

Two-wire Door Station

User's Manual






Foreword

General

This manual introduces the web interface configuration of the door station (hereinafter referred to as "VTO").

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

Version	Revision Content	Release Date
V1.1.0	Updated to V4.5.	December, 2020
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 jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem

occurring when using the device.

- If there is any uncertainty or controversy, we reserve the right of final explanation.

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

- Do not expose the device to direct sunlight or heat source.
- Do not install the device in a humid or dusty environment.
- Horizontally install the device at stable places to prevent it from falling.
- Do not drip or splash liquids onto the device, or put on the device anything filled with liquids.
- Install the device at well-ventilated places and do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device by yourself.
- Transport, use and store the device within allowed humidity and temperature range.

Power Requirement

- The product must use electric wires recommended in your area, and within its rated specification.
- 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, see the label on the device.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Initialization	1
2 Login Interface	2
2.1 Logging In	2
2.2 Resetting Password	2
3 Main Interface	4
4 Local Setting	5
4.1 Basic	5
4.2 Video & Audio	8
4.3 Access Control Settings	9
4.3.1 Local	9
4.3.2 RS-485	10
4.4 Password Management	11
4.5 System	11
4.6 Security	13
4.7 Wiegand	15
4.8 Onvif User	15
4.9 Upload File	16
5 Household Setting	17
5.1 VTO No. Management	17
5.2 VTH Management	18
5.2.1 Adding Room Number	18
5.2.2 Issuing Access Card	20
5.2.3 Issuing Fingerprint	20
5.3 VTS Management	21
5.4 IPC Setting	22
5.5 Status	24
5.6 Publish Information	24
5.6.1 Send Info	24
5.6.2 History Info	24
6 Network Setting	26
6.1 Basic	26
6.1.1 TCP/IP	26
6.1.2 Port	26
6.1.3 P2P	27
6.2 UPnP	27
6.2.1 Enabling UPnP Services	27
6.2.2 Adding UPnP Services	28
6.3 SIP Server	28
6.4 Firewall	30
7 Log Management	31
Appendix 1 Cybersecurity Recommendations	32

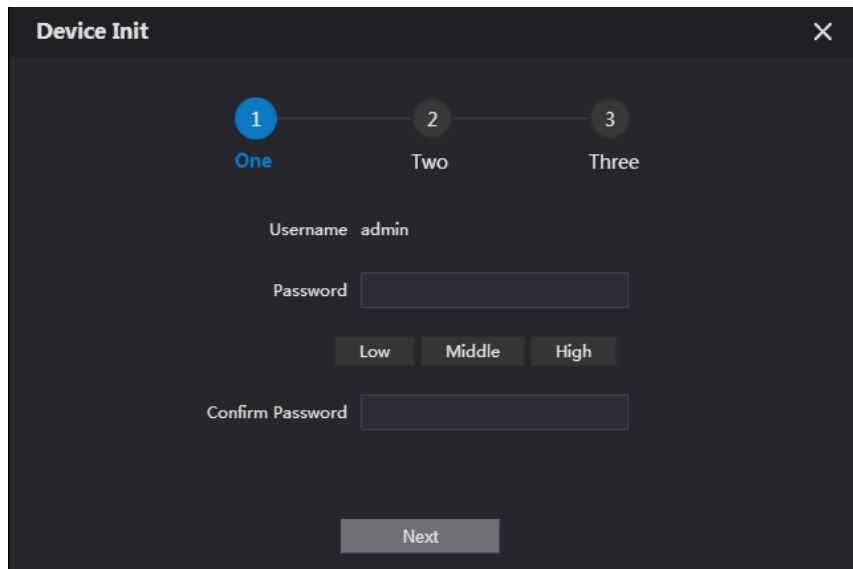
1 Initialization

For first time login or after the VTO being reset, you need to initialize it on the web interface. The default IP address of the VTO is 192.168.1.1108 and make sure the PC is in the same network segment as the VTO.

Step 1 Power on the VTO.

Step 2 Go to the default IP address of the VTO in the browser.

Figure 1-1 Device initialization



Device Init

1 — 2 — 3
One Two Three

Username admin

Password

Low Middle High

Confirm Password

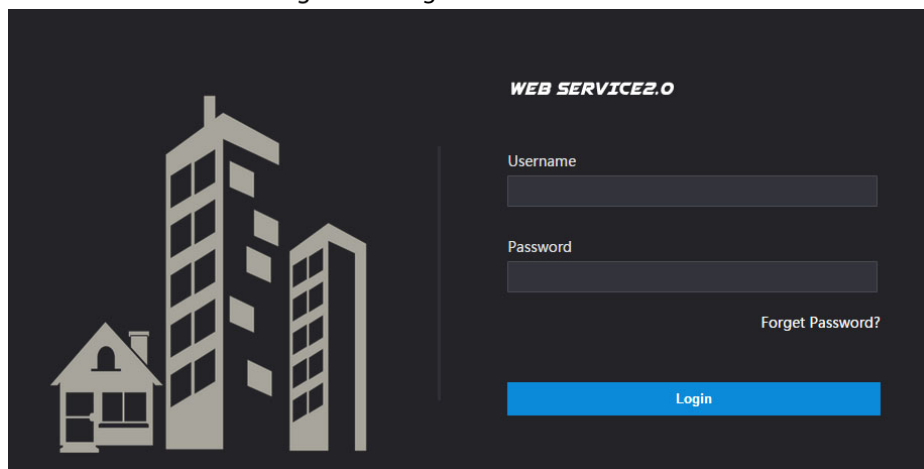
Next

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

Step 4 Enter an Email address for resetting password.

Step 5 Click **Next**, and then click **OK**.

Figure 1-2 Login interface



WEB SERVICE2.0

Username

Password

[Forget Password?](#)

Login

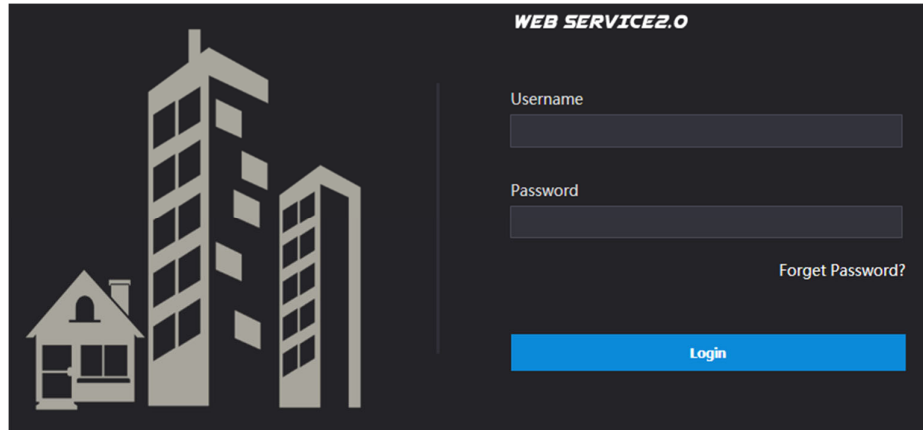
2 Login Interface

2.1 Logging In

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

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

Figure 2-1 Login interface

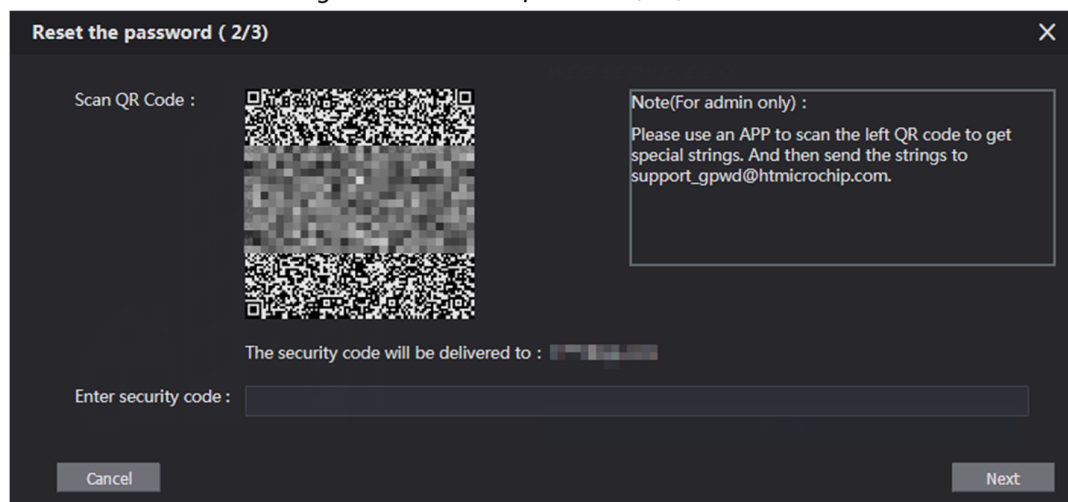
The login interface for WEB SERVICE 2.0. It features a dark background with a stylized illustration of a house and two skyscrapers on the left. On the right, there is a login form with fields for 'Username' and 'Password'. Below the password field is a link for 'Forget Password?'. At the bottom of the form is a blue 'Login' button.

