Modular VTO

User’s Manual

V1.0.0

Foreword

General

This manual introduces the operation of the modular outdoor station web interface.

Safety Instructions

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

Signal Words	Meaning
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	September, 2018

About the Manual

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

occurred when using the device.

- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

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

Operating Requirement

- Do not place and install the device in an area exposed to direct sunlight or near heat generating device.
- Do not install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids, in order to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; don’t block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- Transport, use and store the device within allowed humidity and temperature range.

Power Requirement

- The product shall use electric wires (power wires) required by the region where the device will be used.
- 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

1 Initialization

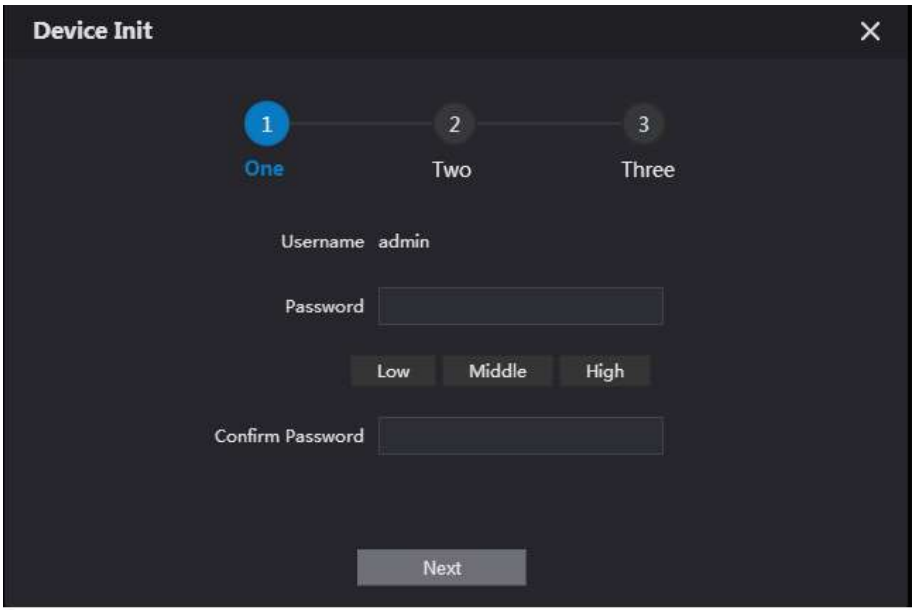
For first time login or after the VTO being reset, you need to initialize the web interface. The default IP address of the VTO is 192.168.1.110, and make sure the PC is in the same network segment as the VTO.

Step 1 Connect the VTO to power source, and then boot it up.

Step 2 Open the internet browser on the PC, then enter the default IP address of the VTO in the address bar, and then press Enter.

The **Device Init** interface is displayed. See Figure 1-1.

Figure 1-1 Device initialization



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

The email setting interface is displayed.

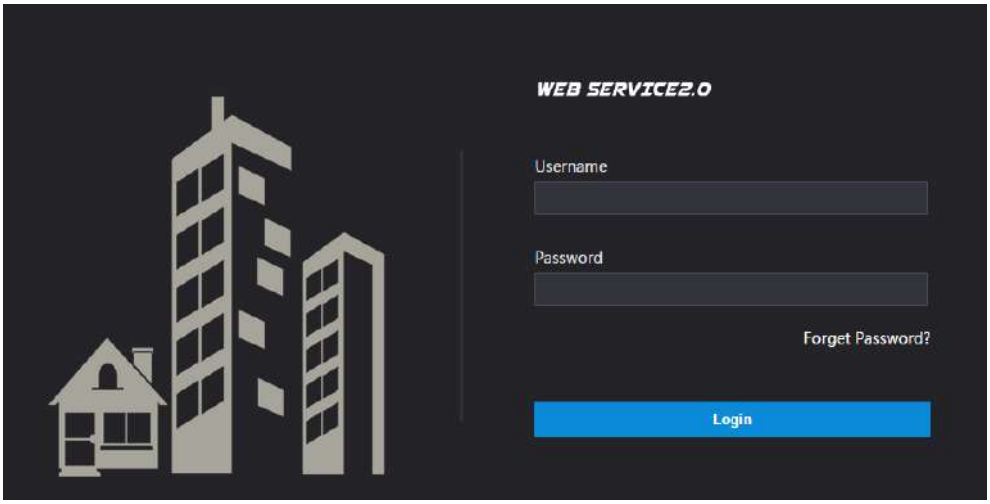
Step 4 Select the **Email** check box, and then enter your Email address. This Email address can be used to reset the password, and it is recommended to finish this setting.

Step 5 Click **Next**. The initialization succeeded.

Step 6 Click **OK**.

The login interface is displayed. See Figure 1-2.

Figure 1-2 Login interface



2 Login Interface

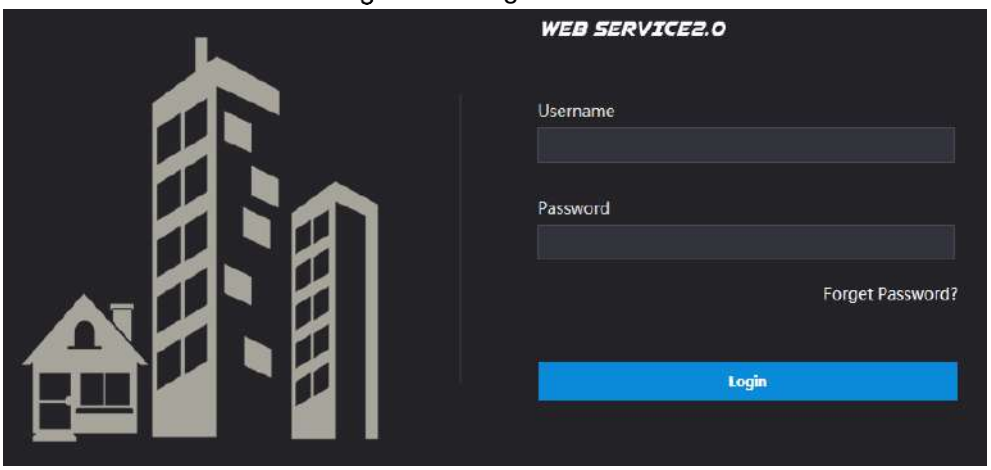
2.1 Login

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

Step 1 Open internet browser on the PC, then enter the VTO IP address in the address bar, and then press Enter.

The login interface is displayed. See Figure 2-1.

Figure 2-1 Login interface



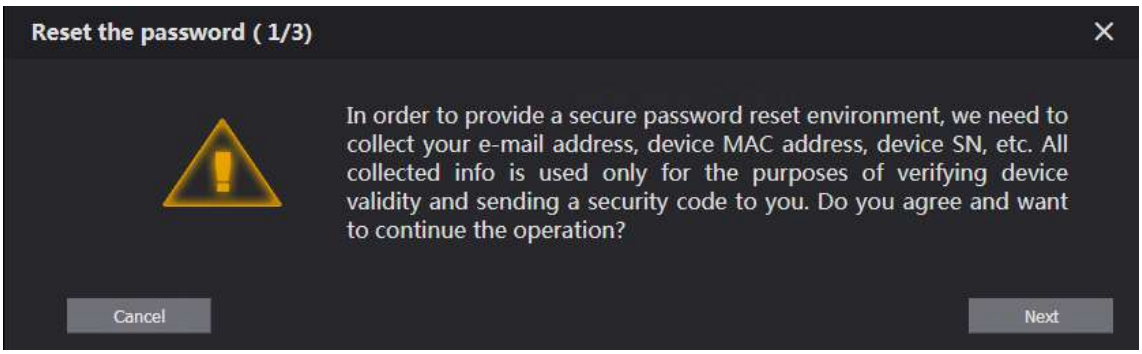
Step 2 Enter the username ("admin" by default), and then enter the password you set during initialization, and then click **Login**.

2.2 Resetting Password

Step 1 On the login interface (Figure 2-1), click **Forgot Password?**.

The **Reset the password (1/3)** dialog box is displayed. See Figure 2-2.

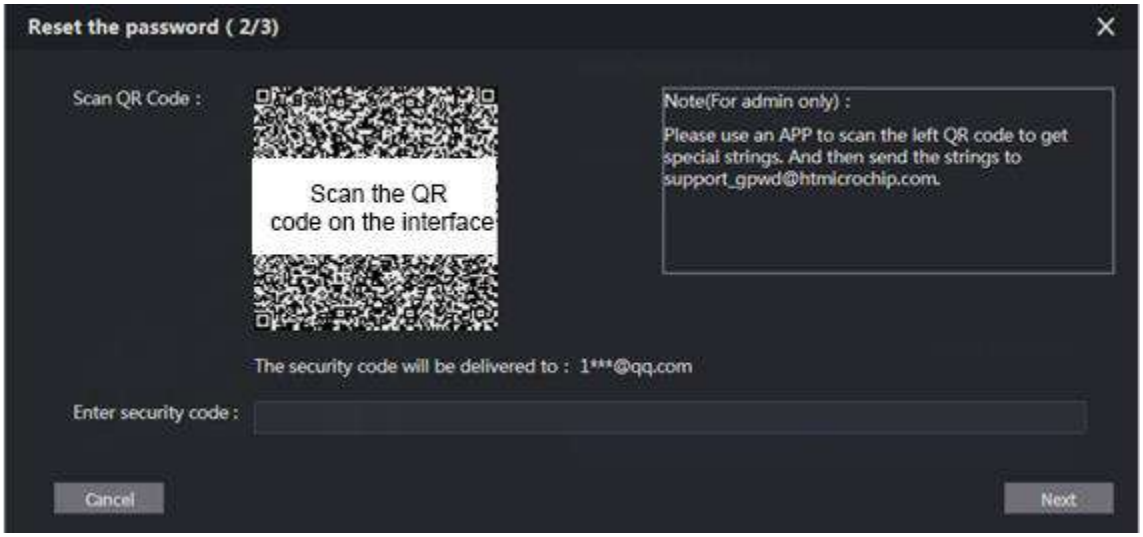
Figure 2-2 Reset the password (1/3)



Step 2 Click **Next**.

