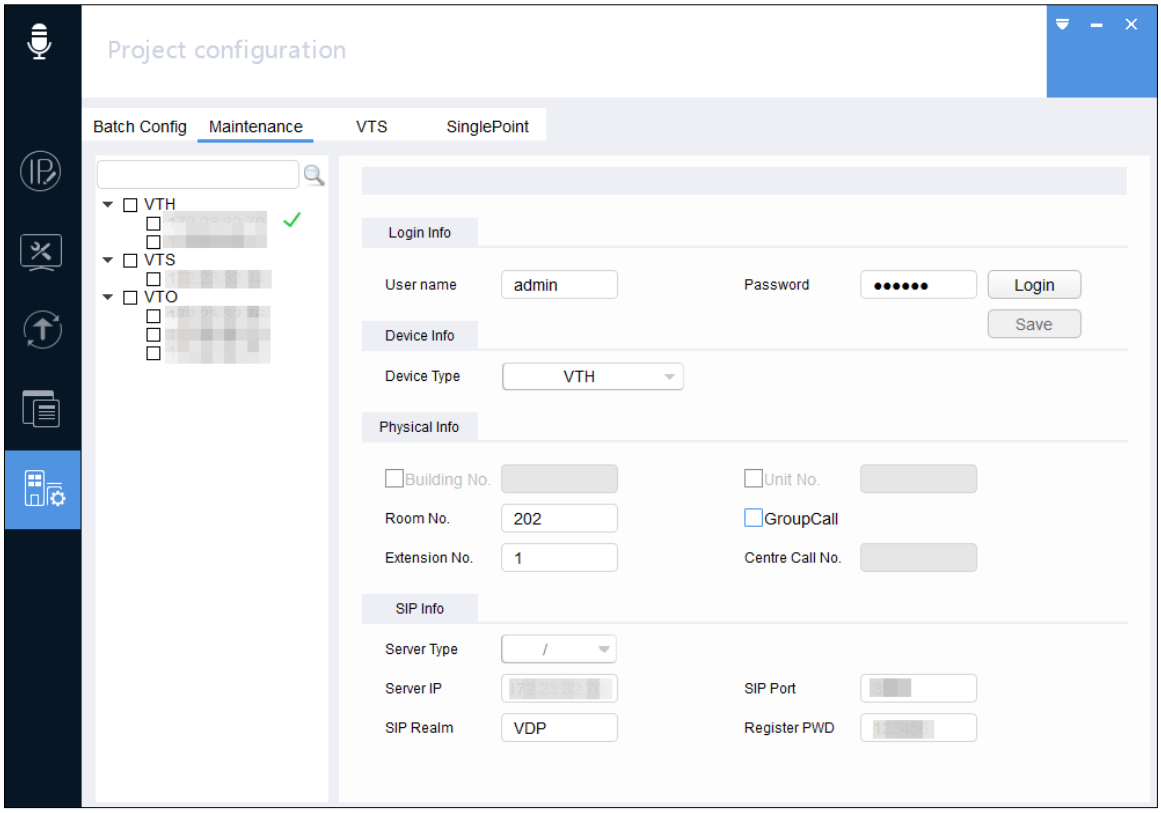
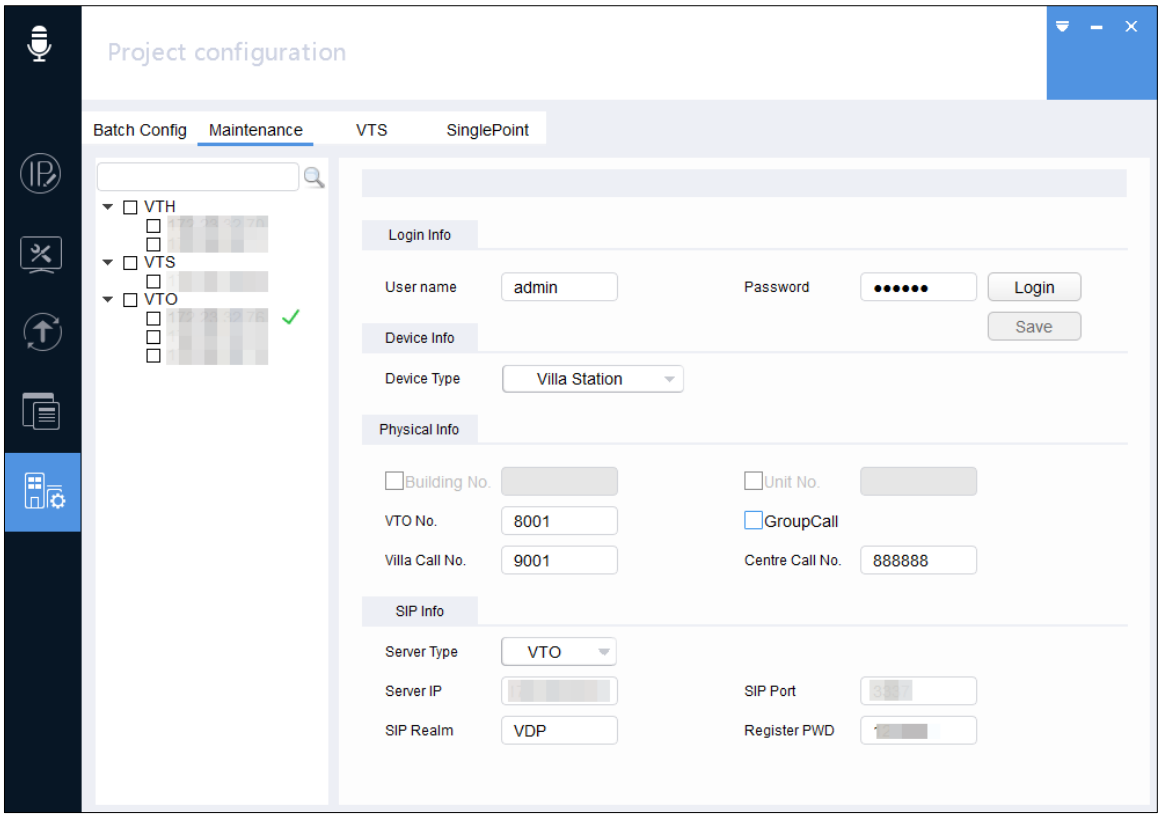