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, click **Forgot Password?**, and then click **Next**.

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

A dialog box titled 'Reset the password (2/3)'. It contains a 'Scan QR Code :' label next to a QR code. To the right of the QR code is a text box with the following text: 'Note(For admin only) : Please use an APP to scan the left QR code to get special strings. And then send the strings to support_gpwd@htmicrochip.com.' Below the QR code, it says 'The security code will be delivered to : ' followed by a blurred area. At the bottom, there is a label 'Enter security code : ' followed by a text input field. There are 'Cancel' and 'Next' buttons at the bottom corners.

Step 2 Scan the QR code to request the security code, enter it, and then click **Next**.



- If you did not set an email address during initialization, contact the supplier or customer service for help.
- To obtain security code again, scan the QR code again.

- The security code will be valid only for 24 hours upon receipt.
- If you enter the wrong security code for 5 consecutive times, your account will be locked for 5 minutes.

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

3 Main Interface

Log in to the web interface of the VTO.

Figure 3-1 Main interface

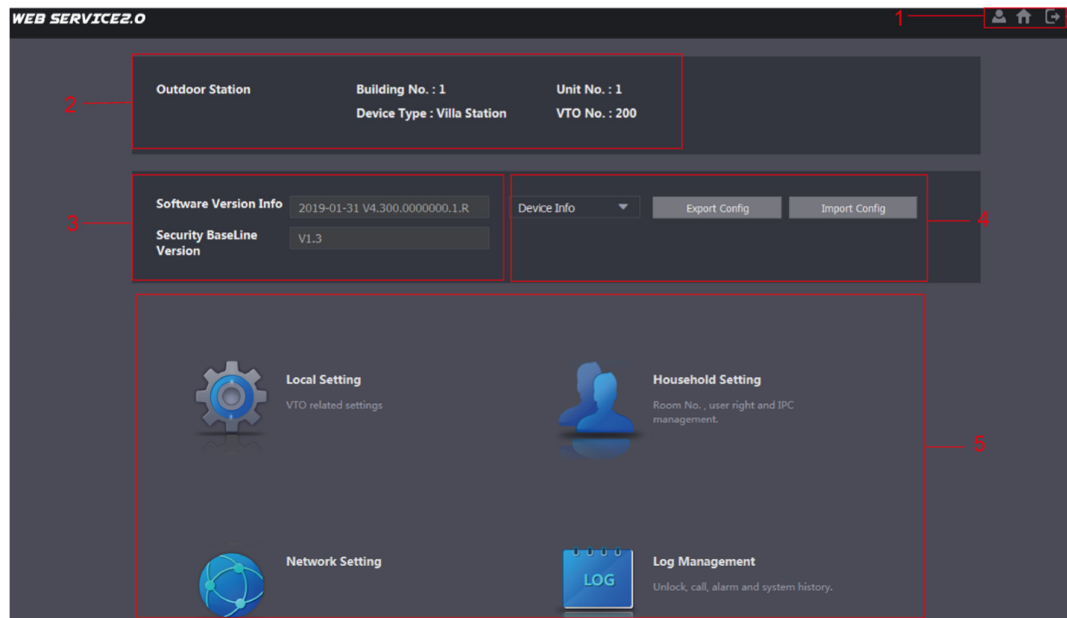


Table 3-1 Main interface introduction

No.	Function	Description
1	General function	<ul style="list-style-type: none"> : Change the password and your Email address. : Go to the main interface. : Log out, restart the VTO or restore the VTO to factory settings. <p></p> <p>If you restore the VTO to factory settings, all data except external storage will be deleted. You can format the external storage device to delete the data in it.</p>
2	VTO information	—
3	System information	—
4	Configuration manager	Export or import VTO configuration or user information.
5	Function area	—

4 Local Setting

This chapter introduces detailed configuration to the VTO.

4.1 Basic

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

Figure 4-1 Basic

The screenshot displays the 'WEB SERVICE2.0' web interface. The top navigation bar includes 'Local Settings', 'Household Setting', 'Network', 'Search Log', and a language dropdown set to 'English'. The left sidebar lists configuration categories: 'Basic' (selected), 'Video & Audio', 'Access Control Settings', 'System', and 'Security'. The main panel, titled 'Device Properties', contains the following settings:

- Device Type:** Villa Station (dropdown menu)
- Device Name:** (empty text field)
- No.:** 8001 (text field)
- Center Call No.:** 888888 (text field)
- Calling Center Period:** 00:00:00 to 23:59:59 (time range selector with a 'Setting' button)
- Group Call:** ☒ (checkbox with a warning message: 'Warning: The device will be rebooted after modifying group call enable status.'

Step 2 Configure the parameters.

Table 4-1 Basic parameter description

Parameter	Description
-----------	-------------



- Building and unit number are available only when other servers work as the SIP server. See "6.2 UPnP
- When the VTO works as the SIP server, you can configure the UPnP function to allow WAN devices to log in to the VTO.

Prerequisites

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

4.1.2 Enabling UPnP Services

- Step 1 Select **Network > UPnP**.
- Step 2 Enable the services as needed.
- Step 3 Select the **Enable** check box.
- Step 4 Click **Save**.

4.1.3 Adding UPnP Services

- Step 5 Select **Network > UPnP**.
- Step 6 Click **Add**.
- Step 7 Configure the parameters as needed.

Figure 4-2 Add a UPnP service

Add

ON

OFF

Service Name

Service Type

Protocol

TCP

Internal Port

External Port

Save

Cancel

Table 4-2 Parameter description

Parameter	Description
Service Name	Enter the information as needed.
Service Type	
Protocol	Select TCP or UDP as needed.
Internal Port	Use port number 1024 to 5000.



Device Type

Centre Call No.	The default number is 888888, and you can set it to any number with up to 9 digits.
Device Name	—
Call Centre Period	Time period in which you are allowed to call the management centre.
No.	Used to differentiate each VTO, and we recommend setting it according to unit or building number, and then you can add VTOs to the SIP server with their numbers.
Periods in which Calls can be Made	Specify a period when you will not receive any call.

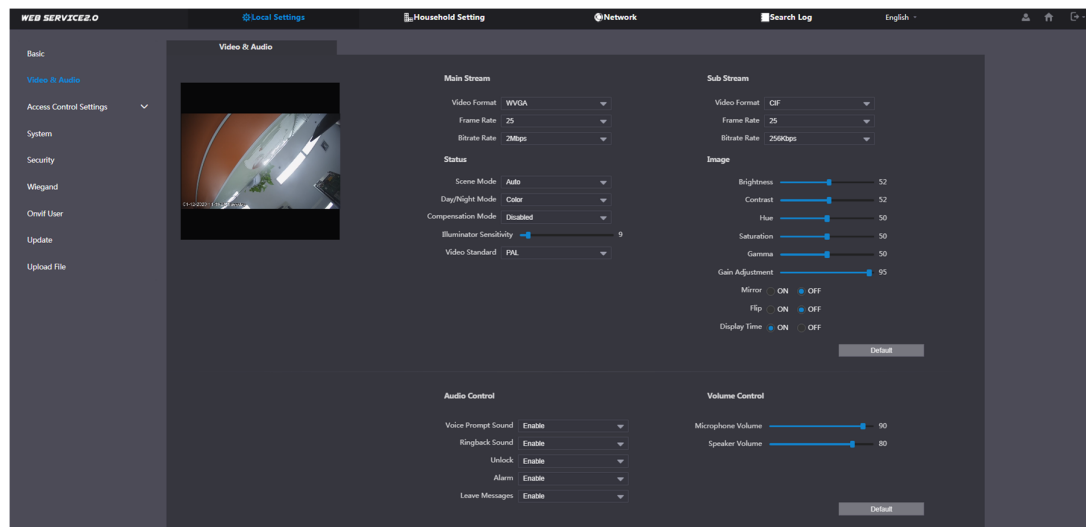
Step 8 Click **Save**.

4.2 Video & Audio

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

Step 1 Select **Local Setting > Video & Audio**.

Figure 4-3 Video & Audio



Step 2 Configure the parameters, which will take effect upon change.