The **Reset the password (2/3)** dialog box is displayed. See Figure 2-3.

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



Step 3 Scan the QR code on the web interface to obtain the security code in your mailbox, and then enter the security code in the input box.

- If you did not configure email during initialization, contact the supplier or customer service for help.
- To obtain security code again, refresh QR code interface.
- Use the security code within 24 hours after receiving it. Otherwise, it will become invalid.
- If wrong security code is entered for 5 times continuously, this account will be locked for 5 min.

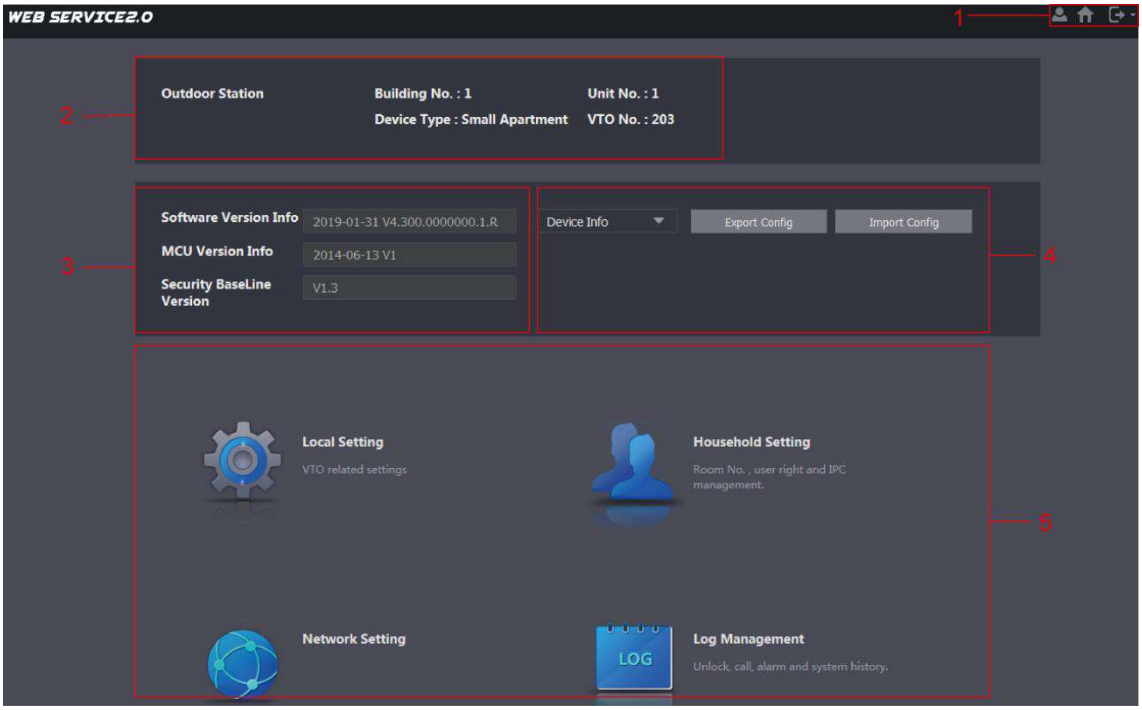
Step 4 Click **Next**, and then the **Reset the password (3/3)** dialog box is displayed.

Step 5 Set and confirm the new password as instructed, and then click **OK**.

3 Main Interface

Log in to the web interface of the VTO, and then the main interface is displayed. See Figure 3-1.

Figure 3-1 Main interface



For the introduction of the main interface, see Table 3-1.

Table 3-1 Main interface introduction

No.	Function	Description
1	General function	These buttons are displayed all the time ● Click  to change the password and your Email address. ● Click  to go to the main interface. ● Click  to log out, reboot the VTO or restore the VTO to factory settings.
2	VTO information	You can view the general information of the VTO, including building No., unit No., device type, and VTO No..
3	System information	You can view the software version, MCU version, and security baseline version.
4	Config manager	Select **Device Info** or **User Info**, and then you can export the VTO configuration or user information to the PC or import VTO configuration or user information to the VTO from PC.
5	Function area	Click the buttons to go to the corresponding menu.

4 Local Setting

This chapter introduces how to configure VTO type, VTO No., video and audio, access password, system time, and security function.

General operations:

- After every configuration, click **Confirm** to save, and click **Refresh** to view the latest change.
- If you click **Default**, all the configurations in the current page would be restored to the default, and you need to click **Confirm** to save.

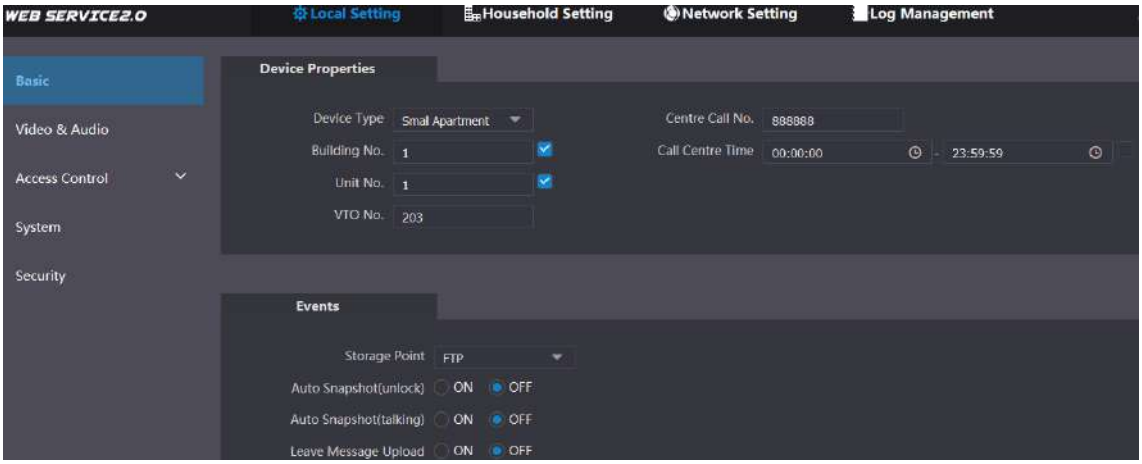
4.1 Basic

This section introduces the configuration of VTO device type, VTO number and auto storage.

Step 1 On the main interface (Figure 3-1), select **Local Setting > Basic**.

The **Basic** interface is displayed. See Figure 4-1.

Figure 4-1 Basic



Step 2 Configure parameters, and for the detailed description, see Table 4-1.

Table 4-1 Basic parameter description

Parameter	Description
Device Type	Select **Small Apartment**. Building number and unit number are available only when other servers work as SIP server. See "6.3 SIP Server."
Centre Call No.	Configure the number of the management centre, and you can call the management centre on every VTO or VTH in the network. The default number is 888888.
Call Centre Time	Time period in which you are allowed to call the management centre.
VTO No.	The VTO number can be used to differentiate each VTO, and it is normally configured according to unit or building number. You can add VTO devices to the SIP server with their numbers.

Parameter	Description
Storage Point	You can only select **FTP**, and all the snapshots will be saved to the FTP server automatically. ● Auto Snapshot (unlock) Select **ON** to enable this function, and then the system takes snapshot every time when the door is unlocked. ● Auto Snapshot (talking) Select **ON** to enable this function, and then the system takes snapshot every time when VTH user answers a call from the VTO. ● Leave Message Upload Select **ON** to enable this function, and then the system uploads the messages from visitors to the FTP server automatically. ● You need to enable FTP function first. See "6.2 FTP." ● If there is SD card in the main VTH, the messages left will be saved to the SD card by default. ● To receive message, the **VTO Message Time** must be configured to be more than 0. See the VTH user's manual.

Step 3 Click **Confirm** to save.

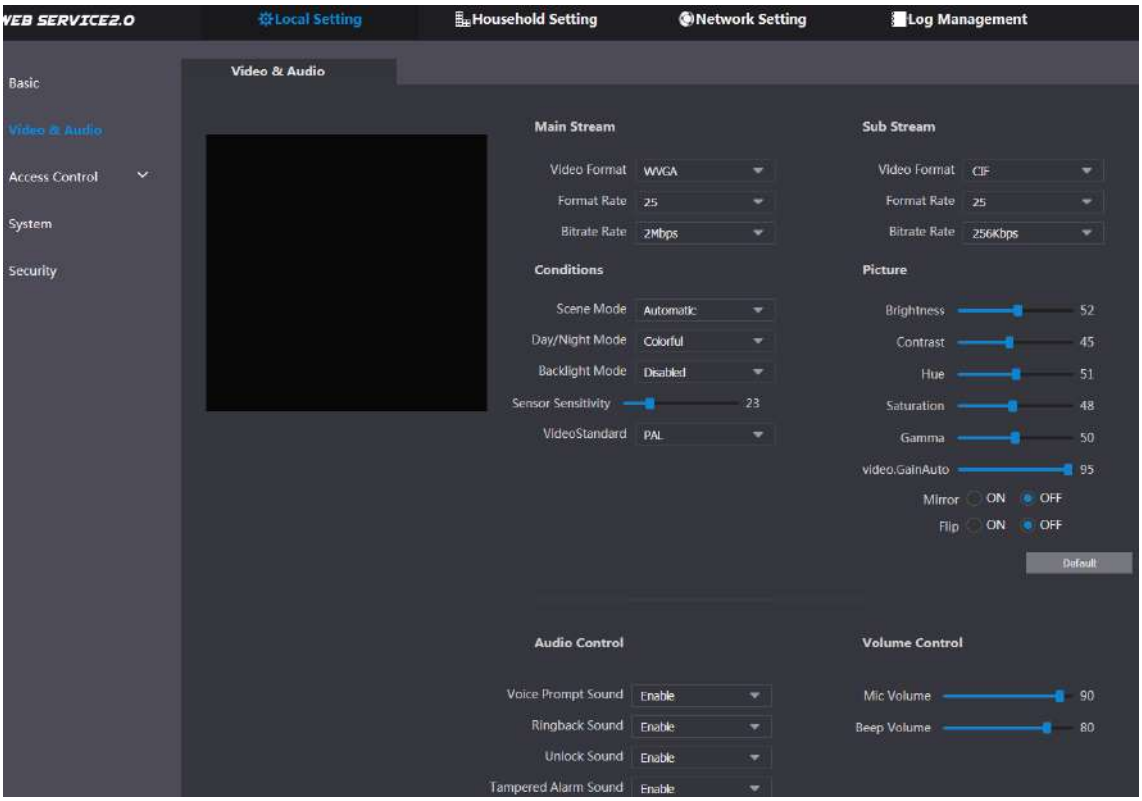
4.2 Video & Audio

This section introduces how to configure the format and quality of the video that the VTO records, and the audio control settings.

