

IP Audio Indoor Station

Quick Start Guide

V1.0.2



Please scan the QR code to view the user's manual.

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

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

2. Update Firmware

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

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

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

2. Change Default HTTP and TCP Ports:

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

3. Enable HTTPS/SSL:

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

4. Enable IP Filter:

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

5. Change ONVIF Password:

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

6. Forward Only Ports You Need:

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

site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

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

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

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

10. UPnP:

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

11. SNMP:

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

12. Multicast:

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

13. Check the Log:

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

14. Physically Lock Down the Device:

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

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

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

16. Isolate NVR and IP Camera Network






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

General

This document mainly introduces installation and basic operation of IP audio indoor station.

Safety Instructions

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

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

Revision History

No.	Version	Revision Content	Release Date
1	V1.0.0	First release	2017.10.18
2	V1.0.1	Change size	2017.11.27
3	V1.0.2	Add privacy protection notice	2018.05.23

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 User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's 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 Guide (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.

Important Safeguards and Warnings

The following description is the correct application method of the device. Please read the document carefully before use, in order to prevent danger and property loss. Strictly conform to the document during application and keep it properly after reading.

Power Requirement

- Please modify user's default password timely after device deployment, in order to prevent embezzlement.
- Please don't place and install the device in an area exposed to direct sunlight or near heat generating device.
- Please don't install the device in a humid, dusty or fuliginous area.
- Please keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Please don't drip or splash liquids onto the device; don't put on the device anything filled with liquids, in order to prevent liquids from flowing into the device.
- Please install the device at well-ventilated places; don't block its ventilation opening.
- Use the device only within rated input and output range.
- Please don't dismantle the device arbitrarily.

Operating Requirement

- The product shall use electric wires (power wires) recommended by this area, which shall be used within its rated specification!
- Please use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, please refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, please keep an angle that facilitates operation.

Table of Contents

Cybersecurity Recommendations	II
Foreword	V
Important Safeguards and Warnings	VII
1 Product Overview	1
1.1 Front Panel	1
1.2 Rear Panel Interface.....	2
2 Device Installation	4
2.1 Before Installation	4
2.2 Installation	4
3 Device Debugging	6
3.1 Debugging Settings	6
3.1.1 VTO Debugging.....	6
3.1.2 VTH Debugging.....	14
3.2 Debugging Verification	20
4 Functional Operation	21
4.1 Function of Talk with Management Center.....	21
4.1.1 Call Management Center	21
4.1.2 Call from Management Center	21
4.2 Function of Talk with VTO.....	21
4.3 Unlock Function.....	21
4.4 DND Function.....	21
4.4.1 Enable DND	21
4.4.2 Disenable DND	22
4.5 Arm and Disarm.....	22
4.5.1 Arm	22
4.5.2 Disarm.....	22
4.6 Alarm Prompt and Uploading Function.....	22
5 FAQ	23
Appendix 1 Technical Parameter	24
Appendix 2 Packing List	25

1 Product Overview

1.1 Front Panel

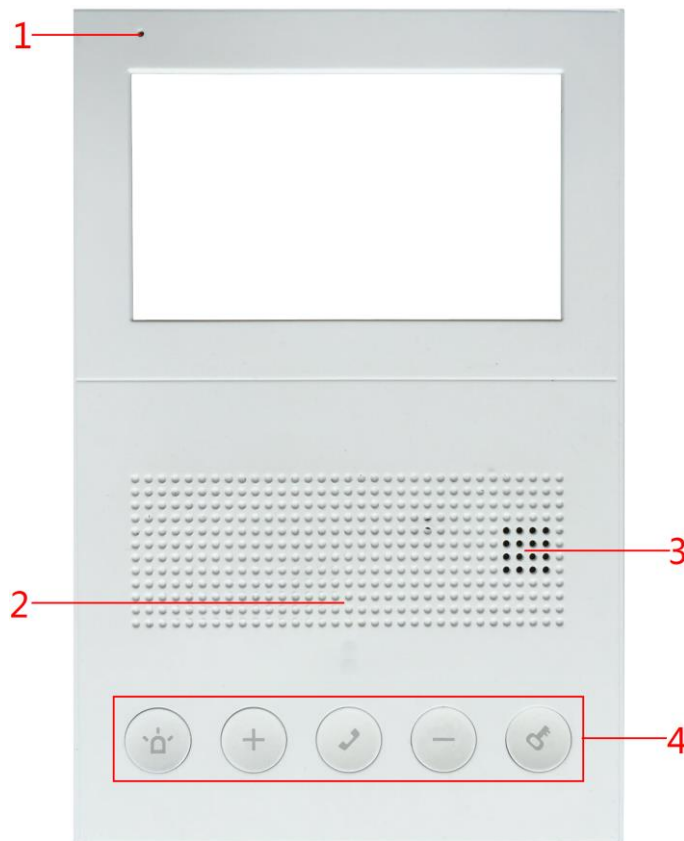





Figure 1-1

No.	Name	Description	
1	Microphone	Audio input.	
2	Concealed indicator light	<ul style="list-style-type: none">● Indicator light flashes: device deployment.● Indicator light is normally on: the device is in DND status.● Indicator light is off: the device is normal.	
3	Speaker	Audio output.	
4		SOS	Press this key to call Management Center at once.
		Plus Sign	<ul style="list-style-type: none">● In call status, press this key to increase talk volume.● In standby status, press this key to increase ring volume.
		Call	<ul style="list-style-type: none">● In case of incoming call, press this key to answer the call.● During talk, press this key to hang up.● In case of messages, in standby status, press this key to play





No.	Name	Description
		the messages.
	 Subtraction Sign	<ul style="list-style-type: none"> In call status, press this key to reduce talk volume. In standby status, press this key to reduce ring volume. In standby status, press this key to reduce main VTH volume to 0, and the device enters DND status.
	 Unlock	Press this key during talk, and the corresponding VTO unlocks.
	 Plus Sign+ Call Key	<ul style="list-style-type: none"> In standby status, press “Plus Sign+ Call Key” to arm and disarm. In disarmed status, press this combination key to arm. Indicator light flashes and the device beeps continuously. In armed status, press this combination key to disarm. Indicator light turns off and the device beeps twice.
	 Subtraction Sign+ Call Key	<ul style="list-style-type: none"> In standby status, press “Subtraction Sign+ Call Key” to switch rings.

Table 1-1

1.2 Rear Panel Interface

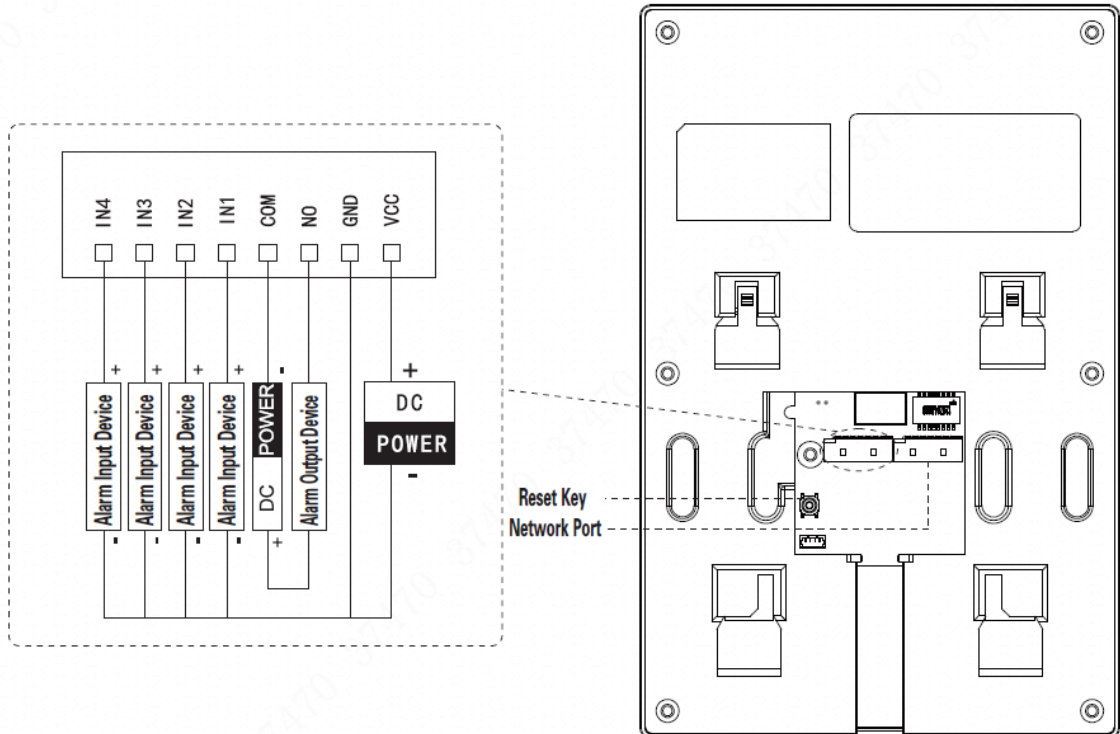


Figure 1-2

Reset Key

Press this key shortly to carry out voice broadcast of present IP address.
Press it for 5s, and the device restores factory defaults.