Table 4-3 Video parameter description

Parameter		Description
Main Stream	Video Format	—
	Format Rate	Larger value for smoother video.
	Bitrate Rate	Larger value for better quality.
Sub Stream	Video Format	—
	Format Rate	Larger value for smoother video.
	Bitrate Rate	Larger value for better quality.
Status	Scene Mode	Select as needed according to the lighting condition. Automatic is selected by default.
	Day/Night Mode	Change the image to colorful or black and white manually or automatically.
	BackLight Mode	<ul style="list-style-type: none"> ● Disabled: No back light. ● Backlight: When the camera is against the light, it can

Parameter		Description
		<p>get clearer image of the dark areas on the target.</p> <ul style="list-style-type: none"> ● Wide dynamic: The system dims bright areas and compensates dark areas to ensure the overall clarity. ● Inhibition: the system constrains bright areas and reduces halo size to dim the overall brightness.
	Sensor Sensitivity	Larger value for higher sensitivity.
	Video Standard	—
Image	Brightness	Larger value for brighter image. Configure the value as appropriate.
	Contrast	Larger value for more the contrast between bright and dark areas. Configure the value as appropriate.
	Hue	Make the color brighter or darker. The default value is made by the light sensor, and We recommend keep it default.
	Saturation	Larger value for thicker color.
	Gamma	Changes the picture brightness and improves the picture dynamic range in a non-linear way. Larger value for brighter image.
	Video.GainAuto	Amplify the video signal to increase image brightness. If the value is too large, there will be more noise in the image.
	Mirror	Display the image with left and right side reversed.
	Flip	Display the image upside down.
Audio Control	—	Turn on or off each type of sound.
Volume Control	Mic Volume	—
	Beep Volume	—

4.3 Access Control Settings

This section introduces how to configure the two locks.


4.3.1 Local

Step 1 Select **Local Setting > Access Control > Local**.

Figure 4-4 Local

Step 2 Configure the parameters.

Table 4-4 Local access control parameter description

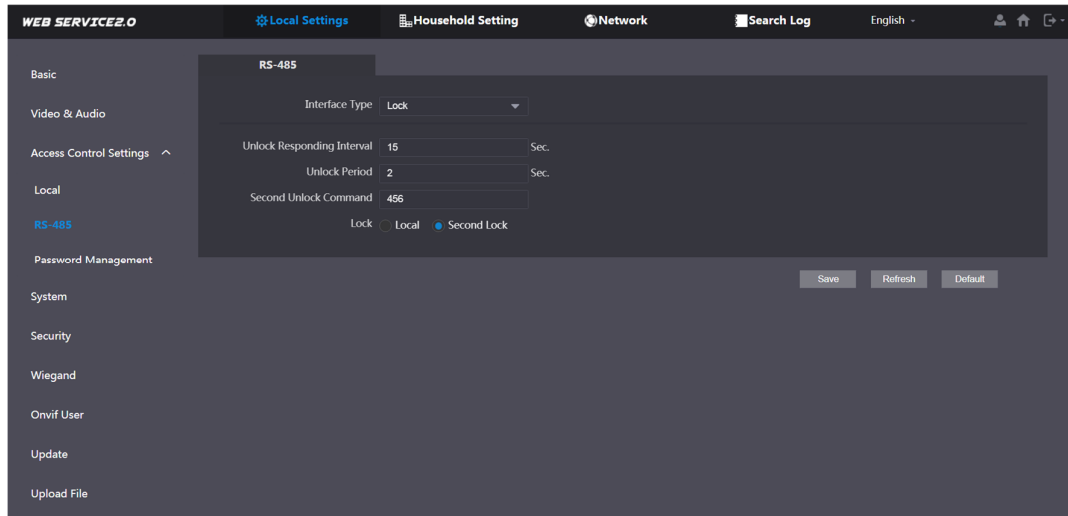
Parameter	Description
Unlock Responding Interval	The interval between two unlocks.
Unlock Period	The time for which the lock stays unlocked.
Door Sensor Check Time	<ul style="list-style-type: none"> Enable it, and the door will not be locked until the door sensors contact each other. If the door is unlocked longer than the Door Sensor Check Time, the door sensor alarm will be triggered, and the alarm will be sent to the management center. If you do not enable it, the door will be locked after the Unlock Period.  <p>You need to install a door contact to configure this parameter.</p>
First/Second Unlock Command	You can connect a third-party phone, such as a SIP phone, to the VTO, and use the command to open the door remotely.
Door Contact Type	<ul style="list-style-type: none"> NC: Normally closed. NO: Normally on.
Door Sensor Enable	Turn off or on door contact detection.
Lock	Non-remote methods, such as password or card, will unlock the lock you select.
IC Card Encrypt	Access cards issued by the VTO will be encrypted and unclonable.

Step 3 Click **Save**.

4.3.2 RS-485

Select **Local Setting** > **Access Control** > **Local**, and then configure the parameters of the lock connected through the RS-485 port. See Table 4-4 for parameter description.

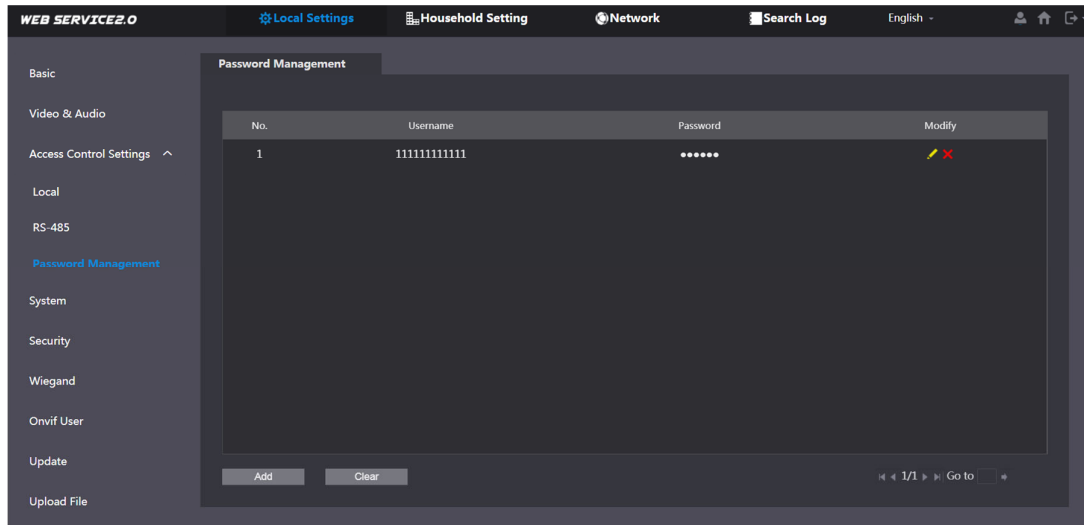
Figure 4-5 Lock connected through the RS-485 port



4.4 Password Management

Click **Add**, and then you can add a username and password used to unlock the door.

Figure 4-6 Password management



4.5 System



Configure time-related format, NTP server, and more.


Step 1 Select **Local Setting > System**.

Figure 4-7 System

Step 2 Configure the parameters.

Table 4-5 System parameter description

Parameter	Description
Date Format	—
Time Format	—
System Time	 <p>Changing system time might cause problems on video searching and information publication. Turn off video recording and auto snapshot before changing it.</p>
Time Zone	—
Sync PC	Synchronize the system time between the VTO and PC.
DST	Daylight saving time.
DST Type	<ul style="list-style-type: none"> ● Date: Define a specific date ● Week: You need to configure the begin and end time.
Begin Time	Configure the begin time and end time of DST.
End Time	
NTP Enable	Enable NTP and enter the IP address of the NTP server, and then the VTO will synchronize time with the NTP server automatically.
NTP Server	
Port	NTP server port number.
Interval	VTO time update cycle. Maximum 30 minutes.
Auto Maintenance	Schedule when the VTO will restart automatically.
SSH	<p>You can connect debugging devices to the VTO through SSH protocol.</p>  <p>We recommend turning it off, and turn on security mode and password protection. Otherwise, the VTO might be exposed to security risks and data leakage.</p>

