Intercom Modular Outdoor Station

DHI-VTO4202F Series

User's Manual

V1.0.2

Foreword

General

This manual offers reference material and general information about the basic operation, maintenance, and troubleshooting for a Dahua security device. Read, follow, and retain the following safety instructions. Heed all warnings on the unit and in the operating instructions before operating the unit. Keep this guide for future reference.

Safety Instructions

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

Signal Words	Meaning
WARNING	Indicates a medium or low potential hazard that, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk that, if not avoided, could result in property damage, data loss, lower performance, or unpredictable results.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	January 2019
2	V1.0.1	Revised for North America	July 2019
3	V1.0.3	Minor Formatting and Typographical Corrections	June 2021

Privacy Protection Notice

As the device user or data controller, you may collect personal data such as face images, fingerprints, license plate number, email address, phone number, GPS location and other sensitive or private information. You must ensure that your organization complies with local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures including but not limited to providing clear and visible identification to inform data subjects of the existence of surveillance area and providing related contact

About the Guide

- This user guide has been compiled with great care and the information it contains has been thoroughly reviewed and verified.
- The text was complete and correct at the time of printing. This guide may be periodically updated to reflect changes to the product or to correct previous information and the content of this guide can change without notice.
- If you encounter an error or have, any questions regarding the contents of this guide, contact customer service for the latest documentation and supplementary information.
- Dahua accepts no liability for damage resulting directly or indirectly from faults, incompleteness, or discrepancies between this guide and the product described. Dahua is not liable for any loss caused by installation, operation, or maintenance inconsistent with the information in this guide.
- All the designs and software are subject to change without prior written notice. The product updates may cause some differences between the actual product and the Guide. Contact the customer service for the latest program and supplementary documentation.
- Video loss is inherent to all digital surveillance and recording devices; therefore, Dahua cannot be held liable for any damage that results from missing video information. To minimize the occurrence of lost digital information, Dahua recommends multiple, redundant recording systems, and adoption of backup procedures for all data.
- All trademarks, registered trademarks and the company names in the Guide are the properties of their respective owners.
- Please visit our website, contact the supplier, or customer service if a problem occurs when using the device.
- Contact the supplier or customer service if you encounter any issues while using this unit.

Important Safeguards and Warnings

This chapter describes the contents covering proper handling of the device, hazard prevention, and prevention of property damage. Read these contents carefully before using the device, comply with them when using, and keep it for future reference.

Installation and Maintenance Professionals Requirements

- All installation and maintenance professionals must have adequate qualifications or experiences to install and maintain CCTV systems and electric apparatus. The professionals must have the following knowledge and operation skills:
- Basic knowledge and installation of CCTV systems.
- Basic knowledge and operation skills of low voltage wiring and low voltage electronic circuit wire connection.
- Basic knowledge and operation skills of electric apparatus installation and maintenance in hazardous sites.

Power Requirements

- Install the unit in accordance with the manufacturer's instructions and in accordance with applicable local codes.
- All installation and operation must conform to your local electrical safety codes.
- Do not overload outlets and extension cords, which may cause fire or electrical shock.
- Do not place the camera near or in a place where the camera may contact overhead power lines, power circuits, or electrical lights.
- Ensure power conforms to SELV (Safety Extra Low Voltage) and that the limited power source is rated AC 24V as specified in IEC60950-1. (Power supply requirement is subject to the device label).
- All input/output ports are SELV circuits. Ensure that SELV circuits are connected only to other SELV circuits.
- Ground the unit using the ground connection of the power supply to protect the unit from damage, especially in damp environments.
- Please install easy-to-use device for power off before installing wiring, which is for emergent power off when necessary.
- Protect the plug and power cord from foot traffic, being pinched, and its exit from the unit.
- Do not attempt to service the unit. Opening or removing covers may expose you to dangerous voltage or other hazards. Refer all servicing to qualified personnel.
- If the unit is damaged and requires service, unplug the unit from the main AC power supply and from the PoE supply and refer to qualified service personnel. Damage may include, but is not limited to:
  - ◇ The power supply cord or plug is damaged.
  - ◇ Liquid has spilled in or on the unit.
  - ◇ An object has fallen on the unit.
  - ◇ The unit has been dropped and the housing is damaged.
  - ◇ The unit displays a marked change in performance.
  - ◇ The unit does not operate in the expected manner when the user correctly follows the proper operating procedures.

- Ensure a service technician uses replacement parts specified by the manufacturer, or that have the same characteristics as the original parts. Unauthorized parts may cause fire, electrical shock, or other hazards. Dahua is not liable for any damage or harm caused by unauthorized modifications or repairs.
- Perform safety checks after completion of service or repairs to the unit.
- Use attachments and accessories only specified by the manufacturer. Any change or modification of the equipment, not expressly approved by Dahua, could void the warranty.
- Incorporate a readily accessible disconnect device in the building installation wiring for quick power disconnect to the camera.
- Dahua assumes no liability or responsibility for any fire or electrical shock caused by improper handling or installation.

Application Environment Requirements

- Please use the device within the allowed humidity (<95%RH) and altitude (<3000m).
- Transport, use, and store the unit within the specified temperature and humidity range.
- Do not place the unit in a wet, dusty, extremely hot or an extremely cold environment; and avoid environments with strong electromagnetic radiation or unstable lighting.
- Do not use the device in the corrosive environment such as high salt fog area (sea, beach and coastal area), acid gas environment and chemical plants.
- Do not use the device in applications with strong vibrations such as in boats and vehicles.
- Never push objects of any kind into this unit through openings as they may touch dangerous voltage points or cause a short circuit that may result in fire or electrical shock. Take care to not spill any liquid on the unit.
- If your installation environment is subjected to one of the conditions above, contact our sales staff to purchase cameras intended for the particular environment.
- Do not install the device near the place with heat source, such as radiator, heater, stove or other heating equipment, which is to avoid fire.
- Do not aim the lens at an intense radiation source (such as the sun, a laser, and molten steel for example) to avoid damage to the thermal detector.
- Use the factory default package or material with equal quality to pack the device when transporting.

Operation and Maintenance Requirements

- Do not touch the heat dissipation component of the unit. This part of the unit is hot and may cause a burn.
- Do not open or dismantle the device; there are no components that a user can fix or replace. Opening the unit may cause water leakage or expose components to direct light. Contact the manufacturer or a qualified service representative to service the camera or to replace a component, including the desiccant.
- Dahua recommends the use of a thunder-proof device in concert with the unit.
- Do not touch the CCD or the CMOS optic sensor. Use a blower to clean dust or dirt on the lens surface. Use a dry cloth dampened with alcohol and gently wipe away any dust on the lens.

- Use a dry soft cloth to clean the unit's housing. If the unit is particularly dusty, use water to dilute a mild detergent, apply the diluted detergent to a soft cloth, and then gently clean the device. Finally, use a dry cloth to wipe the unit dry. Do not use a volatile solvent like alcohol, benzene, or thinner; or use a strong detergent with abrasives, which may damage the surface coating or reduce the working performance of the unit.
- Do not touch or wipe a dome cover during installation; this cover is an optical device. Refer to the following methods clean the dome cover:
- Stained with dirt: Use an oil-free soft brush or blower to gently remove the dirt.
- Stained with grease or fingerprints: Use a soft cloth to wipe gently the water droplet or the oil from the dome cover. Then, use an oil-free cotton cloth or paper soaked with alcohol or detergent to clean the lens from the center of the dome to the outside edge. Change the cloth several times to ensure the dome cover is clean.

 WARNING

- Modify the default password after login.
- Use attachments and accessories only specified by the manufacturer. Any change or modification of the equipment, not expressly approved by Dahua, could void the warranty.
- Internal and external ground connection should be stable.
- Do not supply power via the Ethernet connection (PoE) when power is already supplied via the power connector.
- Disconnect power before device maintenance and overhaul. It is prohibited to open the cover with power on in an explosive environment.
- Please contact the local dealer or the nearest service center if the device fails to work normally, please do not dismantle or modify the device.

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

- Change Passwords and Use Strong Passwords
  - ◇ The number one reason systems are “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 eight characters and a combination of special characters, numbers, and upper and lower case letters.
- 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.

Recommendations to improve your network security

- Change Passwords Regularly
  - ◇ The length should be greater than 8 characters;
  - ◇ Include at least two types of characters; character types include upper and lower case letters, numbers, and symbols;
  - ◇ Do not use an account name or the account name in reverse order;
  - ◇ Do not use sequential characters, such as 123, abc, etc.;
  - ◇ Do not use repeated characters, such as 111, aaa, etc.;
- 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 and 65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.
- Update Firmware and Client Software
  - ◇ Keep your network-enabled equipment (such as NVRs, DVRs, IP cameras, 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.
  - ◇ Download and use the latest version of client software.
- Enable HTTPS/SSL
  - ◇ Set up an SSL Certificate and enable HTTPS to encrypt all communication between your devices and recorder.
- Enable IP Filter
  - ◇ Enable the IP filter to prevent unauthorized access to the system.
- Change ONVIF Password
  - ◇ Older IP camera firmware does not automatically change the ONVIF password when the system credentials are changed. Update the camera’s firmware to the latest revision or manually change the ONVIF password.

- Forward Only Ports You Need
  - ◇ Forward only the HTTP and TCP ports that are requited. Do not forward a wide range of numbers to the device. Do not DMZ the device's IP address.
  - ◇ Do not forward any ports for individual cameras if they are all connected to a recorder on site. Simply forward the NVR port.
- Use a Different Username and Password for DSS
  - ◇ Do not use a username/password combination that you have in use for other accounts, including social media, bank account, or email in case the account is compromised. Use a different username and password for your security system to make it difficult for an unauthorized user to gain access to the IP system.
- Limit Features of Guest Accounts
  - ◇ Ensure that each user has rights to features and functions they need to perform their job.
- Disable Unnecessary Services and Choose Secure Modes
  - ◇ Turn off specific services, such as SNMP, SMTP, and UPnP, to reduce network compromise from unused services.
  - ◇ It is recommended to 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 a mailbox server.
  - ◇ FTP: Choose SFTP and use strong passwords.
  - ◇ AP hotspot: Choose WPA2-PSK encryption mode and use strong passwords.
- Multicast
  - ◇ Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast. Deactivate this feature if not in use to enhance network security.
- Check the Log
  - ◇ The information stored in the network log file is limited due to the equipment’s limited storage capacity. Enable the network log function to ensure that the critical logs are synchronized to the network log server if saving log files is required.
  - ◇ Check the system log if you suspect that someone has gained unauthorized access to the system. The system log shows the IP addresses used to login to the system and the devices accessed.
- Physically Lock Down the Device
  - ◇ Perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement access control permission and key management to prevent unauthorized personnel from accessing the equipment.
- 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.
- Isolate NVR and IP Camera Network
  - ◇ Ensure that the network for the NVR and IP cameras should not be the same network as a public computer network. Separate networks prevent unauthorized users accessing the same network the security system.

- Secure Auditing
  - ◇ Check online users regularly to ensure unauthorized accounts are not logged in to a device.
  - ◇ Check the equipment log to access the IP addresses used to login to devices and their key operations.

Table of Contents

1 Overview

The Dahua Intercom Modular System is a complete intercom solution that offers full customization of the entire system. This intercom system starts with a 2 MP outdoor video intercom module that offers a wide-angle view lens, high-resolution images even in dark environments, and two-way talk. Then, add optional modules that offer door access capability (card reader, fingerprint reader, and keypad), call buttons, information text display, and status light indicators. The system also offers optional accessories to flush-or surface-mount a two-or three-module intercom system.

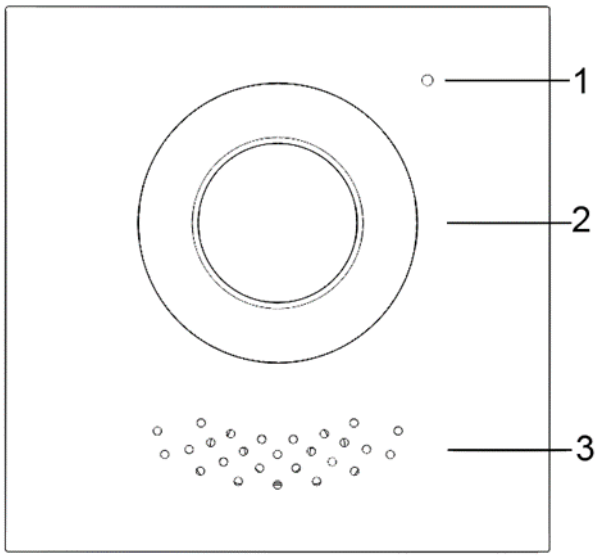
1.1 Modular Intercom Components

- DHI-VTO4202F-P-S2: 2 MP Outdoor Video Intercom (Required)
- DHI-VTO4202F-MB5: Five-button Call Panel
- DHI-VTO4202F-MF: Fingerprint Reader
- DHI-VTO4202F-MK: Keypad
- DHI-VTO4202F-ML: Status Light Panel
- DHI-VTO4202F-MN: Blank Panel
- DHI-VTO4202F-MR: IC Card Reader
- DHI-VTO4202F-MS: Information Text Display

2 Intercom Modules

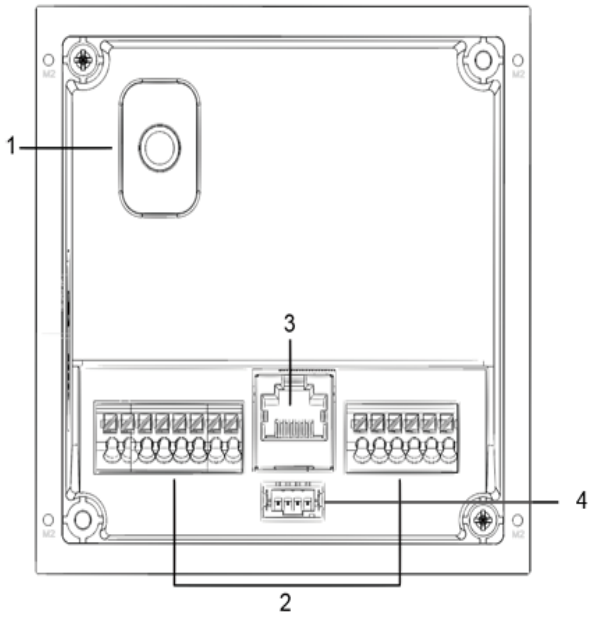
2.1 Camera Module

Front Panel



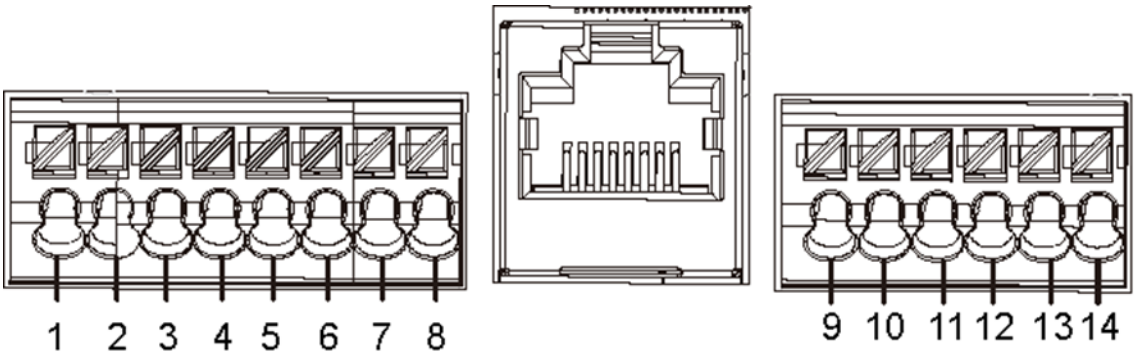
Ref	Name	Description
1	MIC	Inputs audio.
2	Camera	Monitors door area.
3	Speaker	Outputs audio.