Network Port

Provide network communications and power supply function.

2 Device Installation

2.1 Before Installation

- Engineering installation and debugging shall be implemented by professional teams. In case of device faults, please don't dismantle or repair by yourself; please contact our after-sales department.
- Try not to install VTH in poor environment, such as condensation, high-temperature, stained, dusty, chemically corrosive or direct sunlight environment.
- In case of any abnormality after insertion of network cable and power on, please unplug the network cable to cut off power supply at once. Connect power supply again after troubleshooting.

2.2 Installation



It is suggested that installation height of device central point shall be 1.4cm~1.6cm above the ground.

Step 1 Drill holes in the wall according to hole positions of the installation bracket.

Step 2 Fix installation bracket directly onto the wall with M4×30 screws.

Step 3 Fix the device onto installation bracket with snap joint.

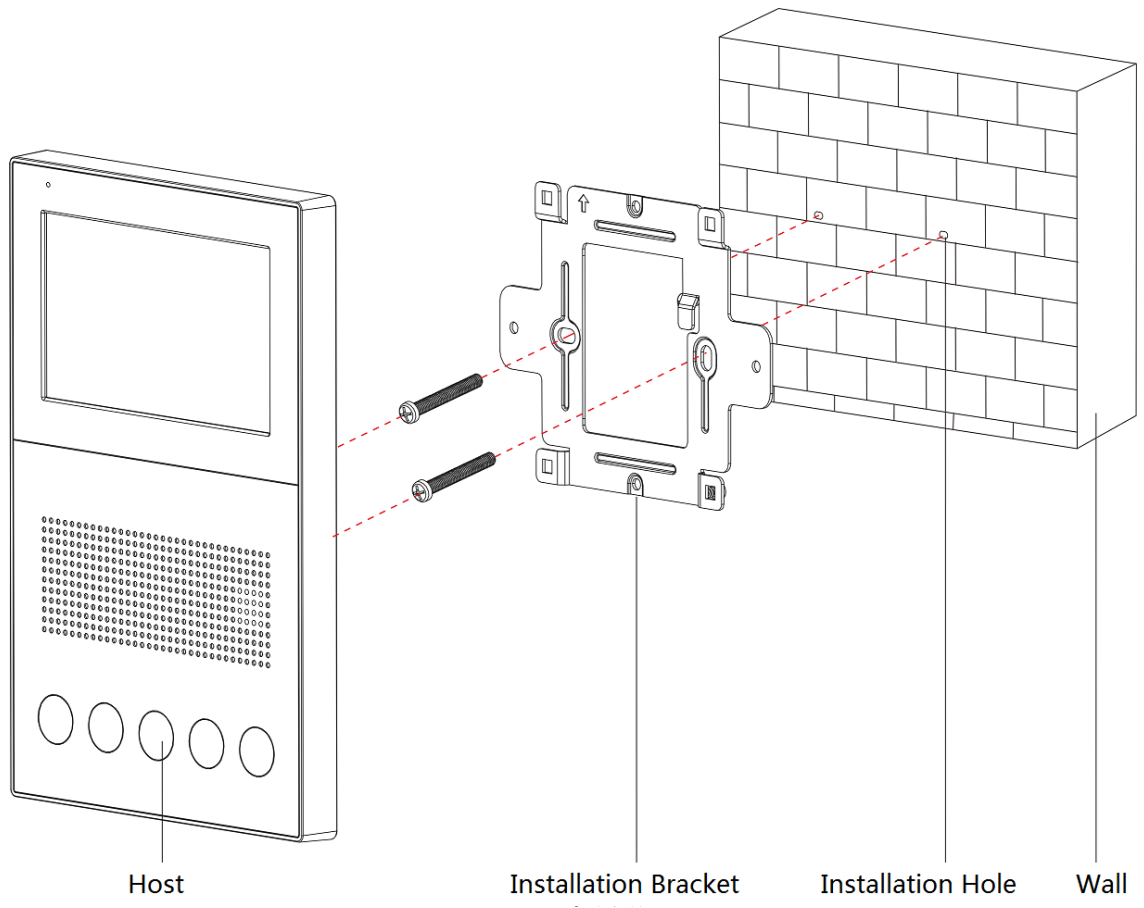


Figure 2-1

Carry out debugging to ensure that the device can realize basic network access, call and monitoring functions after installation. Before debugging, please check whether the following work has been completed.

- Check whether there is short circuit or open circuit. Power on the device only after the circuit is confirmed to be normal.
- Every device IP, VTO and VTH no. has been planned.

3.1 Debugging Settings

- This device is used with VTO of SIP system.
- Every VTO and VTH in the network shall be debugged.

3.1.1 VTO Debugging

3.1.1.1 WEB Interface Initialization

For the first time, please initialize and modify login password.

 Note

Please ensure that default IP addresses of PC and VTO are in the same network segment.

Default IP address of VTO is 192.168.1.110.

Step 1 Connect VTO power and boot up.

Step 2 Enter default IP address of VTO at the address bar of PC browser.

The system displays “Setting” interface, as shown in Figure 3-1.

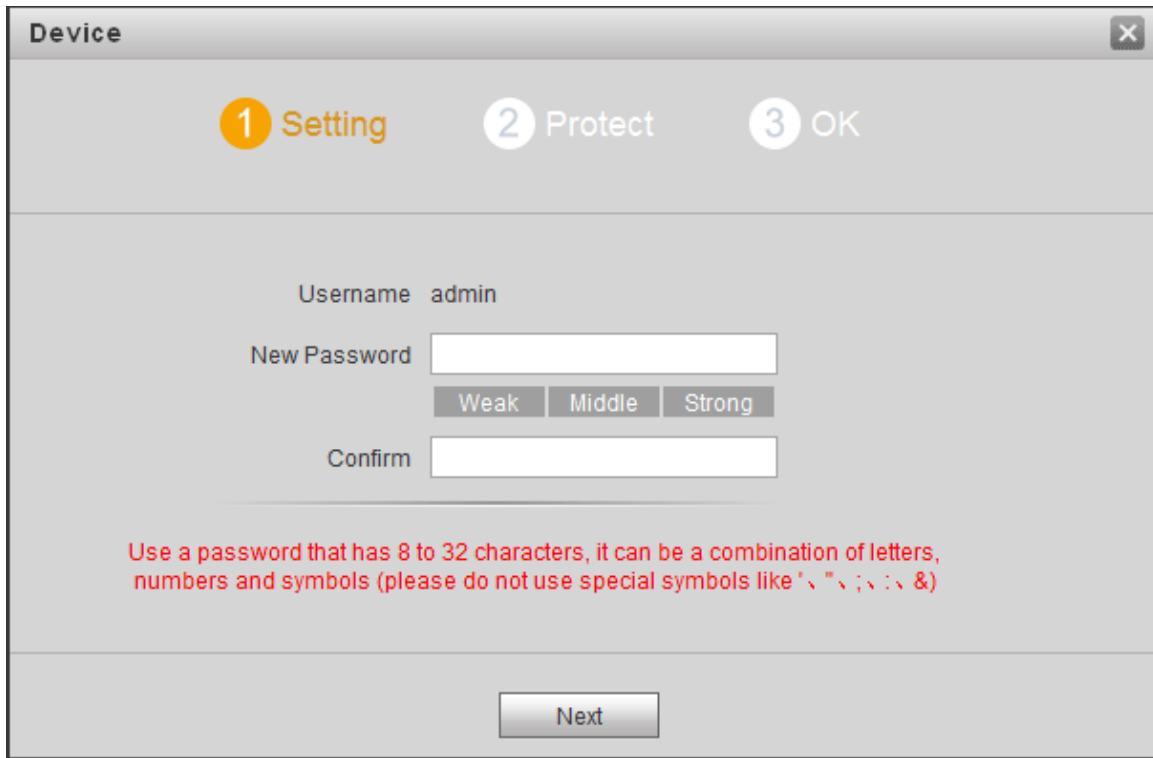


Figure 3-1

Step 3 Enter “New Password” and “Confirm”, and click “Next”.