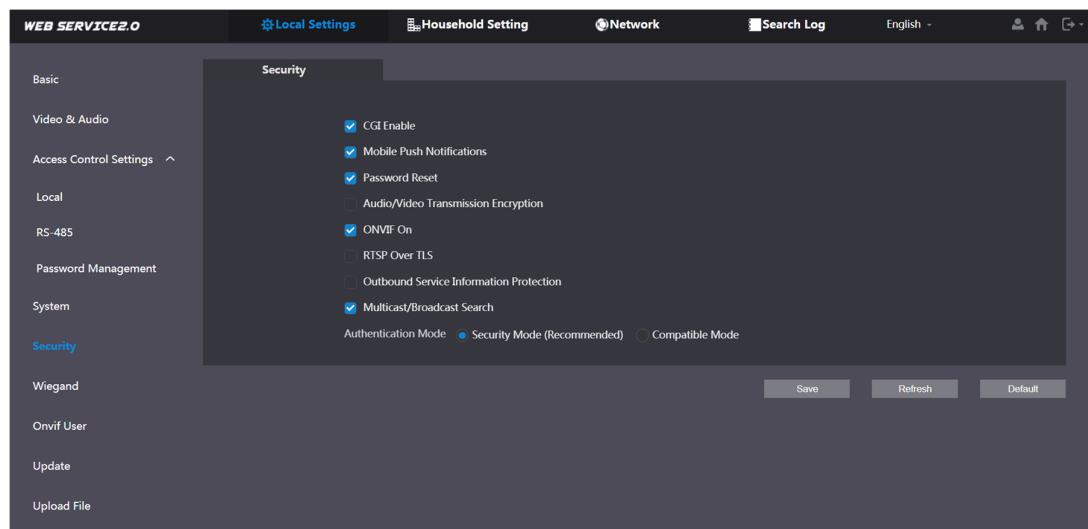
Emergency Maintenance	<p>Enable it for fault analysis and repair.</p>  <p>This function will occupy 8088 and 8087 ports.</p>
-----------------------	---

Step 3 Click **Save**.

4.6 Security









Step 1 Select **Local Setting > Security**.


Figure 4-8 Security



Step 2 Configure the parameters.

Table 4-6 Security parameter description

Parameter	Description
CGI Enable	<p>Enable the use of CGI command.</p>  <p>We recommend turning it off. Otherwise, the VTO might be exposed to security risks and data leakage.</p>
Mobile Push Notification	<p>Send information to the app on the smartphone.</p>  <p>The VTO might be exposed to security risks and data leakage. We recommend turning it off if do not need this function.</p>
Password Reset	 <p>If turned off, you will not be able to reset password.</p>
Audio/Video Transmission Encryption	<p>Encryp all data during voice or video call.</p>  <p>We recommend turning it off. Otherwise, the VTO might be exposed to security risks and data leakage.</p>
ONVIF On	<p>Enable other devices to pull video stream of the VTO through the ONVIF protocol.</p>  <p>We recommend turning it off. Otherwise, the VTO might be exposed to security risks and data leakage.</p>
RTSP Over TSL	<p>Output encrypted bit stream through RTSP.</p>  <p>We recommend turning it on. Otherwise, the VTO might be exposed to security risks and data leakage.</p>
Outbound Service Information Protection	 <p>Protect your passwords.</p> <p>We recommend turning it on. Otherwise, the VTO might be exposed to security risks and data leakage.</p>
Multicast/Broadcast Search	<p>Enable it and the VTO will be found by other devices.</p>  <p>We recommend turning it off. Otherwise, the VTO might be exposed to security risks and data leakage.</p>

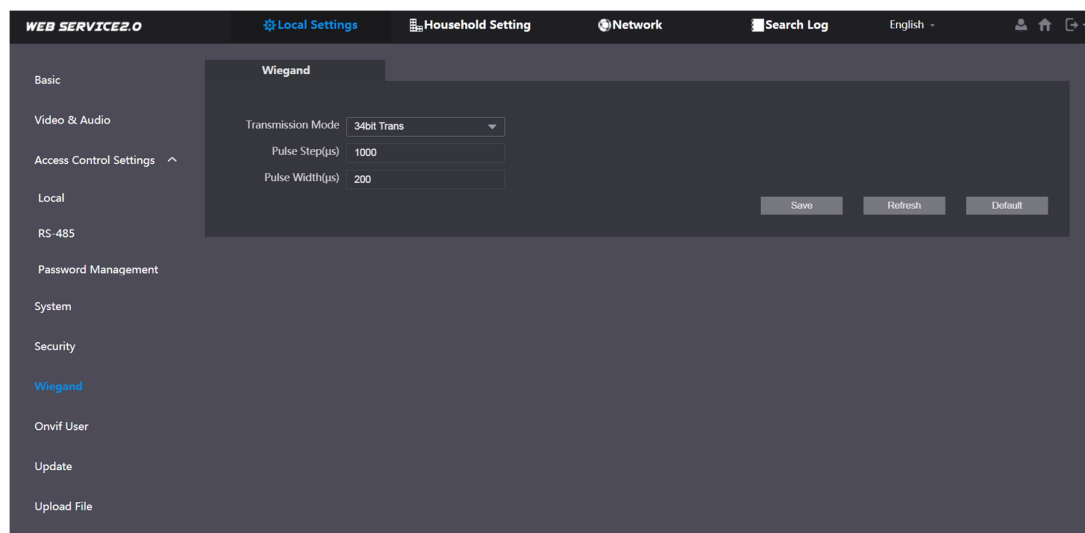
Authentication Mode	<ul style="list-style-type: none"> ● Security Mode (recommended): Support logging in with Digest authentication. ● Compatible Mode: Use the old login method.  <p>We recommend security mode. Compatible mode might expose the VTO to security risks and data leakage.</p>
---------------------	---

Step 3 Click **Save** to save.

4.7 Wiegand

Configure the parameters as needed when connected to other devices through the Wiegand port.

Figure 4-9 Wiegand



4.8 Onvif User

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

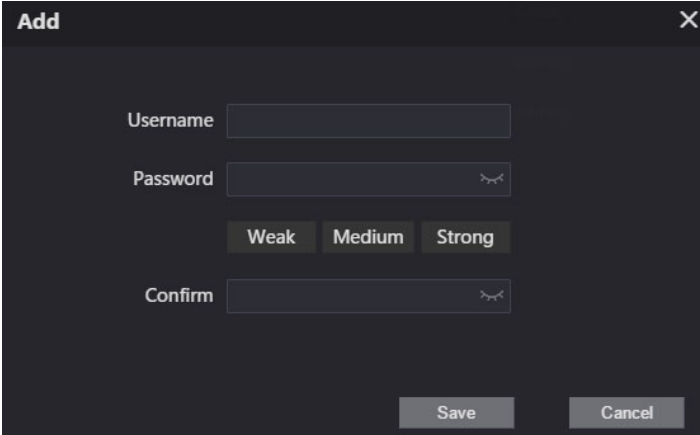


If you delete an account, it cannot be undone.

Step 1 Select **Local Settings > Onvif User**.

Step 2 Click **Add**.

Figure 4-10 Add an onvif user account

A dark-themed dialog box titled "Add" with a close button (X) in the top right corner. It contains four input fields: "Username", "Password", "Confirm", and a strength indicator. The "Password" and "Confirm" fields have a small eye icon to toggle visibility. Below the "Password" field are three buttons: "Weak", "Medium", and "Strong". At the bottom right are "Save" and "Cancel" buttons.

Add

Username

Password

Weak Medium Strong

Confirm

Save Cancel

Step 3 Enter the information, and then click **Save**.

Onvif devices can now monitor the VTO using the account. See the corresponding manual for details.

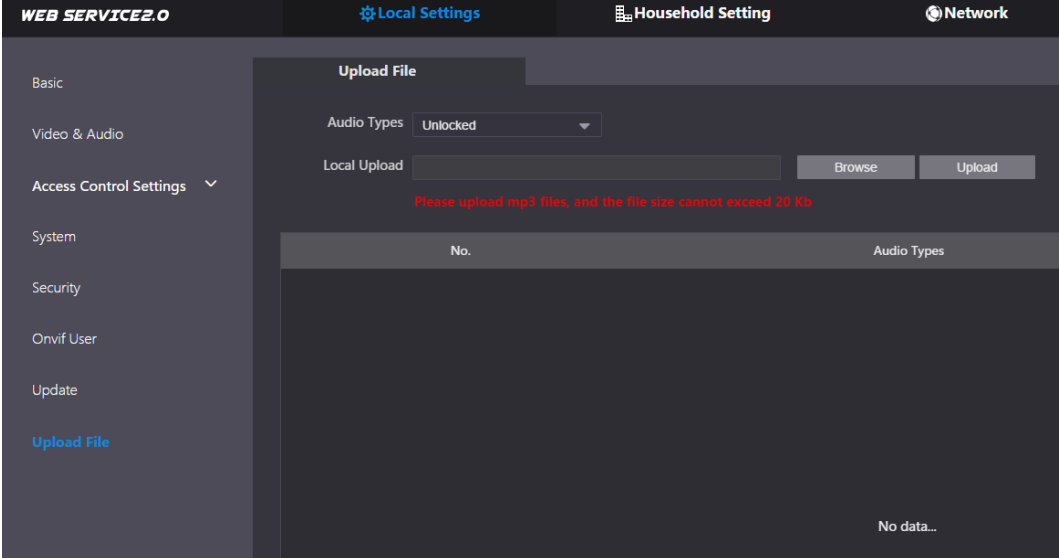
4.9 Upload File

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

Step 1 Select **Local Settings > Upload File**.