Figure 2-46 VTO



Step 5 Configure the settings.

Table 2-8 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**.

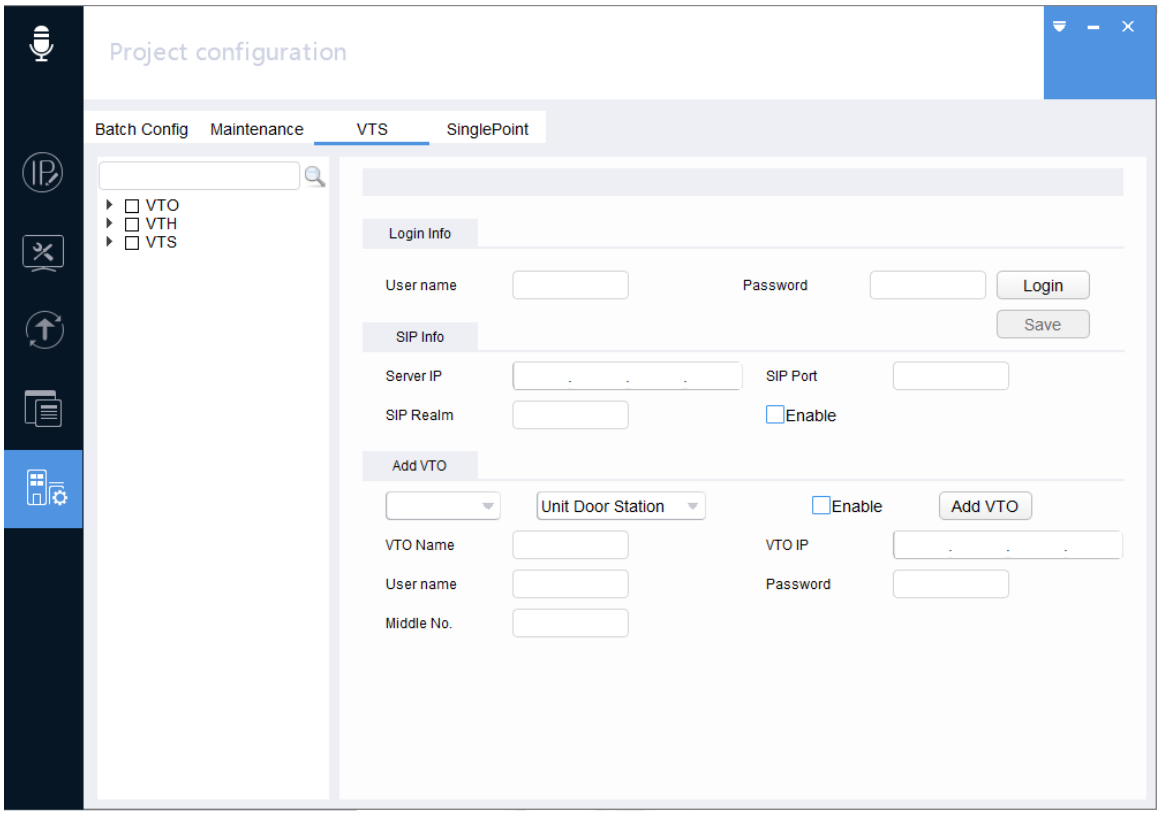
You can click the success icon ( ) or click the failure icon ( ) for the details.