Step 1 On the main interface (Figure 3-1), select **Local Setting > Video & Audio**.

The **Video & Audio** interface is displayed. See Figure 4-2.

Figure 4-2 Video & Audio



Step 2 Configure parameters, and these configurations take effect immediately. See Table 4-2.

Table 4-2 Video parameter description

Parameter		Description
Main Stream	Video Format	Select the video resolution from **720P**, **WVGA**, and **D1**.
	Format Rate	Configure the number of frames in 1 second. You can select from **1** to **25** under **PAL**, and **1** to **30** under **NTSC**. The larger the value is, the smoother the video will be.
	Bitrate	Configure the data amount that transmitted in 1 second. You can select as needed. The larger the value is, the better the video quality will be.
Sub Stream	Video Format	Select the video resolution from **CIF**, **WVGA**, **QVGA**, and **D1**.
	Format Rate	Configure the number of frames in 1 second. You can select from **1** to **25** under **PAL**, and **1** to **30** under **NTSC**. The larger the value is, the smoother the video will be.
	Bitrate Rate	Configure the data amount that transmitted in 1 second. You can select as needed. The larger the value is, the better the video quality will be.
Conditions	Scene Mode	Adjust the video to adapt to different scenarios. You can select from **Automatic** (by default), **Sunny**, **Night** and **Disabled**.
	Day/Night Mode	You can select from **Automatic**, **Colorful** or **Black White** mode.
	BackLight Mode	You can select from the following modes: ● **Disabled**: no back light. ● **Backlight**: the camera gets clearer image of the dark areas on the target when shooting against light. ● **Wide dynamic**: the system dims bright areas and compensates dark areas to ensure the clarity of all the area. ● **Inhibition**: the system constrains bright areas and reduces halo size to dim the overall brightness.
	Sensor Sensitivity	Adjust the value, and the larger the value is, the easier the sensor will be triggered.
	Video Standard	Select from **PAL** or **NTSC** according to your display device.
Picture	Brightness	Changes the value to adjust the picture brightness. The larger the value is, the brighter the picture will be, and the smaller the darker. The picture might be hazy if the value is configured too big.
	Contrast	Changes the contrast of the picture. The larger the value is, the more the contrast will be between bright and dark areas, and the smaller the less. If the value is set too big, the dark area would be too dark and bright area easier to get overexposed. The picture might be hazy if the value is set too small.
	Hue	Makes the color deeper or lighter. The default value is made by the light sensor, and it is recommended.

Parameter		Description
	Saturation	Makes the color deeper or lighter. The larger the value is, the deeper the color will be, and the lower the lighter. Saturation value doesn't change image brightness.
	Gamma	Changes the picture brightness and improves the picture dynamic range in a non-linear way. The larger the value is, the brighter the picture will be, and the smaller the darker.
	Video.GainAuto	Amplify the video signal to increase image brightness. If the value is too big, there will be more noise in the image.
	Mirror	Select **On**, and then the image is displayed with left and right side reversed.
	Flip	Select **On**, and then the image is displayed upside down.
Audio Control	Select **Enable** or **Disabled** to turn on or off each sound.	
Volume Control	Mic Volume	Adjust the value, and the larger the value is, the louder the microphone on the VTO will be.
	Beep Volume	Adjust the value, and the larger the value is, the louder the system sounds will be.

4.3 Access Control

This section introduces how to configure the lock, including unlock responding interval, unlock period, door sensor check time, first unlock command, and door contact type.

4.3.1 Local

Step 1 On the main interface (Figure 3-1), select **Local Setting > Access Control > Local**.

Figure 4-3 Local setting

Step 2 Configure parameters, and for the detailed description, see Table 4-3.

Table 4-3 Local access control parameter description

Parameter	Description
Unlock Responding Interval	The time interval to unlock again after the previous unlock, and the unit is second.
Unlock Period	The time amount for which the lock stays open after unlock, and the unit is second.

Parameter	Description
Door Sensor Check Time	If you have installed door sensor, then you can configure the time period, and If the unlock time exceeds the **Door Sensor Check Time**, the door sensor alarm is triggered, and the alarm will be sent to the management center. ● Select the **Enable** check box, and the door will not be locked until the door sensor contacts each other. ● If you do not select the **Enable** check box, the door will be locked after the **Unlock Period** finishes.
First Unlock Command	You can connect a third-party phone such as SIP phone to your VTO, and use the command to open the door remotely.
Door Contact Type	Select **NC** or **NO** according to the lock you use.

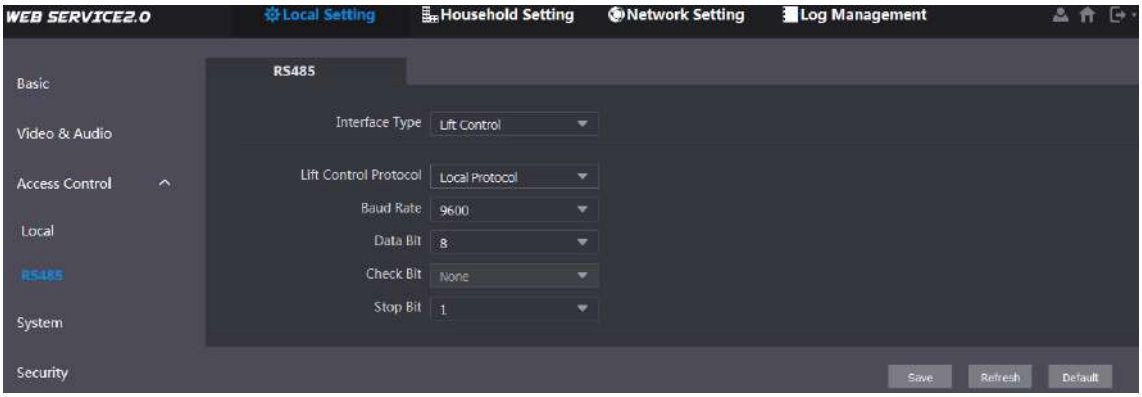
Step 3 Click **Save**.

4.3.2 RS-485

This section introduces the access control configuration of RS-485 devices, including lock and lift control.

Step 1 On the main interface (Figure 3-1), select **Local Setting > Access Control > RS485**. The **RS485** interface is displayed. See Figure 4-4.

Figure 4-4 RS-485



Step 2 Configure parameters, and you can select **Lock** or **Lift Control** in the **Interface Type** list. For the detailed description, see Table 4-4.

Table 4-4 RS-485 access control parameter description

Parameter		Description
Lock	Unlock Responding Interval	The time interval to unlock again after the previous unlock, and the unit is second.
	Unlock Period	The time amount for which the lock stays open after unlock, and the unit is second.
	Second Unlock Command	You can connect a third-party phone such as SIP phone to your VTO, and use the command to open the door remotely.
	Second Lock	You can connect one more door to RS-485 device. ● If you select the **Enable** check box, then the second lock will be opened by default when pressing unlock button, swiping access card or using unlock password.

Parameter		Description
		● If you do not select the **Enable** check box, then the first lock will be opened by default when pressing unlock button, swiping access card or using unlock password.
Lift Control	Lift Control Protocol	Select the protocol as needed to enable the lift control function, and then you can configure the floors that lift users can go to.
	Baud Rate	Enter the baud rate of the third party RS-485 device that you need.
	Data Bit	These items can be used for serial port debugging.
	Check Bit	
	Stop Bit	

Step 3 Click **Save**.

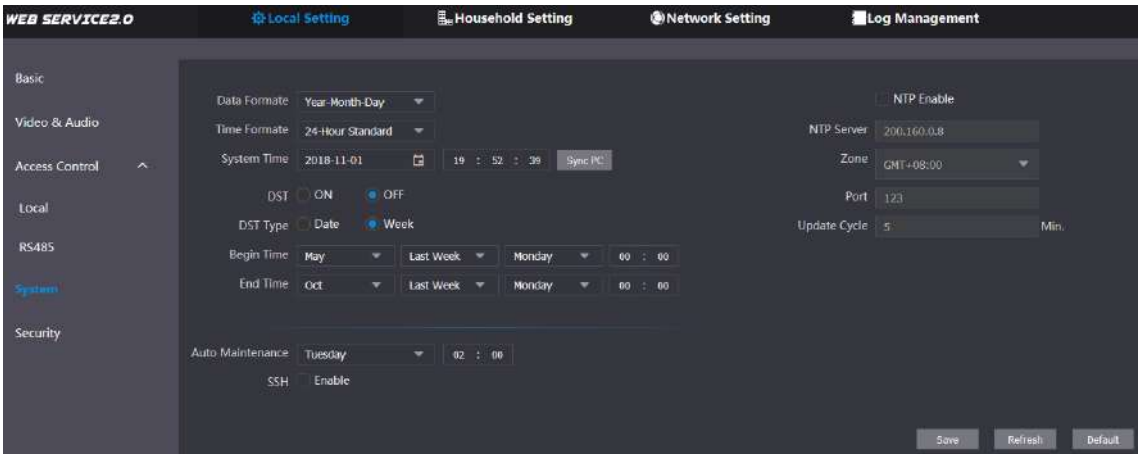
4.4 System

This section introduces how to configure the date format, time format, and the NTP server.