Step 2 Select an audio type, and then click **Browser** to select the audio file as needed.

Figure 4-11 Change the sound prompt

A screenshot of the "WEB SERVICE 2.0" interface. The top navigation bar includes "Local Settings" (selected), "Household Setting", and "Network". The left sidebar lists various settings categories, with "Upload File" highlighted in blue. The main content area is titled "Upload File" and features a dropdown menu for "Audio Types" set to "Unlocked". Below this is a "Local Upload" section with a file input field, "Browse", and "Upload" buttons. A red error message states: "Please upload mp3 files, and the file size cannot exceed 20 Kb". At the bottom, there is a table header with columns "No." and "Audio Types", followed by a large empty area with the text "No data..." at the bottom right.

WEB SERVICE 2.0 Local Settings Household Setting Network

Upload File

Audio Types Unlocked

Local Upload Browse Upload

Please upload mp3 files, and the file size cannot exceed 20 Kb

No.	Audio Types
No data...	

Step 3 Click **Upload**.

5 Household Setting

This chapter is applicable when the VTO works as the SIP server, and introduces how to add, modify, and delete VTO, indoor monitor ("VTH"), VTS, and IPC devices, and how to send messages from the SIP server to other VTOs and VTHs. If you are using other servers as the SIP server, see the corresponding manual for details.

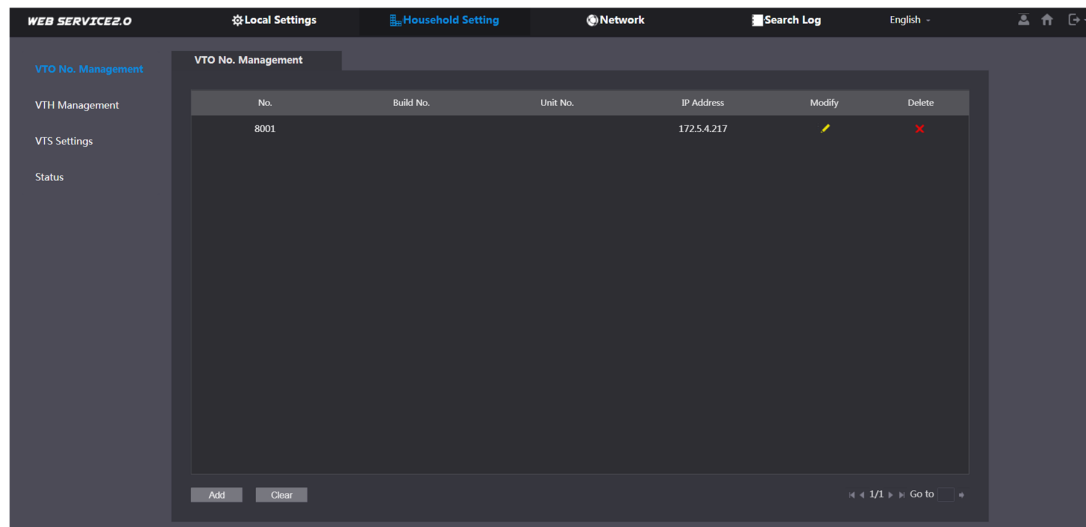
5.1 VTO No. Management

Adding VTO

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

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

Figure 5-1 VTO number management



Step 2 Click **Add**.

Figure 5-2 Add VTO

Step 3 Configure the parameters.





The SIP server must be added.

Table 5-1 Add VTO configuration

Parameter	Description
Rec No.	The VTO number you configured. See Table 4-1 for details.
Register Password	Keep it default.
Build No.	Available only when other servers work as the SIP server.
Unit No.	
IP Address	IP address of the VTO.
Username	Web interface login username and password of the VTO.
Password	

Step 4 Click **Save**.



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

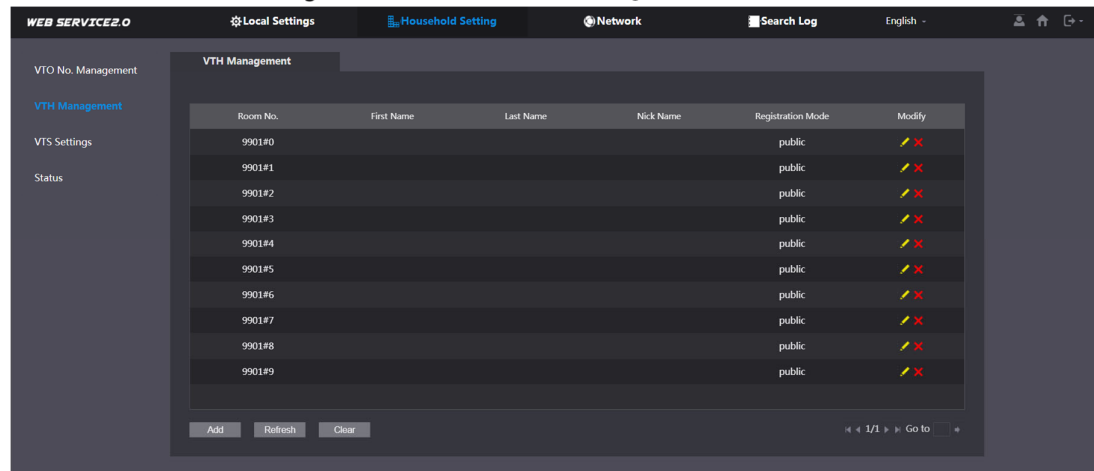
5.2 VTH Management

5.2.1 Adding Room Number

You can add room numbers to the SIP server, and then configure the room number on the VTHs to connect them to the network.

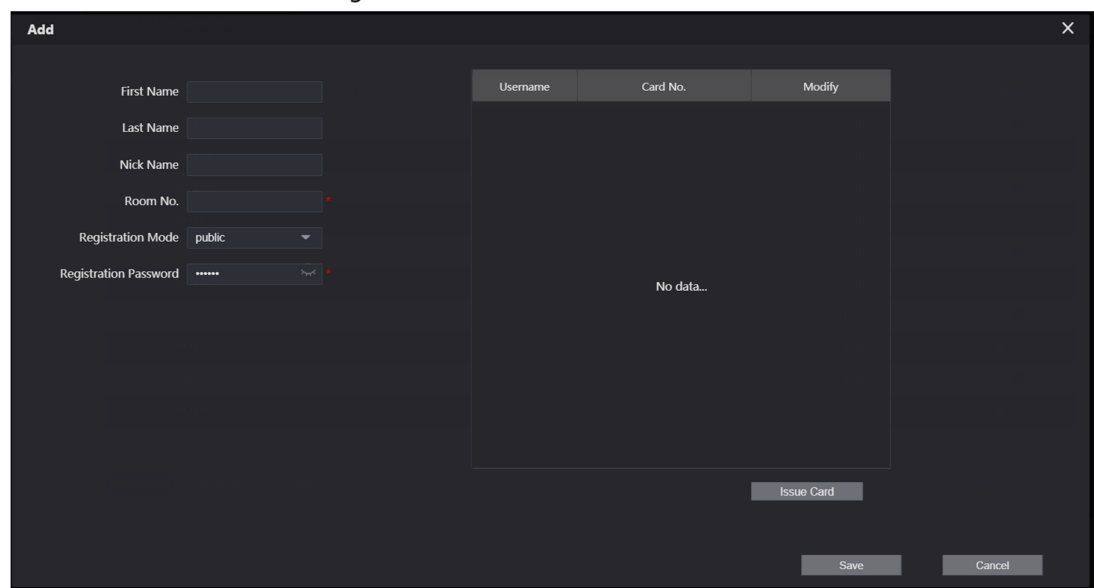
Step 1 Log in to the web interface of the SIP server, and then select **Household Setting > VTH Management**.

Figure 5-3 Room number management



Step 2 Click the **Add**.

Figure 5-4 Add a room number





Step 3 Configure the parameters.

Table 5-2 Room information

Parameter	Description
First Name	Enter the information you need to differentiate each room.
Last Name	
Nick Name	
Room No.	—
Register Type	Select public .
Register Password	Keep it default.

Step 4 Click **Save**.



Click  or  to modify or delete a room number.