Rear Panel



Ref	Name	Description
1	Tamper Switch	The VTO issues an alarm sound if it is removed from the wall by force, and sends the alarm to the management center.
2	Ports	Connect to power supply, electric control lock, solenoid lock, and exit button.
3	Ethernet Port	Connects unit to Ethernet network.
4	Cascade Connection	Connection to another Intercom module.

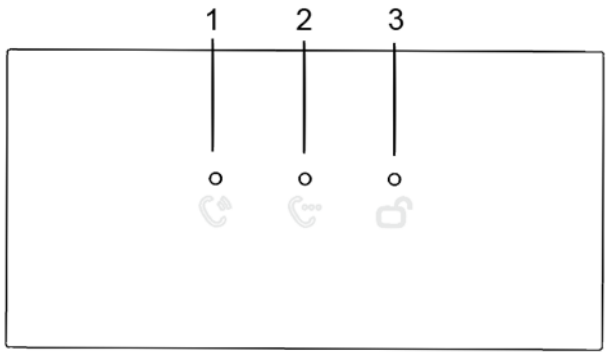
Ports



Ref	Name	Ref	Name
1	GND	8	EOC1 (2wires –(GND) for a 2-wire camera module)
2	+12V_OUT	9	DOOR_BUTTON
3	RS-485_B	10	DOOR_FEEDBACK
4	RS-485_A	11	GND
5	ALARM_NO	12	DOOR_NC
6	ALARM_COM	13	DOOR_COM
7	EOC2 (2wires +(48V) for a 2-wire camera module)	14	DOOR_NO

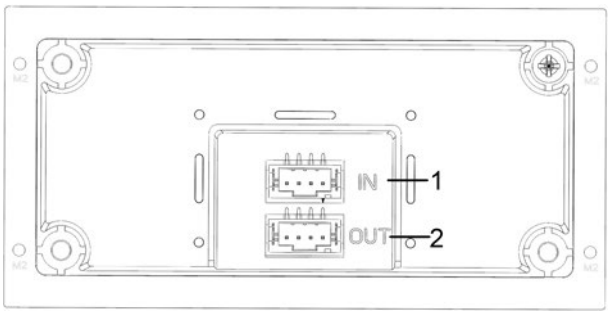
2.2 Status Light Panel

Front Panel



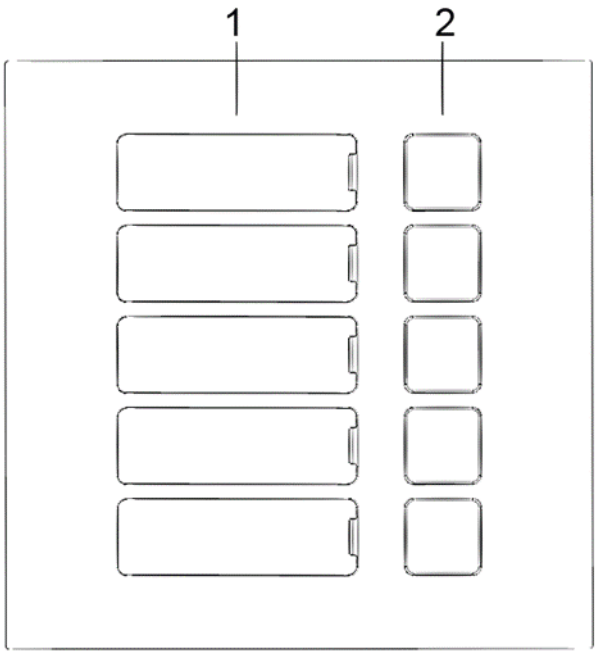
Ref	Description
1	Call indicator
2	Talk indicator
3	Unlock indicator

Rear Panel



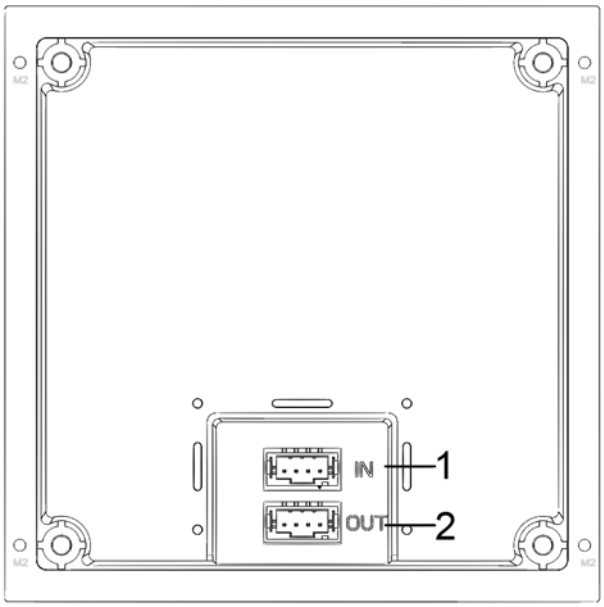
Ref	Description
1	Cascade input
2	Cascade output

2.3 Five-button Call Panel



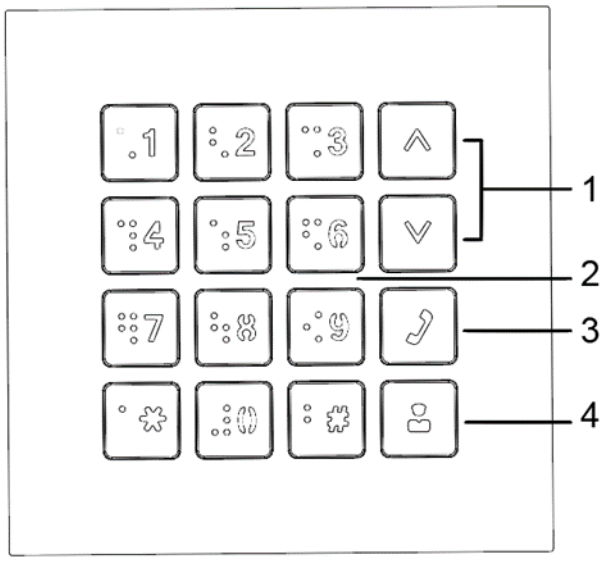
Ref	Name	Description
1	User directory	Add a physical name cards to the slots.
2	Call buttons	Call a VTH Monitor or the management center. Requires programming in the VTO interface.

Rear Panel



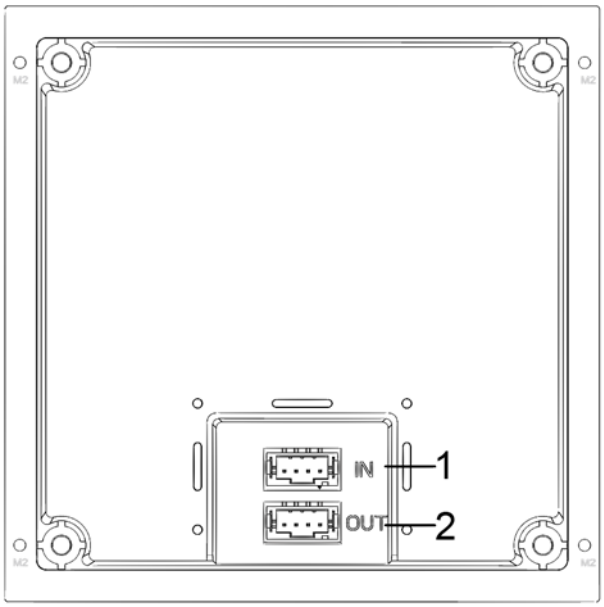
Ref	Description
1	Cascade input
2	Cascade output

2.4 Keypad Module



Ref	Description
1	Selection
2	Numbers
3	Place call
4	Call management center

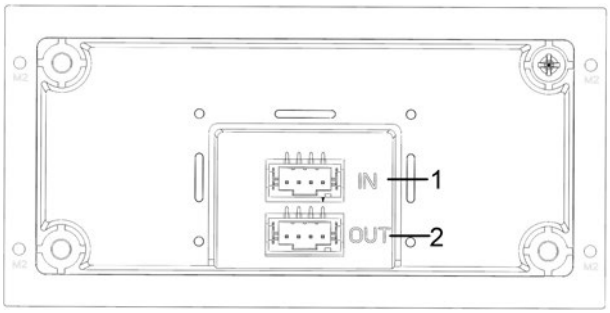
Rear Panel



Ref	Description
1	Cascade input
2	Cascade output

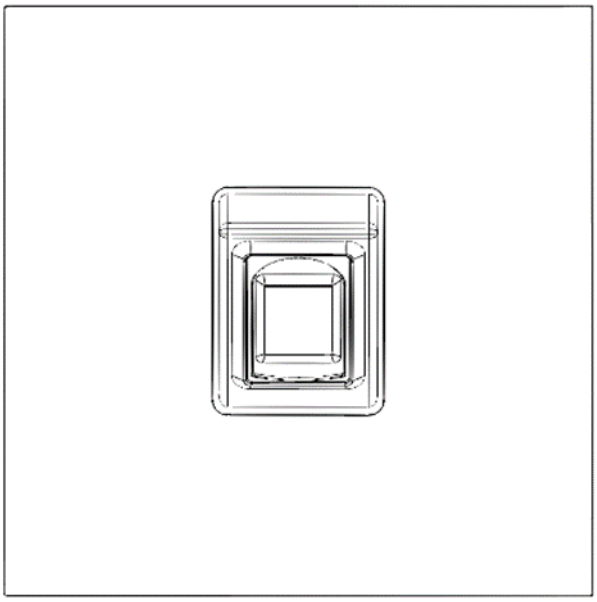
2.5 IC Card Reader

Rear Panel

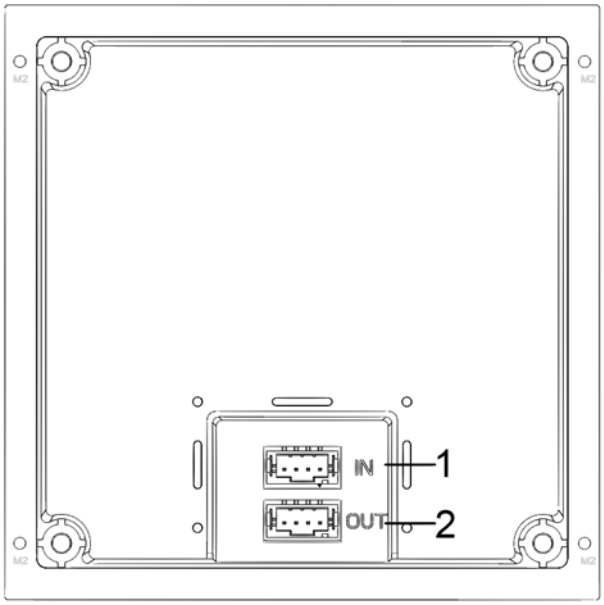


Ref	Description
1	Cascade input
2	Cascade output

2.6 Fingerprint Reader

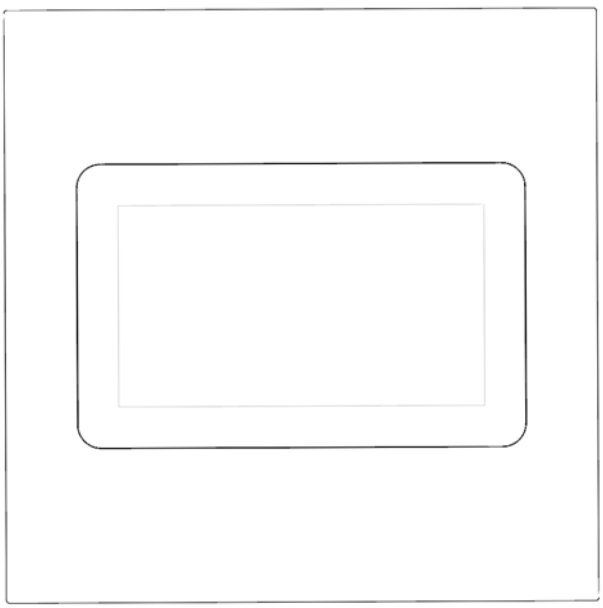


Rear Panel

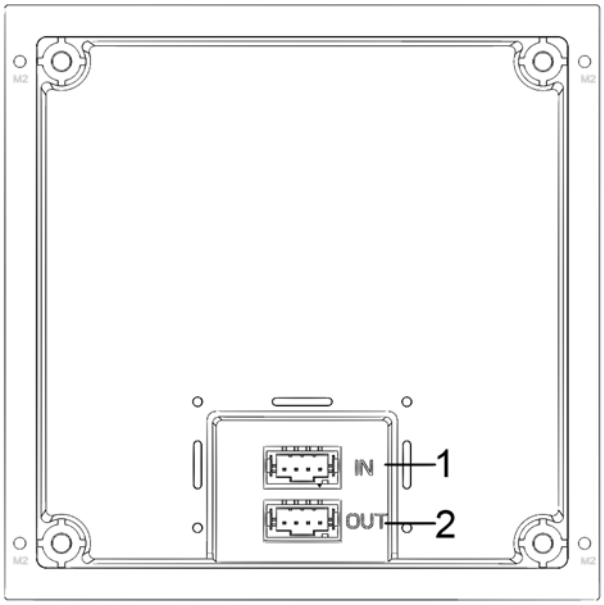


Ref	Description
1	Cascade input
2	Cascade output

2.7 Information Text Display



Rear Panel

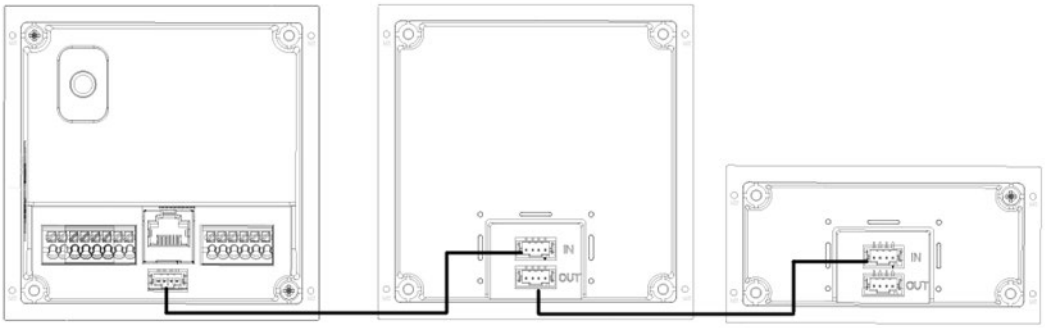


Ref	Description
1	Cascade input
2	Cascade output

2.8 Blank Module

This module is used to cover extra space if no other functional modules are needed.