The system displays “Protect” interface, as shown in Figure 3-2.

 Note

This password is used to login WEB interface. It shall be at least 8 characters, and shall include at least two types of number, letter and symbol.

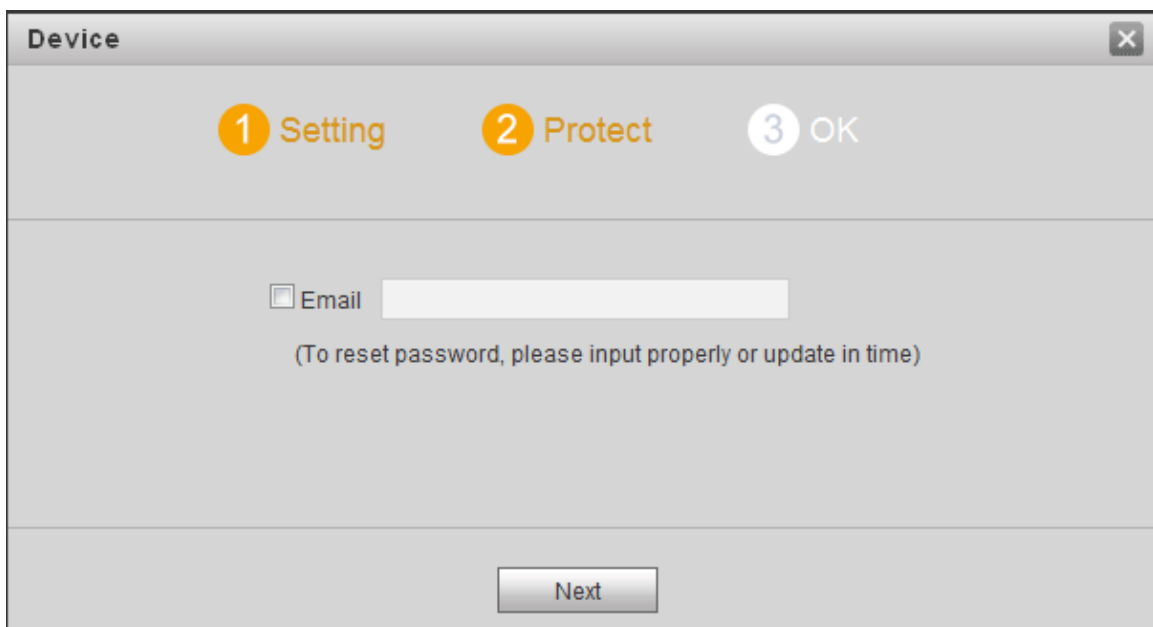


Figure 3-2

Step 4 Select “Email” and enter your Email address.

This Email address is used to reset the password, so it is recommended that it should be set.

Step 5 Click “Next”.

The system displays “OK” interface, as shown in Figure 3-3, and shows “Device

initialization succeeded!”

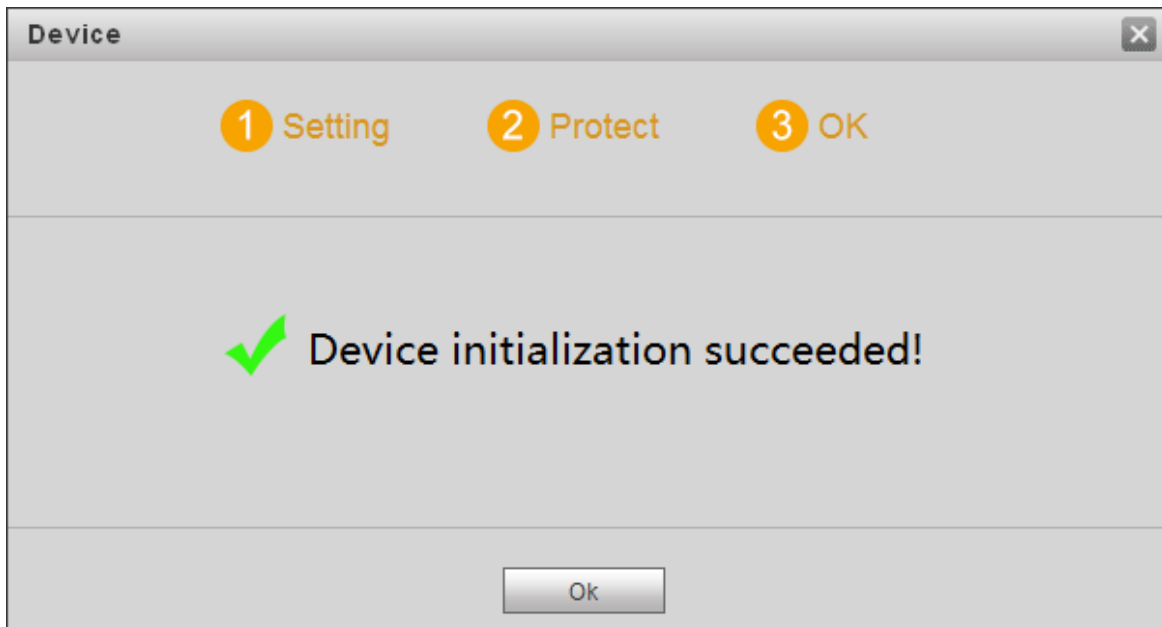


Figure 3-3

Step 6 Click “OK”.


The system displays WEB login interface, as shown in Figure 3-4.



Figure 3-4

Step 7 Enter user name and password, and click “Login”.

Log in the WEB interface of the device.

 Note

- Default user name is admin.
- Password is the one set during initialization.

3.1.1.2 Modify IP Address of the Device

Modify default IP address of VTO to the planned IP address, and connect it into the network.

Step 1 Select “System Config> Network Config> Network Config”.

The system displays “Network Config” interface, as shown in Figure 3-5.

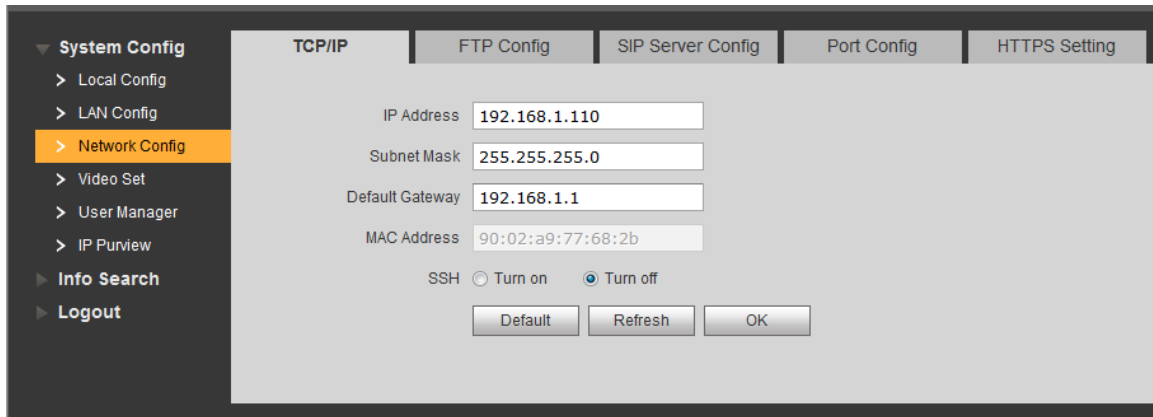


Figure 3-5

Step 2 Enter the planned “IP Address”, “Subnet Mask” and “Default Gateway”, and click “OK”. After modification is completed, VTO reboots automatically, while the following two cases occur at WEB interface.

- If PC is in the planned network segment, WEB interface jumps to new IP login interface automatically.
- If PC is not in the planned network segment, the webpage cannot be displayed. Please enter a new IP address in the browser.

3.1.1.3 LAN Config

Configure server type and number.

Step 1 Log in WEB interface again.

Step 2 Select “System Config> LAN Config”.

The system displays “LAN Config” interface, as shown in Figure 3-6.