2.8.3 Configuring VTS

You can configure VTS.

Step 1 Click , and click the **VTS** tab.

Figure 2-47 VTS (1)



Step 2 Click ▸ next to the device type.

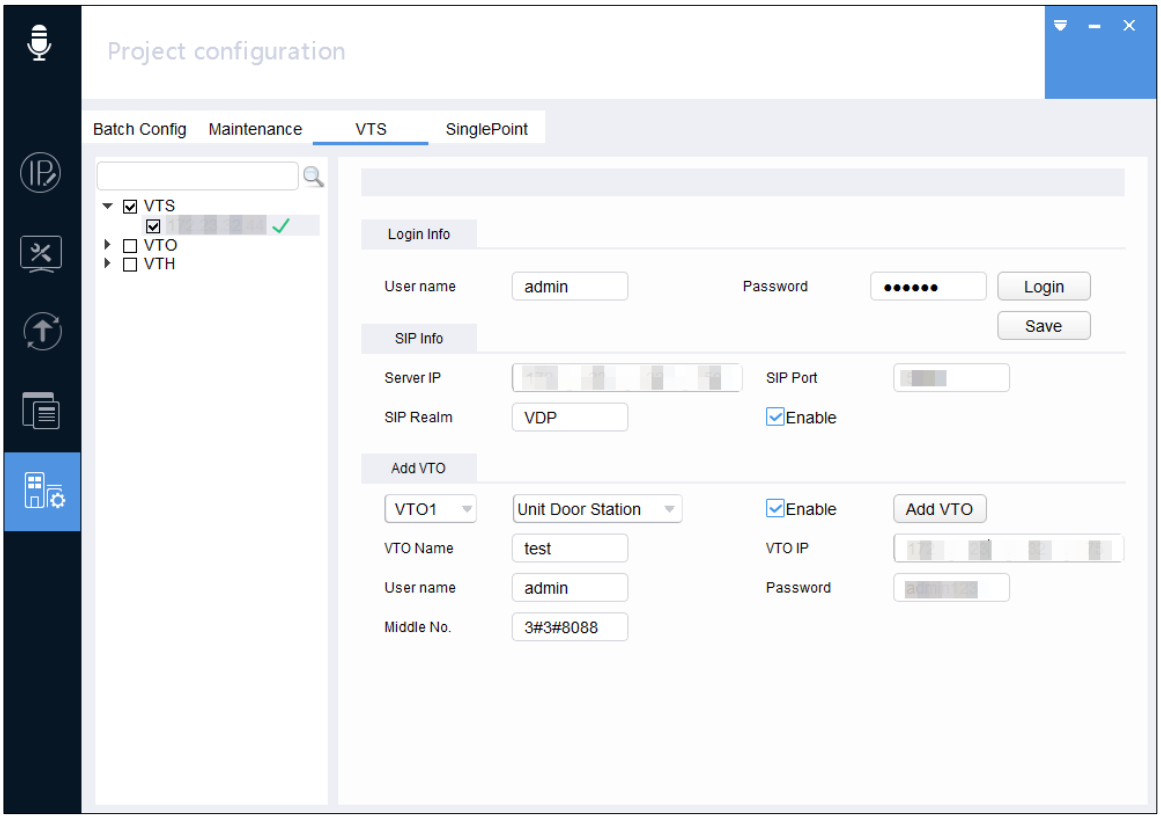
The device list is displayed.

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**.

Figure 2-48 VTS (2)



Step 5 Configure **SIP Info**

Table 2-9 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.