2.9 Making Cascade Connections



The cascade connections are required for all modules. The Outdoor Video Intercom Panel (the left-most panel above) is the only required module and is the starting point for the cascade connections.

Note:

- The VTO connection must be made to an Input port.
- Connect “Out” ports only to "In" ports.

3 Initializing the VTO

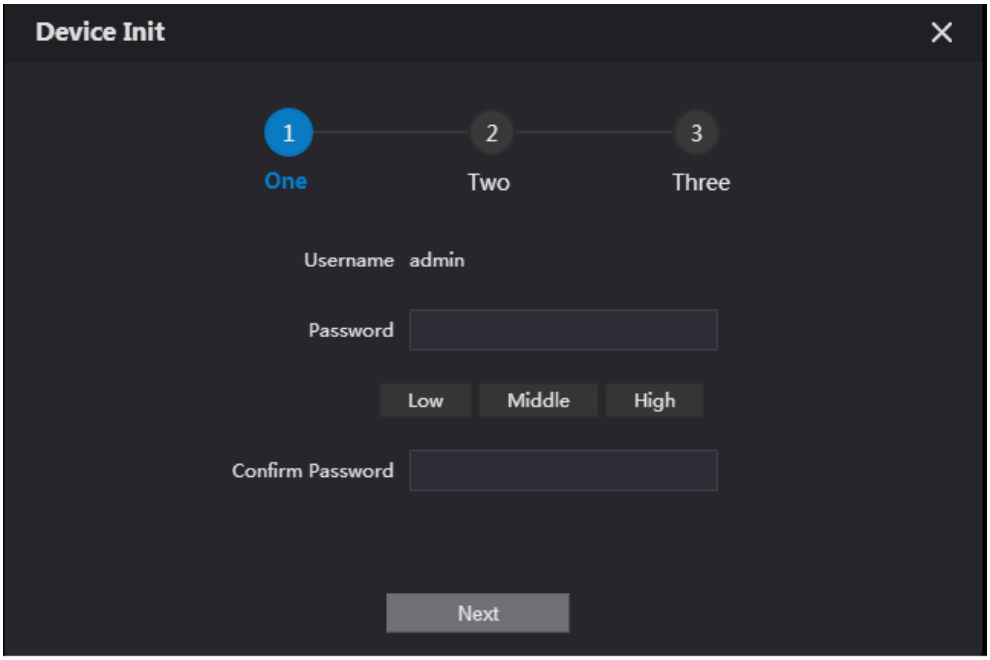
For first-time login or after resetting the VTO, initialize the device on the web interface.

Step 1 Power on the VTO.

Step 2 Enter the default IP address (192.168.1.108) of the VTO in the browser address bar.

Make sure that the IP address of your PC is in the same network segment as the VTO.

Figure 3-1 Device initialization



Step 3 Enter and confirm the password, and then click Next.

Step 4 Enter an email address for resetting the password.

Step 5 Click Next, and then click OK.

4 Login and Reset the Password

4.1 Login

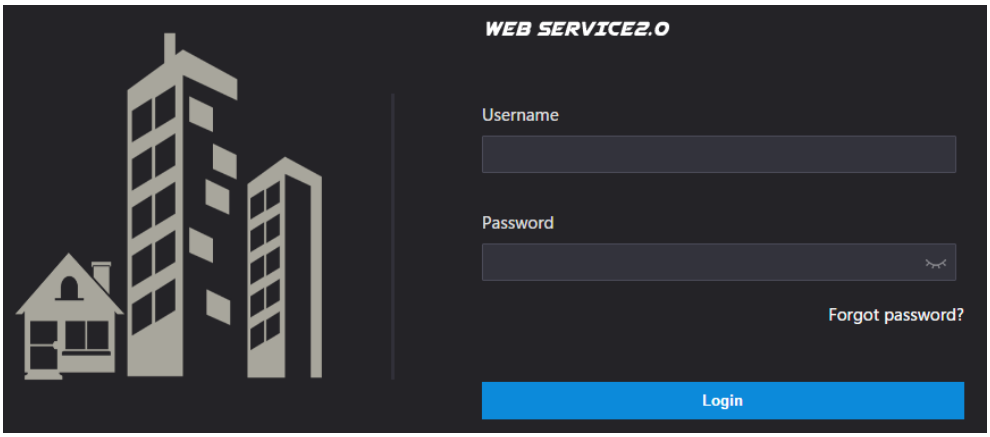
Before login, make sure that the PC is in the same network segment as the VTO.

Step 1 Go to the IP address of the VTO in the browser.

For first-time login, enter the default IP. If you have multiple VTOs, we recommend changing the default IP address (Network > Basic) to avoid conflict.

Step 2 Enter "admin" as username and the password you set during initialization, and then click Login.

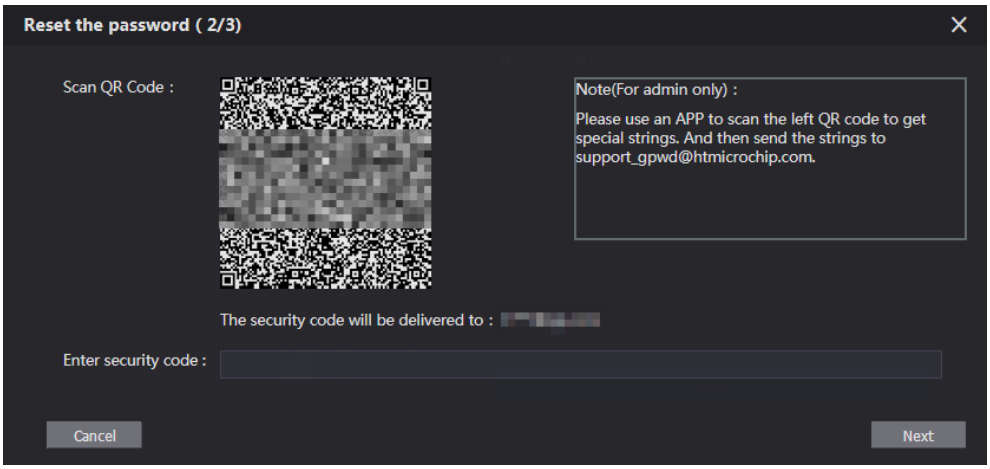
Figure 4-1 Login interface



4.2 Resetting the Password

Step 1 Click Forgot Password? and then click Next.

Figure 4-2 Reset the password (2/3)



Step 2 Scan the QR code to receive a get a string of numbers and letters.

Step 3 Send the string to the following email address: support_gpwd@htmicrochip.com.

The security code is sent to the email address configured during initialization.

Step 4 Enter the security code in the input box, and then click Next.

- If you did not set an email address during initialization, contact your supplier or customer service for help.
- The security code is valid for 24 hours upon receipt.
- If you enter the wrong security code for five consecutive times, your account will be locked for 5 minutes.

Step 5 Enter and confirm the new password, and then click OK.

5 Main Interface

Figure 5-1 Main interface

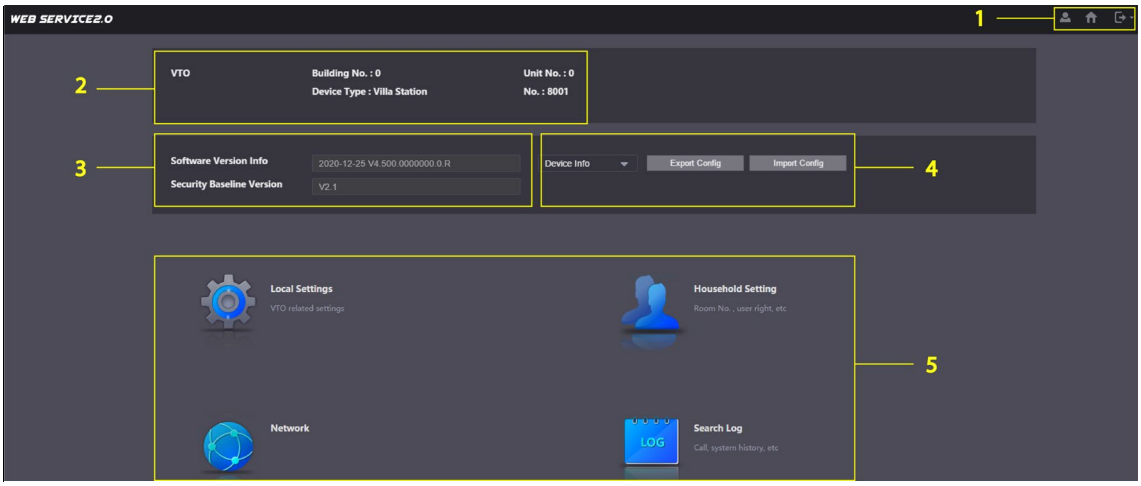


Table 5-1 Main interface introduction

No.	Function	Description
1	General function	• : Change the password and your email address. • : Return to the main interface. • : Log out, restart the VTO or restore the VTO to factory settings. ⚠ If you restore the VTO to factory settings, the unit deletes all data except the external storage. You can format the SD card to delete the data in it.
2	VTO information	View the VTO and system information.
3	System information	
4	Configuration manager	Export or import VTO configuration or user information.
5	Function	Configure parameters for different functions. 📖 Interface and function might vary with the device type you configured for the VTO.

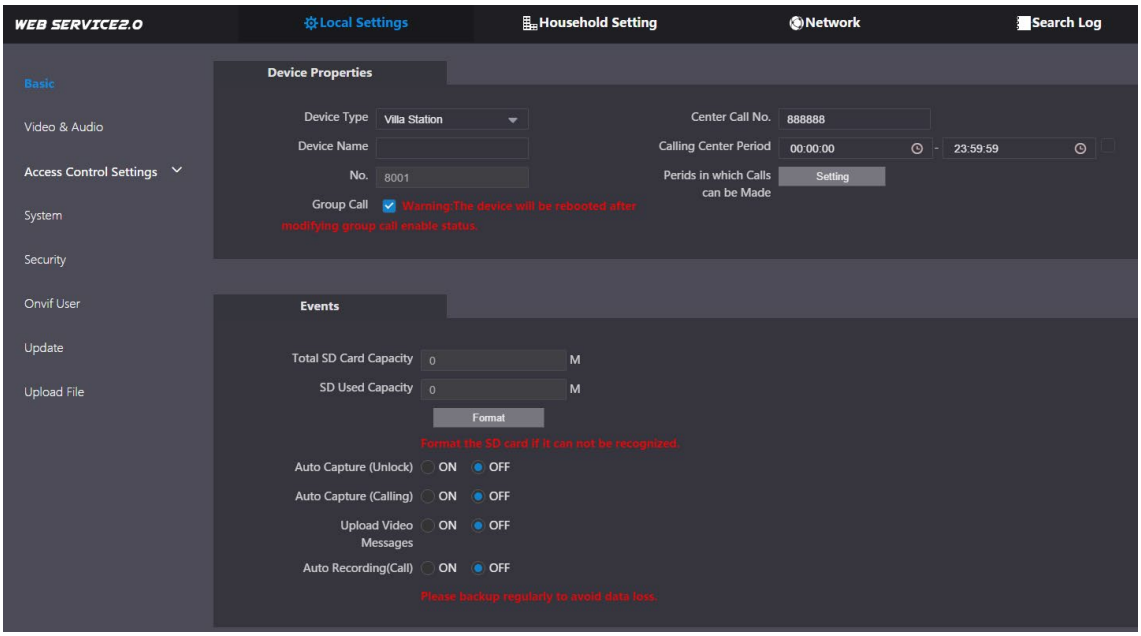
6 Local Settings

This chapter introduces the detailed configuration of the VTO.

6.1 Basic

Step 1 Select Local Settings > Basic.

Figure 6-1 Basic



Step 2 Configure the parameters.

Table 6-1 Basic parameter description

Parameter	Description
Device Type	Select Villa Station or Small Apartment.
Center Call No.	The default phone number for the management center is 888888.
Device Name	This name appears when other devices are monitoring this VTO.
Calling Center Period	Time period in which the management center can be called.
No.	Used to differentiate each VTO. Recommend setting the number according to unit or building number, and then adding VTOs to the SIP server by using their numbers. Change the number of the VTO when it is not working as the SIP server.
Periods in which Calls can be Made	Specify a time period to receive calls.
Group Call	Enable this function on the VTO that works as the SIP server. Use this to indicate when a main VTH receives a call, all extension VTHs also receive the call.
Total SD Card Capacity	Displays the total and used capacity of the SD card. Click Format to delete all the data in the SD card.