Step 1 On the main interface (Figure 3-1), select **Local Setting > System**.

The **System** interface is displayed. See Figure 4-5.

Figure 4-5 System



Step 2 Configure parameters, and for the detailed description, see Table 4-5.

Table 4-5 System parameter description

Parameter	Description
Date format	You can select from Year-Month-Day, Month-Day-Year, and Day-Month-Year.
Time format	Configure the time format, and you can select from **12-Hour** or **24-Hour**.
System Time	Configure the VTO system date, time and time zone. Do not change the system time arbitrarily; it might cause problems on video searching and publishing snapshot or notice. Before changing the system time, turn off video recording or auto snapshot.
Sync PC	Click to sync the VTO system time and the PC system time.

Parameter	Description
DST	Select **ON** to enable DST.
DST Type	Select **Date** to define a specific date for DST or select **Week** for it.
Begin Time	Configure the begin time and end time for DST.
End Time	
NTP Enable	Select the check box to enable NTP timing.
NTP Server	Enter the domain name of the NTP server.
Zone	The time zone of the current area.
Port	The port number of the NTP server.
Update Cycle	The time interval that the VTO syncs time with the NTP server, and it is 30 min at most.
Auto Maintenance	Select the day and time for the auto maintenance, and the VTO will reboot then.
SSH	Select the **Enable** check box, and then you can connect debugging devices to the VTO through SSH protocol.

Step 3 Click **Save**.

4.5 Security

Step 1 On the main interface (Figure 3-1), select **Local Setting > Security**.
The **Security** interface is displayed. See Figure 4-6.

Figure 4-6 Security

Step 2 Configure parameters, and for the detailed description, see Table 4-6.

Table 4-6 Security parameter description

Parameter	Description
CGI Enable	Select the check box to enable CGI, and then you can use CGI command.
Reset Password	Select the check box to enable password resetting, and then the password resetting is available.

Step 3 Click **Save**.

5 Household Setting

This chapter applies to the condition in which the VTO works as SIP server (see 6.3 SIP Server), and it introduces how to add, modify, and delete VTO, VTH, VTS, and IPC devices, and how to send messages from the SIP server to other VTO and VTH devices. If you are using other servers as SIP server, see the corresponding manual for the detailed configuration.

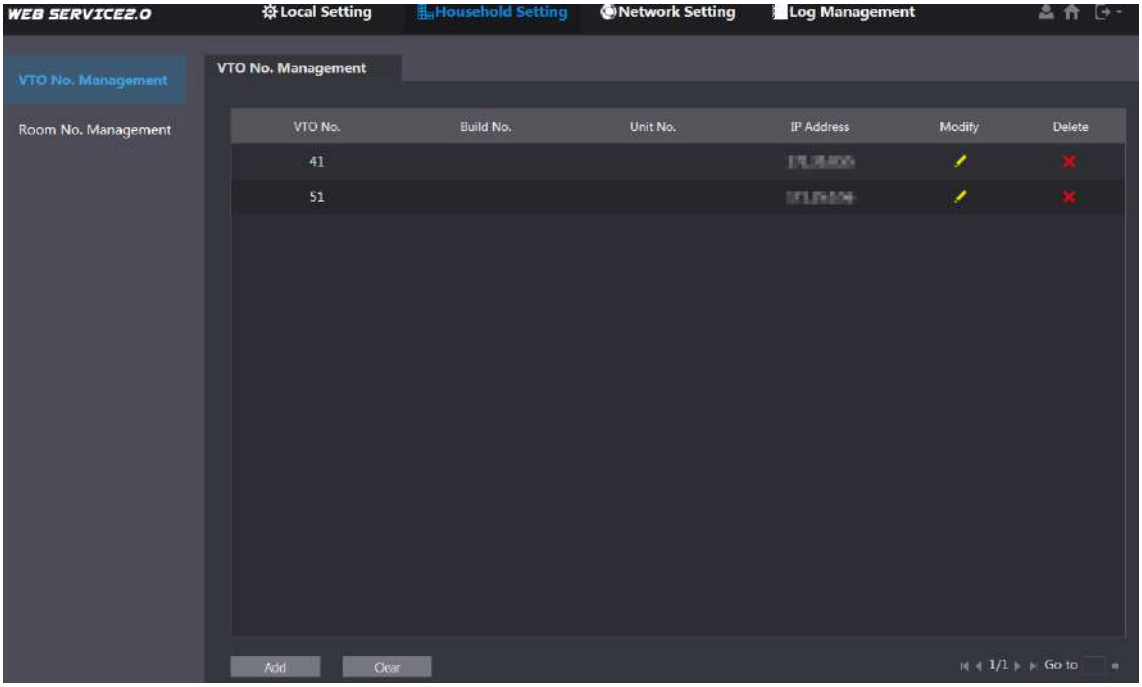
5.1 VTO No. Management

5.1.1 Adding VTO

You can add VTO devices to the SIP server, and all the VTO devices connected to the same SIP server can make video call between each other.

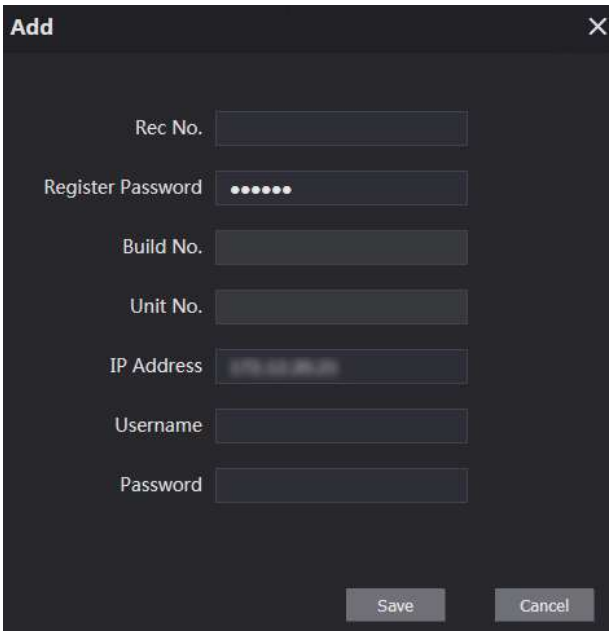
Step 1 Log in to the web interface of the SIP server, and then select **Household Setting > VTO No. Management**.

Figure 5-1 VTO No. management



Step 2 Click **Add**.

Figure 5-2 Add VTO



Step 3 Configure the parameters, and be sure to add the SIP server itself too. See Table 5-1.

Table 5-1 Add VTO configuration

Parameter	Description
Rec No.	The VTO number you configured for the target VTO. See the details in "Table 4-1."
Register Password	Keep default value.
Build No.	Available only when other servers work as SIP server.
Unit No.	
IP Address	The IP address of the target VTO.
Username	The user name and password for the WEB interface of the target VTO.
Password	

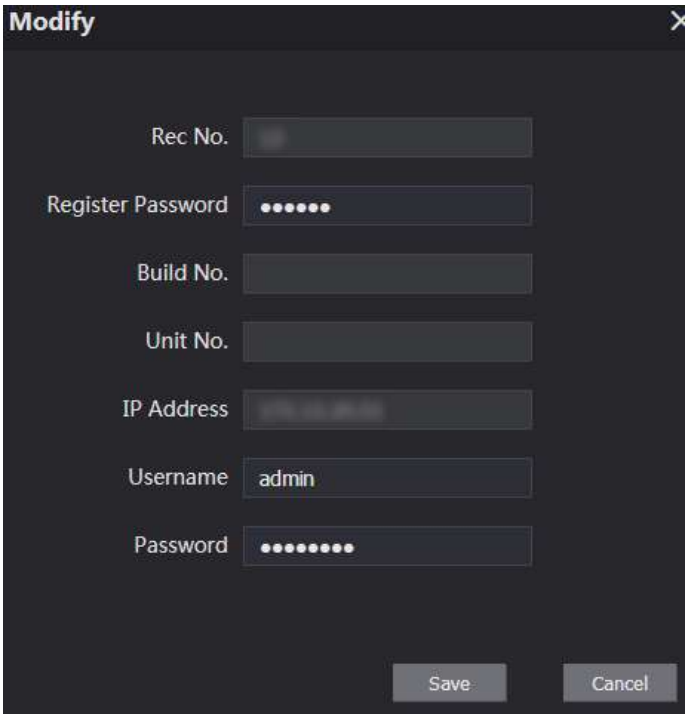
Step 4 Click **Save**.

5.1.2 Modifying VTO

The VTO that is currently at use cannot be modified or deleted.

Step 1 On the **VTO No. Management** interface (Figure 5-1), click .

Figure 5-3 Modify VTO



Step 2 You can modify the **Rec No.**, **Username**, and **Password**. See Table 5-1 for the details.

Step 3 Click **Save**.

5.1.3 Deleting VTO

The VTO that is currently at use cannot be modified or deleted.

On the **VTO No. Management** interface (Figure 5-1), click to delete VTO one by one; and click **Clear** to delete all the VTO.