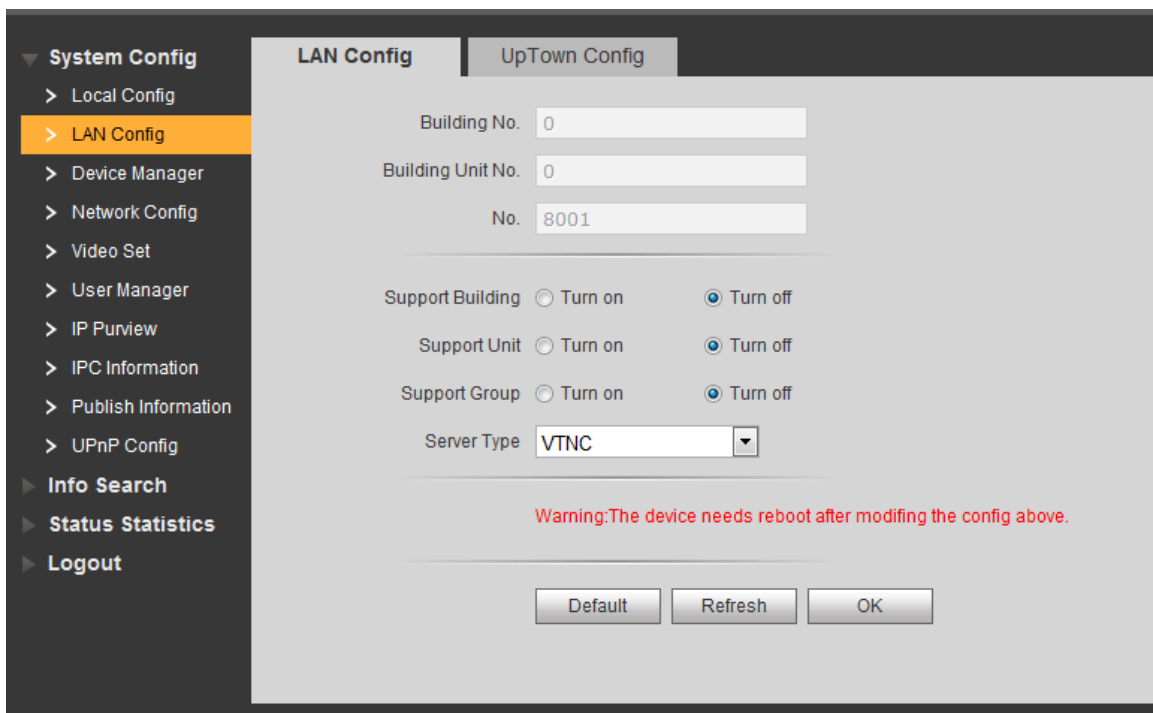


Figure 3-6

- This VTO or other VTO works as SIP server
Select “Server Type” to be “VTO”, and click “OK” to save configurations.



To support group call, tick “Enable”. After enabling group call, the device will reboot and put it into effect.

- Platform (VTSS5000) works as SIP server
Select “Server Type” to be “VTSS5000”, and click “OK” to save configurations.



- To set “Building No.” and “Building Unit No.”, please turn on “Support Building” and “Support Unit” functions.
- To “Support Group Call”, please turn on “Support Group Call” function. The device will reboot and put it into effect.

3.1.1.4 SIP Server Config

Configure SIP server info.

Select “System Config> Network Config> SIP Server Config”. The system displays “SIP Server Config” interface, as shown in Figure 3-7.

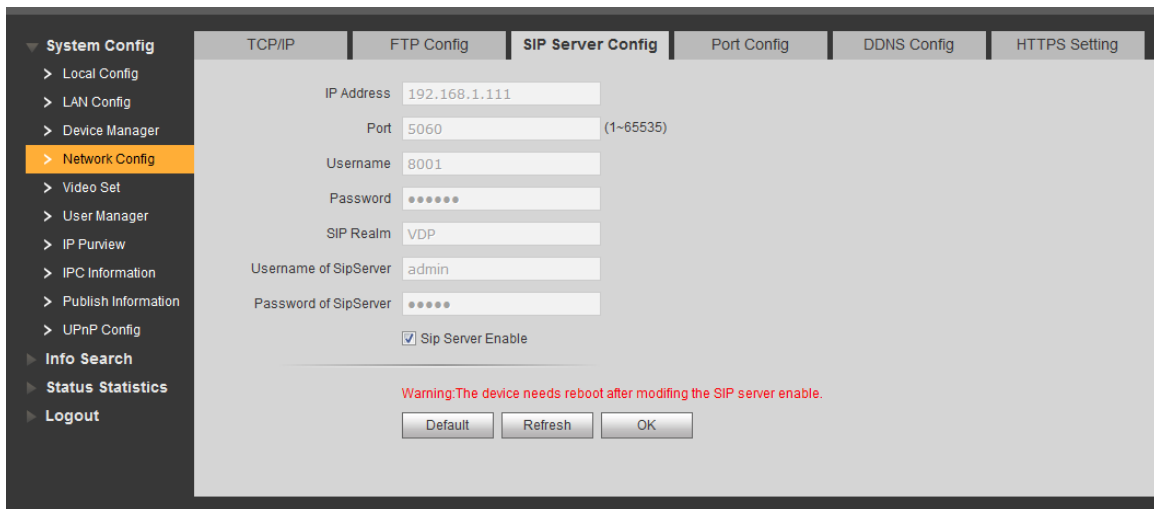


Figure 3-7

- This VTO works as SIP server
Tick “Sip Server Enable” and click “OK” to save the configuration. VTO reboots automatically, and WEB interface jumps to login interface.
- Other VTO or platform works as SIP server
Configure the parameters and refer to Table 3-1 for details. Click “OK” to save the configuration. VTO reboots automatically, and WEB interface jumps to login interface.

Parameter	Description
IP Address	<ul style="list-style-type: none"> When VTO works as SIP server, this is IP address of the VTO. When the platform works as SIP server, this is IP address of the platform.
Port	<ul style="list-style-type: none"> When VTO works as SIP server, default value is 5060. When the platform works as SIP server, port is 5080.
Username	Use the default values.
Password	

Parameter	Description
SIP Realm	<ul style="list-style-type: none"> When VTO works as SIP server, SIP realm shall be VDP. When the platform works as SIP server, SIP realm can be null, or remain default value.
Username of Sip Server	Username and password to log in SIP server.
Password of Sip Server	

Table 3-1



- If the platform or other VTO works as SIP server, VTO debugging configuration has been completed.
- If this VTO works as SIP server, “Device Manager” will appear in the left parameter tab. VTO and VTH shall be added. For details, please refer to “Add VTO” and “3.1.1.6 Add VTH”.

3.1.1.5 Add VTO

Add all VTO info.



Caution

VTO shall be added only when this VTO works as SIP server.

Step 1 Log in WEB interface again.

Step 2 Select “System Config> Device Manager>Outdoor Station Manager”.

The system displays “Outdoor Station Manager” interface, as shown in Figure 3-8.

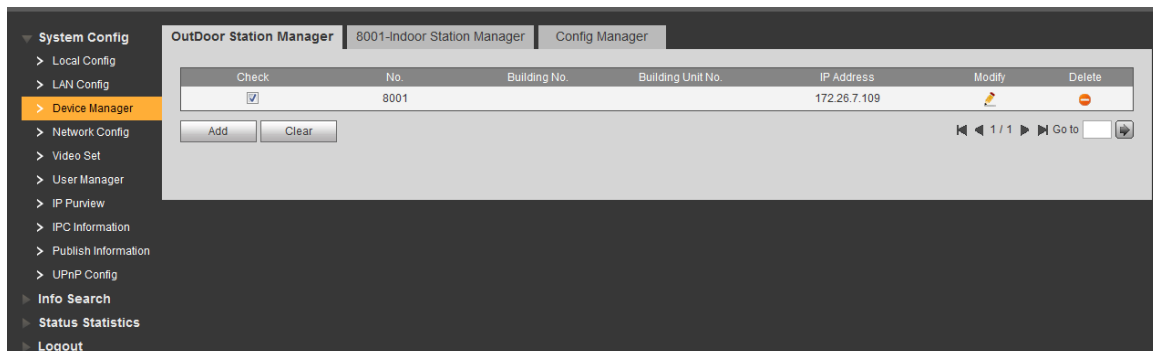


Figure 3-8

Step 3 Click “Add”.

The system displays “Add” interface, as shown in Figure 3-9.

Figure 3-9

Step 4 Configure VTO parameters. Please refer to Table 3-2.

Parameter	Description
No.	VTO number.
Register Password	It is used during signaling interaction of SIP system. Use the default value.
IP Address	IP address of VTO.
Username	Username and password to login WEB interface of this VTO.
Password	

Table 3-2

Step 5 Click “OK” to complete adding.

According to above operation, add info about VTO in the network in sequence.

3.1.1.6 Add VTH

Add all VTH info.



Caution

1. VTH shall be added only when this VTO works as SIP server.
2. When there are main VTH and extension VTH, both shall be added.

Step 1 Select “System Config> Device Manager>8001-Indoor Station Manager”.

The system displays “8001-Indoor Station Manager” interface, as shown in Figure 3-10.