Parameter	Description
SD Used Capacity	
Format	
Auto Capture (Unlock)	VTO takes two snapshots when the door is unlocked and saves the images to the SD card.
Auto Capture (Calling)	Takes a snapshot and saves to the SD card of the VTO when the VTO receives a call.
Upload Video Messages	When enabled: ● If an SD card is installed in both the VTH and VTO, the video message will be saved to the SD cards of both the VTH an the VTO. ● If an SD card is installed in either the VTH or the VTO, the video message will be saved in either the SD card of the VTH or the VTO (whichever has the SD card installed) ● If no SD card is installed in the VTH or VTO, no video message will be saved.
Auto Recording (Call)	Record video when the VTO is in a call, and save the recording in the SD card of the VTO.

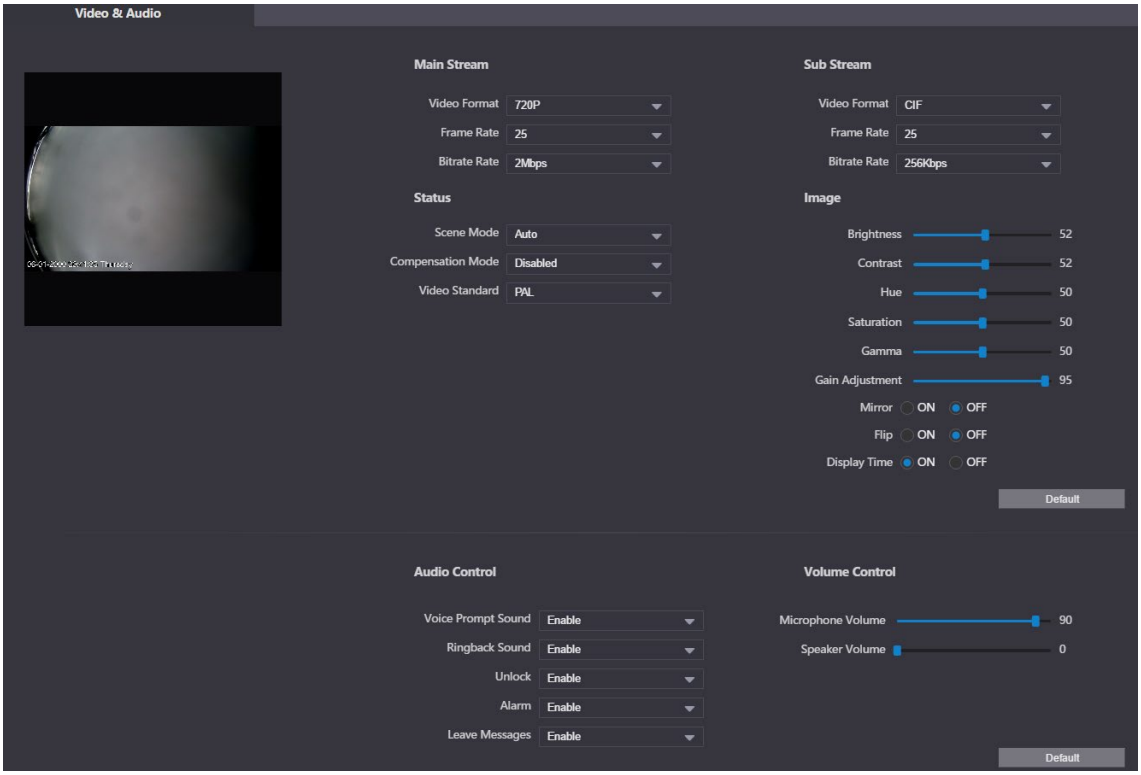
Step 3 Click Save.

6.2 Video and Audio

Configure the video format, quality, and audio for the VTO.

Step 1 Select Local Settings > Video & Audio.

Figure 6-2 Video and audio



Step 2 Configure the parameters to take effect as you make changes.

Table 6-2 Video parameter description

Parameter		Description
Main/Sub Stream	Video Format	Select a resolution appropriate for your needs: ● 1080P: 1920 × 1080. ● 720P: 1280 × 720. ● WVGA: 800 × 480. ● QVGA: 320 × 240. ● D1: 720 × 480. ● CIF: 352 × 288.
	Frame Rate	The larger the value, the smoother the video, but requires more bandwidth.
	Bitrate Rate	The larger the value, the better the video quality, but requires more bandwidth.
Status	Scene Mode	Select as needed according to the lighting condition. Auto is selected by default.
	Compensation Mode	● BLC: Back light compensation. Improves the clarity of the target in the image. ● WDR: Wide dynamic range. Enhances the brightness of dark areas and reduces the brightness of brighter areas to improve the image. ● HLC: High light compensation. Reduces the brightness of the brighter areas to improve the overall image.
	Video Standard	Select PAL or NTSC according to your area. PAL is used in China and Europe, and NTSC primarily in the United States and Japan.
Image	Brightness	The larger the value, the brighter the image.
	Contrast	Set a larger value for more contrast between bright and dark areas.
	Hue	Makes the color brighter or darker. The light sensor determines the default value. It is recommend to keep the default value.
	Saturation	The brighter the value, the bolder the color.
	Gamma	Changes the picture brightness and improves the picture dynamic range in a non-linear way. The larger the value, the brighter the image.
	Gain Adjustment	Amplifies the video signal to increase image brightness. If the value is too large, there will be more noise in the image.
	Mirror	Displays the image with left and right side reversed.
	Flip	Displays the image upside down.
	Display Time	Displays the current time and date on the video image.
Audio Control	—	Turn on or off sound for each type of event.
Volume Control	Microphone Volume	Adjust the volume as needed.
	Speaker Volume	

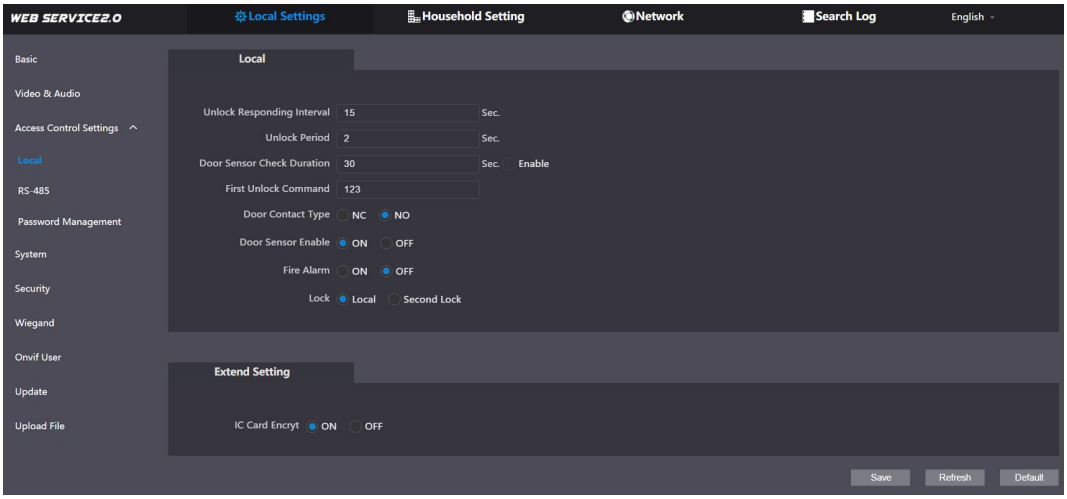
6.3 Access Control Settings

This section details the configuration of the two locks connected to the lock ports or to the RS-485 port on the VTO.

6.3.1 Local

Step 1 Select Local Settings > Access Control Settings > Local.

Figure 6-3 Local



Step 2 Configure the parameters.

Table 6-3 Local access control parameter description

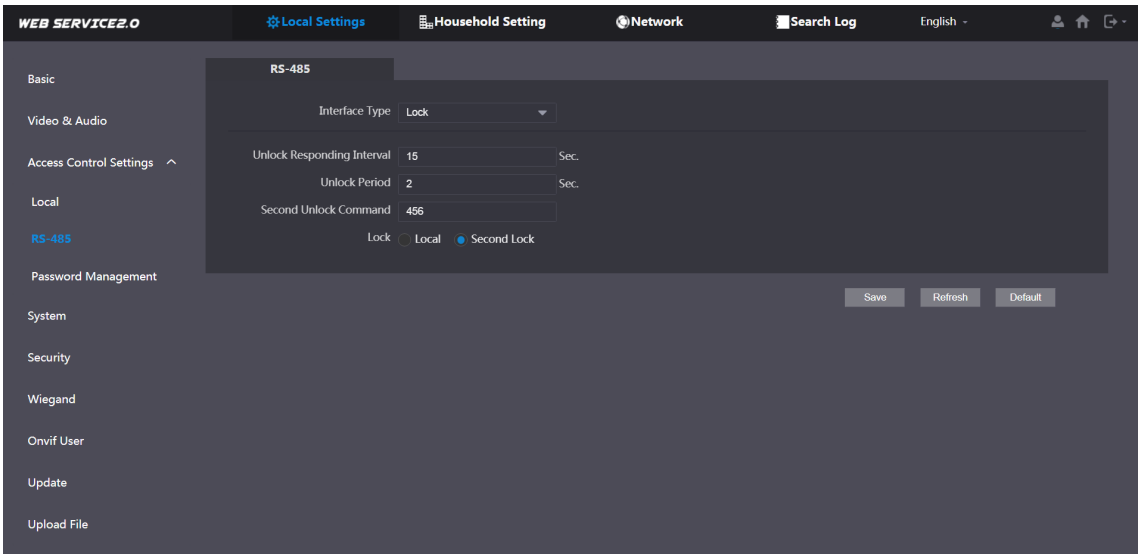
Parameter	Description
Unlock Responding Interval	The door can only be unlocked again after the interval.
Unlock Period	The time during which the lock stays unlocked.
Door Sensor Check Duration	● Enable to lock the door until the door sensors make contact. If the door is unlocked longer than the Door Sensor Check Duration, the door triggers an alarm and sends an alert to the management center. ● Disable to lock the door after the Unlock Period. Install a door contact to configure this parameter.
First/Second Unlock Command	Connect a third-party phone, such as a SIP phone, to the VTO, and use the command to open the door remotely.
Door Contact Type	● NC: Normally closed. ● NO: Normally open.
Door Sensor Enable	Synchronizes door sensor status to indoor monitors (VTHs).
Fire Alarm	Connects an alarm device to the port that is originally for the door contact.
Lock	Non-remote methods, such as password or card, will unlock the lock you select.
IC Card Encrypt	Access cards issued by the VTO will be encrypted and unclonable.

Step 3 Click Save.

6.3.2 RS-485

Select Local Settings > Access Control Settings > RS-485, and then configure the parameters of the lock connected through the RS-485 port. See Table 6-3 for parameter description.

Figure 6-4 Lock connected through the RS-485 port

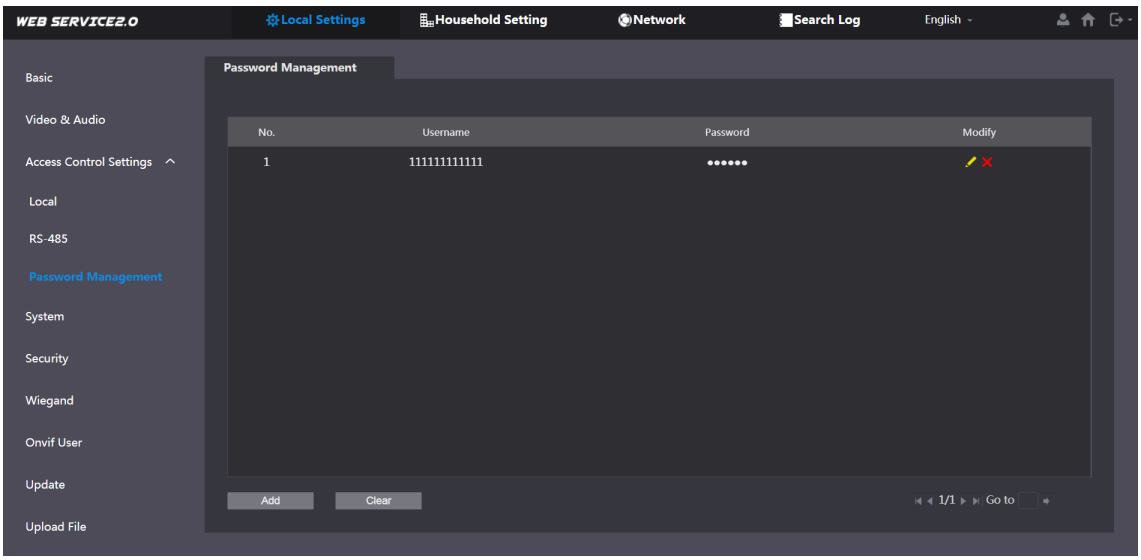


6.3.3 Password Management

Add a username and password used to unlock the door.

Select Local Settings > Access Control Settings > Password Management.

Figure 6-5 Password management

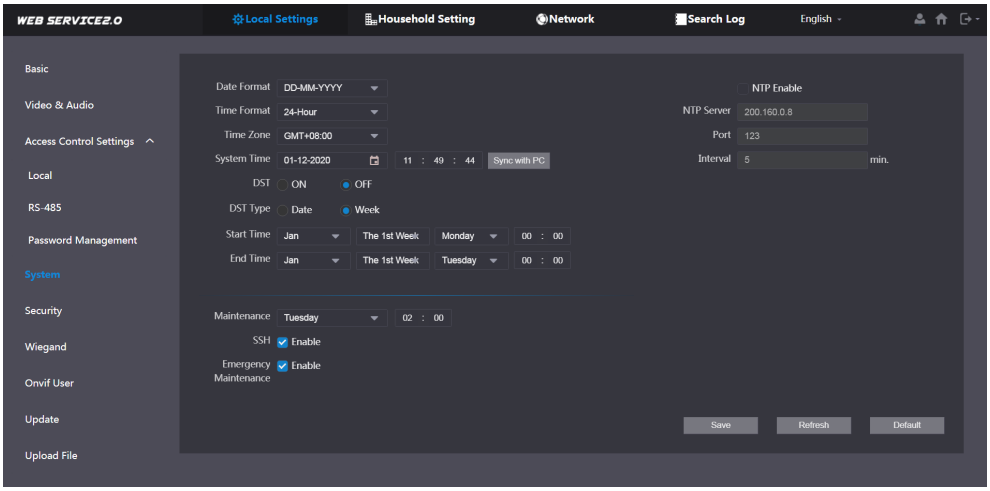


6.4 System

Configure time parameters, NTP server, and more.

Step 1 Select Local Settings > System.

Figure 6-6 System



Step 2 Configure the parameters.