5.2.2 Issuing Access Card

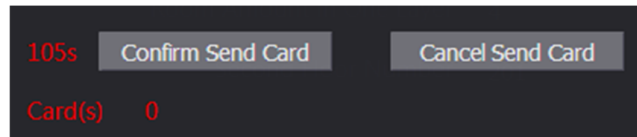
Issue access card to unlock the door of a room.



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

Step 1 When adding or modifying a room number, click **Issue Card**.

Figure 5-5 Countdown notice



Step 2 Swipe the card on the VTO.

Figure 5-6 Issue card

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

Figure 5-7 Issued access card

Username	Card No.	Modify
mm	201#000000	

Other Operations

- Click to set it to the main card, and then the icon turns into . The main card can be used to issue access cards for this room on the VTO.
- Click to set it to loss, and then the icon turns into . The lost card cannot be used to open the door.
- Click or to modify the username or delete the card.

5.2.3 Issuing Fingerprint

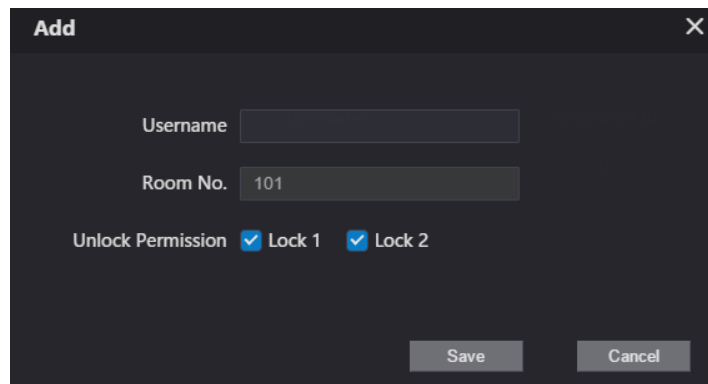
Issue fingerprints to unlock the door of a room.



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

Step 1 When adding or modifying a room number, click **Issue Card**.

Figure 5-8



The 'Add' dialog box is a dark-themed window with a close button (X) in the top right corner. It contains two text input fields: 'Username' and 'Room No.', with the value '101' entered in the 'Room No.' field. Below these fields are two checkboxes labeled 'Unlock Permission', 'Lock 1', and 'Lock 2', all of which are checked. At the bottom right, there are two buttons: 'Save' and 'Cancel'.

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

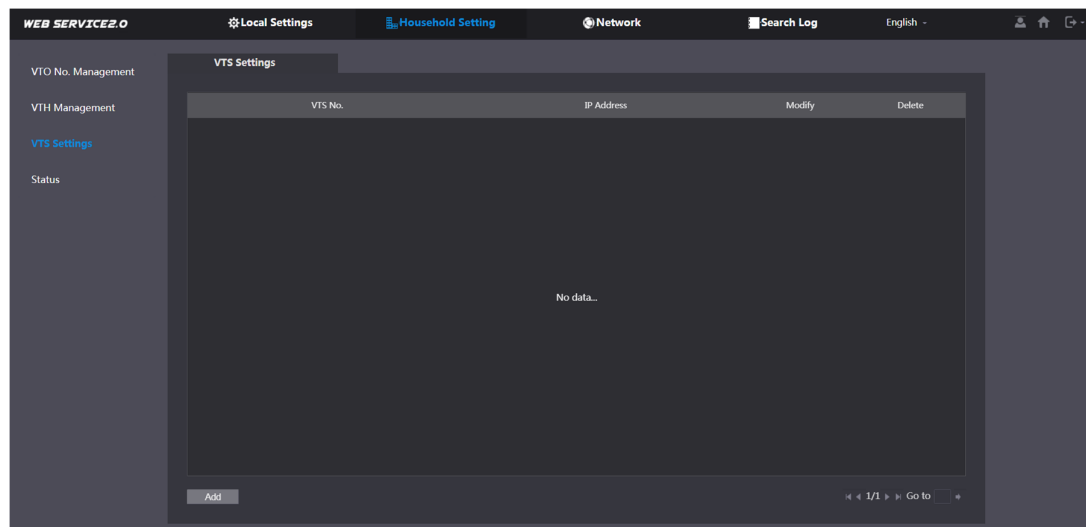
Step 3 Press your fingerprint on the fingerprint scanner.

5.3 VTS Management

You can add a VTS to the SIP server, and then it can be used as the management center. It can also manage, call, or receive calls from all the VTOs and VTHs in the network. See the corresponding user's manual for details.

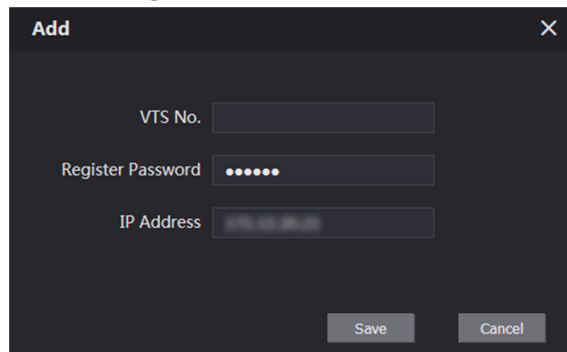
Step 1 Log in to the web interface of the VTO working as the SIP server, and then select **Household Setting > VTS Settings**.

Figure 5-9 VTS management



Step 2 Click **Add**.

Figure 5-10 Add VTS



The 'Add' dialog box contains three input fields: 'VTS No.' with a numeric keypad, 'Register Password' with a password mask (dots), and 'IP Address' with an IP address mask. At the bottom right are 'Save' and 'Cancel' buttons.

Step 3 Configure the parameters.

Table 5-3 Add VTS configuration

Parameter	Description
VTS No.	—
Register Password	Keep it default.
IP Address	VTS IP address.

Step 4 Click **Save**.

5.4 IPC Setting

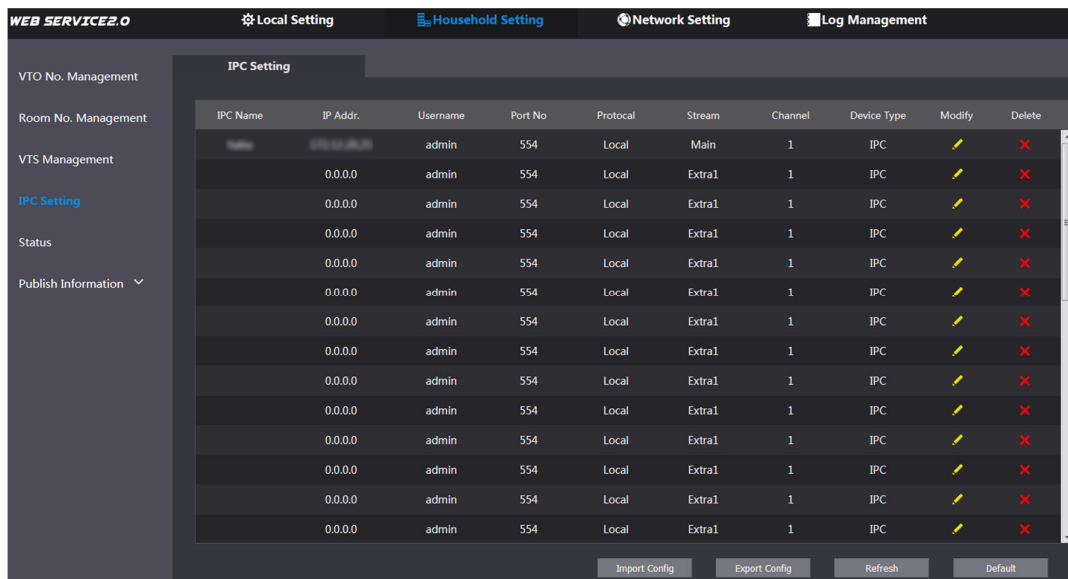
You can add IPC and NVR to the SIP server, and then all the connected VTH can monitor them.



Interfaces may vary with different products. The actual interface shall prevail.

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

Figure 5-11 IPC setting



The screenshot shows the 'IPC Setting' page in the 'WEB SERVICE 2.0' interface. The left sidebar has a menu with 'IPC Setting' selected. The main area displays a table of IPC devices with columns for Name, IP Address, Username, Port No., Protocol, Stream, Channel, Device Type, Modify, and Delete. At the bottom are buttons for 'Import Config', 'Export Config', 'Refresh', and 'Default'.