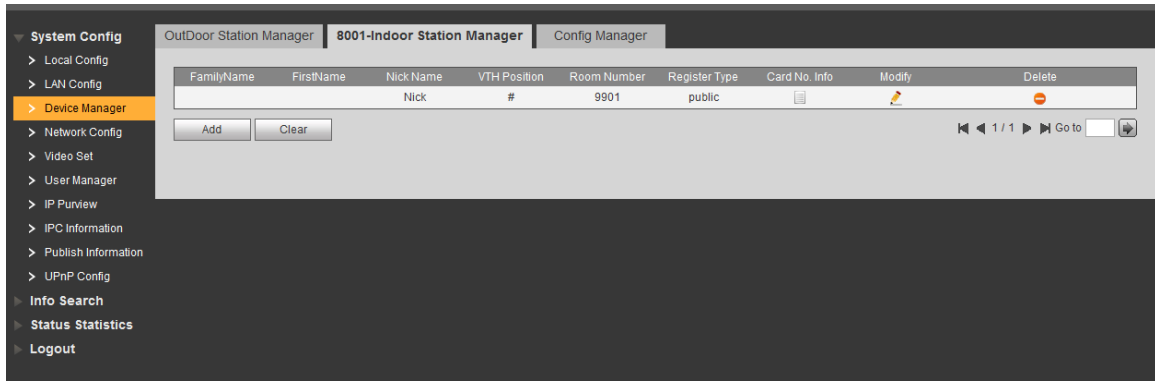


Figure 3-10

Step 2 Click “Add”.

The system displays “Add” interface, as shown in Figure 3-11.

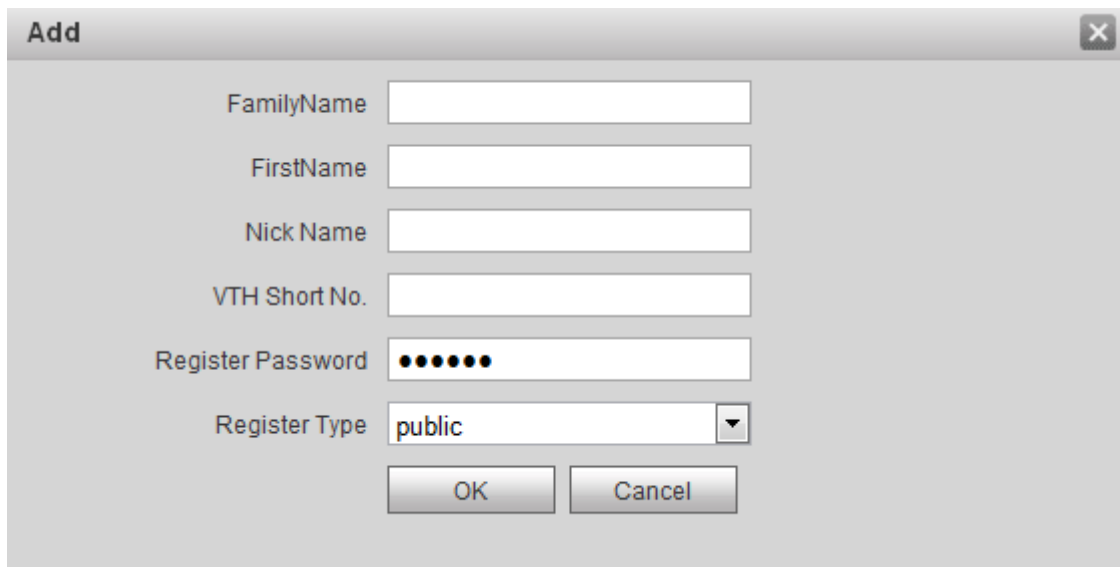


Figure 3-11

Step 3 Configure VTH parameters. Please refer to Table 3-3.


Parameter	Description
Family Name	Configure VTH username and nick name, just to distinguish them.
First Name	
Nick Name	
VTH Short No.	Configure VTH room number.  Note VTH short no. is consistent with room no. on VTH device. Sub-VTH is represented with “-”. For example, main VTH is 9901, sub-VTH is 9901-1, 9901-2 and so on.
Register Password	It is used during signaling interaction of SIP system. Use the default value.
Register Type	

Table 3-3

Step 4 Click “OK” to complete adding.

According to above operation, add info about VTH in the network in sequence.

3.1.2 VTH Debugging

VTH shall be debugged with VDPconfig tool.

 Note

Please ensure that default IP addresses of PC and VTH are in the same network segment.
Default IP address of VTO is 192.168.1.110.

Step 1 Search the device.

1. In VDPConfig tool, click “ >  Search setting ”.

The system displays “Setting” interface, as shown in Figure 3-12.

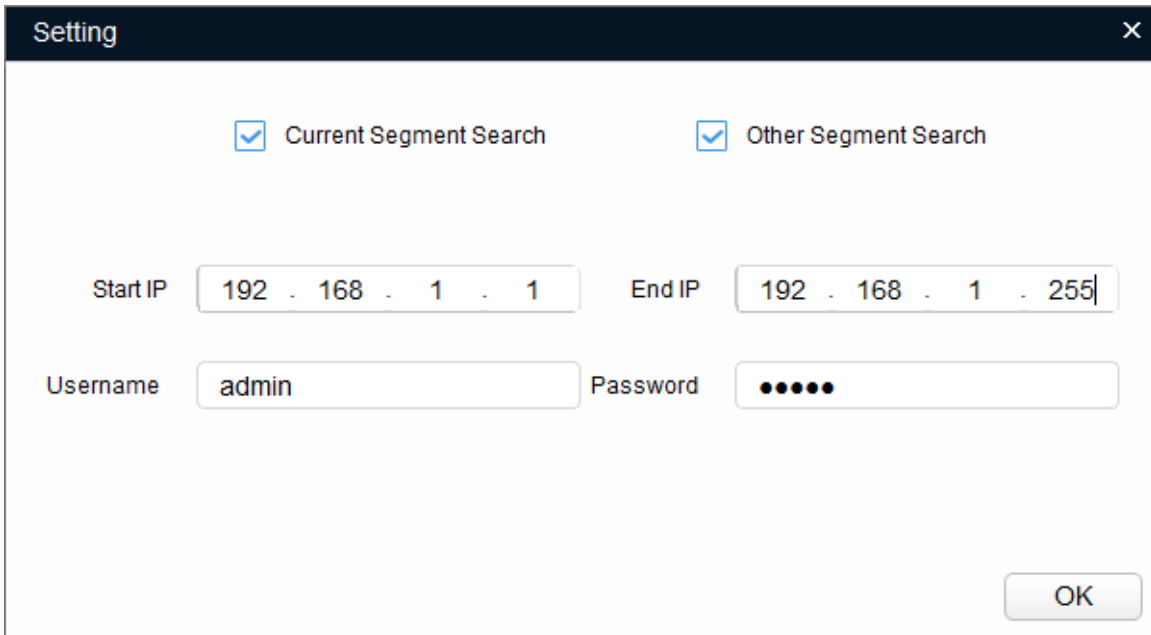


Figure 3-12

2. Select the search mode according to actual conditions.
 - ◇ Current segment search: tick “Current Segment Search”, set “Username” and “Password”, so the system searches devices in current segment. Default setting is “Current Segment Search”.
 - ◇ Other segment search: tick “Other Segment Search”, set “Start IP”, “End IP”, “Username” and “Password”, so the system searches devices in the set segment.

 Note

- By ticking “Current Segment Search” and “Other Segment Search” at the same time, the system searches devices in current segment and the set segment at the same time.
 - “Username” and “Password” refer to the username and password to log in the device when modifying IP, configuring system parameter info and upgrading the device.
3. Click “OK” to search the device.
On completion, the system displays the found devices, as shown in Figure 3-13.