Table 6-4 System parameter description

Parameter	Description
Date Format	Select a format as needed.
Time Format	
System Time	Changing system time may cause issues when searching video. Turn off video recording and auto snapshot before changing the time. Ensure the system time is accurate.
Time Zone	Configure the time zone as needed.
Sync with PC	Synchronize the VTO system time with the PC you are accessing the VTO's web interface from.
DST	Daylight saving time. Enable this setting if daylight savings is applicable to your area. Configure DST type, start time, and end time.
DST Type	Select Date or Week as needed, and then configure the specific period.
Start Time	Configure the start time and end time of DST.
End Time	
NTP Enable	Enable NTP and enter the IP address of the NTP server. The VTO syncronizes time with the NTP server automatically.
NTP Server	
Port	NTP server port number.
Interval	VTO time update cycle. 30 minutes is the maximum time period.
Maintenance	Define the time when the VTO will restrart automatically.
SSH	Enable this setting when connecting a debugging device to the VTO through the SSH protocol. It is recommend to turn off this function and to turn on the security mode and outbound service information protection.
Emergency Maintenance	Enable the function for fault analysis and repair. This function occupies ports 8088 and 8087.

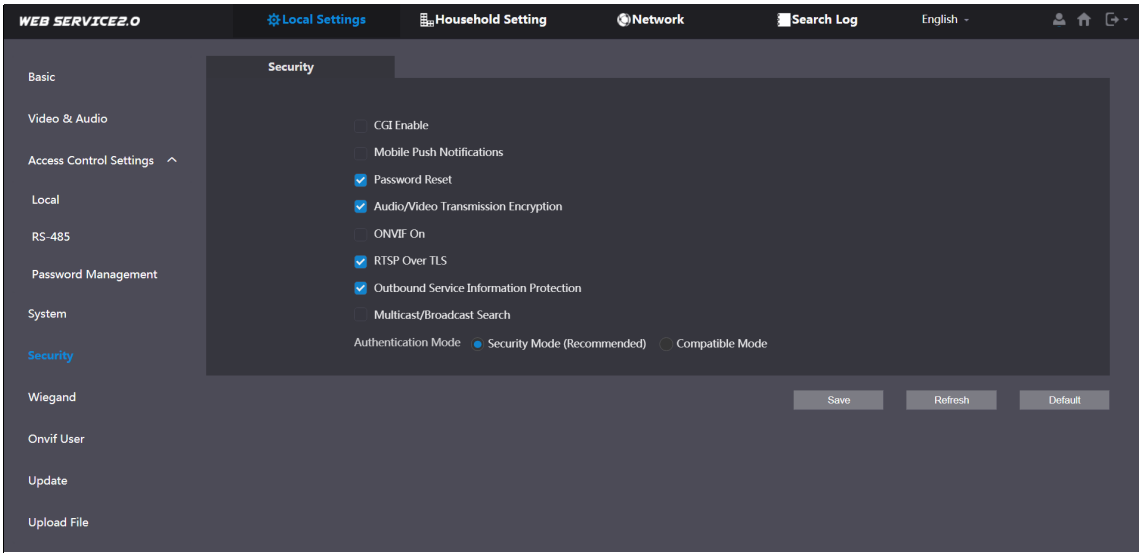
Step 3 Click Save.

6.5 Security

Configure functions that involve device security.

Step 1 Select Local Settings > Security.

Figure 6-7 Security



Step 2 Configure the parameters.

Table 6-5 Security parameter description

Parameter	Description
CGI Enable	Enable the use of CGI commands. ⚠ It is recommended to disable this function or the VTO might be exposed to security risks and data leakage.
Mobile Push Notification	Sends information to the DMSS Mobile Application. ⚠ It is recommended to disable this function or the VTO might be exposed to security risks and data leakage.
Password Reset	If turned off, you will not be able to reset the password.
Audio/Video Transmission Encryption	Encrypts all data during voice or video calls.
ONVIF On	Allows third-party devices to pull the video stream from the VTO through the ONVIF protocol. ⚠ It is recommended to disable this function or the VTO might be exposed to security risks and data leakage.
RTSP Over TSL	Outputs encrypted bit stream through RTSP.

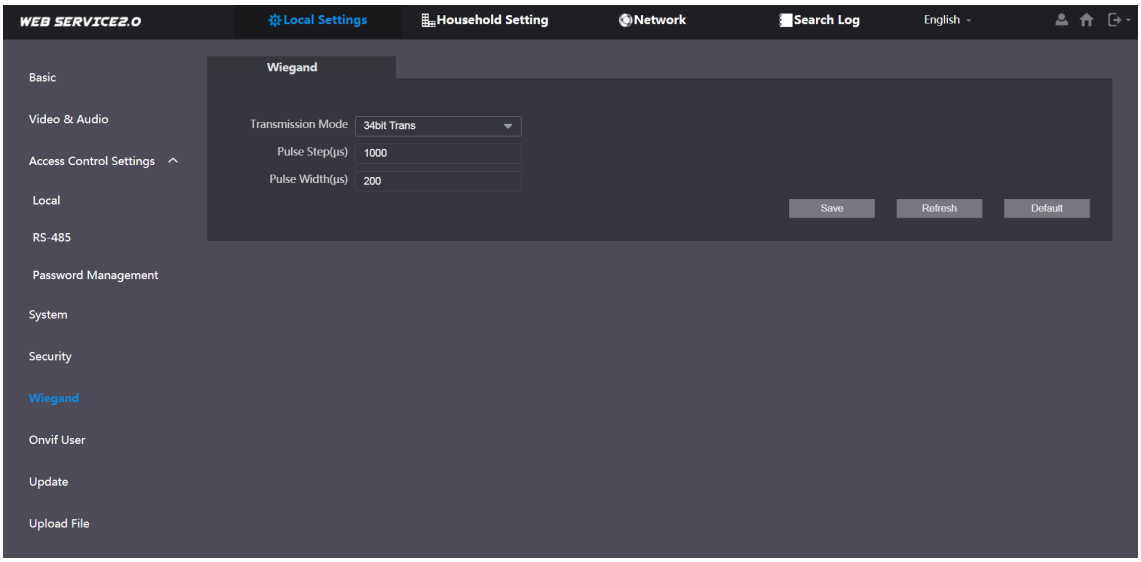
Parameter	Description
	⚠ It is recommended to enable this function or the VTO might be exposed to security risks and data leakage.
Outbound Service Information Protection	Protects your passwords. ⚠ It is recommended to enable this function or the VTO might be exposed to security risks and data leakage.
Multicast/Broadcast Search	Allows other devices to find this VTO. ⚠ It is recommended to disable this function or the VTO might be exposed to security risks and data leakage.
Authentication Mode	• Security Mode (recommended): Supports logging in with Digest authentication. • Compatible Mode: Use the old login method. ⚠ It is recommended to use the security mode. Compatible mode might expose the VTO to security risks and data leakage.

Step 3 Click Save.

6.6 Wiegand

Configure the parameters as needed when connected to other devices, such as a card reader with a Wiegand port.

Figure 6-8 Wiegand



6.7 ONVIF User

Add accounts for devices to monitor the VTO through the ONVIF protocol.

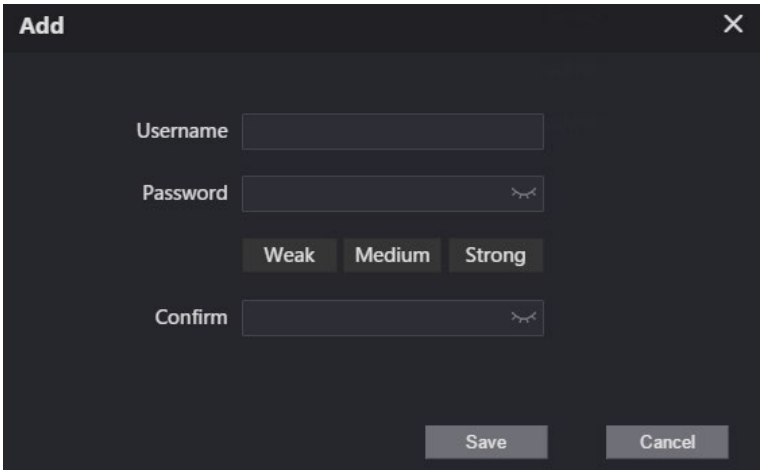
⚠

Deleting an account cannot be undone.

Step 1 Select Local Settings > Onvif User.

Step 2 Click Add.

Figure 6-9 Add an ONVIF user



Step 3 Enter the information and click Save.

ONVIF devices monitor the VTO by using the account. See the user's manual of the ONVIF device for details.

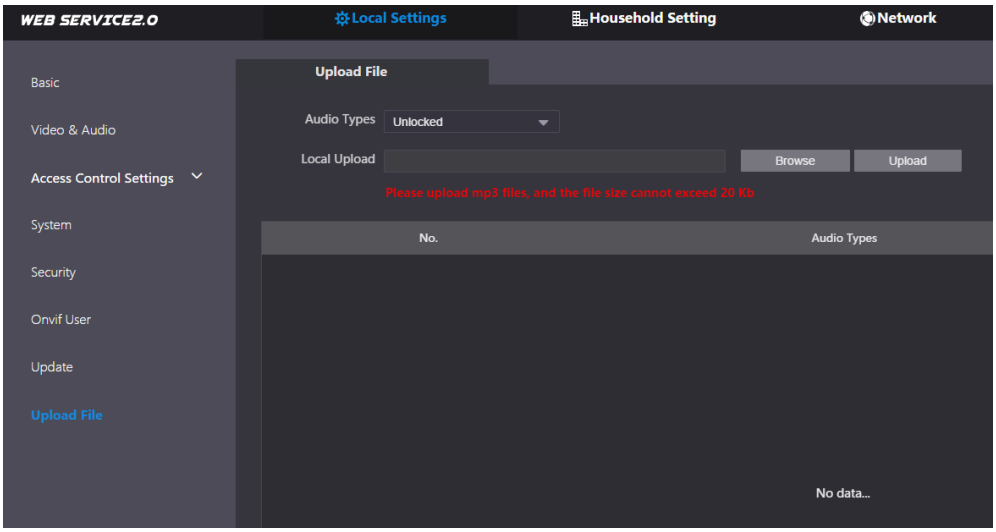
6.8 Upload File

Upload audio files to change the sound when calling, unlocking the door, and more.

Step 1 Select Local Settings > Upload File.

Step 2 Select an audio type and click Browse to select the audio file as needed.

Figure 6-10 Change the sound prompt



Step 3 Click Upload.

7 Household Setting

This chapter details the following steps:

- Add, modify, and delete VTO, VTH, VTS, and IP cameras.
- Send messages from the SIP server to VTOs and VTHs when the VTO works as the SIP server. If you are using other servers as the SIP server, see the corresponding manual for details.

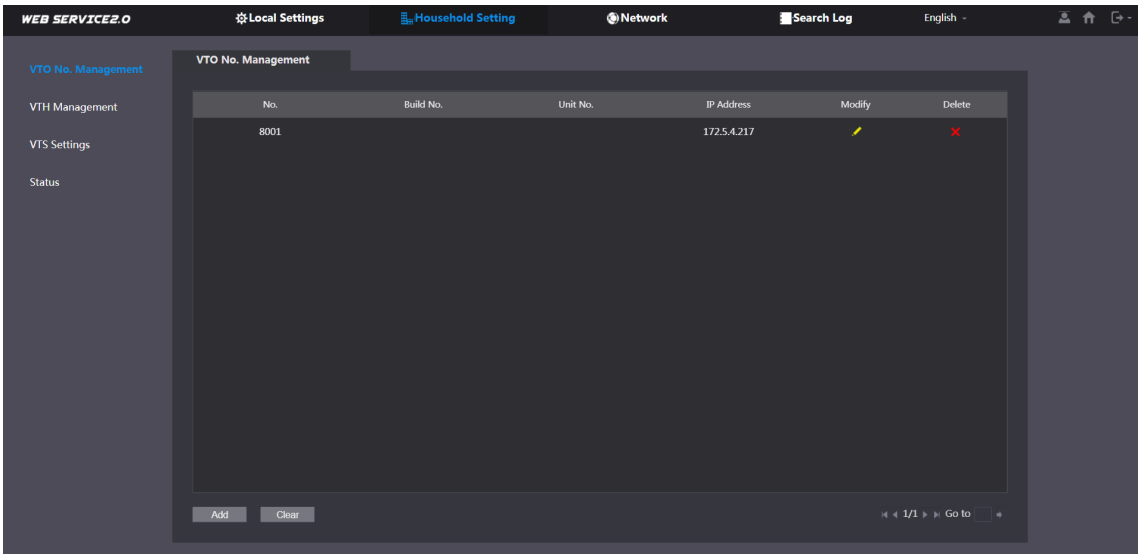
To configure SIP server parameters, see "SIP Server" for details.

7.1 VTO No. Management

Adding the VTO to the SIP server allows this VTO to contact all VTOs connected to the same SIP server.

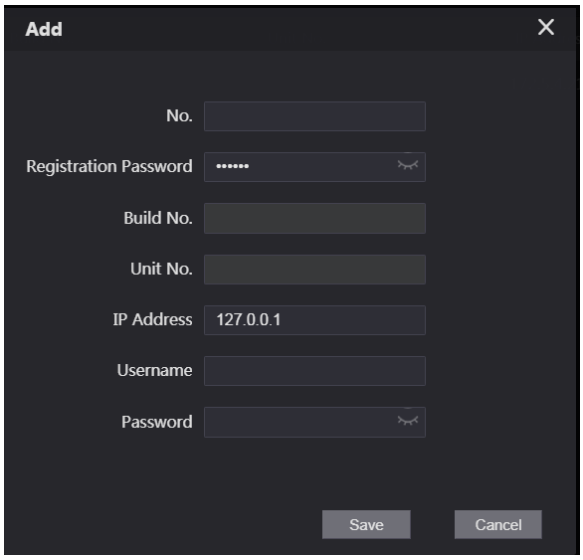
Step 1 Log in to the web interface of the VTO working as the SIP server, and then select Household Setting > VTO No. Management.

Figure 7-1 VTO management



Step 2 Click Add.

Figure 7-2 Add VTO



Step 3 Configure the parameters.

Table 7-1 Add VTO configuration

Parameter	Description
No.	The VTO number configured. See Table 6-1 for details.
Registration Password	Default.
Build No.	Available only when other servers work as the SIP server.
Unit No.	
IP Address	IP address of the VTO.
Username	Web interface login username and password of the VTO.
Password	

Step 4 Click Save.