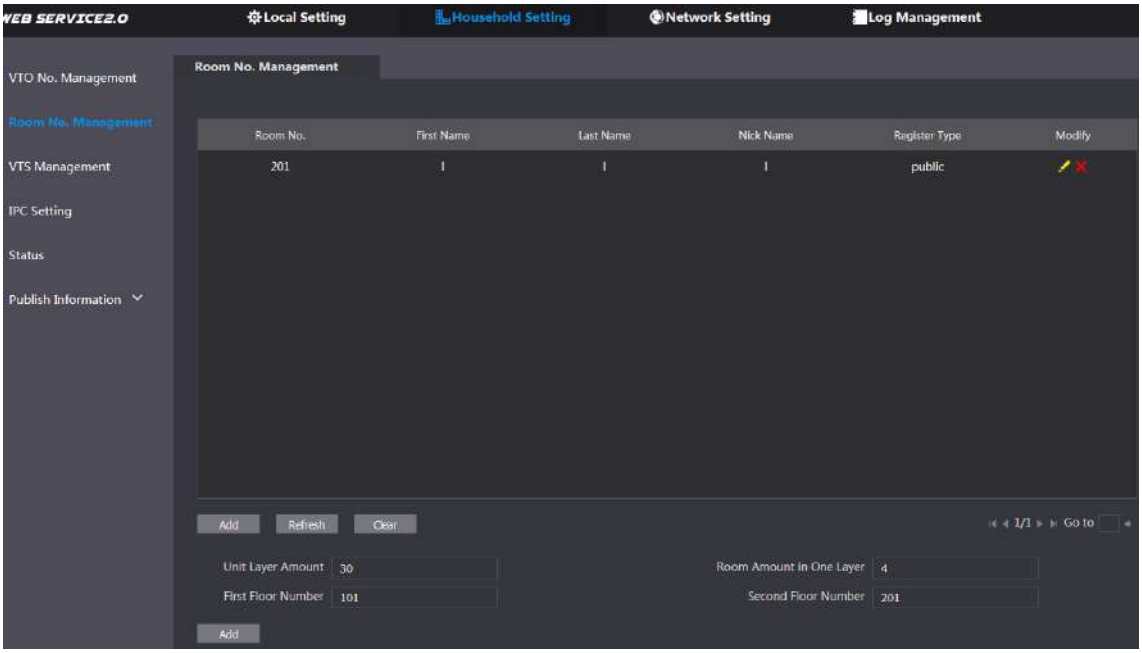
5.2 Room No. Management

5.2.1 Adding Room Number

You can add the planned room number to the SIP server, and then configure the room number on VTH devices to connect them to the network.

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

Figure 5-4 Room No. Management

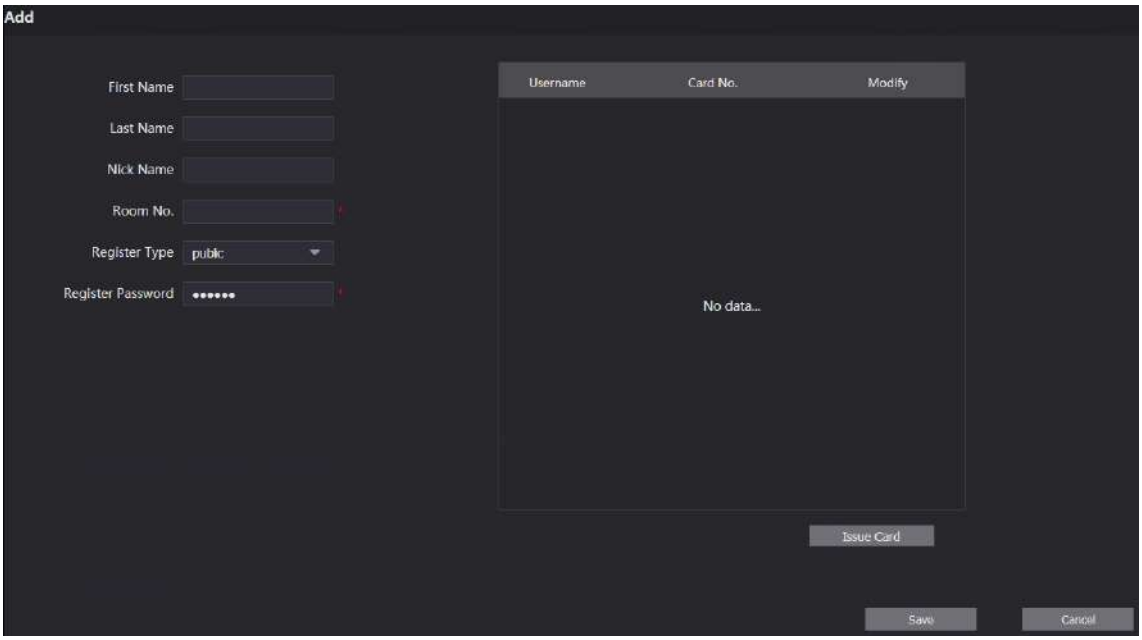


Step 2 You can add single room number or do it in batch.

- Add single room number

1) Click the **Add** at the mid lower position.

Figure 5-5 Add single room number



2) Configure room information, and for the detailed description.

Table 5-2 Room information

Parameter	Description
First Name	Enter the information you need to differentiate each room.
Last Name	
Nick Name	
Room No.	The room number that you planned.
Register Type	Select **public**. **Local** is reserved for future use.
Register Password	Keep the default value.

3) Click **Save**.

The added room number is displayed. Click to modify room information, and click to delete a room.

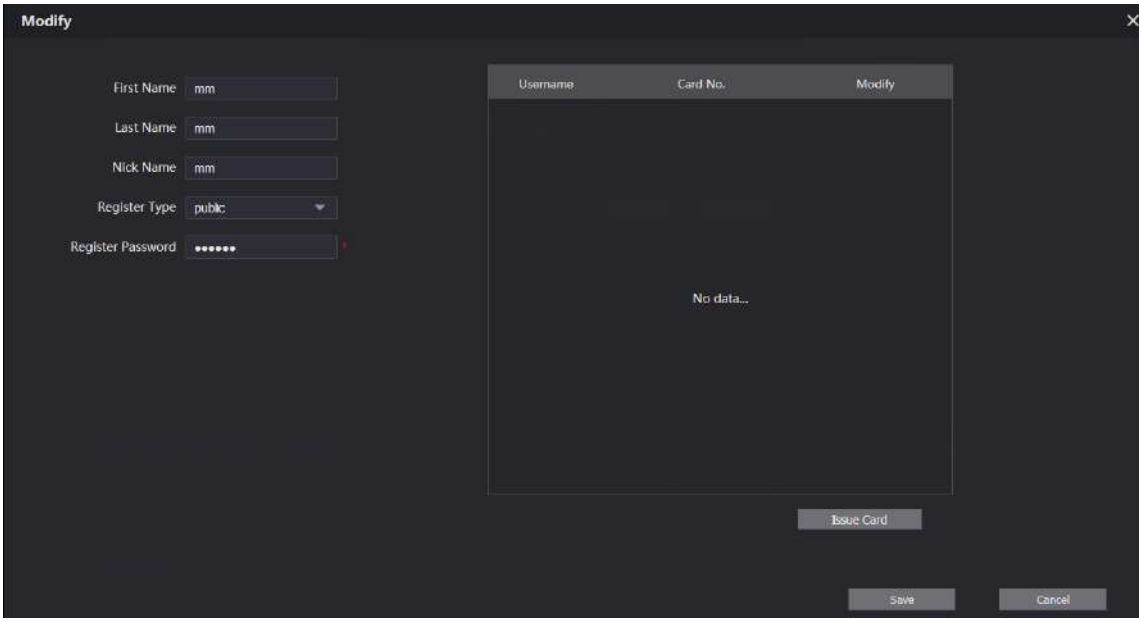
- Add room numbers in batch

4) Configure the **Unit Layer Amount**, **Room Amount in One Layer**, **First Floor Number**, and **Second Floor Number** according to the actual condition.
5) Click the **Add** at the bottom position.
All the added room numbers are displayed. Click **Refresh** to view the latest status, and click **Clear** to delete all the room numbers.

5.2.2 Modifying Room Number

Step 1 On the **Room No. Management** interface (Figure 5-4), click .

Figure 5-6 Modify room number



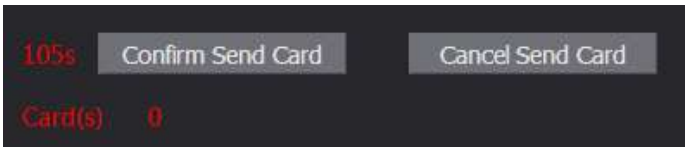
Step 2 You can modify the names for the room. See Table 5-2 for the details.
Step 3 Click **Save**.

5.2.3 Issuing Access Card

You can issue card to a room, and can also set it to be the main card, or to the lost state.

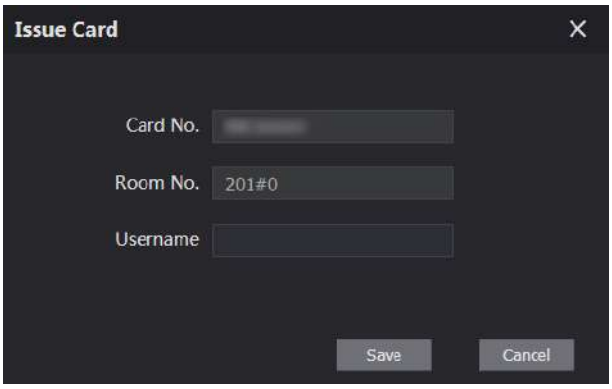
Step 1 On the **Modify room number** interface (Figure 5-6), click **Issue Card**.

Figure 5-7 Countdown notice



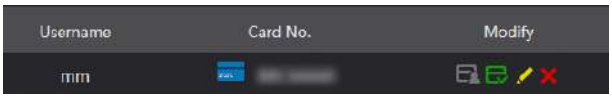
Step 2 Swipe the card that needs to be authorized on the VTO, and then the **Issue Card** dialogue box is displayed. See Figure 5-8.

