Unit VTO (Version 4.3)

User’s Manual

V1.0.1

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

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

2. Update Firmware

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

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

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

2. Change Default HTTP and TCP Ports:

● Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.

● These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

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

4. Enable IP Filter:

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

5. Change ONVIF Password:

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

6. Forward Only Ports You Need:

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

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

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

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

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

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

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

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

14. Physically Lock Down the Device:

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

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

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

16. Isolate NVR and IP Camera Network

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

Foreword

General

This Manual introduces the operation of the 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

Privacy Protection Notice

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

About the Manual

- The Manual is for reference only. If there is inconsistency between the Manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Manual.
- The Manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product

updates might cause some differences between the actual product and the Manual. Please contact the customer service for the latest program and supplementary documentation.

- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

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

Operating Requirement

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

Power Requirement

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

Table of Contents

1 Initialization

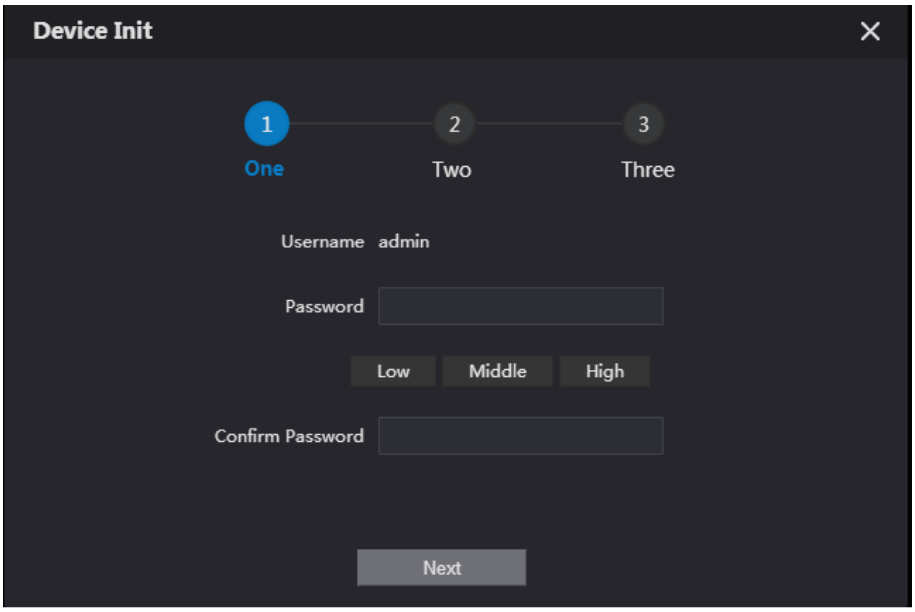
For first time login or after the VTO being reset, you need to initialize the web interface. The default IP address of the VTO is 192.168.1.110, and make sure the PC is in the same network segment as the VTO.

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.

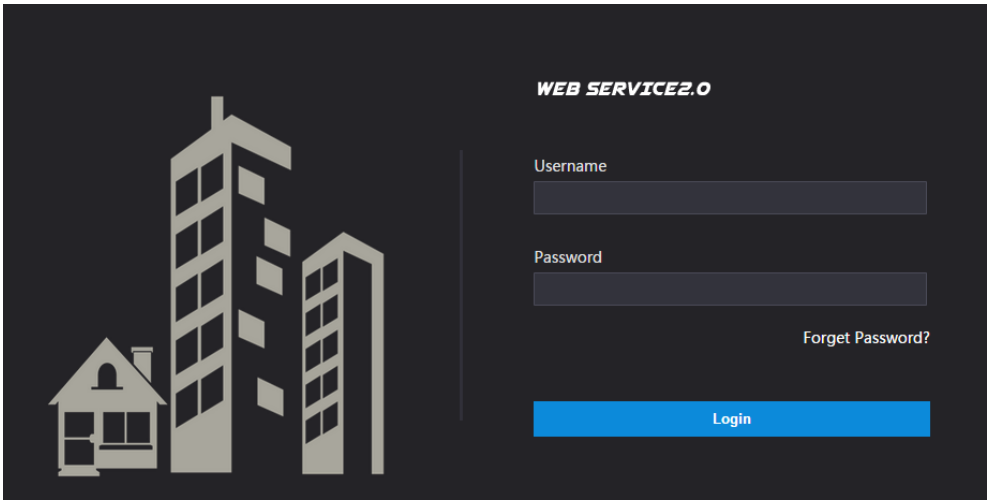
Step 4 Select the **Email** check box, and then enter your Email address. This Email address can be used to reset the password, and it is recommended to finish this setting.

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

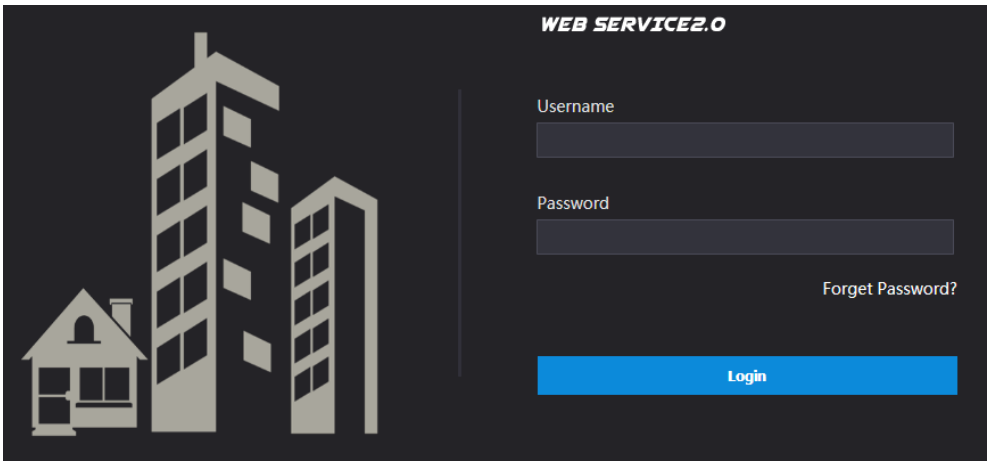
2.1 Logging In

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



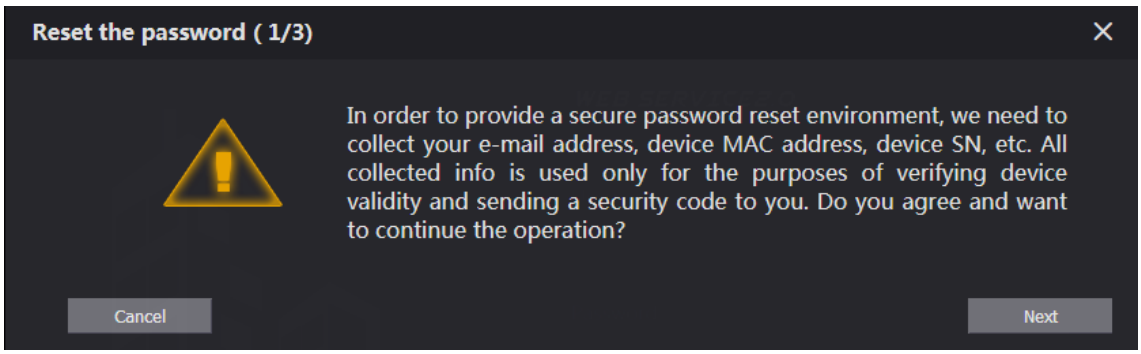
Step 2 Enter "admin" as username, then the password you set during initialization, and then click **Login**.

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.

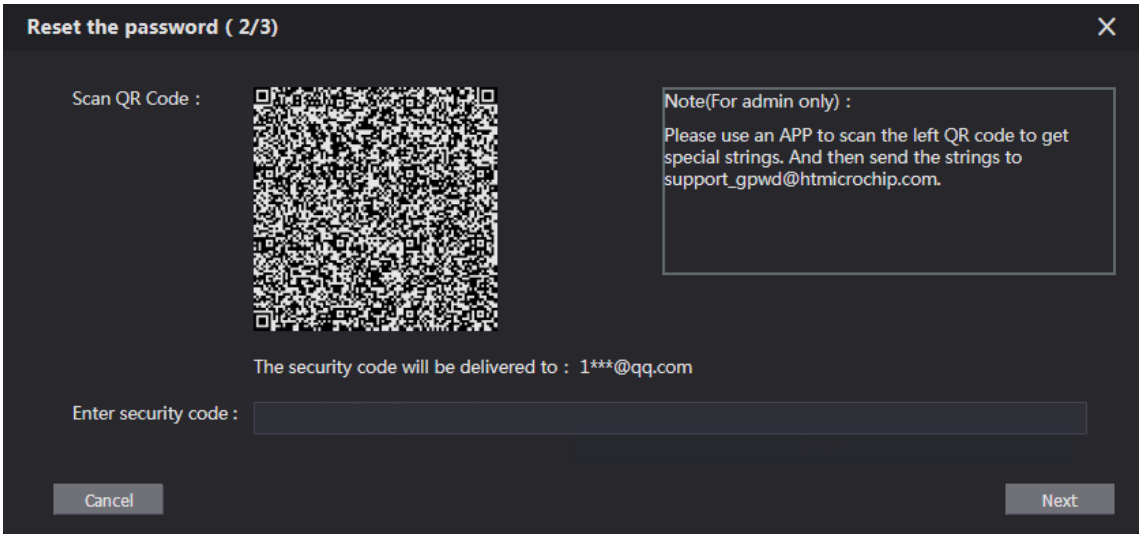
Figure 2-2 Reset the password (1/3)



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 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.