Click or to modify or delete a VTO, or Clear to delete all added VTOs, but the one that you have logged in to cannot be modified or deleted.

7.2 VTH Management

7.2.1 Adding Room Number

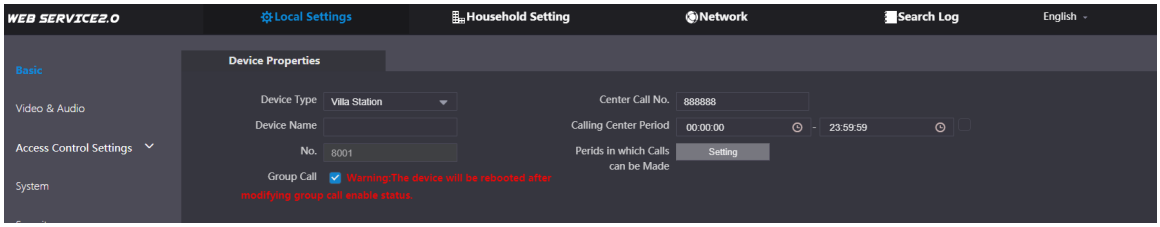
Add the planned room number to the SIP server, and then configure the room number on VTH devices to connect them to the network. This section is applicable when the VTO works as the SIP server, and if you use other servers as SIP server, see the corresponding manual of the servers for detailed configuration.

The room number can contain up to six (6) alphanumeric character. The room number cannot be the same as any VTO number.

Using the VTO in a House

Step 1 Log in to the web interface of the SIP server, and then select Local Settings > Basic.

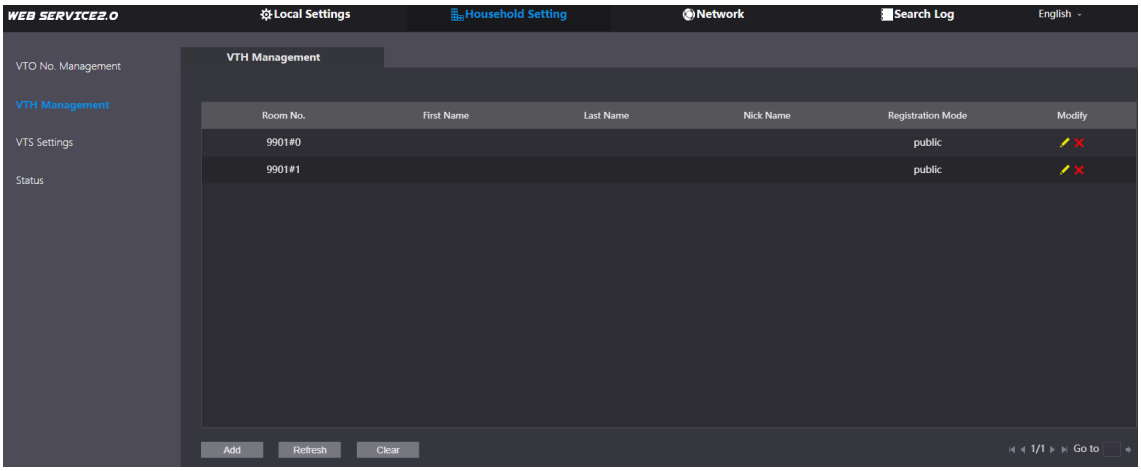
Figure 7-3 Device properties (1)



Step 2 Set Device Type to Villa Station, and then click Save.

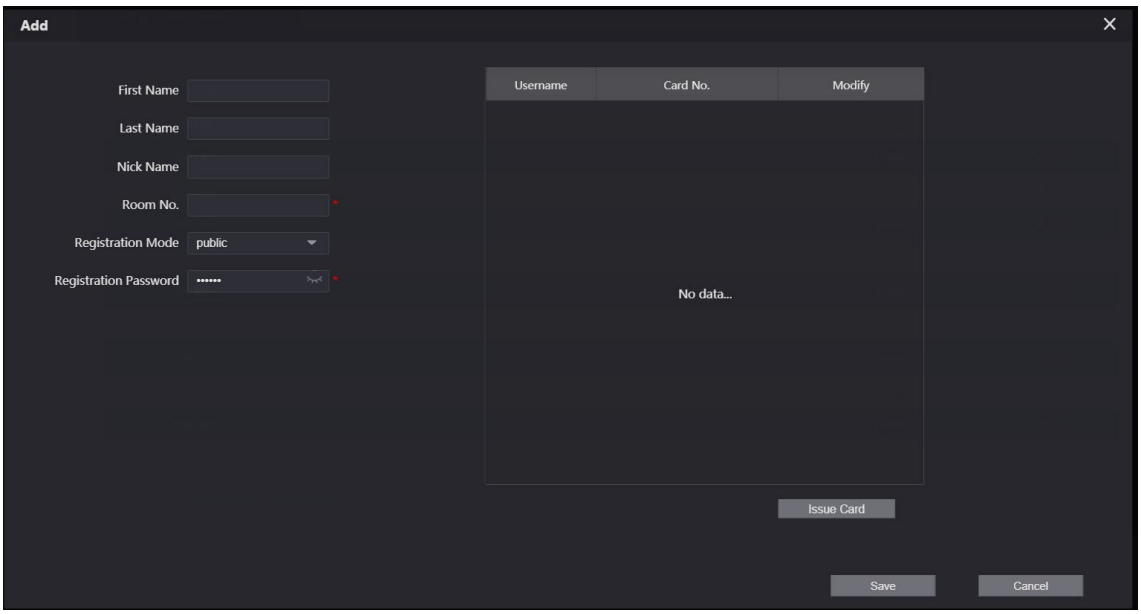
Step 3 Select Household Setting > VTH Management.

Figure 7-4 Room number management



Step 4 Click Add.

Figure 7-5 Add a room number



Step 5 Configure the parameters on the left.

Table 7-2 Room information

Parameter	Description
First Name	Provide the the information to differentiate each room.
Last Name	
Nick Name	
Room No.	Enter a room number, and then configure the number on a VTH to connect it to the network.
Registration Type	Select public.
Registration Password	Default.

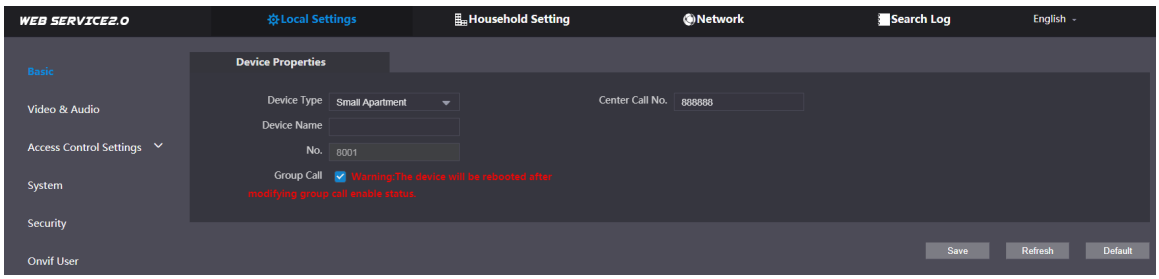
Step 6 Click Save.

- Click or to modify or delete a room number.
- Click Clear to delete all room numbers.

Using the VTO in an Apartment

Step 1 Log in to the web interface of the SIP server, and then select Local Settings > Basic.

Figure 7-6 Device properties (2)

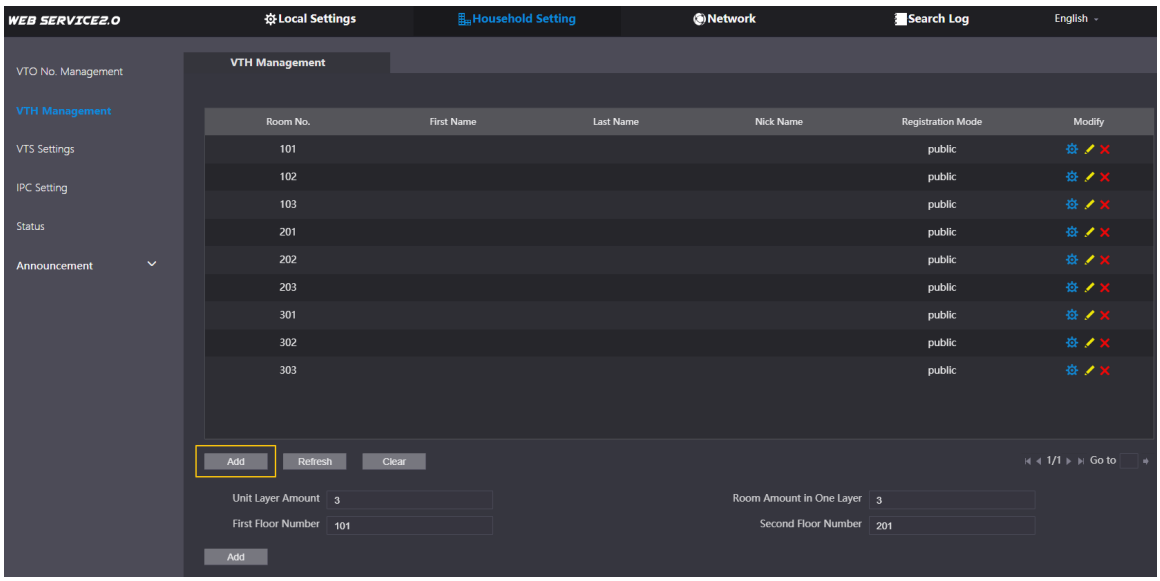


Step 2 Set Device Type to Small Apartment, and then click Save.

Step 3 Select Household Setting > VTH Management. You can add a single room number or add them in batches.

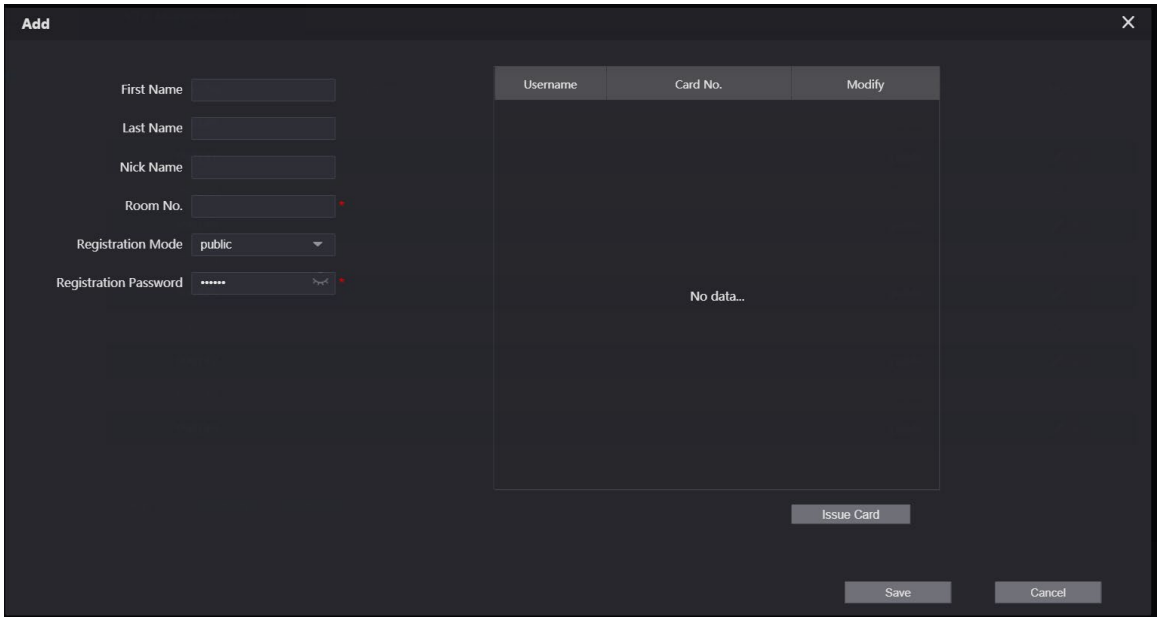
- Add a single room number.

Figure 7-7 Add room numbers



1) Click Add.

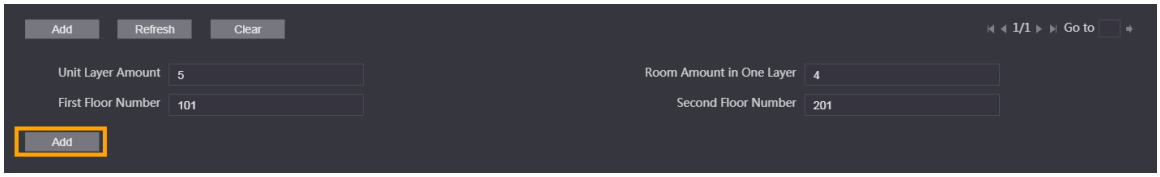
Figure 7-8 Add a single room number



2) Configure the information on the left. See Table 5-2 for details.
3) Click Save.

- Adding multiple room numbers.

Figure 7-9 Add room numbers in batches



1) Configure the information.
   - ◇ Unit Layer Amount: The number of floors in the apartment.
   - ◇ Room Amount in One Layer: The number of rooms on one floor.
   - ◇ First Floor Number: The first room number on the first floor.
   - ◇ Second Floor Number: The first room number on the second floor.

2) Click Add, and then click Refresh to view the latest status

- Click or to modify or delete a room number.
- Click Clear to delete all room numbers.

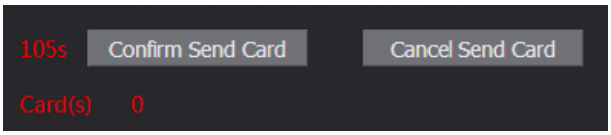
7.2.2 Issuing an Access Card

Issue an access card to unlock a door connected to the VTO.

To use this function, the VTO must have a card reader.

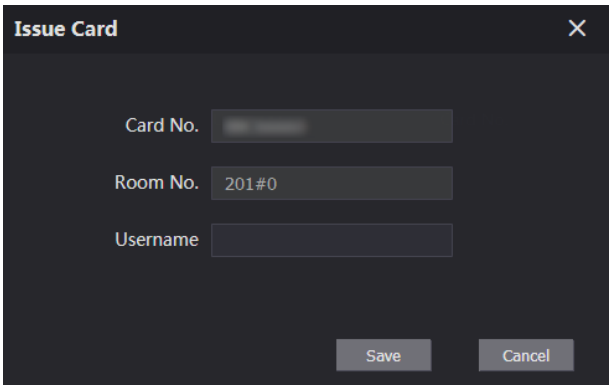
Step 1 Select Household Setting > VTH Management, click Add, and then click Issue Card.