Table 2-10 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.
Password	Enter the web login password.

Parameter	Description
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.

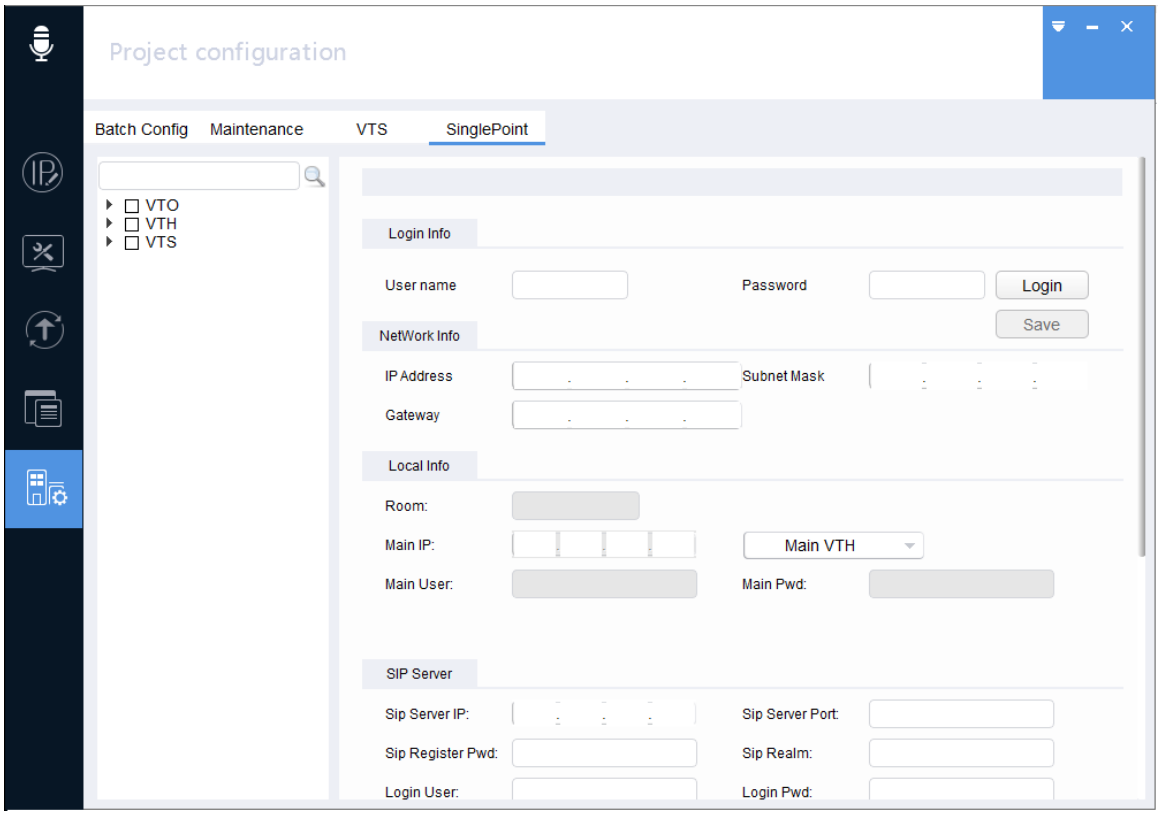
2.8.4 Configuring VTH by Single Point

You can configure parameters of VTH, such as configuring the related VTO information of VTH. And you can only configure one device at a time.

VTO and VTS are not supported.

Step 1 Click , and click the **SinglePoint** tab.

Figure 2-49 Single point (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**.

Step 5 Configure settings.