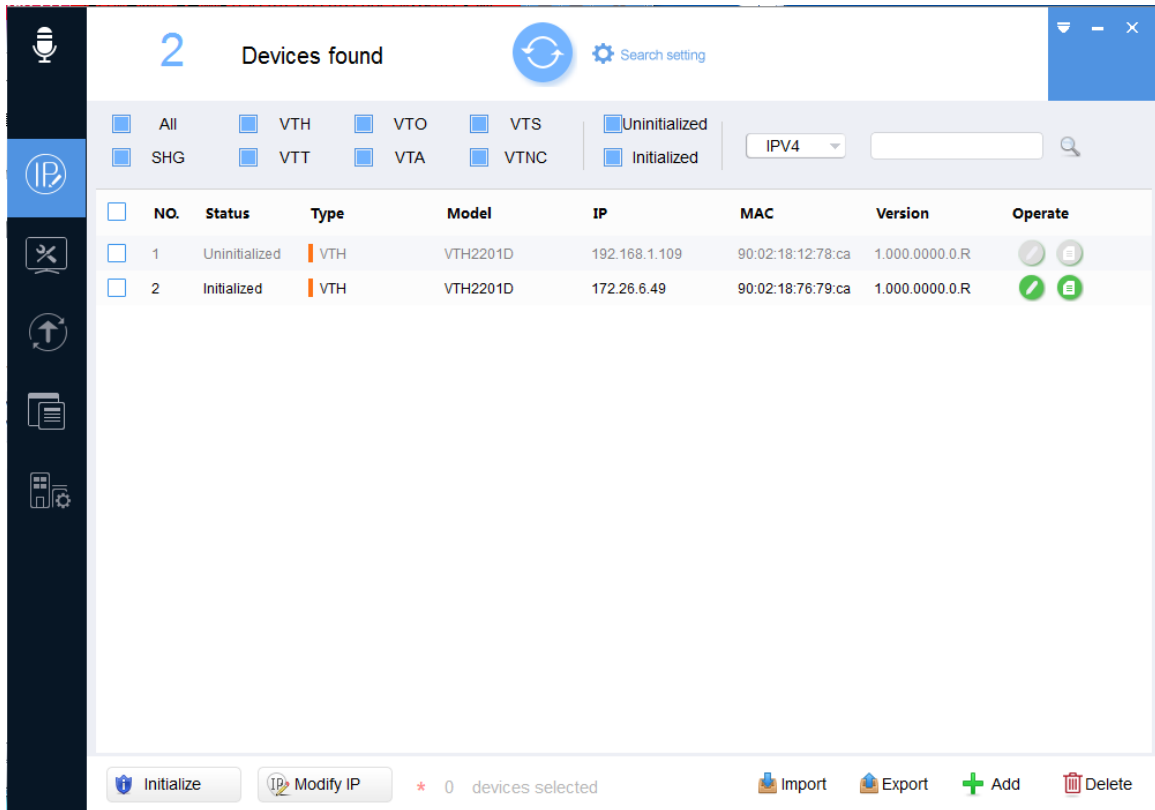


Figure 3-13

Step 2 Device initialization.

1. Select devices that have not been initialized.

2. Click  Initialize.

The system displays "Device Initialization" interface, as shown in Figure 3-14.

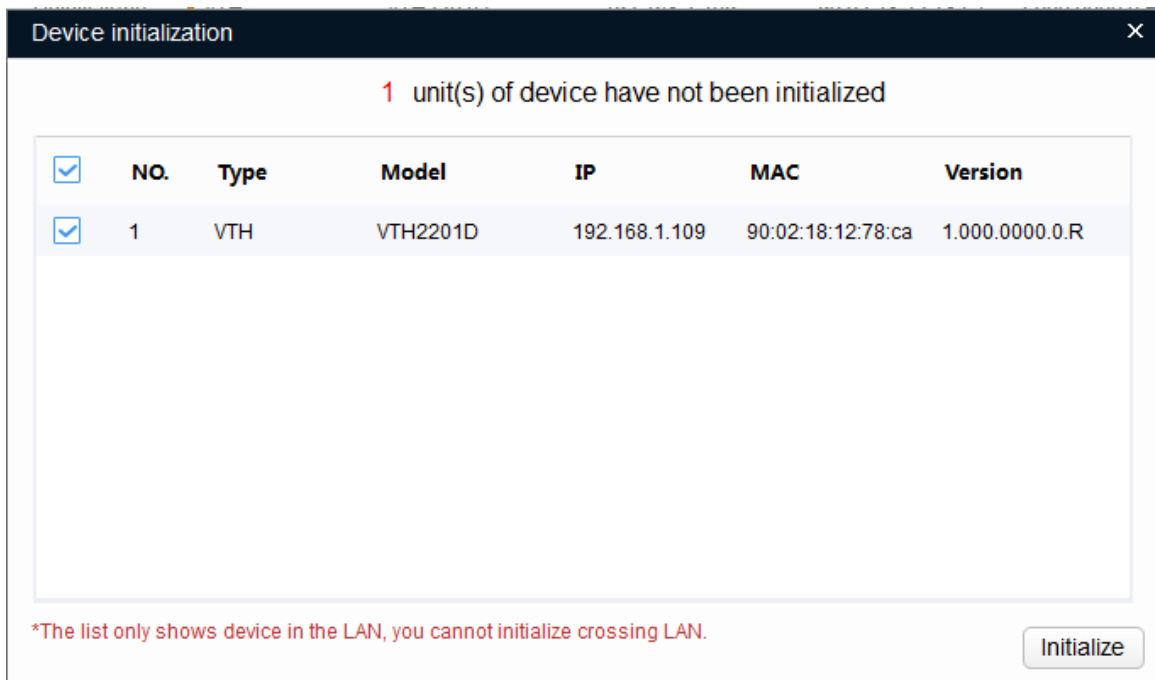


Figure 3-14

3. Select the device that shall be initialized, and click "Initialize".

The system displays "Device Initialization" interface, as shown in Figure 3-15.

Figure 3-15

4. Configure device initialization parameters. Please refer to Table 3-4 for details.

Parameter	Description
Username	Default username is admin.
New Password	Enter new password of the device, which consists of 6 numbers.
Confirm Password	Confirm the new password.
Email Address	It is ticked by default. This Email address will be used to reset the password.

Table 3-4

5. Click "Initialize".
The system displays "Auto-check" interface, as shown in Figure 3-16.

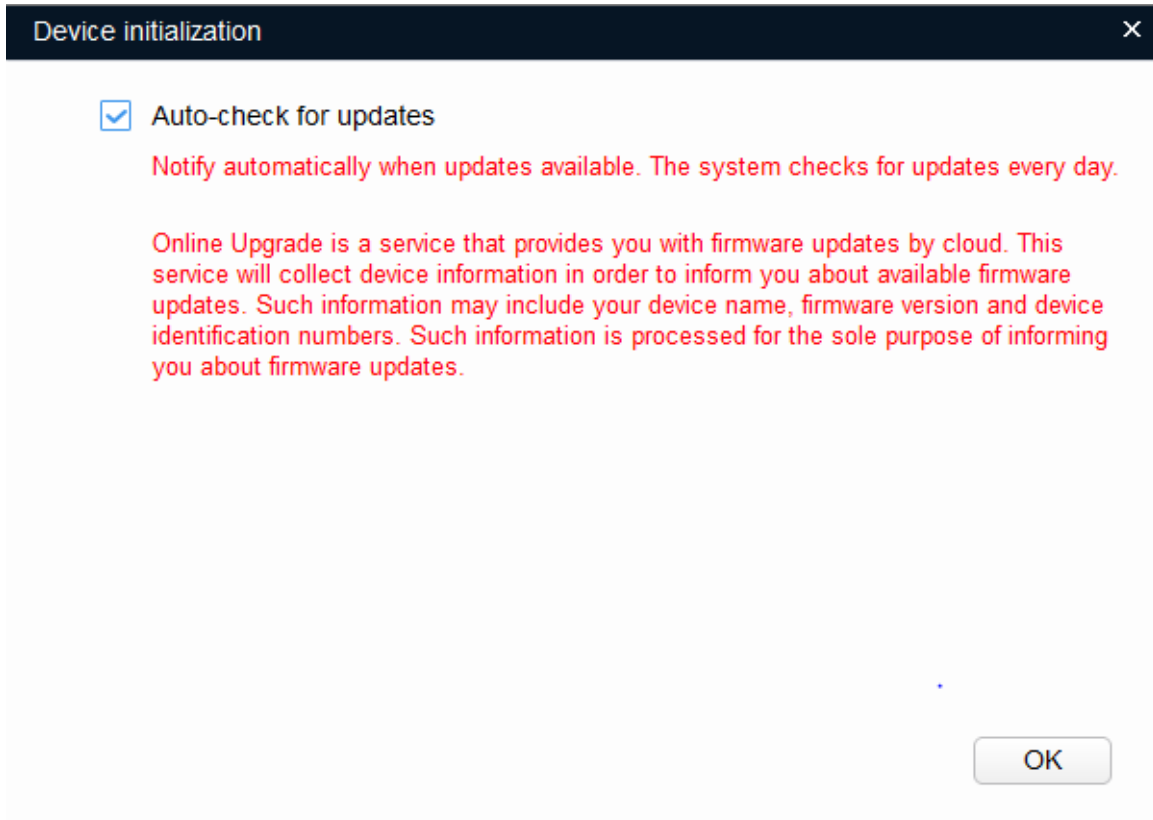


Figure 3-16

6. Use the default settings; click “OK” to start initialization. On completion, the system displays Figure 3-17.
 - ✓ will be displayed if initialization succeeded and ⚠ will be displayed if initialization failed. Click the icon to view details.