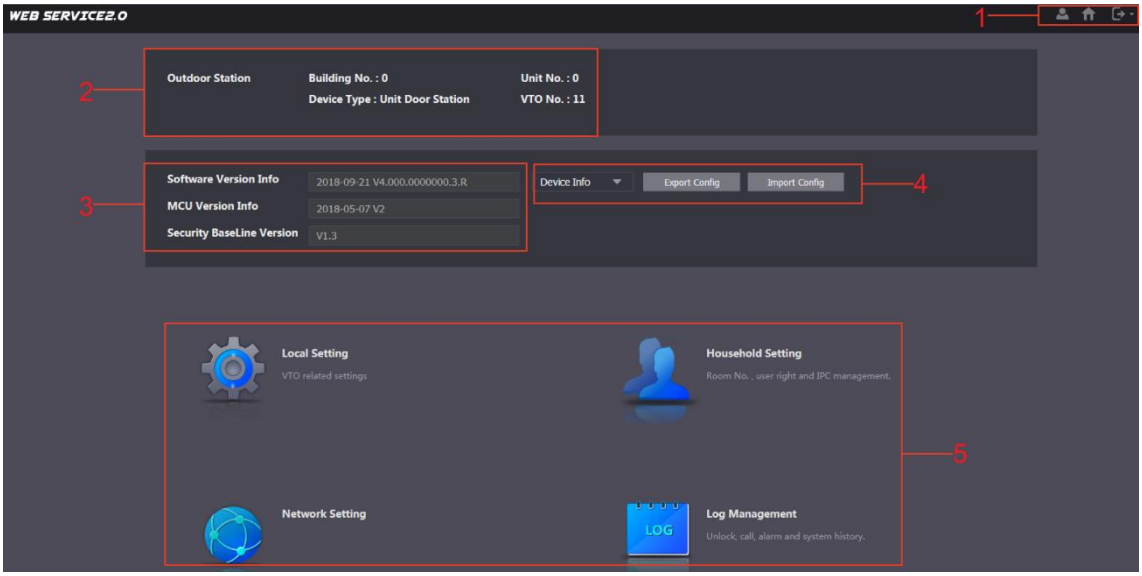
Step 4 Click **Next**, and then the **Reset the password (3/3)** dialog box is displayed.

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

3 Main Interface

Log in 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 them from it.
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.

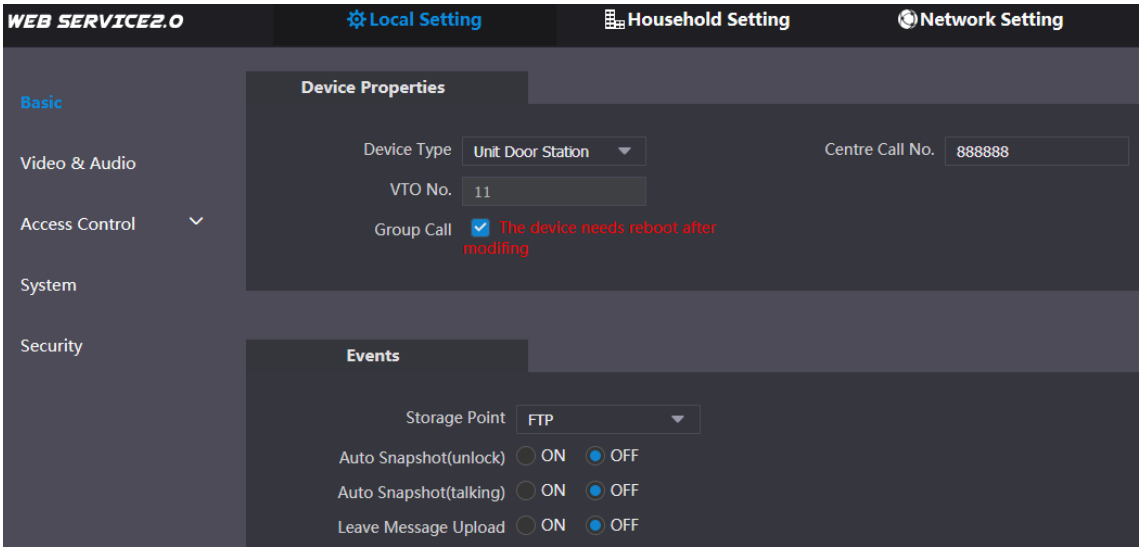
4.1 Basic

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	You can select Unit Door Station or Fence Station. ● **Unit Door Station**: Normally installed inside the community with a specific building number or unit number. ● **Fence Station**: Normally installed at the community gate, and you need to enter the building number, unit number, and room number to call a specific room. You cannot leave message or view contact on fence station. ● Building number and unit number are available only when other servers work as SIP server. See "6.4 SIP Server."

Parameter	Description
	● Fence station is normally used when other servers work as 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.
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. If a VTO does not serve as a SIP server, then its VTO No. can be modified (log in the web page of the VTO, and then you can modify it.).
Group Call	Select the check box to enable this function, and when calling a master VTH, the extension VTH devices receive the call as well.
Storage Point	You can only select **FTP**, and all the snapshots would 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 left messages would 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.

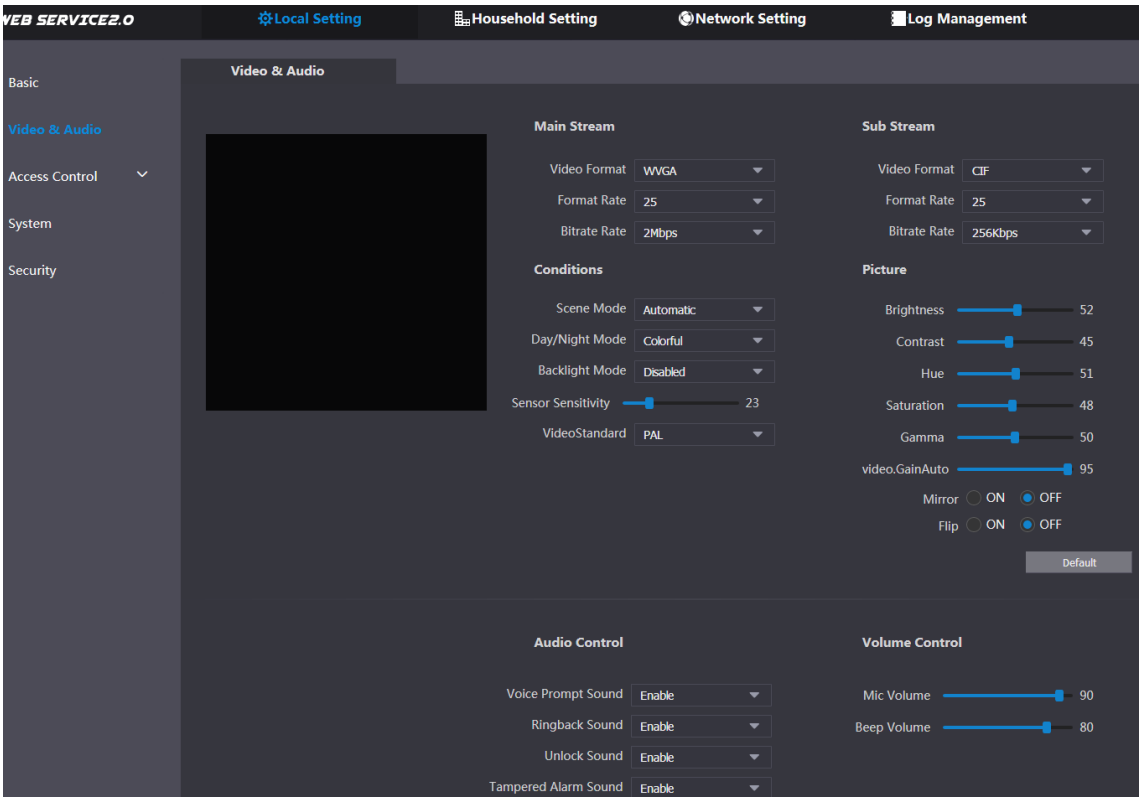
4.2 Video & Audio

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 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.
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**, **Sunny**, **Night** and **Disabled**. It is **Automatic** by default.
	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

Parameter		Description
		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.
	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.

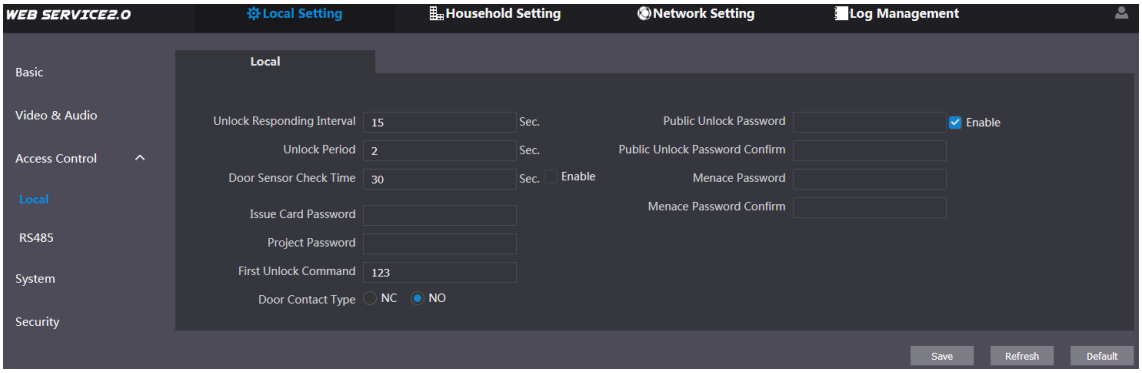
4.3 Access Control

This section introduces how to configure the lock, including unlock responding interval, open door command, issue card password, duress password and lift control protocol.

4.3.1 Local

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

Figure 4-3 Local



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.
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.
Issue Card Password	This password can be used to issue new card. ● This password is only for admin people or engineer. ● It is 888888 by default.
Project Password	It can be used to go to the engineering interface, and it is 888888 by default. Project password is only for admin people or engineers.
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.
Public Unlock Password	Select the **Enable** check box, then configure the public unlock password, and then all the residents in this unit can open the door with this password.
Public Unlock Password Confirm	

Parameter	Description
Menace Password	Under any of these two situations you can use menace password. ● By default, the menace password is entering the public unlock password reversed. ● You can configure any number as needed. Once the duress password is used ● When using VTO as SIP server, there will be an alarm record at **Log Management > Alarm**. ● When using platform as SIP server, you can connect alarm output device to get alarm notice.
Menace Password Confirm	

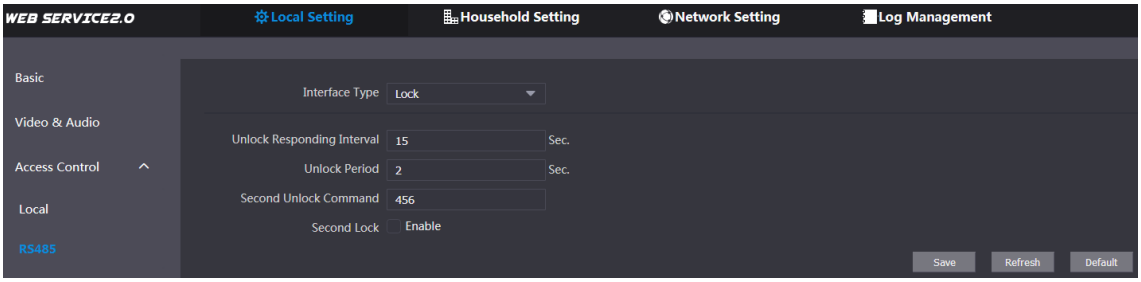
Step 3 Click **Save**.