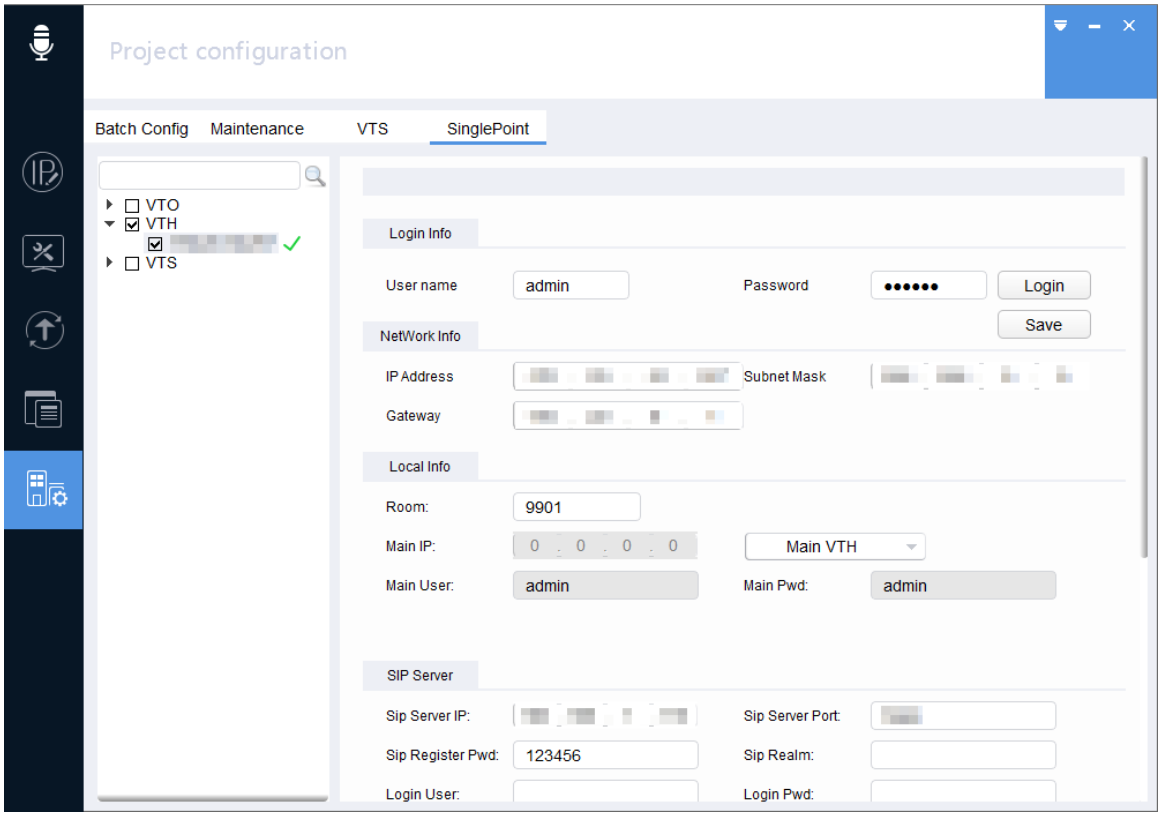
Table 2-11 Single point parameters

Parameter		Description
Network Info	IP Address	Enter the IP address of the device.
	Subenet Mask	Enter the subnet mask of the device.
	Gateway	Enter the gateway of the device.
Local Info	Room	Enter the room number.
	Main IP	Select the device type as **Main VTH** or **Sub VTH**. And then enter the IP address.
	Main User	Enter the username of the main VTH. It is not available when you select device type as **Main VTH**.
	Main Pwd	Enter the password of the main VTH. It is not available when you select device type as **Main VTH**.
SIP Server	SIP Server IP	Enter the IP address of the SIP server.
	SIP Server Port	Enter the port number of the SIP server.
	SIP Register Pwd	Enter the registration password of the SIP server.
	SIP Realm	Enter the domain name of the SIP server.
	Login User	Enter the login username of SIP server.
	Login Pawword	Enter the login password of SIP server.
	Enable Status	Select the check box to enable the server.
Network Termi	Mater VTO Name	Select the VTO to connect. Up to connect 1 main VTO and 19 salve VTO. You can set the mater Vto name.
	Mater VTO IP	Enter the IP address of the VTO to be connected.
	Mater VTO User	Enter the username of the VTO to be connected.
	Mater VTO Pwd	Enter the password of the VTO to be connected.
	Enable Status	Select the check box to enable the connection.

Step 6 Click **Save**.

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

Figure 2-50 Single point (2)



Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

2. **Update Firmware and Client Software in Time**

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

3. **Set and Update Passwords Reset Information Timely**

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

4. **Enable Account Lock**

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

5. **Change Default HTTP and Other Service Ports**

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

6. **Enable HTTPS**

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

7. **Enable Whitelist**

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

8. **MAC Address Binding**

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

9. **Assign Accounts and Privileges Reasonably**

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

10. **Disable Unnecessary Services and Choose Secure Modes**

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

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

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

11. **Audio and Video Encrypted Transmission**

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

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

12. **Secure Auditing**

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

13. **Network Log**

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

14. **Construct a Safe Network Environment**

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

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is

suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device