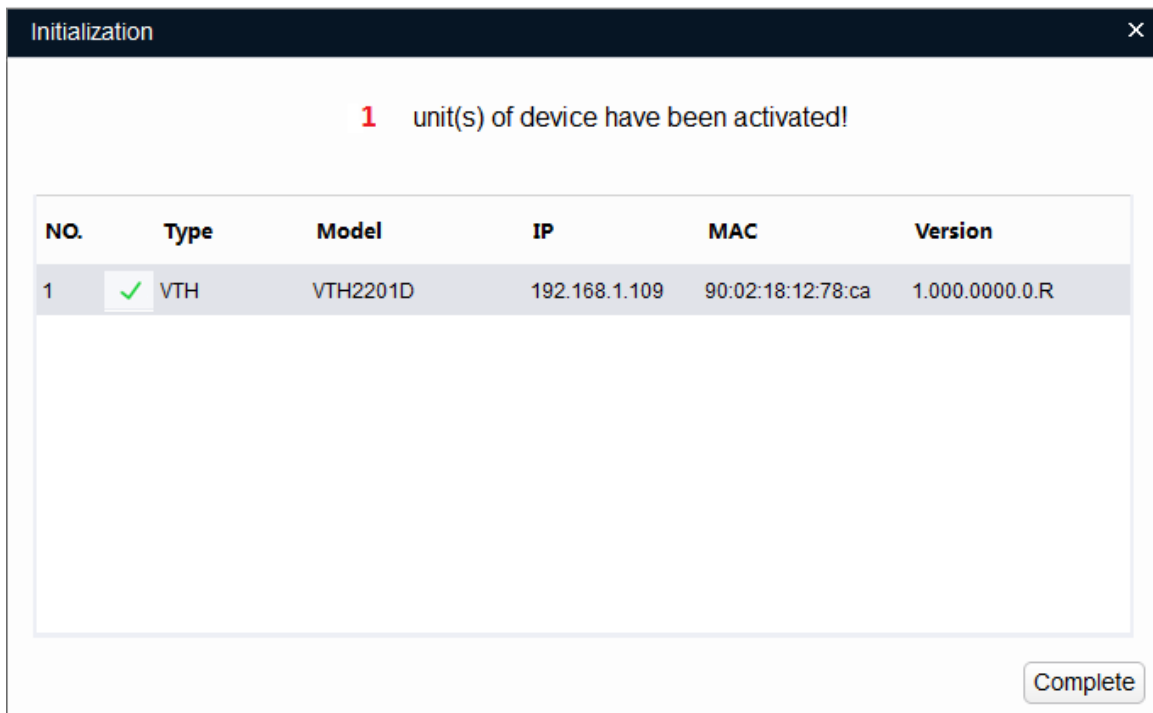


Figure 3-17

7. Click “Complete” to complete device initialization. On completion, device status on the main interface has turned into “Initialized”. Device info will be displayed at other interfaces of the tool.

Step 3 Configure SIP server.

1. Click “ > Config”.

The system displays “Config” interface, as shown in Figure 3-18.

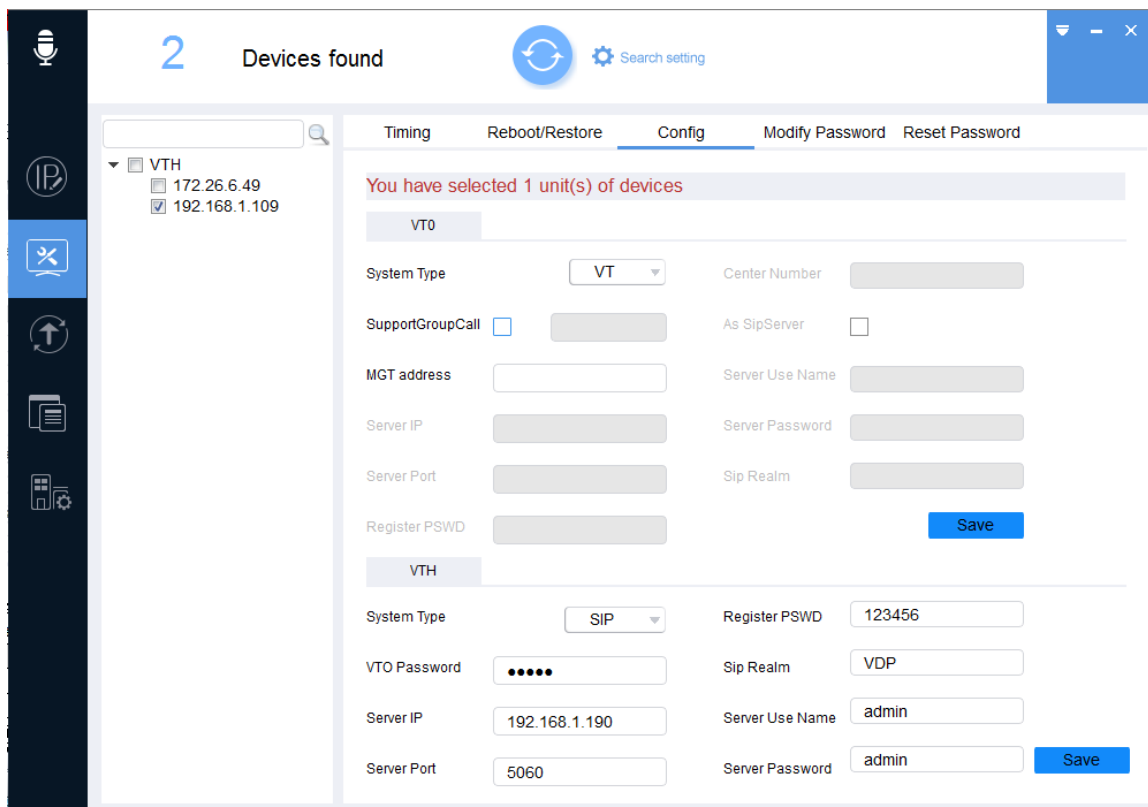


Figure 3-18

2. In the organization tree in the left, select IP of the device to be configured.
3. Configure SIP server parameters in the right VTH. Please refer to Table 3-5 for details.

Parameter	Description
System Type	Select “SIP”.
Register PSWD	Default password is 123456. It shall be consistent with register password set when adding the device on SIP server.
VTO Password	Password to log in VTO WEB interface.
Sip Realm	<ul style="list-style-type: none"> • When VTO works as SIP server, realm name shall be VDP. • When the platform works as SIP server, realm name can be null, or keep default value.
Server IP	IP address of SIP server.
Port	<ul style="list-style-type: none"> • When VTO works as SIP server, port is 5060. • When the platform works as SIP server, port is 5080.

Table 3-5

4. Click “Save” to save configurations.

Step 4 Import corresponding relation info of VTO and VTH.

1. Click .

The system displays “Project Configuration” interface, as shown in Figure 3-19.