4.3.2 RS485

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 RS485



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. ● 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

Parameter		Description
		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**.

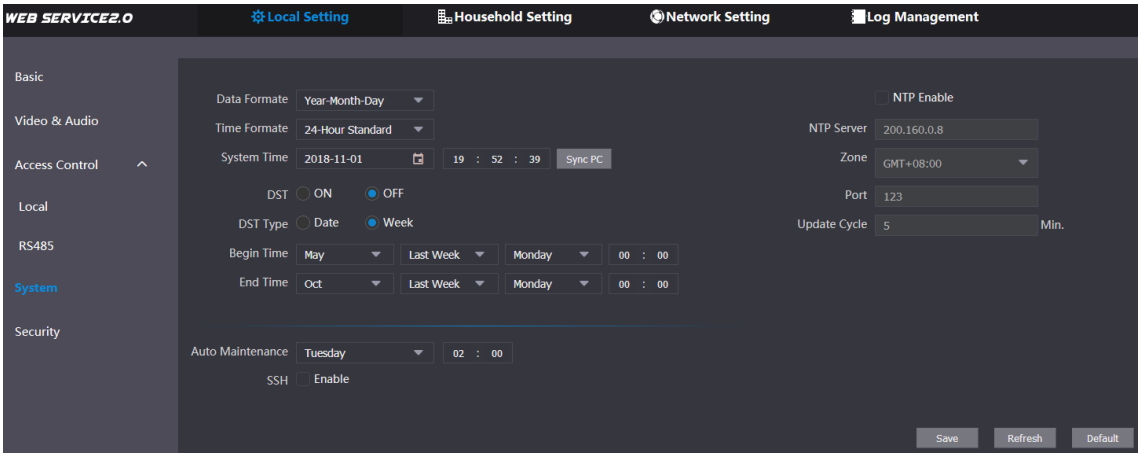
4.4 System

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.
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.

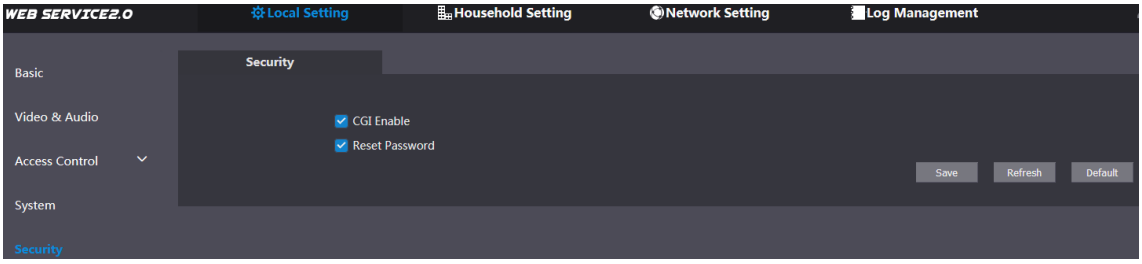
Parameter	Description
NTP Server	Enter the domain name of the NTP server.
Zone	The time zone of the current area.
Port	The port number of the NTP server.
Update Cycle	The time interval that the VTO syncs time with the NTP server, and it is 30 min at most.
Auto Maintenance	Select the day and time for 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, and then you can use CGI command.
Reset Password	Select the check box to enable, and then the password resetting is available.

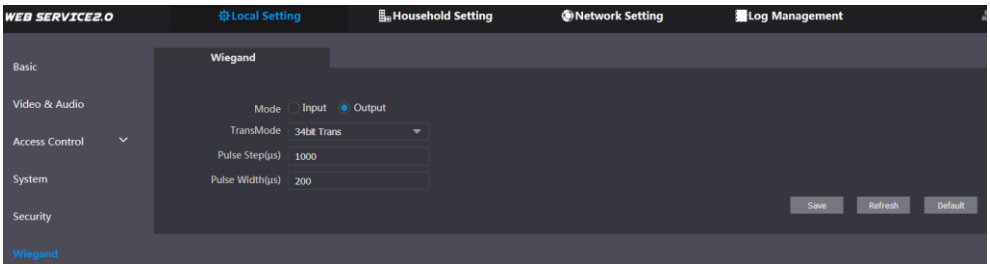
Step 3 Click **Save** to save.

4.6 Wiegand

This section introduces how to configure the parameters for Wiegand devices.

Step 1 On the main interface (Figure 3-1), select **Local Setting > Wiegand**.
The **Wiegand** interface is displayed. See Figure 4-7.

Figure 4-7 Wiegand



Step 2 Configure parameters. See Table 4-7.

Table 4-7 Wiegand parameter

Parameter	Description
Mode	Select **Input** or **Output** according to Wiegand device type.
TransMode	Select transmitting speed from **34 bit**, **66 bit**, and **26 bit**. The larger the value is, the faster the transmission will be.
Pulse Step (μs)	The Wiegand signal frequency, it is 1000 by default.
Pulse Width (μs)	The max value of Wiegand signal, it is 200 by default.

Step 3 Click **Save**.

4.7 Face Recognition

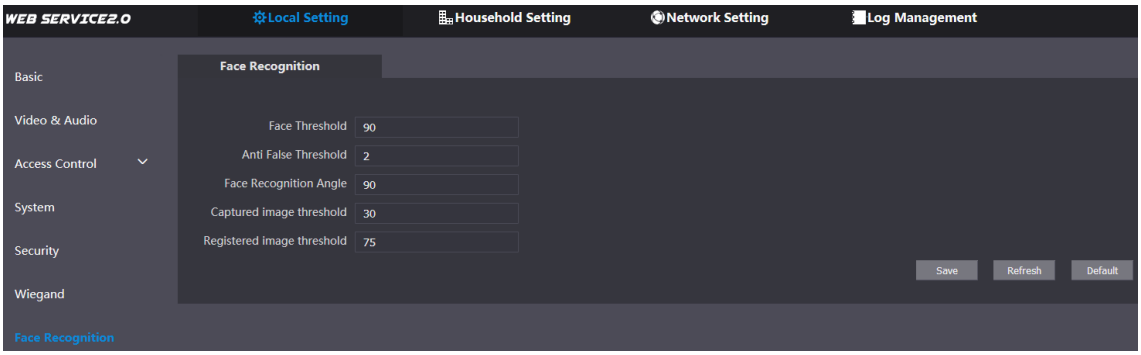
Face recognition is available on select models.

This section introduces how to configure face recognition threshold, anti-false threshold, and face recognition angle.

Step 1 Select **Local Setting > Face Recognition**.

The **Face Recognition** interface is displayed. See Figure 4-8.

Figure 4-8 Face recognition



Step 2 Configure face recognition parameters. See Table 4-8.

Table 4-8 Face recognition parameter description

Parameter	Description
Face Threshold	The larger the value is, the more similar the target and the saved face data is required to open the door.
Anti False Threshold	The larger the value is, the less the chance that the system defines a target as human face, hence the more accurate it will be.
Face Recognition Angle	The larger the value is, the larger the angle that the target is allowed to turn his face during recognition.
Captured image threshold	The quality of the captured images, the larger the value is, the better the quality will be.
Registered image threshold	The required image quality to register successfully, the larger the value is, the better the quality is required to be.

Step 3 Click **Save**.

5 Household Setting

This chapter applies to the condition in which the VTO works as SIP server (see 6.4 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

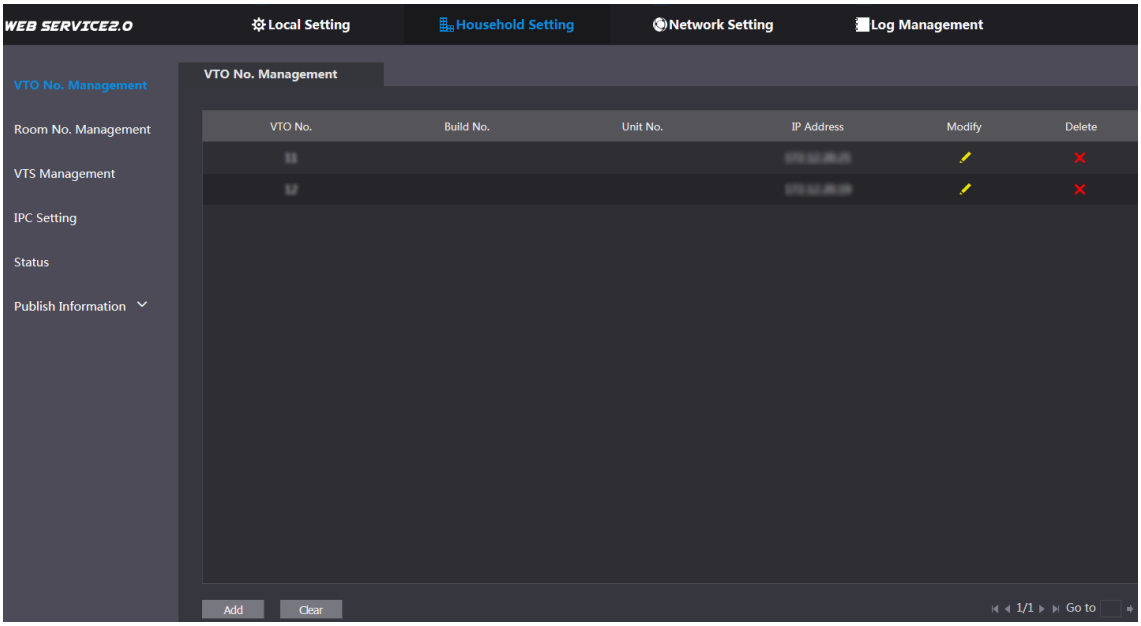
5.1.1 Adding VTO

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 the web interface of the SIP server, and then select **Household Setting > VTO No. Management**.

The **VTO No. Management** interface is displayed. See Figure 5-1.