Figure 7-10 Countdown notice



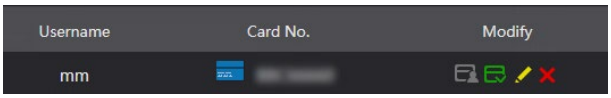
Step 2 Swipe the card on the VTO. You must swipe the card before the countdown time reaches zero.

Figure 7-11 Issue card



Step 3 Enter the username, click Save, and then click Confirm Send Card.

Figure 7-12 Issued access card



Other Operations

- Click to set this card as the main card. Once set, the icon will change to . Use the main card to issue access cards for this room on the VTO.
- Click to set that this card as lost. The icon changes to . The lost card cannot be used to open the door.
- Click or to modify the username or delete the card.

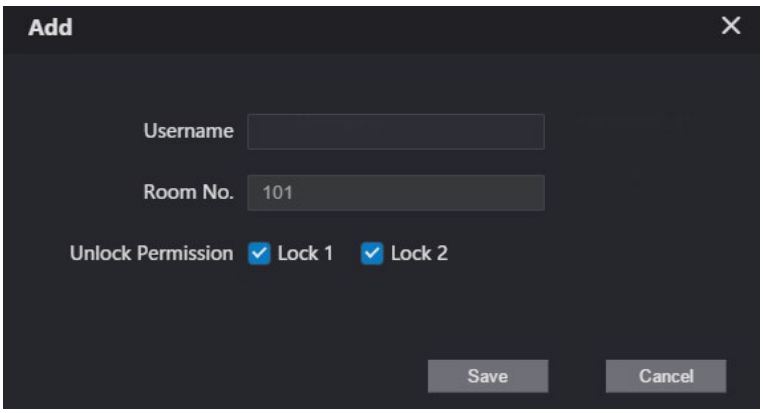
7.2.3 Reading Fingerprints for Access

Creates a fingerprint image used to unlock a door.

To use this function, the VTO must have a fingerprint scanner.

Step 1 Select Household Setting > VTH Management, click Add, and then click Issue Fingerprint.

Figure 7-13 Issue fingerprint



Step 2 Enter a username, assign unlock permission as needed, and then click Save.

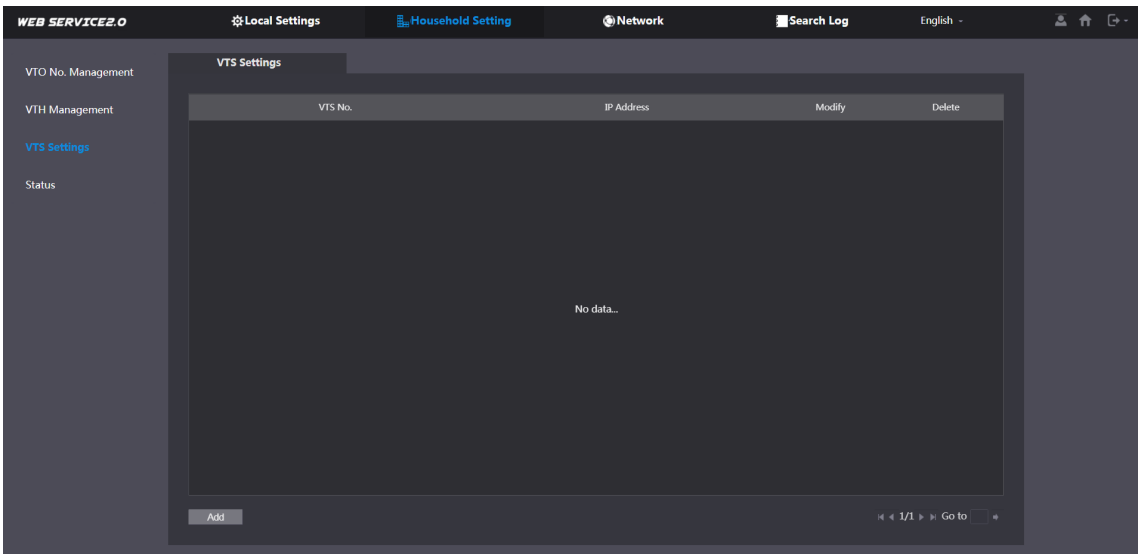
Step 3 Press the finger onto the scanner.

7.3 VTS Management

Add a VTS to the SIP server to use it as the management center. The VTS can also manage, call, or receive calls from all the VTOs and VTHs in the network. See the corresponding user's manual for details.

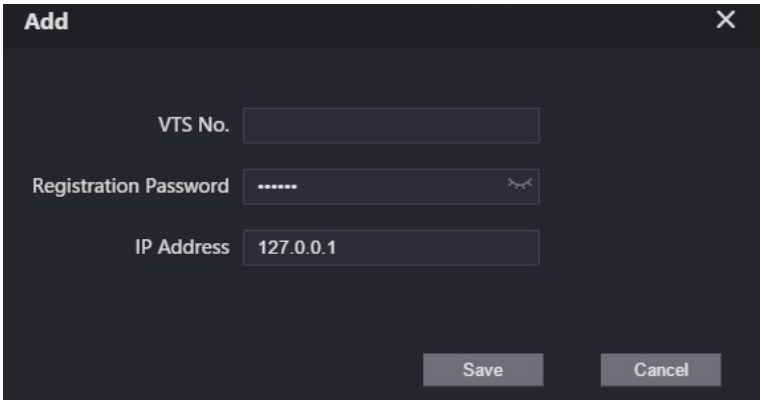
Step 1 Log in to the web interface of the VTO working as the SIP server, and then select Household Setting > VTS Settings.

Figure 7-14 VTS management



Step 2 Click Add.

Figure 7-15 Add VTS



Step 3 Configure the parameters.

Table 7-3 Add VTS configuration

Parameter	Description
VTS No.	The number of the VTS.
Registration Password	Default
IP Address	VTS IP address.

Step 4 Click Save.

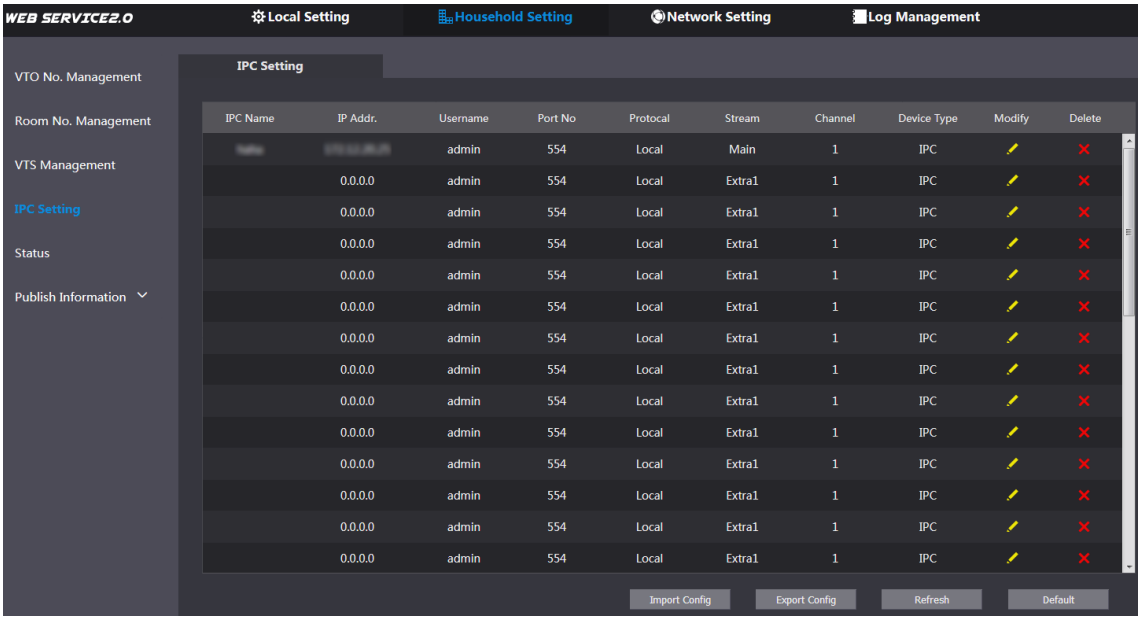
7.4 IP Camera Setting

Add an IP camera and an NVR to the VTO working as the SIP server. Once added all connected VTH monitors can monitor the video.

Interfaces might vary with different products.

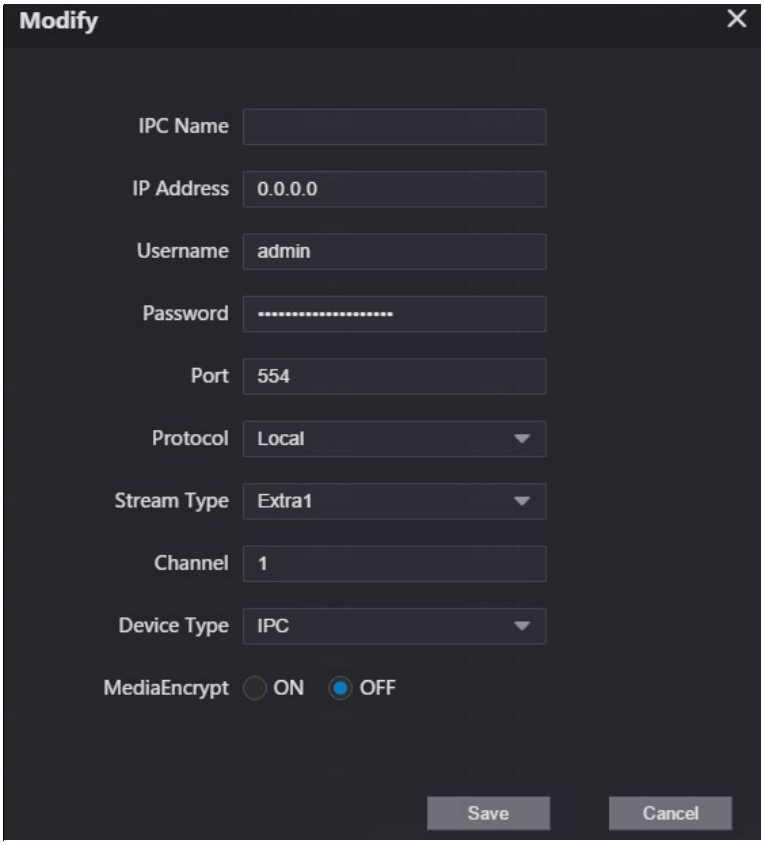
Step 1 Log in to the web interface of the VTO working as the SIP server, and then select Household Setting > IPC Setting.

Figure 7-16 IPC setting



Step 2 Click  next to a camera an available camera in the list.

Add IPC



Step 3 Configure the parameters.

Table 7-4 Add IPC configuration

Parameter	Description
IPC Name	Enter the name that identifies the IPC.
IP Address	Camera IP address.
Username	Web interface login username and password for the device.
Password	
Port	Keep the default.
Protocol	Select Local or Onvif.
Stream Type	● Main: Better video quality but requires more bandwidth. ● Extra1: Smoother video with poorer quality but requires less bandwidth.
Channel	The number of the channels that a device supports.
Device Type	Select the one as needed.
MediaEncrypt	Select ON if the IPC to be added is encrypted.

Step 4 Click Save.

Other Operations

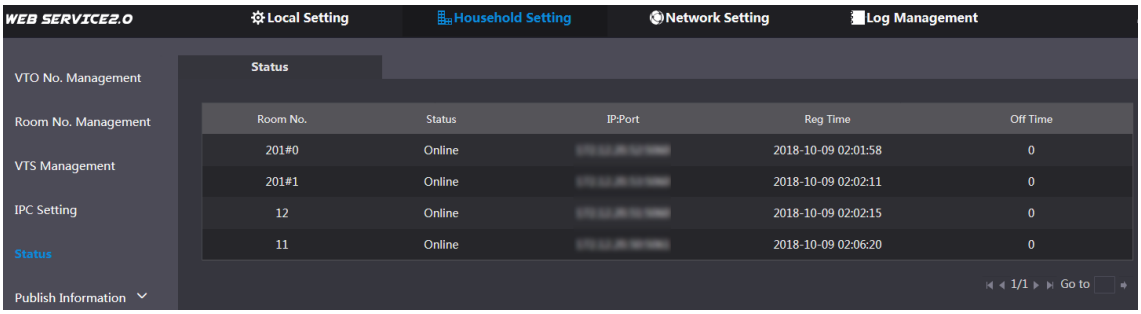
- Export Config: Export the device information to your PC.
- Import Config: Import device information.

7.5 Status

View the online status and IP addresses of all the connected devices.

Log in to the web interface of the SIP server, and then select Household Setting > Status.

Figure 7-17 Status



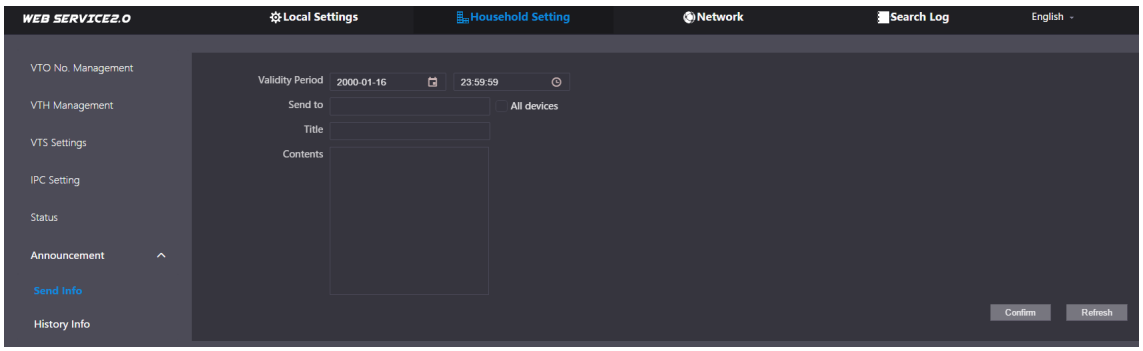
7.6 Publish Information

Allows you to send messages from the SIP server to the VTH devices connected to it, and allows you to view the message history.