IPC Name	IP Addr.	Username	Port No.	Protocol	Stream	Channel	Device Type	Modify	Delete
IPC001	192.168.1.10	admin	554	Local	Main	1	IPC		
IPC002	0.0.0.0	admin	554	Local	Extra1	1	IPC		
IPC003	0.0.0.0	admin	554	Local	Extra1	1	IPC		
IPC004	0.0.0.0	admin	554	Local	Extra1	1	IPC		
IPC005	0.0.0.0	admin	554	Local	Extra1	1	IPC		
IPC006	0.0.0.0	admin	554	Local	Extra1	1	IPC		
IPC007	0.0.0.0	admin	554	Local	Extra1	1	IPC		
IPC008	0.0.0.0	admin	554	Local	Extra1	1	IPC		
IPC009	0.0.0.0	admin	554	Local	Extra1	1	IPC		
IPC010	0.0.0.0	admin	554	Local	Extra1	1	IPC		
IPC011	0.0.0.0	admin	554	Local	Extra1	1	IPC		
IPC012	0.0.0.0	admin	554	Local	Extra1	1	IPC		
IPC013	0.0.0.0	admin	554	Local	Extra1	1	IPC		
IPC014	0.0.0.0	admin	554	Local	Extra1	1	IPC		
IPC015	0.0.0.0	admin	554	Local	Extra1	1	IPC		

Step 2 Click  to add a device.



You can only add as many devices as the ones displayed.

Figure 5-12 Add IPC

The 'Modify' dialog box contains the following fields and values:

- IPC Name: [Empty]
- IP Address: 0.0.0.0
- Username: admin
- Password: [Masked with dots]
- Port: 554
- Protocol: Local
- Stream Type: Extra1
- Channel: 1
- Device Type: IPC
- MediaEncrypt: OFF (selected)

Buttons: Save, Cancel

Step 3 Configure the parameters.

Table 5-4 Add IPC configuration

Parameter	Description
IPC Name	—
IP Address	—
Username	Web interface login use.rname and password of the device.
Password	
Port	Keep it default.
Protocol	Select from Local or Onvif .
Stream Type	<ul style="list-style-type: none"> ● Main: Better video quality but require more bandwidth. ● Extra1: Smoother video with worse quality, but require less bandwidth.
Channel	Define a channel for the device.
Device Type	Select the one as needed.
MediaEncrypt	Select ON if the IPC to be added is encrypted.

Step 4 Click **Save**.

Other Operations

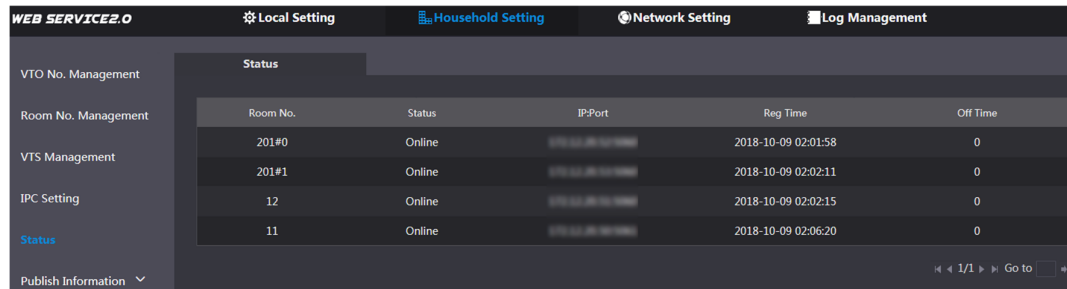
- **Export Config**: Export the current devices information to your PC.
- **Import Config**: Import existing devices information.

5.5 Status

You can view the online status 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 5-13 Status



Room No.	Status	IP-Port	Reg Time	Off Time
201#0	Online	192.168.1.100	2018-10-09 02:01:58	0
201#1	Online	192.168.1.101	2018-10-09 02:02:11	0
12	Online	192.168.1.102	2018-10-09 02:02:15	0
11	Online	192.168.1.103	2018-10-09 02:06:20	0

5.6 Publish Information

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

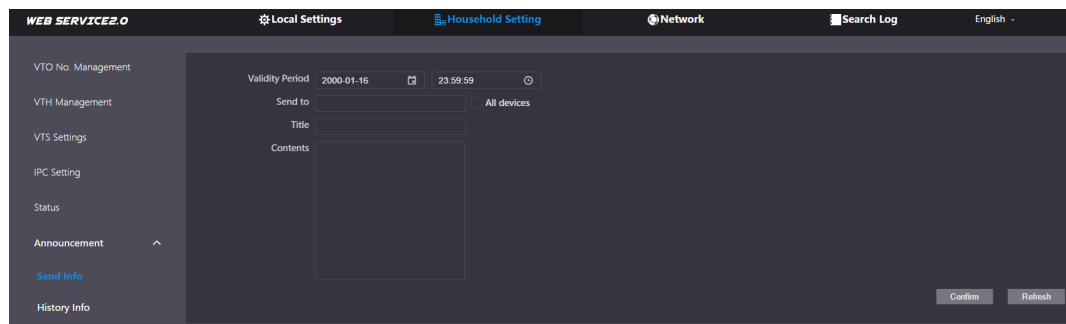


Interfaces may vary with different products. The actual interface shall prevail.

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 5-14 Send information



Step 2 Specify the **Period of validity** that the message will only be valid during this period.

Step 3 Enter the number of a device, or select **All devices** to send the message to all the devices in the network, and then enter the title and content of your message.

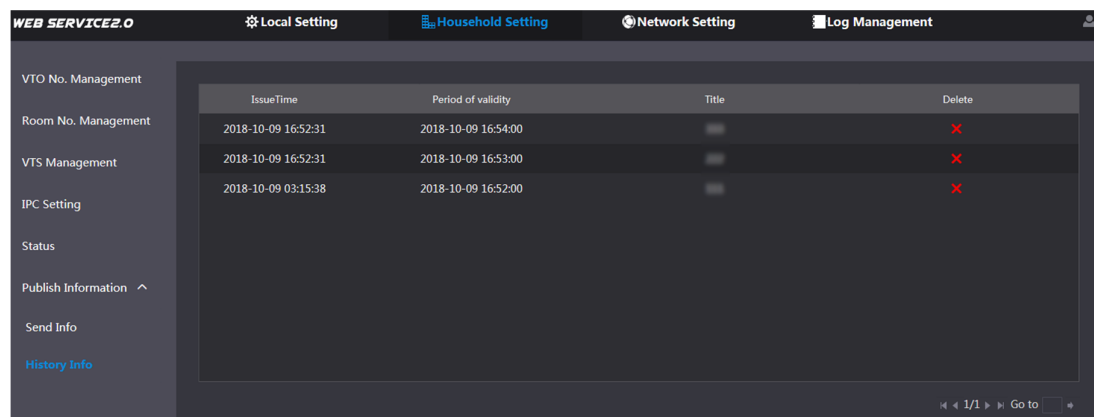
Step 4 Click **Confirm**.

5.6.2 History Info

You can view the information of sent messages.

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

Figure 5-15 History information



The screenshot shows the WEB SERVICE 2.0 web interface. The top navigation bar includes 'Local Setting', 'Household Setting' (selected), 'Network Setting', and 'Log Management'. The left sidebar lists various management options: 'VTO No. Management', 'Room No. Management', 'VTS Management', 'IPC Setting', 'Status', 'Publish Information' (expanded), 'Send Info', and 'History Info' (selected). The main content area displays a table with the following data:

IssueTime	Period of validity	Title	Delete
2018-10-09 16:52:31	2018-10-09 16:54:00		
2018-10-09 16:52:31	2018-10-09 16:53:00		
2018-10-09 03:15:38	2018-10-09 16:52:00		

At the bottom right of the table, there is a pagination control showing '1/1' and a 'Go to' button.

6 Network Setting

This chapter introduces how to configure the network parameters.