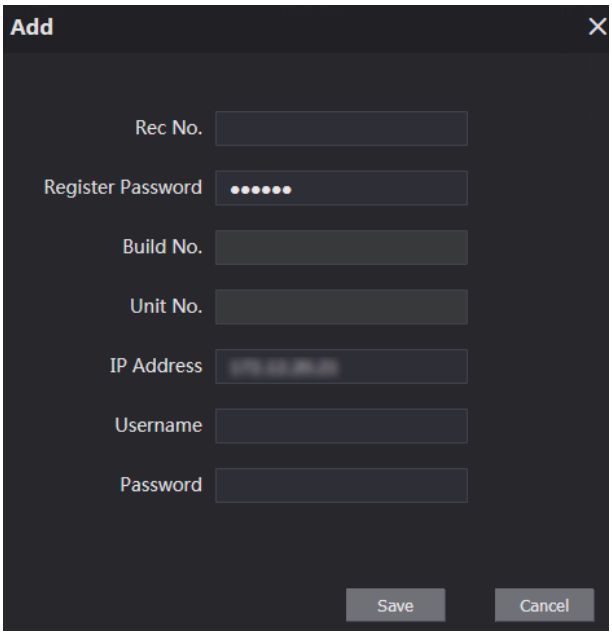
Figure 5-1 VTO No. management



Step 2 Click **Add**.

The **Add** interface is displayed. See Figure 5-2.

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**.

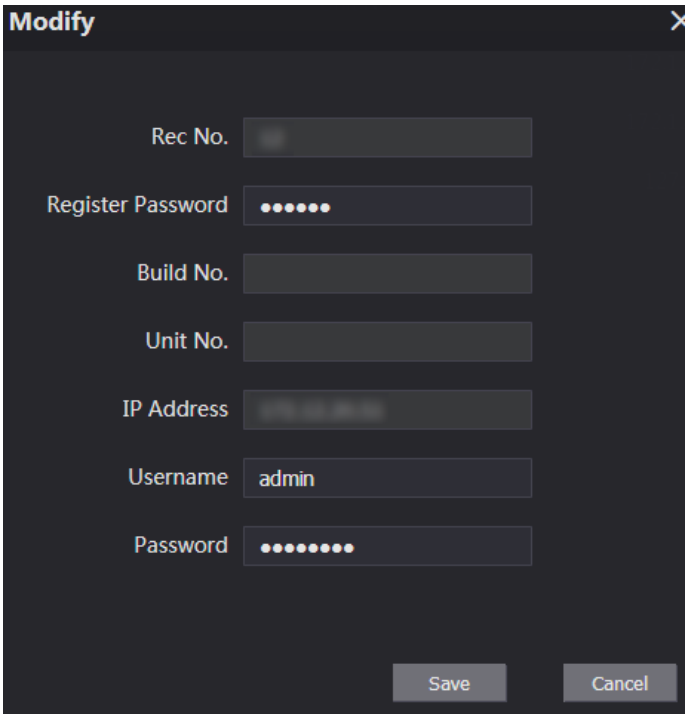
5.1.2 Modifying VTO

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

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

The **Modify** interface is displayed. See Figure 5-3.

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

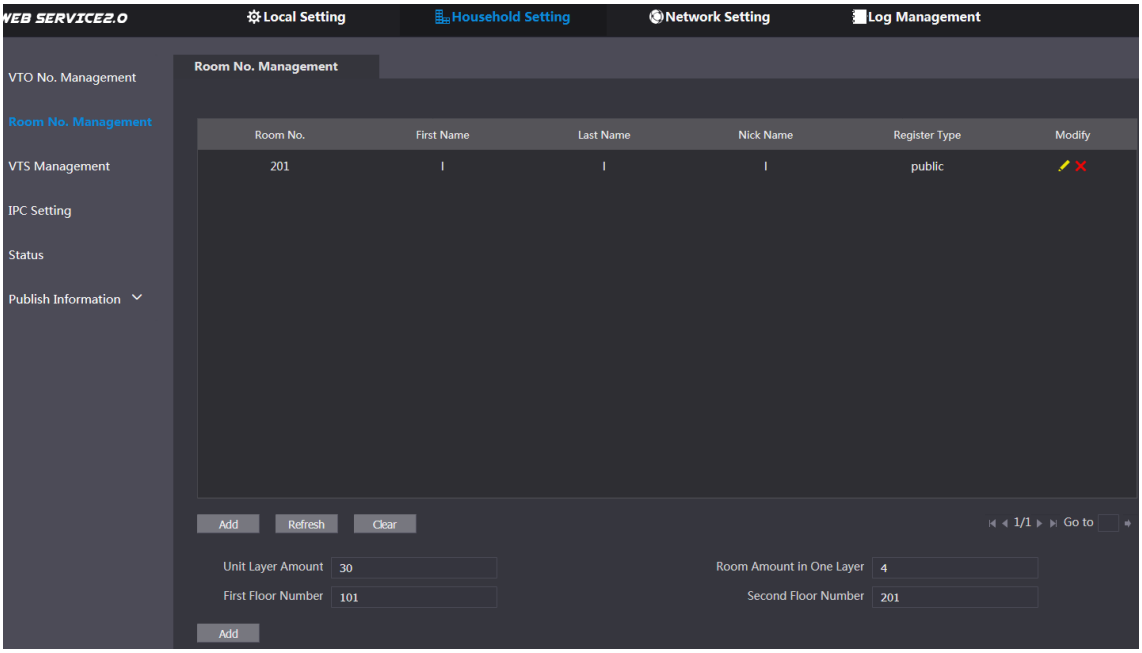
5.2.1 Adding Room Number

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 the web interface of the SIP server, and then select **Household Setting > Room No. Management**.

The **Room No. Management** interface is displayed. See Figure 5-4.

Figure 5-4 Room No. Management

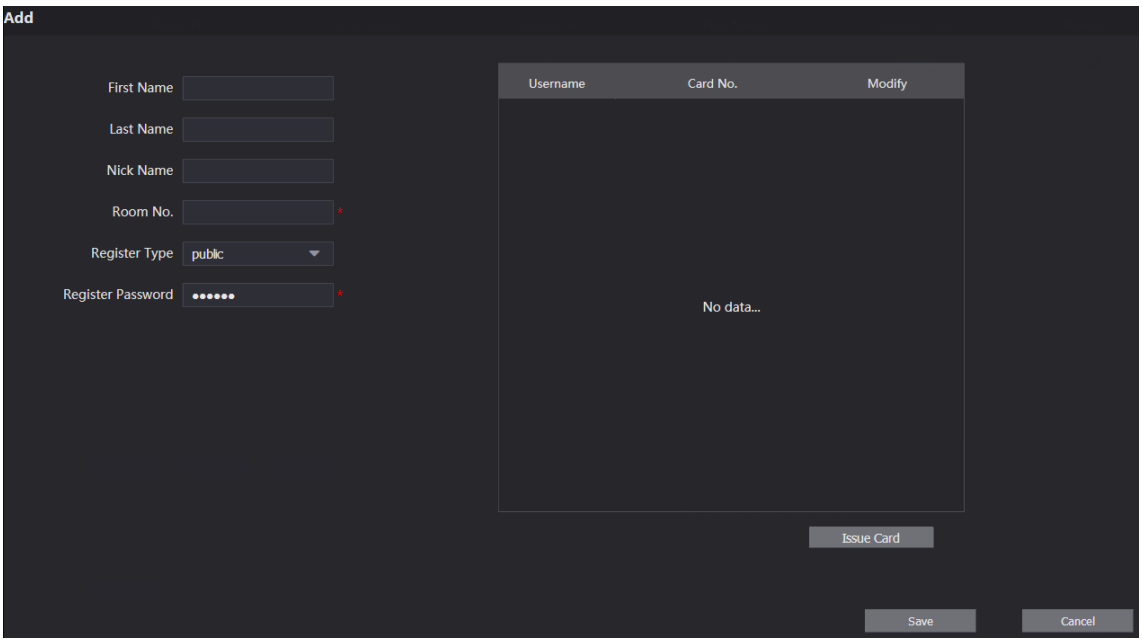


Step 2 You can add single room number or do it in batch.

- Add single room number

1) Click the **Add** at the mid lower position.
The **Add** interface is displayed. See Figure 5-5.

Figure 5-5 Add single room number



2) Configure room information, and for the detailed description. See Table 5-2.

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 you planned.
Register Type	Select **public**, and **local** is reserved for future use.

Parameter	Description
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.

- Adding room number in batch

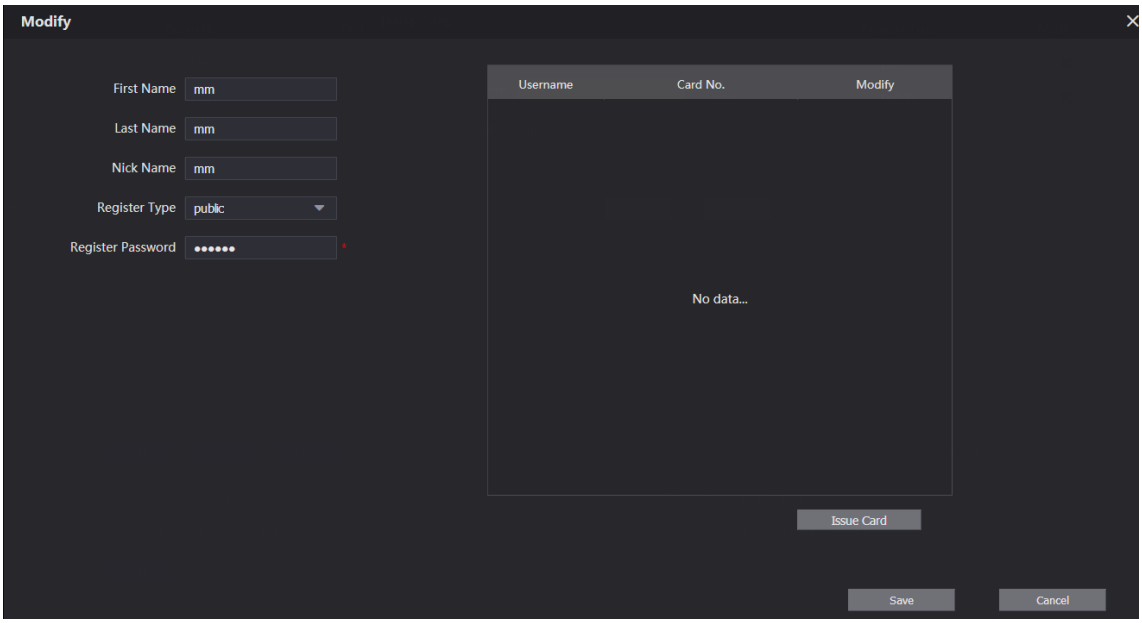
1) Configure the **Unit Layer Amount**, **Room Amount in One Layer**, **First Floor Number**, and **Second Floor Number** according to the actual condition.
2) Click the **Add** at the bottom position.
   All the added room numbers are displayed. Click **Refresh** to view the latest status, and click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

The **Modify** interface is displayed. See Figure 5-6.

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**.