Figure 5-8 Issue card



Step 3 Enter the name you need, then click **Save**, and then click **Confirm Send Card** at the countdown notice (Figure 5-7).

Figure 5-9 Issued access card



Step 4 You can configure the access card.

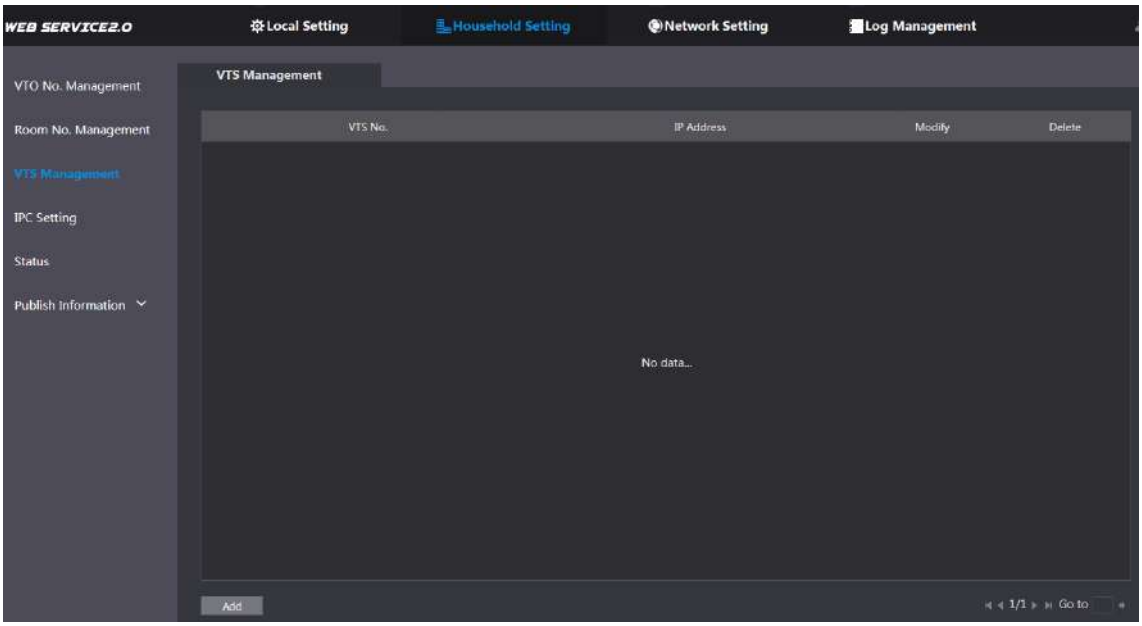
- Click to set it as the main card, and then the icon turns to . The main card can be used to issue access card for this room on the VTO. Click again to resume.
- Click to set it to the lost state, and then the icon turns into . The card under lost state cannot be used to open the door. Click again to resume.
- Click to modify the user name.
- Click to delete the card.

5.3 VTS Management

You can add VTS device to the SIP server, and the VTS can be used as the management center. It can manage all the VTO and VTH devices in the network, make or receive video call from them, and make basic configurations. For the detailed introduction, see the corresponding user's manual.

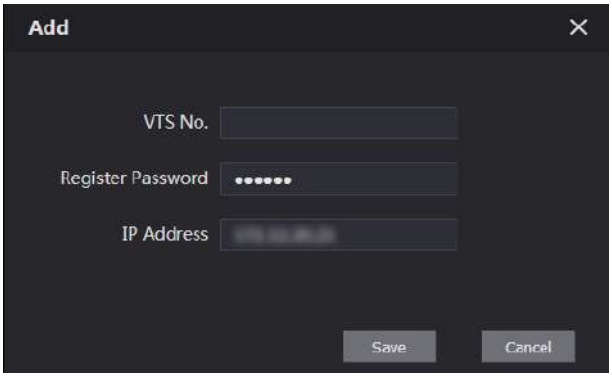
Step 1 Log in to the web interface of the SIP server, and then select **Household Setting > VTS Management**

Figure 5-10 VTS management



Step 2 Click **Add**.

Figure 5-11 Add VTS



Step 3 Configure the parameters, and for the detailed description, see Table 5-3.

Table 5-3 Add VTS configuration

Parameter	Description
VTS No.	The VTS number you configured for the target VTS.
Register Password	Keep default value.
IP Address	The IP address of the target VTS.

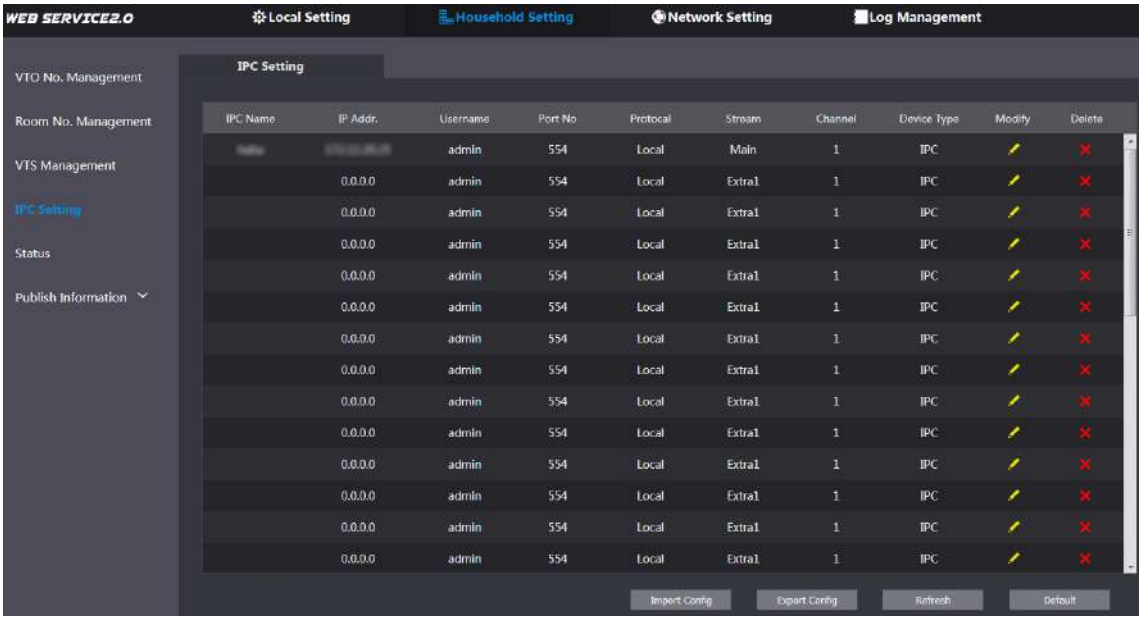
Step 4 Click **Save**, and then the added VTS is displayed. Click to modify IP address, and click to delete.

5.4 IPC Setting

You can add IPC, NVR, HCVR, and XVR to the SIP server, and then all the connected VTH can do monitor with the added cameras.

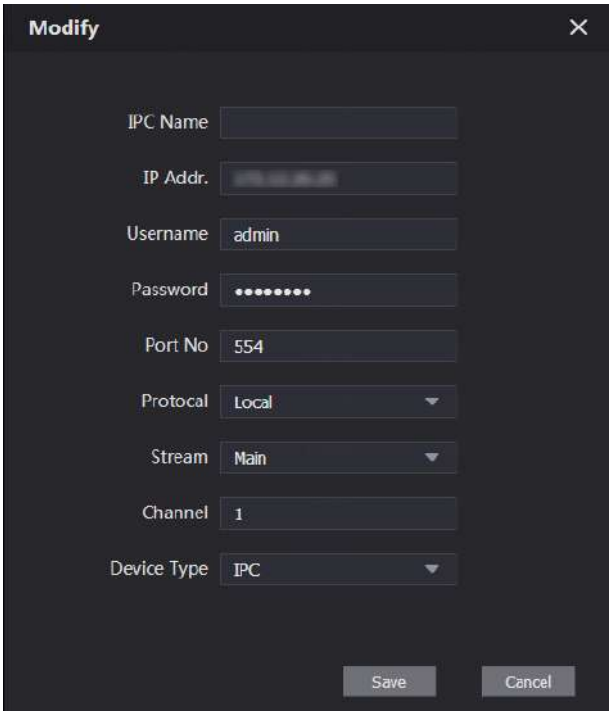
Step 1 Log in to the web interface of the SIP server, and then select **Household Setting > IPC Setting**

Figure 5-12 IPC setting



Step 2 The total quantity of the device you can add is fixed, and you can click  to add the device you need.

Figure 5-13 Modify



Step 3 Configure the parameters, and for the detailed description, see Table 5-4.

Table 5-4 Add IPC configuration

Parameter	Description
IPC Name	Enter the name of the device you need.
IP Addr.	The IP address of the device.
Username	The user name and password for the web interface of the device.
Password	
Port No.	Keep default value.
Protocol	Select from **Local** or **Onvif**.

Parameter	Description
Stream	Select from **Main** or **Extra1**, and the main stream has better image quality, but also requires more bandwidth.
Channel	Define a channel for the device.
Device Type	Select from **IPC**, **NVR**, **HCVR**, and **XVR** as needed.

Step 4 Click **Save**, and then the added device is displayed. Click to modify, and click to delete.