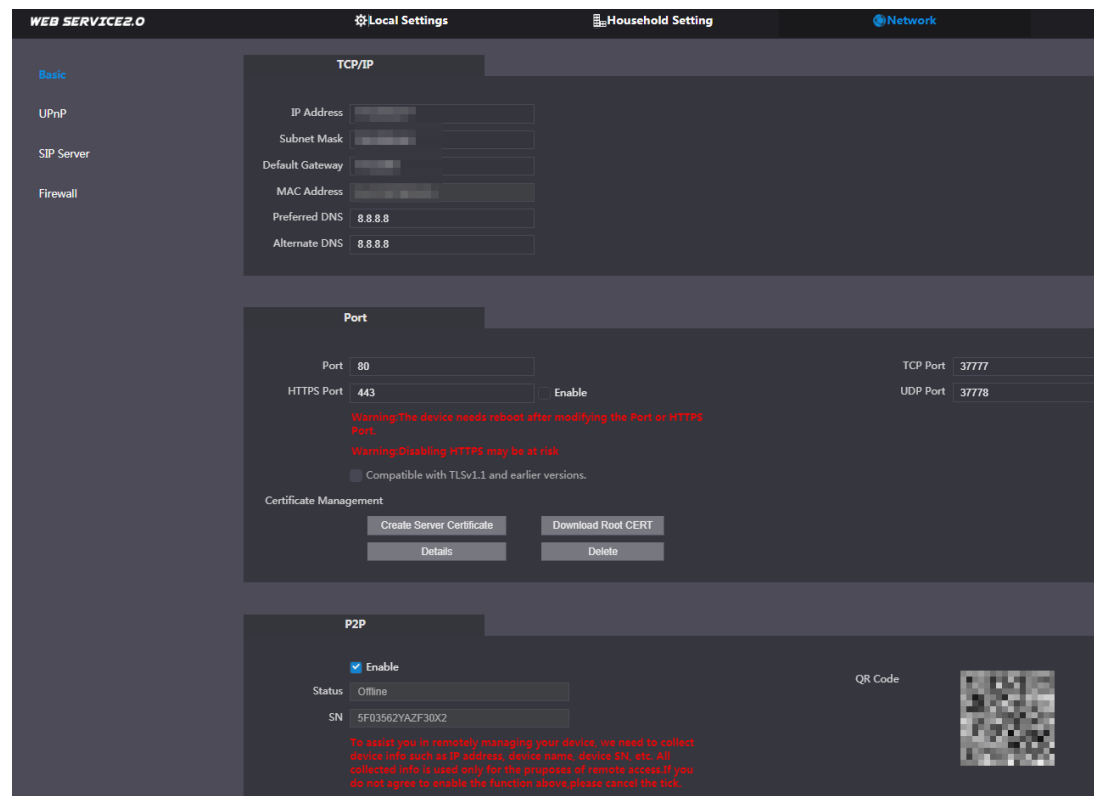
6.1 Basic

6.1.1 TCP/IP

You can modify the IP address, subnet mask, default gateway, and DNS of the VTO.

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

Figure 6-1 TCP/IP and port





Step 2 Configure the parameters, and then click **Save**.

The VTO will restart, 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 Port

Table 6-1 Parameter description

Parameter	Description
Port	80 by default. If already used, choose any number from 1025 to 65535 as needed. You can enter http://VTO IP address:Port to log in to the VTO.

Parameter	Description
HTTPS Port	Enable it and click Save . You can now enter "https://VTO IP address:HTTPS Port" to log in to the VTO.
TCP/UDP Port	Used for accessing the VTO with devices in other networks.
Create Server Certificate	<p>If it is your first time using the VTO or you have changed the IP address of the VTO, you need to go through this process, because this certificate is the unique digital identification of VTO for the SSL protocol.</p>  <p>If you delete the certificate that has been created, it cannot be undone.</p>
Download Root CERT	<p>If you are using a PC that has never logged in to the VTO, you need to download the root certificate, double click to install it, and then you can use the HTTPS function mentioned above.</p>  <p>If you delete the certificate that has been installed, it cannot be undone.</p>

6.1.3 P2P

Enable the **P2P** function, and then you can scan the QR code with your phone to add the VTO to the app on your smartphone. See the quick start guide for details.

6.2 UPnP

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

Prerequisites

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

6.2.1 Enabling UPnP Services

Step 3 Select **Network > UPnP**.

Step 4 Enable the services as needed.

Step 5 Select the **Enable** check box.

Step 6 Click **Save**.

6.2.2 Adding UPnP Services

Step 7 Select **Network > UPnP**.

Step 8 Click **Add**.

Step 9 Configure the parameters as needed.

Figure 6-2 Add a UPnP service

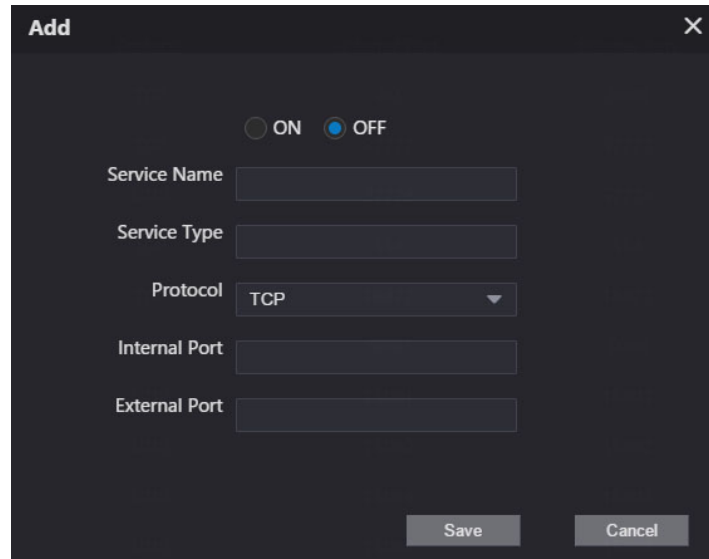



Table 6-2 Parameter description

Parameter	Description
Service Name	Enter the information as needed.
Service Type	
Protocol	Select TCP or UDP as needed.
Internal Port	Use port number 1024 to 5000.
External Port	 <ul style="list-style-type: none">Do not use 1 to 1023 ports to avoid conflict.If you need to configure this function for multiple devices, make sure that the ports will not be the same.The port number you use must not be occupied.The internal and external port number must be the same.

6.3 SIP Server

There must be a SIP server in the network for all the connected VTOs and VTHs to call each other. You can use a VTO or other servers as the SIP server.

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

Figure 6-3 SIP Server

WEB SERVICE2.0 Local Settings Household Setting Network Search Log English

Basic
UPnP
SIP Server
Firewall

SIP Server ☒ Enable

Server Type VTO

IP Address

Port 5080

Username 8001

Password

SIP Domain VDP

SIP Server Username admin

SIP Server Password

Warning: The device will be rebooted after modifying the SIP server enable status.

Save Refresh Default

Step 2 Select a server type as needed.

- The VTO you have logged in as the SIP server:
- Enable **SIP Server**, and click **Save**, and then the VTO will restart. You can add VTOs and VTHs to this VTO. See the details in "0

Household Setting".



If the VTO you have logged in will not be the SIP server, do not enable **SIP Server**; otherwise the connection will fail.

- If another VTO works as the SIP server:
Select **Server Type** to **VTO**, and then configure the parameters.

Table 6-3 SIP server configuration

Parameter	Description
IP Addr.	VTO IP address.
Port	5060.
Username	Keep it default.
Password	
SIP Domain	VDP.
SIP Server Username	Web interface login username and password of the VTO.
SIP Server Password	

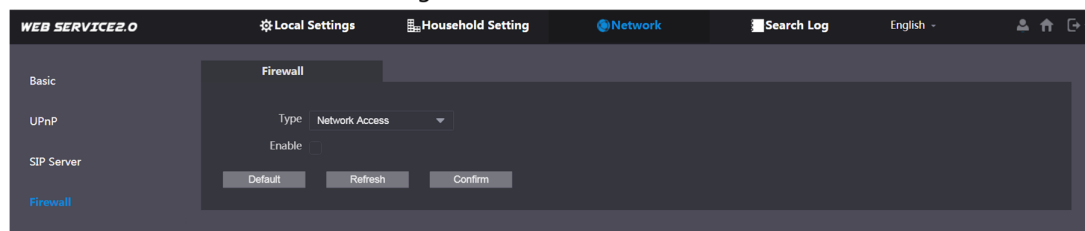
- If other servers work as the SIP server:
Select the **Server Type** as needed, and then see the corresponding manual for the details.

6.4 Firewall

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

Step 1 Select **Network > Firewall**.

Figure 6-4 Firewall



Step 2 Select one or more firewall types, and then enable them.

Step 3 Configure the parameters.

Table 6-4 Firewall type description

Type	Description
Network Access	<ul style="list-style-type: none">• You can choose either Allowlist or Blocklist, and then add an IP address or segment which is allowed or denied to access the VTO.
PING Prohibited	The VTO will not response to ping to avoid ping attacks.
Anti semijoin	Protects the VTO performance by blocking excessive SYN packets.

7 Log Management

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



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

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 device 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 device (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 device is connected to the public network, We recommend 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 device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device 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 device (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 device 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. MAC Address Binding

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

8. Assign Accounts and Privileges Reasonably

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

9. Disable Unnecessary Services and Choose Secure Modes

If not needed, We recommend turning 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.

10. 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.

11. Secure Auditing

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

12. Network Log

Due to the limited storage capacity of the device, 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.

13. Construct a Safe Network Environment

In order to better ensure the safety of device 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.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.