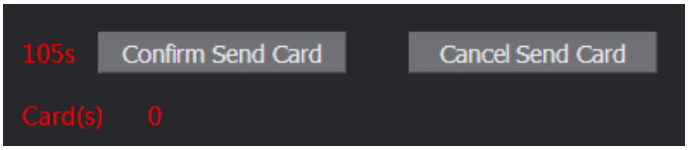
5.2.3 Issuing Access Card

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**.

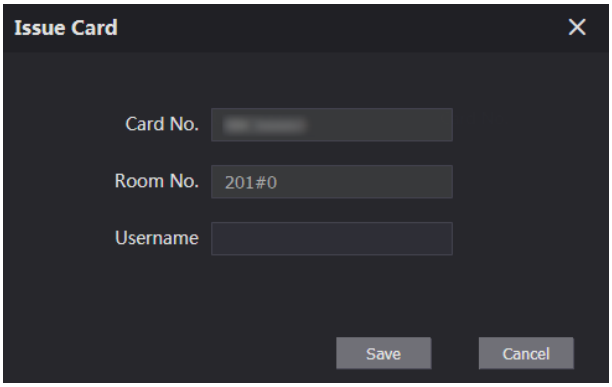
The countdown notice is displayed. See Figure 5-7.

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.

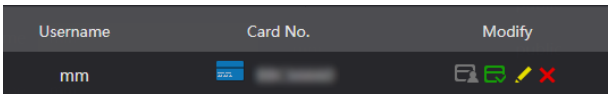
Figure 5-8 Issue Card



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

The issued access card is displayed. See Figure 5-9.

Figure 5-9 Issued access card



Step 4 You can configure the access card.

- Click to set it to the main card, and then the icon turns into . 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.

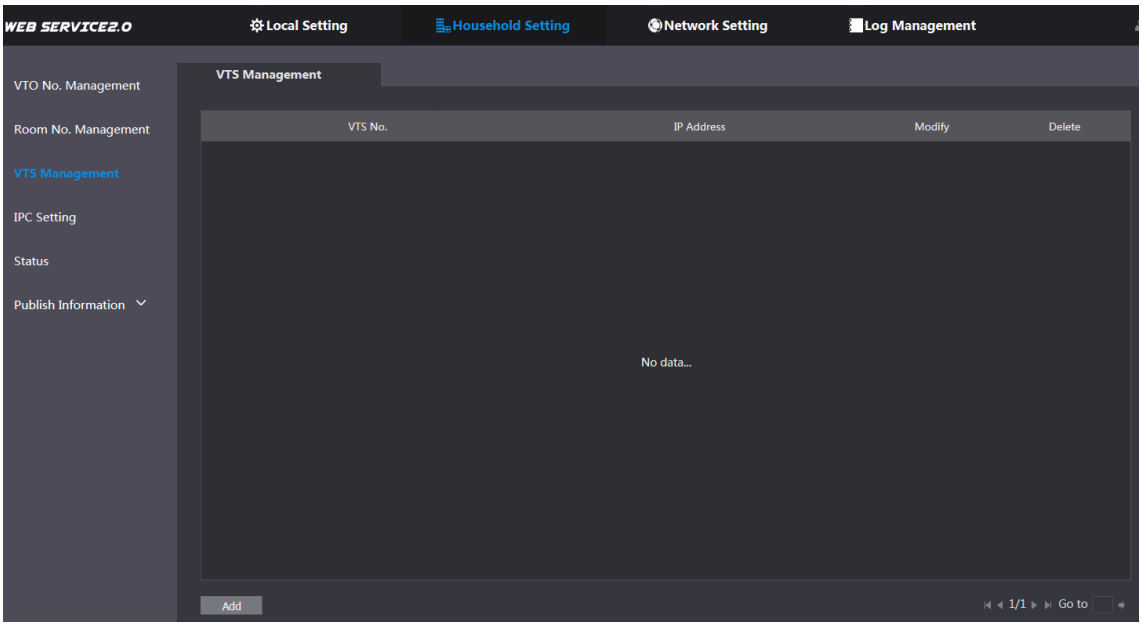
5.3 VTS Management

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 the web interface of the SIP server, and then select **Household Setting > VTS Management**

The **VTS Management** interface is displayed. See Figure 5-10.

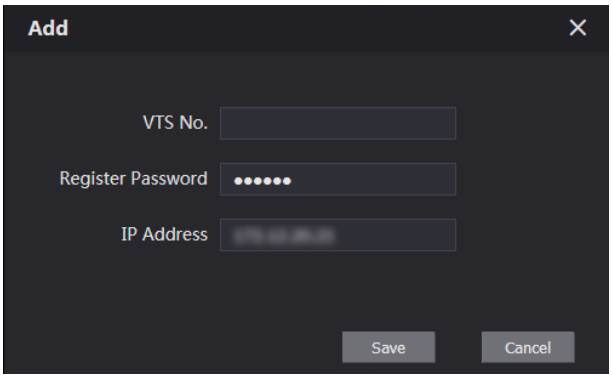
Figure 5-10 VTS management



Step 2 Click **Add**.

The **Add** interface is displayed. See Figure 5-11.

Figure 5-11 Add VTS



Step 3 On VTS, select **Config > Advance Config**, then enter the password (123456 by default), and then select **SIP Server**, the **VTS No.** is displayed as **User Name** (normally it is 888888XXX).

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

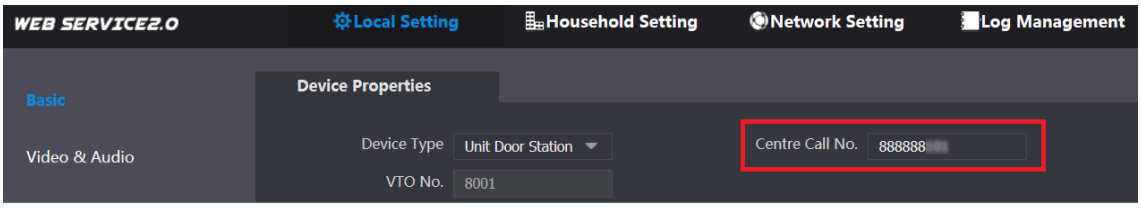
Table 5-3 Add VTS configuration

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

Step 6 Select **Local Setting > Basic**, then enter the VTS No. of the added VTS at **Center Call No.**, and then you can call the VTS by pressing the call center button on the VTO. See Figure 5-12.

Figure 5-12 Center call No.



Step 7 Click **Confirm**.

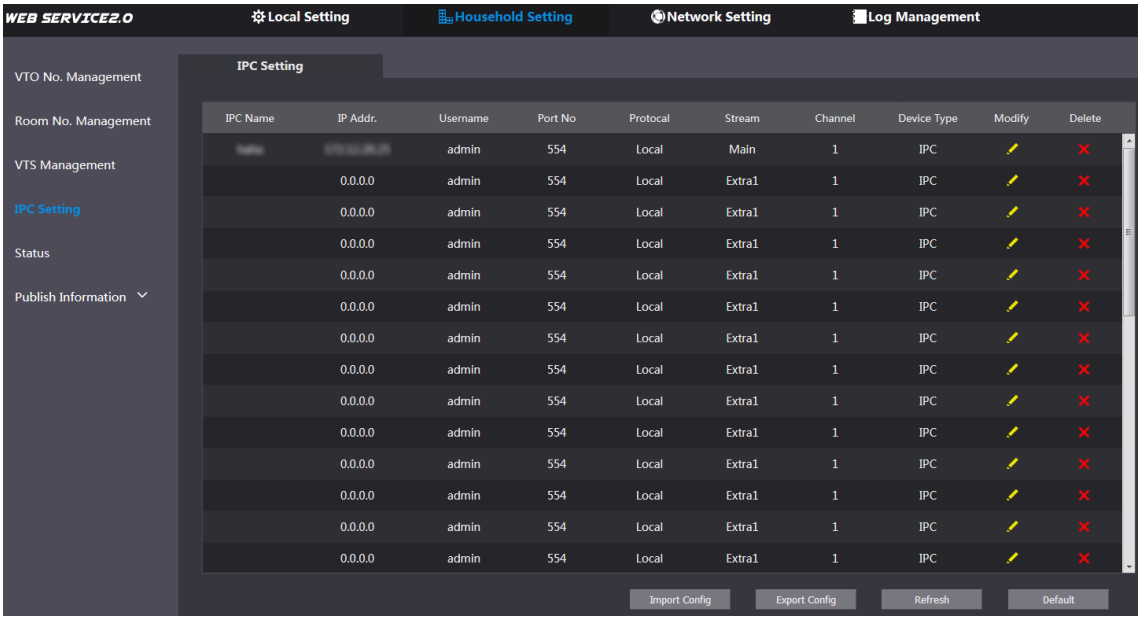
5.4 IPC Setting

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 the web interface of the SIP server, and then select **Household Setting > IPC Setting**

The **IPC Setting** interface is displayed. See Figure 5-13.

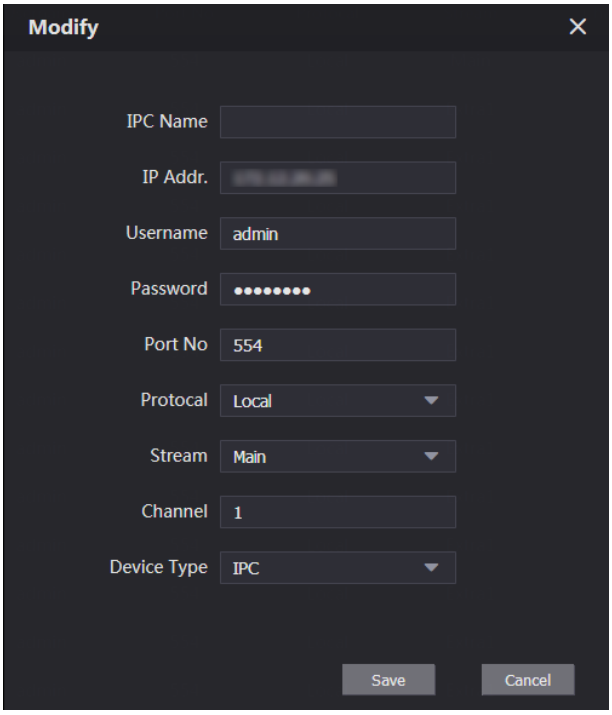
Figure 5-13 IPC setting



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

The **Modify** interface is displayed. See Figure 5-14.

Figure 5-14 Add IPC



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**.
Stream	Select from **Main** or **Extra1**, and the main stream has better image quality, but also costs 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.