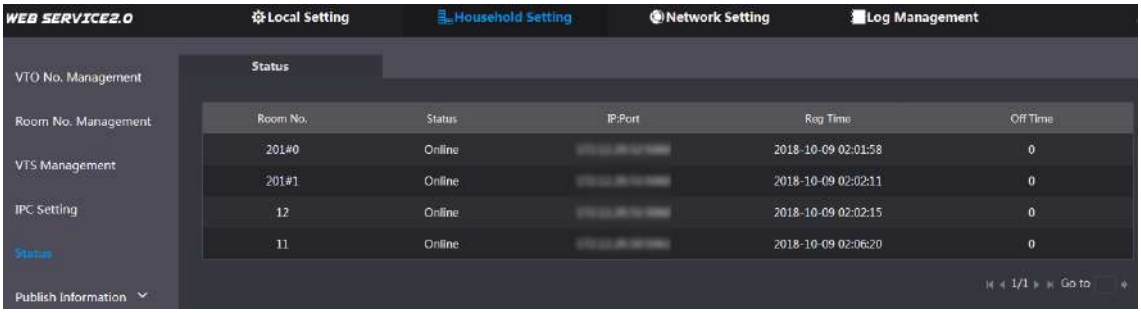
You can also click **Export Config** to export the current devices to the local PC, or click **Import Config** to import the existed configuration.

5.5 Status

You can view the working state and IP address of all the connected devices.

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

Figure 5-14 Status



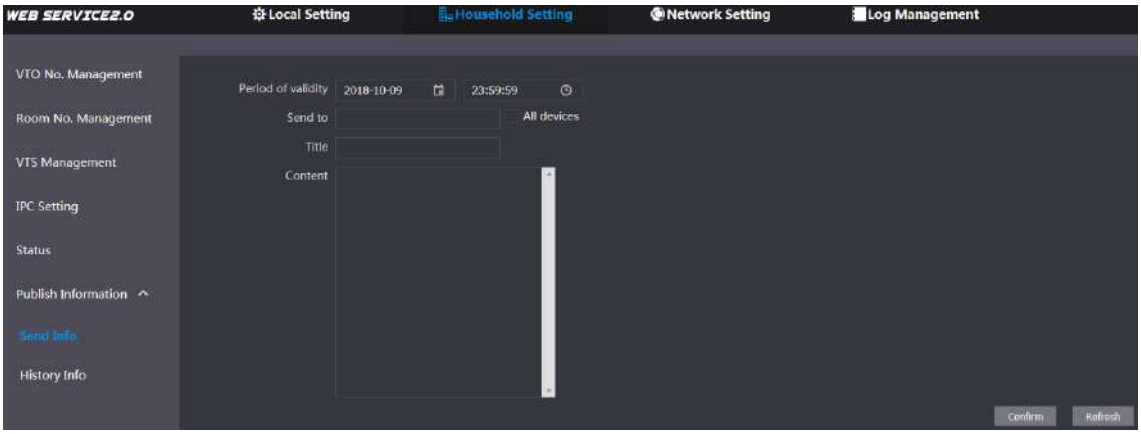
5.6 Publish Information

You can send messages from the SIP server to other VTH devices, and view the message sending history.

5.6.1 Send Info

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

Figure 5-15 Send info



Step 2 Enter the target VTO No. or select **All device** to send the message to all the devices in the network, and then the title and content of your message.

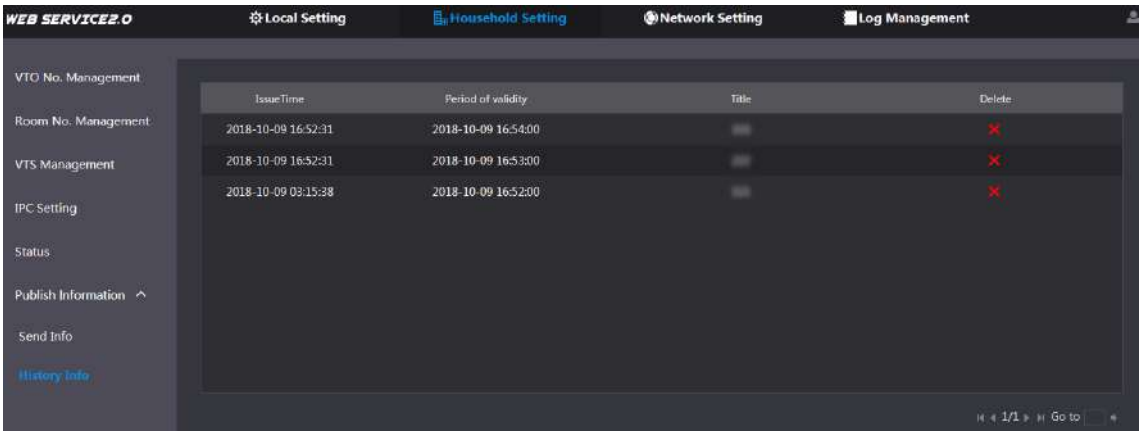
The **Period of validity** is reserved for future use.

Step 3 Click **Confirm**.

5.6.2 History Info

Log in to the web interface of the SIP server, and then select **Household Setting > Publish Information > History Info**. You can view the time and title of the sent messages.

Figure 5-16 History info



6 Network Setting

This chapter introduces how to configure TCP/IP, FTP, SIP server, and IP Permissions.

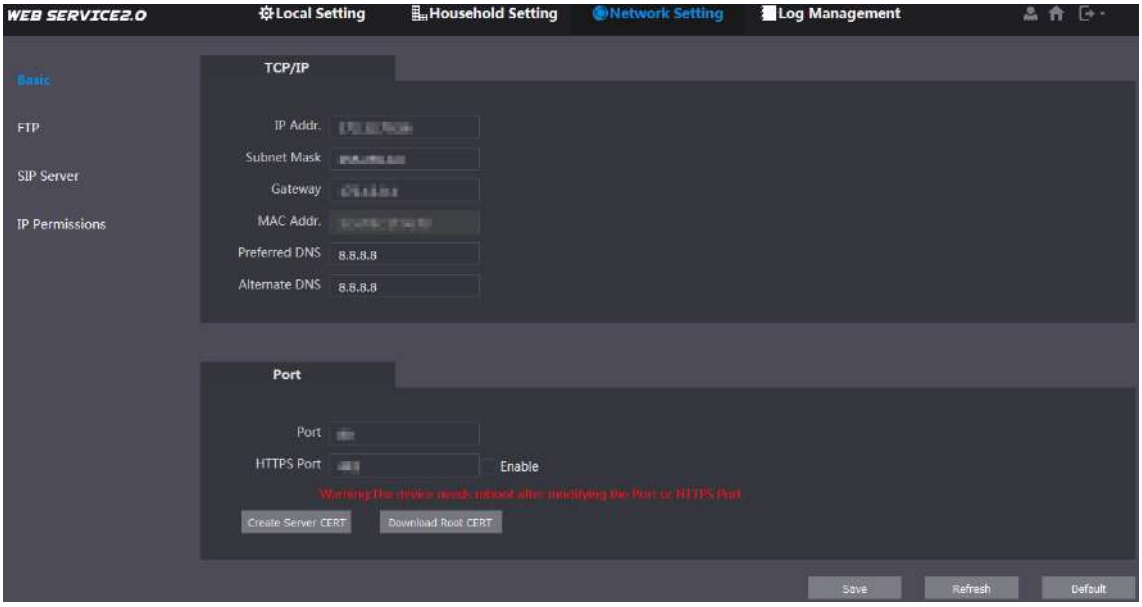
6.1 Basic

6.1.1 TCP/IP

You can modify the IP address and port number of the VTO.

Step 1 Select **Network Setting > Basic**.

Figure 6-1 TCP/IP and port



Step 2 Enter the network parameters and port number that you planned, and then click **Save**. The VTO will restart.

6.1.2 HTTPS

Select the **Enable** check box at **HTTPS Port**, and then the VTO will reboot. After rebooting, you can log in to the VTO by entering "https:// VTO IP address" in the address bar of the explorer.

6.2 FTP

Configure FTP server, and then you can save the recorded videos and snapshots to the FTP server.

Step 1 Select **Network Setting > FTP**.

Figure 6-2 FTP

Step 2 Configure parameters. See Table 6-1.

Table 6-1 FTP parameter description

Parameter	Description
Enable	Select the check box to enable FTP function.
Name	Enter the name of the FTP server as needed.
IP Addr.	The IP address of the FTP server.
Port	It is 21 by default.
Username	The username and password of the FTP server.
Password	

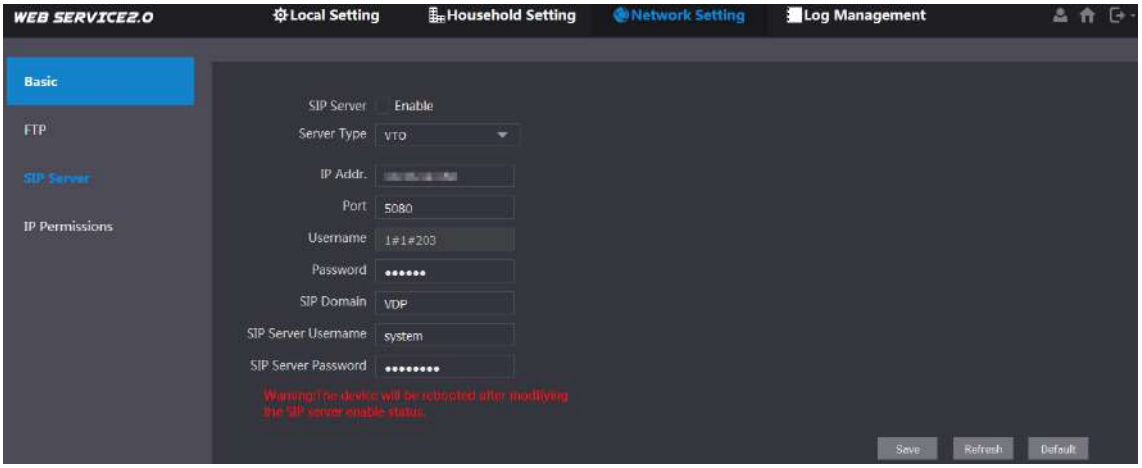
Step 3 Click **Save**.