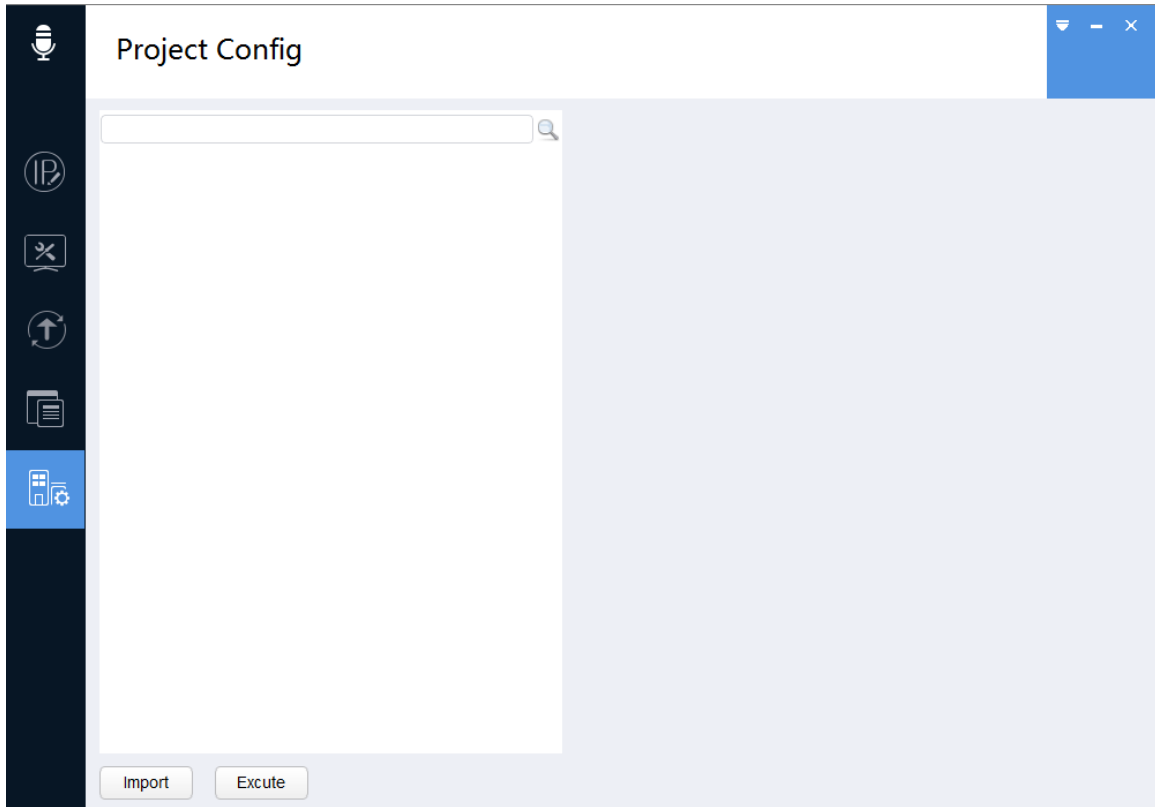


Figure 3-19


2. Click “Import” to select files.


File template in the installation directory is named Project1. Please obtain it in advance, add VTO and VTH info according to template format requirements.

 Note

IP address, gateway and subnet mask in the template shall be filled according to network planning. After importing and matching successfully, the system will modify IP address of the device according to the filled content.

3. In Project1 organization tree, select the device and click “Match”.

If  appears after device IP, it means that matching has succeeded, as shown in Figure 3-20.

If  appears after device IP, it means that matching has failed. Please click

 to look for reasons.

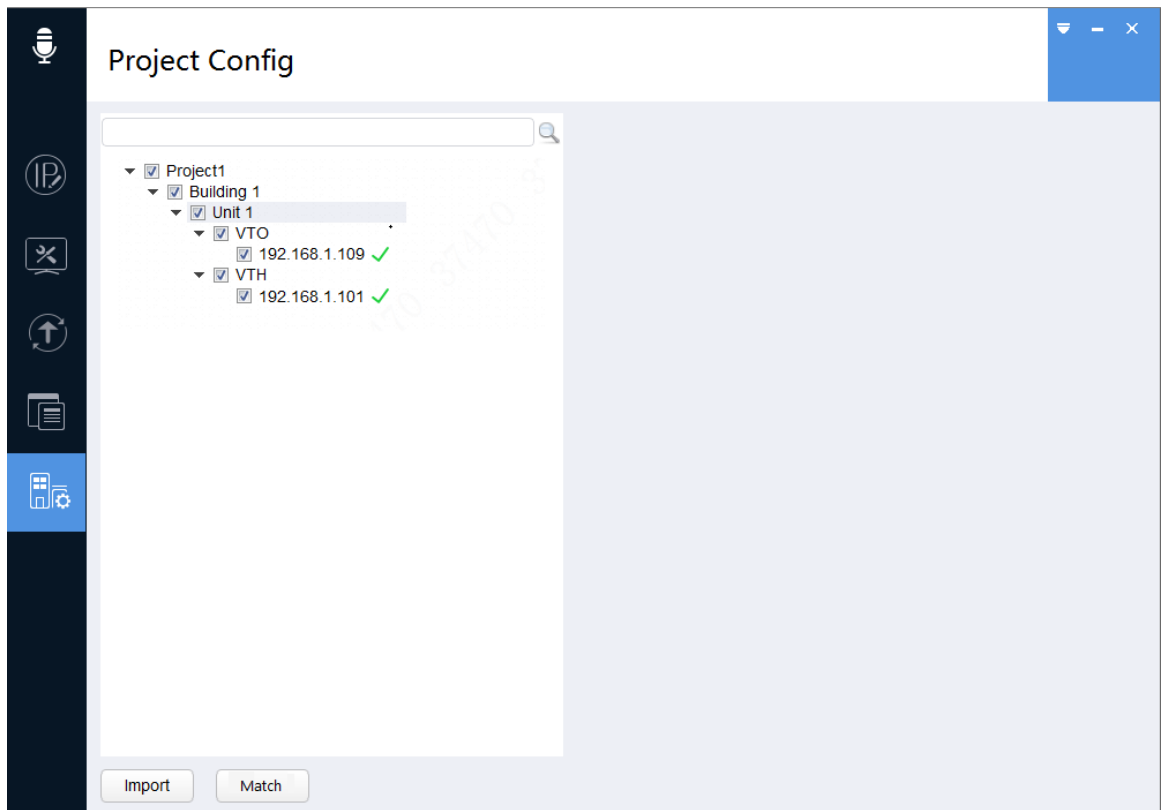


Figure 3-20

3.2 Debugging Verification

Please refer to “4.1 Function of Talk with Management Center”, “4.2 Function of Talk with VTO” and “4.3 Unlock Function”; verify whether VTH debugging has succeeded.

4

Functional Operation

4.1 Function of Talk with Management Center

4.1.1 Call Management Center

Press SOS key on the front panel in any status, and the VTH switches to call Management Center at once.

If calls get through, VTH sends out beep sound, which is ringback tone.

In case of failure, press SOS key on the front panel to finish calling.

4.1.2 Call from Management Center

When Management Center calls VTH, VTH rings. Press “Call Key” on the front panel to pick up the call and talk with each other. Press “Call Key” again to hang up.

4.2 Function of Talk with VTO

When VTO calls VTH, VTH rings. Press “Call Key” on the front panel to pick up the call and talk with each other. Press “Call Key” again to hang up.

4.3 Unlock Function

During talk with VTO, press “Unlock key” on the front panel, to realize remote unlock function of VTO.

4.4 DND Function

After DND function is enabled, VTO cannot call VTH.

4.4.1 Enable DND

In standby status, press subtraction sign. When main VTH volume is reduced to 0, the device enters DND status, while the indicator light is normally on.

4.4.2 Disenable DND

In standby status, press plus sign to increase volume and remove DND manually. In standby status, if main VTH volume is not 0, the device exits DND status, and the indicator light turns off.

4.5 Arm and Disarm

4.5.1 Arm

In disarm status, press “Plus Sign+ Call Key” to arm. The indicator light flashes and the device beeps continuously.

4.5.2 Disarm

In arm status, press “Plus Sign+ Call Key” to disarm. The indicator light turns off and the device beeps twice.

4.6 Alarm Prompt and Uploading Function

The device is able to connect 4 zones at most; the 1st one to the 4th one is SOS button, gas, smoke detector and IR light. In case that any one of 4 zones triggers alarm in arm status, the device will send out alarm ring, and upload the alarm info to Management Center. Meanwhile, the linked alarm output device will output alarm prompts.

 Note

Alarm ring lasts for 15s at most, and the volume is not adjustable.

Q: Fail to call VTH. How to deal with it?

A: Please check whether network cable is inserted well; confirm whether corresponding unit VTO works normally.

Q: VTH doesn't ring when VTO calls. How to deal with it?

A: Please check whether DND function has been enabled.

Q: How to deal with problems that are not confirmed or cannot solved?

A: Please consult professional technical support.

Appendix 1 Technical Parameter

Parameter		Description
Audio	Input	1 microphone input.
	Output	1 speaker output.
Mechanical Key		5 mechanical keys: SOS, plus sign, call, subtraction sign and unlock.
Alarm	Alarm Input	4 channels.
	Alarm Output	1 channel.
Installation		Installation with bracket.
Specification	Power Supply	DC 12V.
	Power Consumption	1W in standby status and at most 4W.
	Device Dimension	192 mm×125 mm×15mm.
	Working Environment	-10℃~+55℃.

Packing List

The following devices and documents are included in the packaging box. Please check earnestly when opening the box and keep them properly.

Name	Quantity	Note
<input type="checkbox"/> Main Device	1 unit	
<input type="checkbox"/> Quick Start Guide	1 guide	
<input type="checkbox"/> Installation Screw	1 bag	
<input type="checkbox"/> Flexible Flat Cable	2 cables	
<input type="checkbox"/> Bracket	1 bracket	