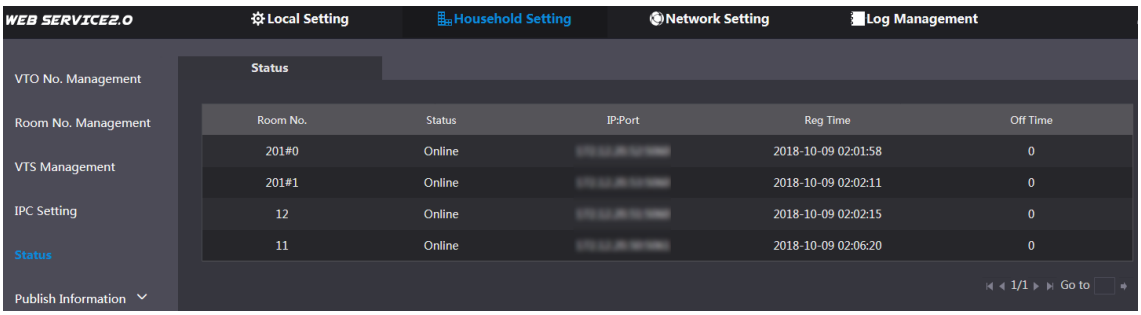
5.5 Status

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

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

The **Status** interface is displayed. See Figure 5-15.

Figure 5-15 Status



5.6 Publish Information

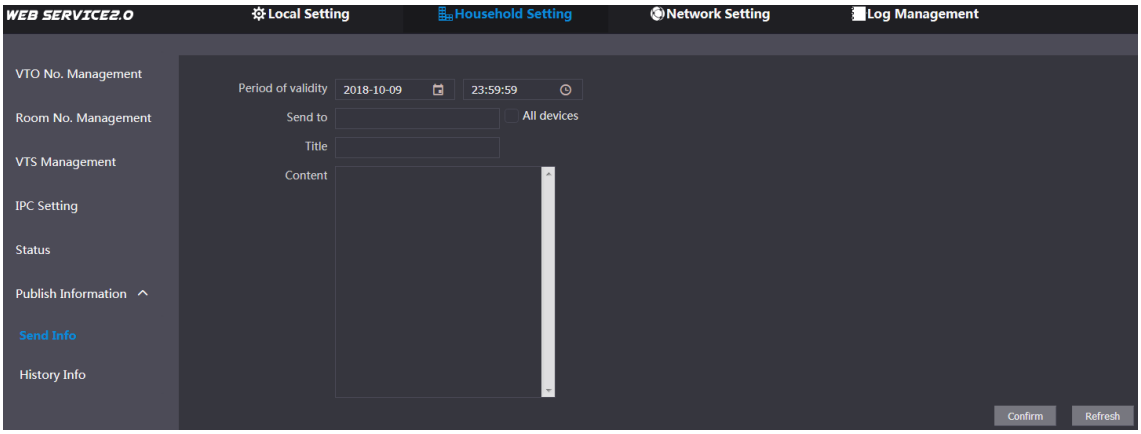
You can send messages from the SIP server to other VTH devices, and view the message sending history.

5.6.1 Send Info

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

The **Send Info** interface is displayed. See Figure 5-16.

Figure 5-16 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.

- If you want to send information to more than one VTH, VTH numbers should be separated by semicolons. For example if you enter 101; 102; 103 and more, and VTH of these VTH numbers will receive information sent by the VTO.
- The Period of validity is reserved for future use.

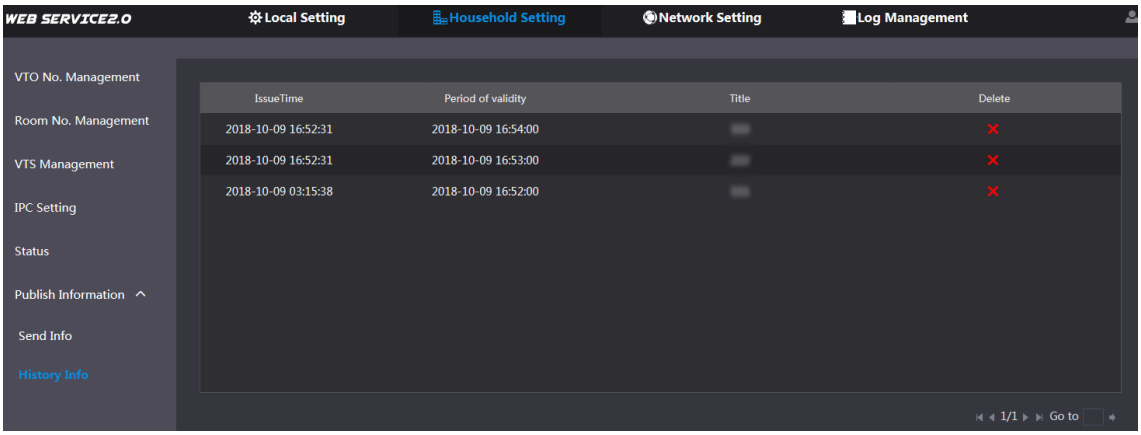
Step 3 Click **Confirm**.

5.6.2 History Info

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

The **History Info** interface is displayed. See Figure 5-17.

Figure 5-17 History info



You can view the time and title of the sent messages.

5.7 Face Management

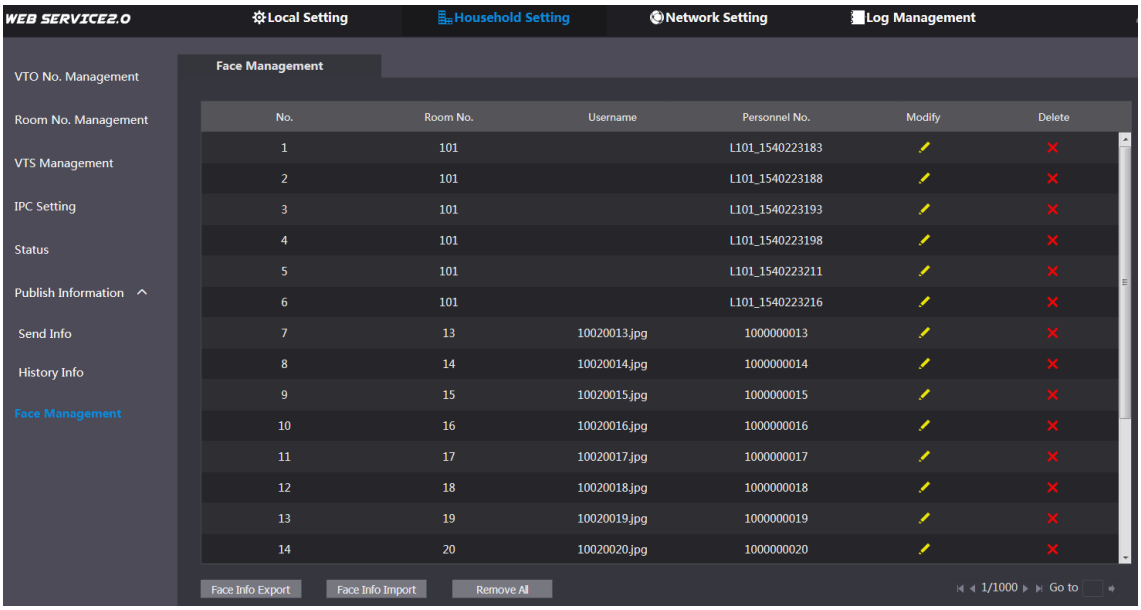
You can add, delete, import, and export face data.

- Face recognition is available on select models.
- The VTO can save 10,000 faces at most.

Select **Household Setting > Face Management**.

The **Face Management** interface is displayed. See Figure 5-18.

Figure 5-18 Face management

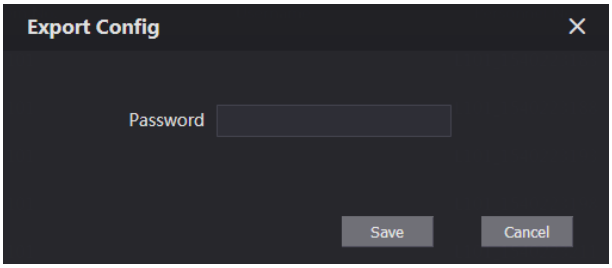


5.7.1 Exporting Face Data

Step 1 Click **Face Info Export**.

The **Export Config** interface is displayed. See Figure 5-19.

Figure 5-19 Export config



Step 2 Enter the password for the Web interface, and then click **Save** to export face data.

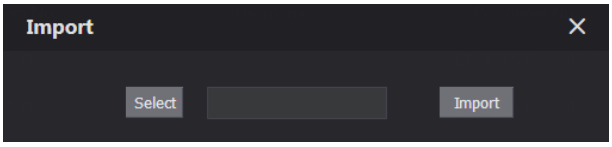
5.7.2 Importing Face Data

Step 1 Click **Face Info Import**.

Step 2 Enter the password for the Web interface, and then click **Save**.

The Import interface is displayed. See Figure 5-20.

Figure 5-20 Import



Step 3 Click **Select**, and then select the file you need.

Step 4 Click **Import**.

5.7.3 Deleting Face Data

Click  to delete single face data.

Click **Remove All** to delete all the face data.

6 Network Setting

This chapter introduces how to configure IP address, FTP, SIP server, DDNS, and UPnP.

6.1 Basic

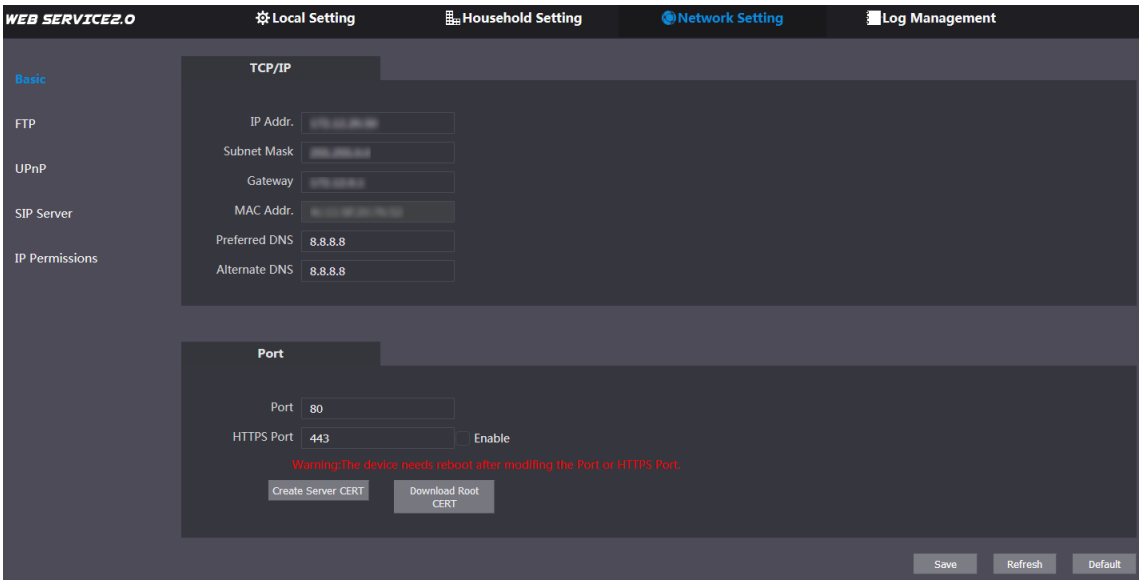
6.1.1 TCP/IP

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

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

The TCP/IP information and port information are displayed. See Figure 6-1.