6.3 SIP Server

The SIP server is required in the network to transmit intercom protocol, and then all the VTO and VTH devices connected to the same SIP server can make video call between each other. You can use VTO device or other servers as SIP server.

Step 1 Select **Network Setting > SIP Server**.

Figure 6-3 SIP Server



Step 2 Select the server type you need.

- If the VTO you are visiting works as SIP server
  Select the **Enable** check box at **SIP Server**, and then click **Save**.
  The VTO will reboot, and after rebooting, you can add VTO and VTH devices to this VTO. See the details in "5 Household Setting."

If the VTO you are visiting does not work as SIP server, do not select the **Enable** check box at **SIP Server**, otherwise the connection will fail.

- If other VTO works as SIP server
  Select **VTO** in the **Server Type** list, and then configure the parameters. See Table 6-2.

Table 6-2 SIP server configuration

Parameter	Description
IP Addr.	The IP address of the VTO which works as SIP server.
Port	5060
Username	Keep the default value.
Password	
SIP Domain	VDP
SIP Server Username	The user name and password for the web interface of the SIP server.
SIP Server Password	

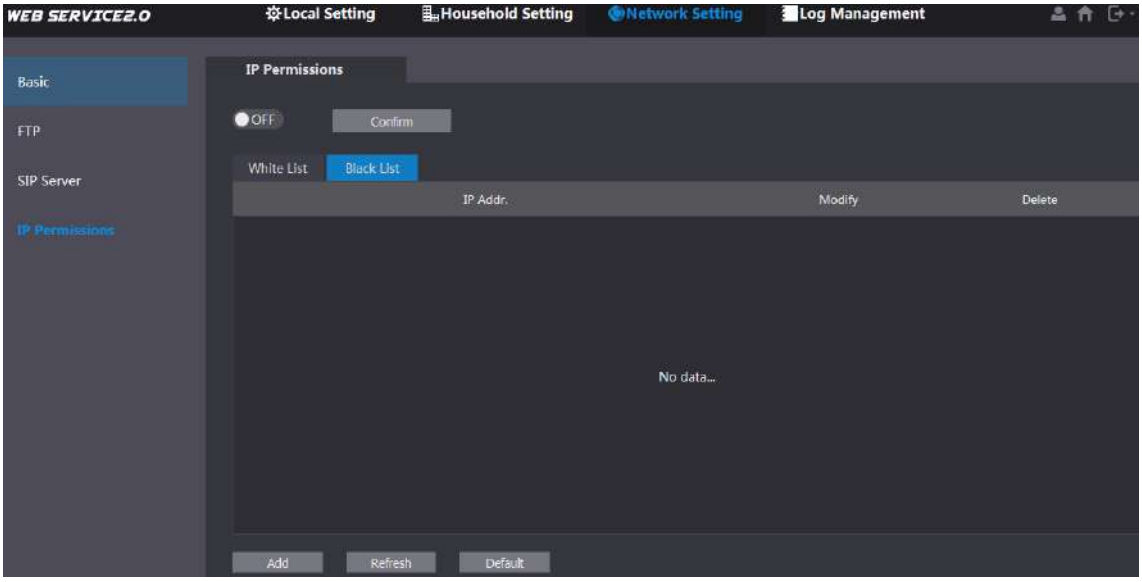
- If other servers work as SIP server
  Select the server type you need at **Server Type**, and then see the corresponding manual for the detailed configuration.

6.4 IP Permissions

To enhance network and data security, you need to configure access authority for different IP addresses.

Step 1 Select **Network Setting > IP Permissions**.

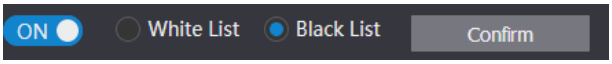
Figure 6-4 IP Permissions



Step 2 Click OFF.

The **White List** option and **Black List** option are displayed. See Figure 6-5.

Figure 6-5 White list and black list



You can only use one of them at a time.

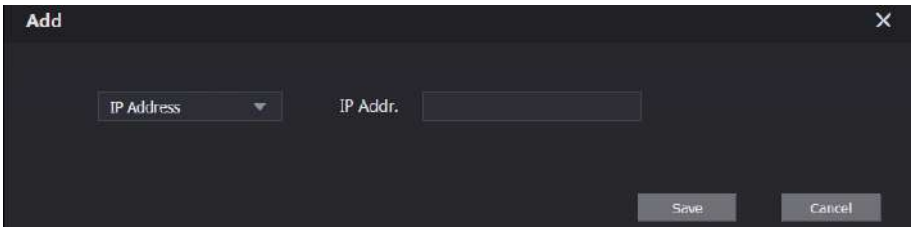
- **White list**: only the IP addresses in the list can log in to the VTO.
- **Black list**: all the IP addresses in the list are prohibited from logging in the VTO.

Step 3 Select **White List** or **Black List**.

- If you need to use black list, select **Black List**, and then click **Confirm**.
- If you need to use white list, select **White List**, and then add an IP address or IP section in the white list before clicking **Confirm**.

Step 4 Click **Add**.

Figure 6-6 Add IP address



Step 5 You can select and enter single IP address or an IP section, and then click **Save**.

7 Log Management

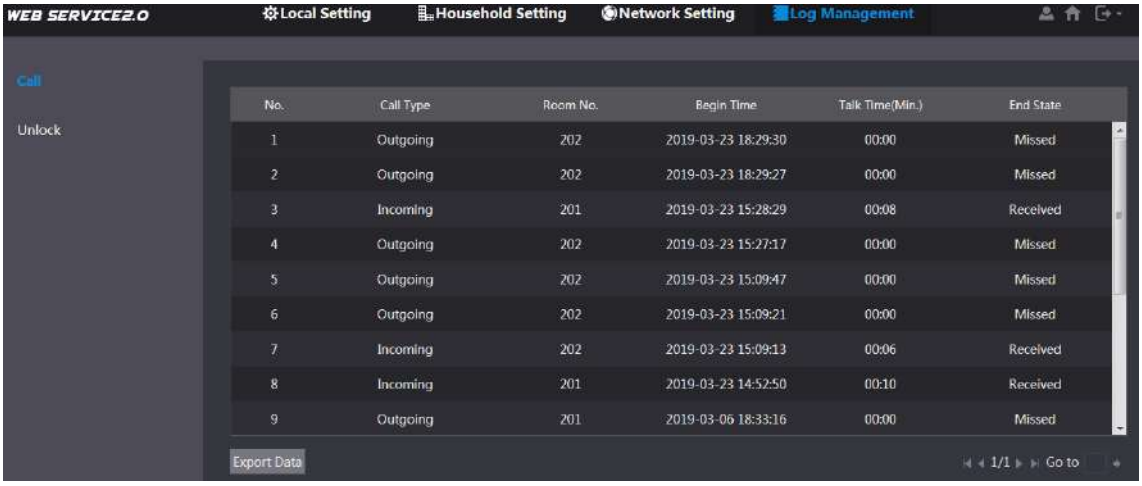
You can view call history, alarm record, unlock record and various system logs.

7.1 Call

You can view the call type, room number, begin time, talk time, and end state.

Step 1 Select **Log Management > C**all.

Figure 7-1 Call



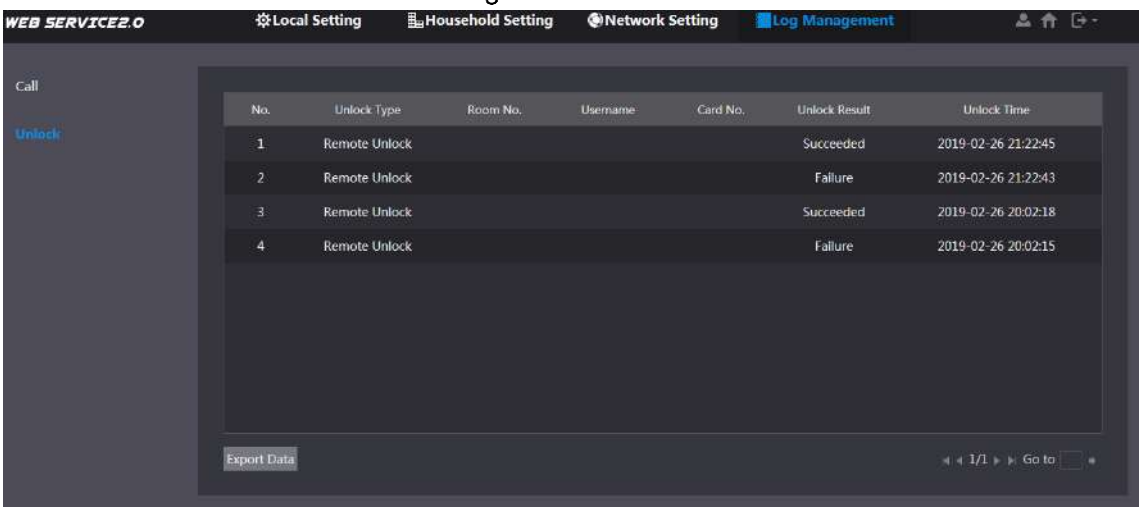
Step 2 Click **Export Data** to export the records to your PC.

7.2 Unlock

You can view various unlock records, including access card unlock, password unlock, remote unlock, and press button unlock.

Step 1 Select **Log Management > Unlock**.

Figure 7-2 Unlock



Step 2 Click **Export Data** to export the records to your PC.

Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

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

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

4. **Enable Account Lock**

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

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

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

6. **Enable HTTPS**

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

7. **Enable Whitelist**

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

8. **MAC Address Binding**

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

9. **Assign Accounts and Privileges Reasonably**

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

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

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

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

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

11. **Audio and Video Encrypted Transmission**

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

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

12. **Secure Auditing**

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

13. **Network Log**

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

14. **Construct a Safe Network Environment**

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

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.

- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.