7.6.1 Send Info

Step 1 Log in to the web interface of the SIP server, and then select Household Setting > Publish Information > Send Info.

Figure 7-18 Send information



Step 2 Specify the Validity Period that the message will be valid.

Step 3 Enter the VTO number or VTH number in the "Send to" field or select All devices to send the message to all the devices in the network

Step 4 Enter the message title in the “Title” Field.

Step 5 Enter the content of the message in the “Contents” field.

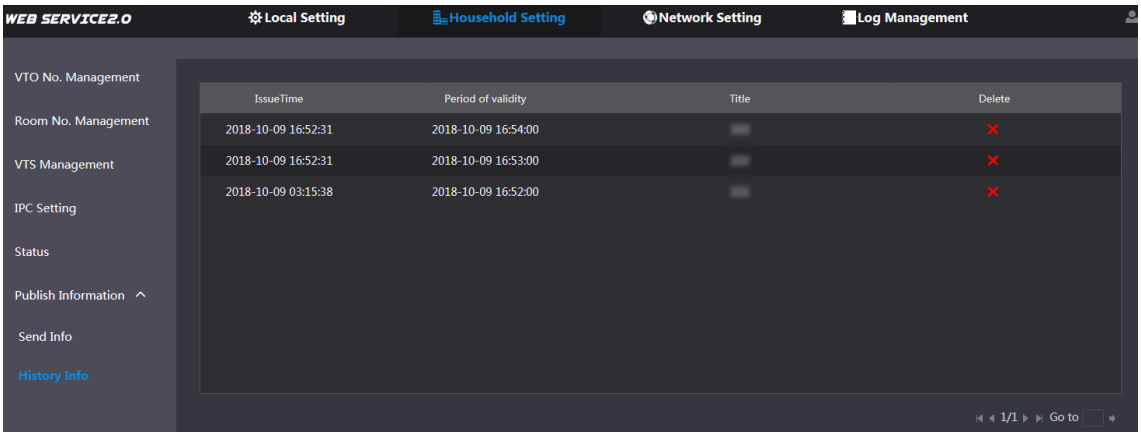
Step 6 Click Confirm.

7.6.2 History Info

View the information contained in previously sent messages.

Log in to the web interface of the SIP server, select Household Setting > Publish Information > History Info. Note: you can delete any of the messages in the list by clicking the "x" button.

Figure 7-19 History information



8 Network

This chapter introduces how to configure the network parameters.

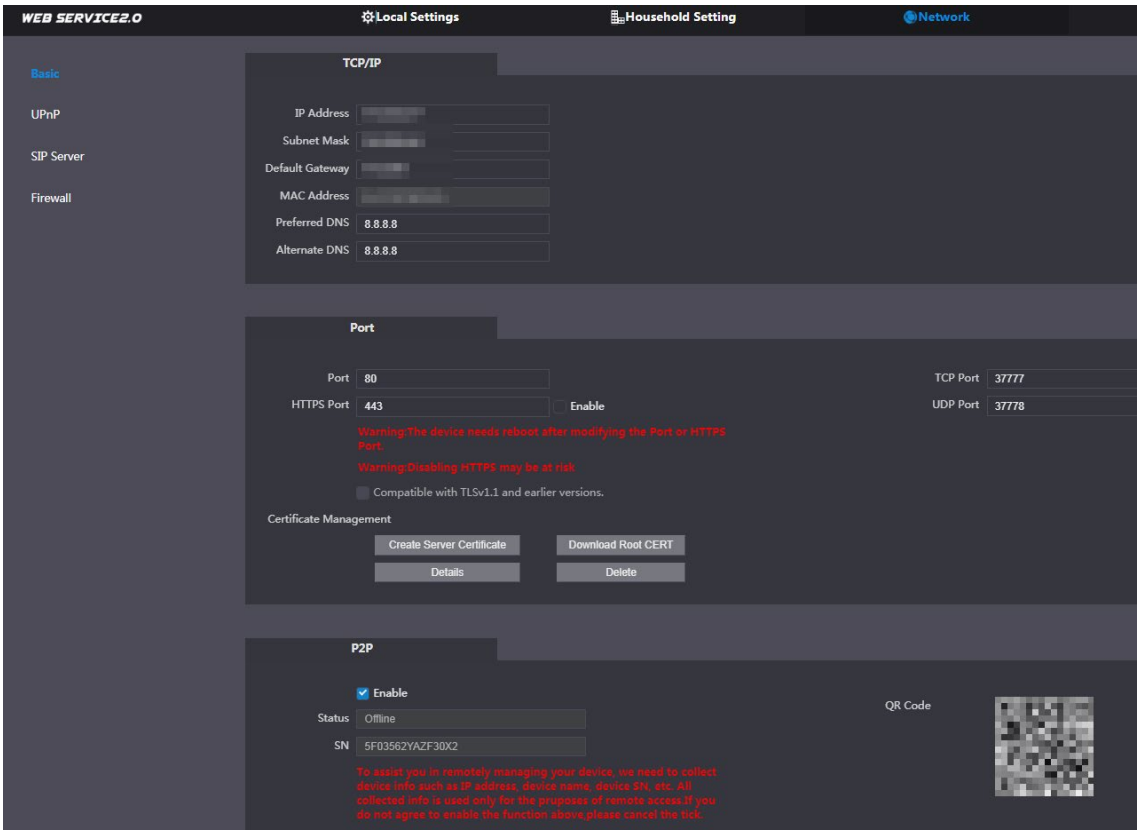
8.1 Basic

8.1.1 TCP/IP

Modify the IP address, subnet mask, default gateway, and DNS of the VTO.

Step 1 Select Network > Basic.

Figure 8-1 TCP/IP and port



Step 2 Configure the parameters and click Save.

The VTO restarts after making any changes. You must modify the IP address of your PC to the same network segment as the VTO to log in again.

8.1.2 Port

Table 8-1 Parameter description

Parameter	Description
Port	HTTP Port 80 by default. If already used, choose any number from 1025 to 65535 as needed. You can enter *http://VTO IP address:Port* to log in to the VTO.
HTTPS Port	Enable this function and click Save. You can now enter *https://VTO IP address:HTTPS Port* to log in to the VTO.
TCP/UDP Port	Used for accessing the VTO with devices in other networks. See "8.2 UPnP" for details.
Create Server Certificate	The unique digital identification of VTO for the SSL protocol. For first-time use or after changing the IP address of the VTO, you need to go through this process. ⚠ If you delete the certificate, it cannot be undone.
Download Root CERT	If you are using a PC that has never logged in to the VTO, download the root certificate and double-click to install it. Now you can use the HTTPS function mentioned above. ⚠ If you delete the certificate, it cannot be undone.

8.1.3 P2P

Enable the P2P function to scan the QR code with a smartphone to add the VTO to the app on your smartphone. Note: The systems displays “Offline" when the network is not properly configured to allow P2P, and displays "Online" if it is configured correctly.

If you set Device type to Small Apartment (see "4.1 Basic"), the QR code will be relocated to Household Setting > VTH Management. Click  of any room number, and then you can see both the serial number and the QR code of the VTO.

8.2 UPnP

When the VTO works as the SIP server, you can configure the UPnP function to allow WAN devices to log in to the VTO.

Preparation

- Enable the UPnP function on the router, and then configure a WAN IP address for the router.
- Connect the VTO to the LAN port of the router.

8.2.1 Enabling UPnP Services

Step 1 Select Network > UPnP.

Step 2 Enable the services listed as needed.

Step 3 Select Enable.

Step 4 Click Save.

8.2.2 Adding UPnP Services

Step 1 Select Network > UPnP.

Step 2 Click Add.

Step 3 Configure the parameters as needed.

Figure 8-2 Add a UPnP service

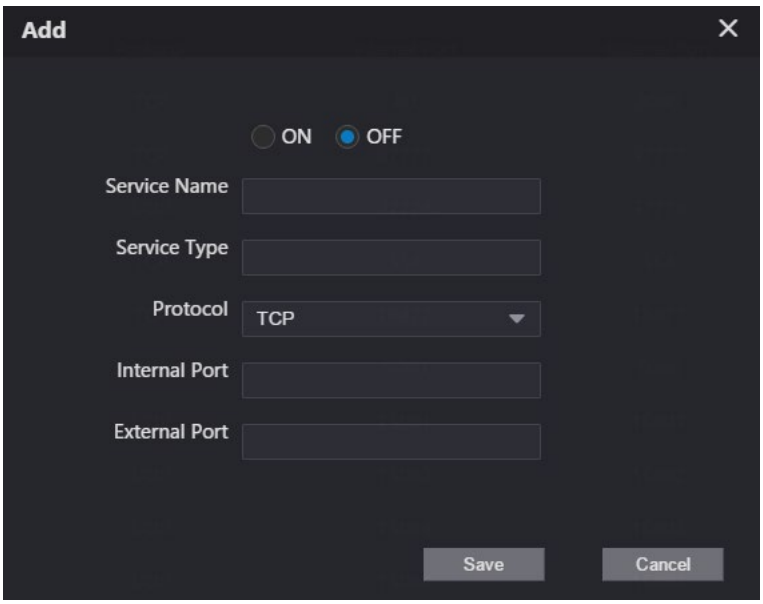


Table 8-2 Parameter description

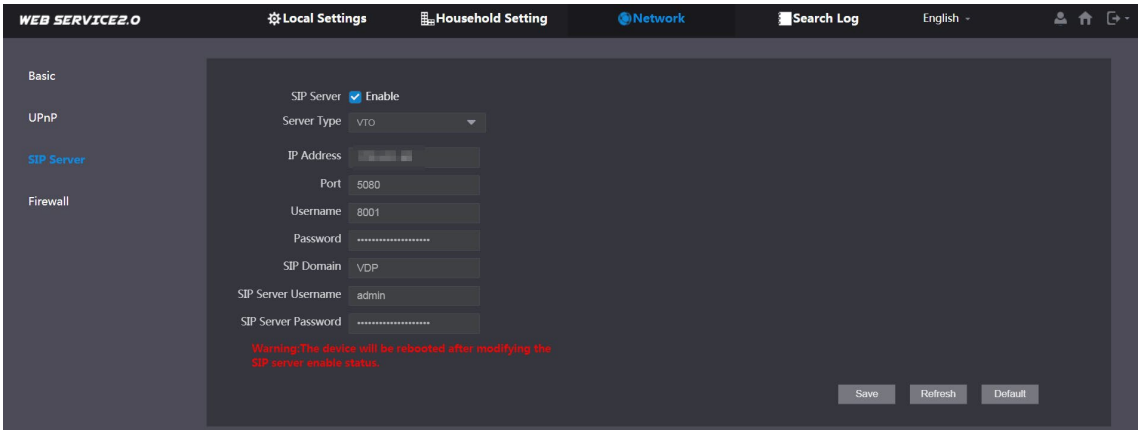
Parameter	Description
Service Name	Enter the information as needed.
Service Type	
Protocol	Select TCP or UDP as needed.
Internal Port	Use port number from 1024 through 5000.
External Port	 ● Do not use port number 1–1023 to avoid conflict. ● If you need to configure this function for multiple devices, make sure that the ports are not the same. ● The port number you use must be available. ● The internal and external port number must be the same.

8.3 SIP Server

There must be a SIP server in the network for all connected VTOs and VTHs to call each other. Use a VTO or another server as the SIP server.

Step 1 Select Network > SIP Server.

Figure 8-3 SIP Server



Step 2 Select a server type as needed.

- To set the VTO you have logged in as the SIP server:
  Check the box next to SIP Server and click Save to restart the VTO. You can add VTOs and VTHs to this VTO. See the details in "5 Household Setting".

  If the VTO you have logged into is not the SIP server, do not check the box for SIP Server.
- If another VTO is setup as the SIP server:
  Uncheck SIP Server. Set Server Type to VTO, configure the parameters, and then click Save.

Table 8-3 SIP server configuration

Parameter	Description
IP Addr.	VTO IP address.
Port	• 5060 by default when the VTO that you are logged into is acting as the SIP server. Note that this needs to be set to the same port that was set on the SIP server, if the VTO is not the SIP server. • 5080 by default when the platform works as SIP server.
Username	Keep the default.
Password	
SIP Domain	VDP by default. Note: this setting must match the SIP Domain value set on the SIP server, if this is not the SIP server.
SIP Server Username	Web interface login username and password of the SIP server. Note: this is the login for the VTO you are on, if it is the server. If this is not the server, then the setting must match the login information of the SIP server.
SIP Server Password	

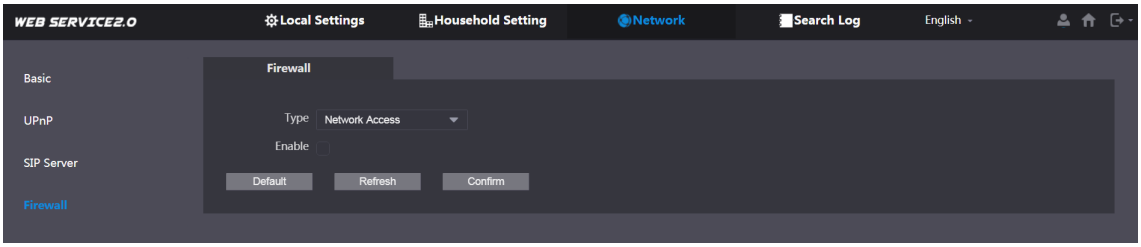
- If other servers work as the SIP server:
  Select the Server Type as needed, and then see the corresponding manual for details.

8.4 Firewall

You can enable different firewall types to control network access to the VTO.

Step 1 Select Network > Firewall.

Figure 8-4 Firewall



Step 2 Select one or more firewall types, and then check the box next to Enable.

Step 3 Configure the parameters.

Table 8-4 Firewall type description

Type	Description
Network Access	Select either Allowlist or Blocklist, and then add an IP address or segment which is allowed or denied to access the VTO.
PING Prohibited	The VTO will not respond to a ping to avoid ping attacks.
Anti-semijoin	Protects the VTO performance by blocking excessive SYN packets.

9 Log Management

Select Search Log to view call history, system logs, and alarm records; unlock records, and export them to your PC as needed.

If storage is full, the oldest records are overwritten. Back up the records as needed.

Dahua Technology USA
15245 Alton Parkway, Suite #100
Irvine, CA 92618

http://us.dahuasecurity.com/

Main Line: 949-679-7777
Support: 877-606-1590

Sales: sales.usa@dahuatech.com
Support: support.usa@dahuatech.com