Figure 6-1 TCP/IP and port



Step 2 Enter the network parameters and port number you planed, and then click **Save**.

The VTO will reboot, and you need to modify the IP address of your PC to the same network segment as the VTO to log in again.

6.1.2 HTTPS

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

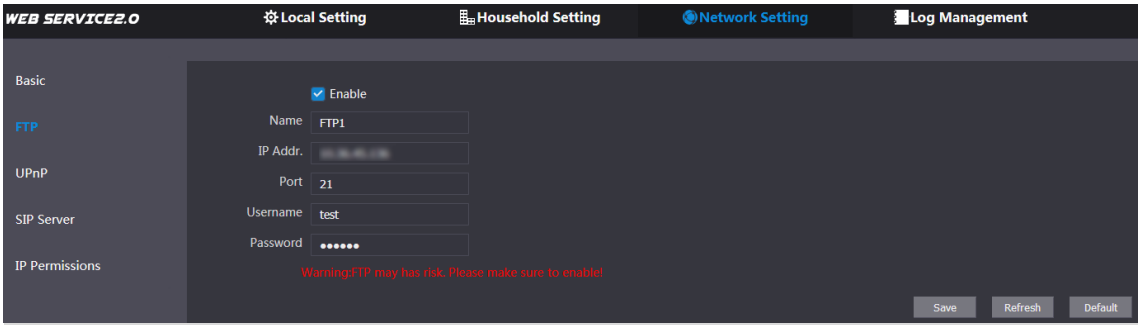
6.2 FTP

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

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

The **FTP** interface is displayed. See Figure 6-2.

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 UPnP

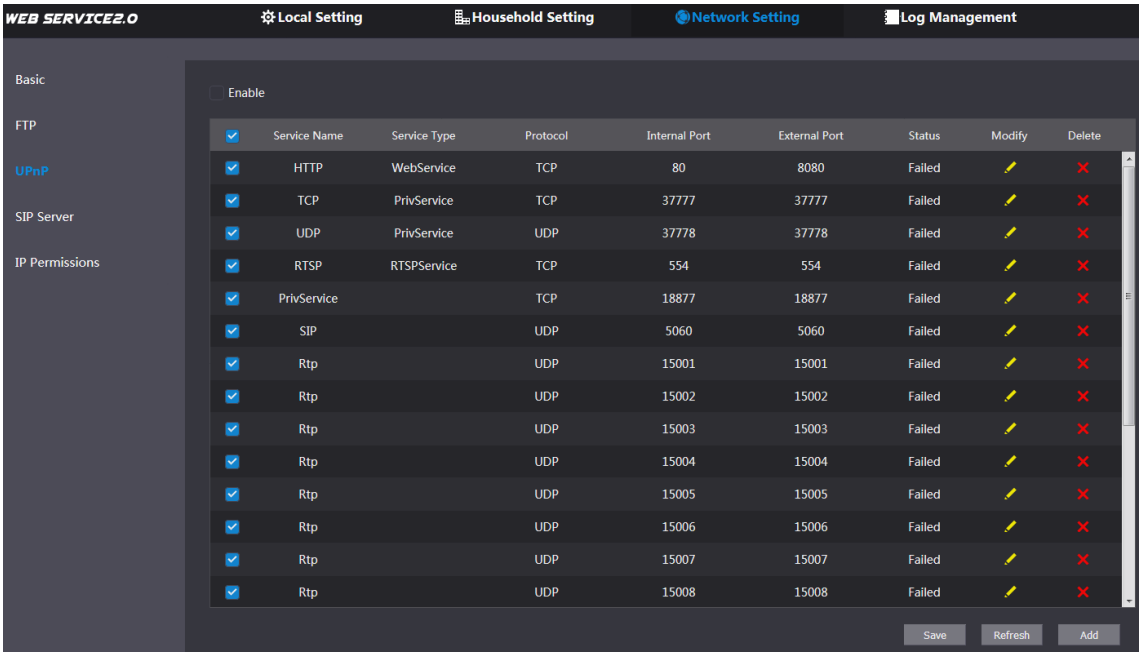
Universal Plug and Play, a protocol that establishes mapping relation of ports in LAN and WAN. This function enables you to visit local area device through wide area network.

- This function is valid only when VTO works as SIP server.
- This function is needed only when the VTO is connected to a router with UPnP function.

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

The **UPnP** interface is displayed. See Figure 6-3.

Figure 6-3 UPnP

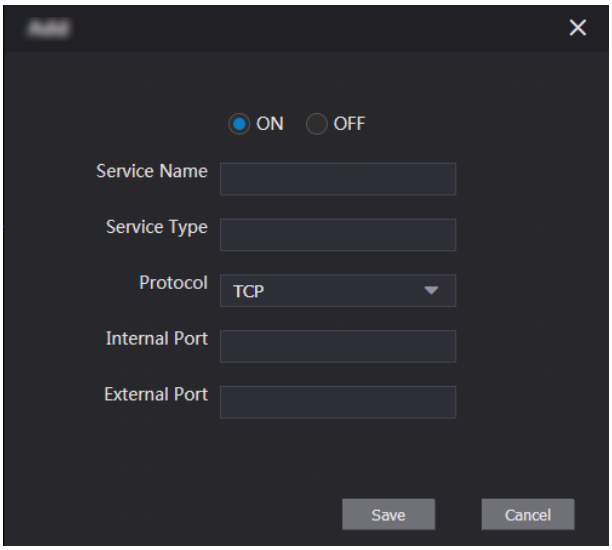


Step 2 Select the **Enable** checkbox to enable UPnP function.

Step 3 There have been some mapping relations done in the factory, and you can click to modify them. Or you can click **Add** to add a new one.

The **Modify/Add** interface is displayed. See Figure 6-4.

Figure 6-4 Modify/Add UPnP



Step 4 Configure parameters. See Table 6-2.

Table 6-2 UPnP parameter description

Parameter	Description
ON/OFF	Select **ON** to enable this mapping relation.
Service Name	The name of the service.
Service Type	Define the type of the service as needed.
Protocol	You can select from **TCP** and **UDP**. For the transmission stability, **TCP** is recommended.

Parameter	Description	
Internal Port	The port on the local area VTO that you need to visit.	 ● Try to use port number between 1024 to 5000 and not between 1 to 255 and 256 to 1023 when mapping ports with router to avoid conflict. ● When mapping multiple devices to the external ports, do the planning in advance to avoid mapping different devices to the same external port. ● Make sure the ports you are using are not being used or constrained. ● The external ports of TCP and UDP must be the same.
External Port	The port on the router that the VTO port is being mapped to.	

Step 5 Click **Save**.

Open the web browser on PC and enter "http:// WAN IP address: external port number", and then you can visit the local area device with corresponding port.

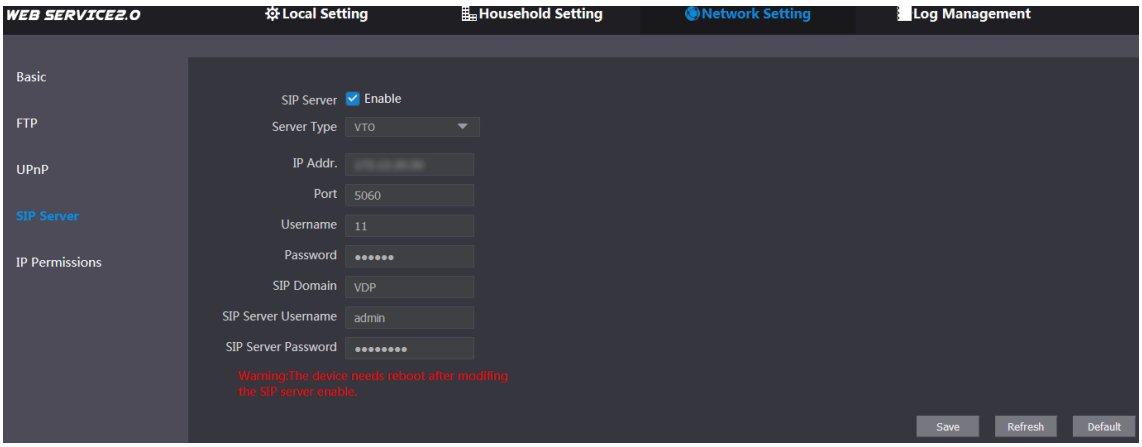
6.4 SIP Server

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**.

The **SIP Server** interface is displayed. See Figure 6-5.

Figure 6-5 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 then 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 6-3.

Table 6-3 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.

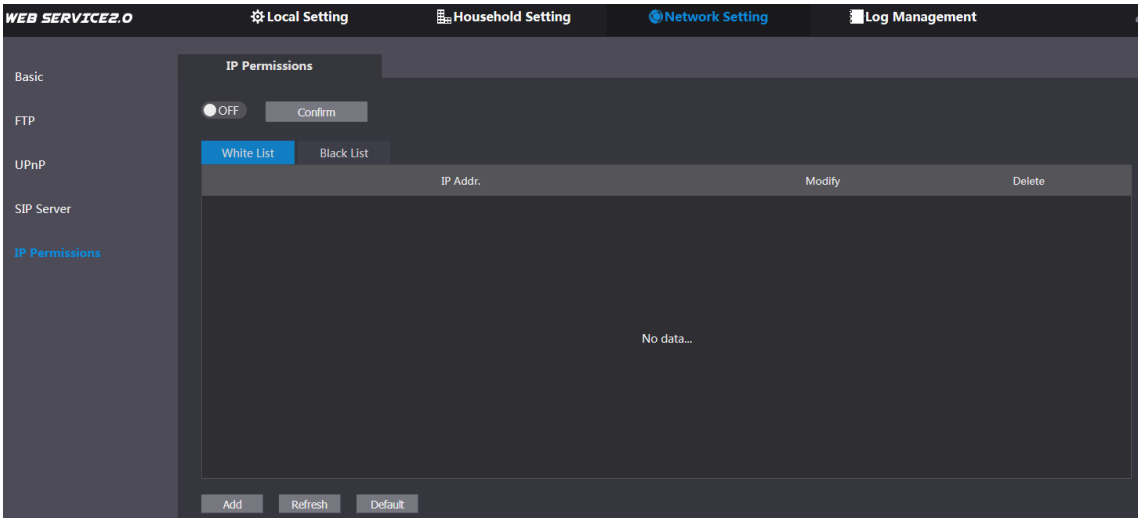
6.5 IP Permissions

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

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

The **IP Permissions** interface is displayed. See Figure 6-6.

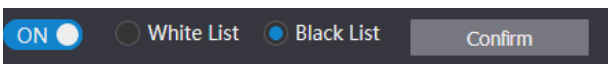
Figure 6-6 IP Permissions



Step 2 Click OFF.

The **White List** option and **Black List** option are displayed. See Figure 6-7.

Figure 6-7 White List and Black List



You can only use one of them at the same time.

- **White list**: only the IP addresses in the list can login 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.

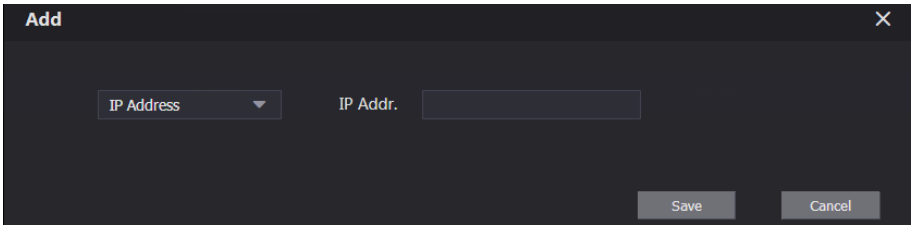
- If you need to use black list, select **Black List**, and then click **Confirm**.

- 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**.

The **Add** interface is displayed. See Figure 6-8.

Figure 6-8 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.

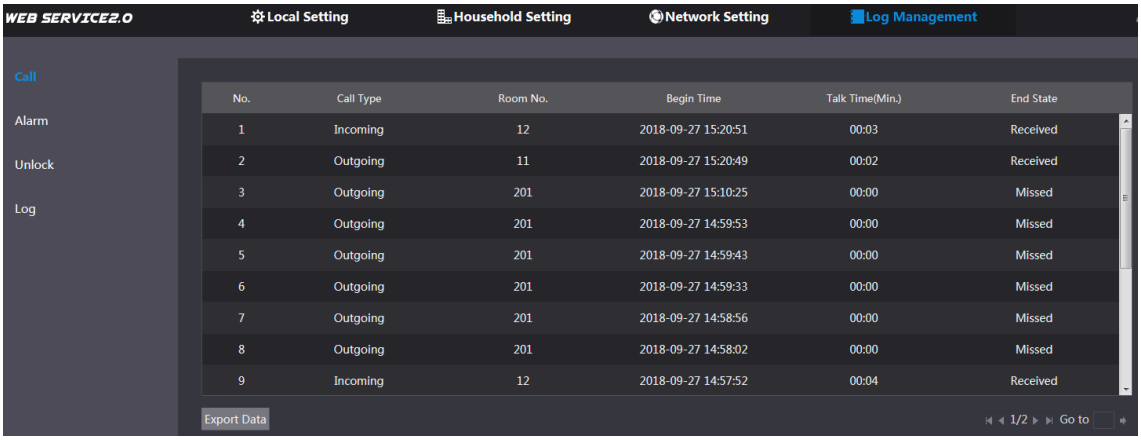
7.1 Call

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

Select **Log Management > Call**.

The **Call** interface is displayed. See Figure 7-1.

Figure 7-1 Call



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

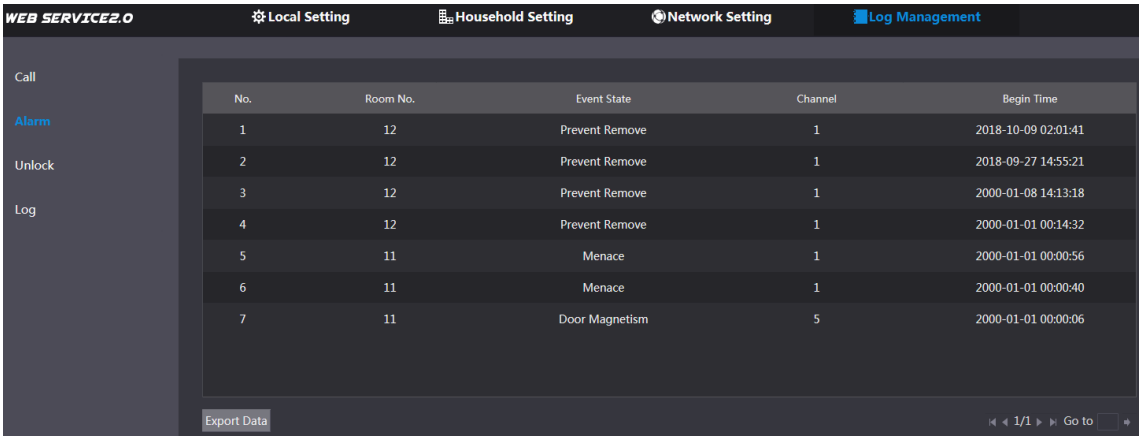
7.2 Alarm

This function is displayed only when the VTO you are visiting works as SIP server, and you can view the VTO and VTH alarm record and duress password alarm record.

Select **Log Management > Alarm**.

The **Alarm** interface is displayed. See Figure 7-2.

Figure 7-2 Alarm



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

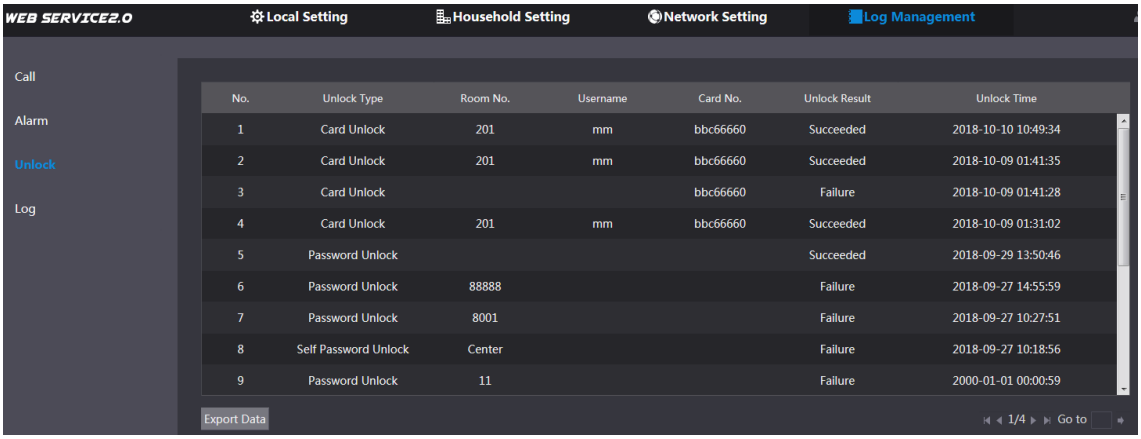
7.3 Unlock

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

Select **Log Management > Unlock**.

The **Unlock** interface is displayed. See Figure 7-3.

Figure 7-3 Unlock



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

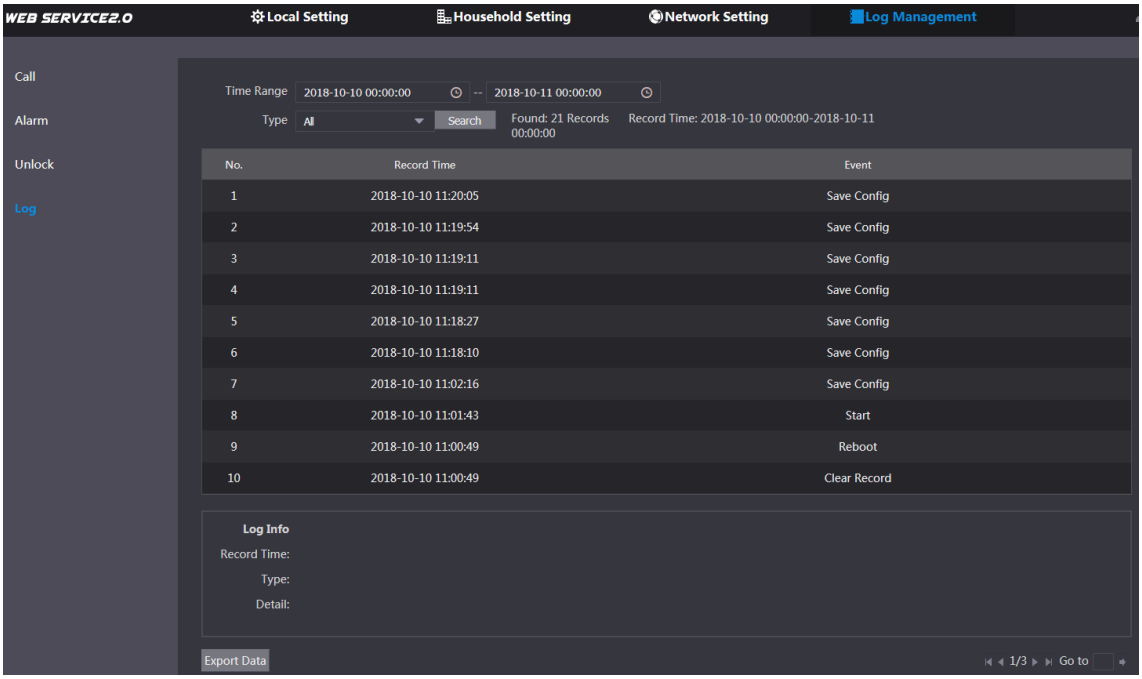
7.4 Log

You can view various system logs, including system, record, config, account, and security.

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

The **Log** interface is displayed. See Figure 7-4.

Figure 7-4 Log



Step 2 Configure the time range, then select the log type you need, and then click **Search**.

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