

Villa Door Station

User's Manual



V1.0.0

Foreword

General

This manual introduces how to configure the villa door station (hereinafter referred to as "VTO") on the web interface.

Safety Instructions

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

Signal Words	Meaning
	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.0	First release.	January 2021

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.
 - L



Important Safeguards and Warnings

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

Operating Requirements

- 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 Requirements

- 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	II
1 Initializing the VTO	
2 Login and Resetting Password	
2.1 Login	2
2.2 Resetting Password	
3 Main Interface	
4 Local Settings	5
4.1 Basic	5
4.2 Video & Audio	6
4.3 Access Control Settings	
4.3.1 Local	
4.3.2 RS-485	10
4.3.3 Password Management	10
4.4 System	10
4.5 Security	12
4.6 Wiegand	13
4.7 Onvif User	14
4.8 Upload File	15
5 Household Setting	
5.1 VTO No. Management	16
5.2 VTH Management	17
5.2.1 Adding Room Number	17
5.2.2 Issuing Access Card	19
5.2.3 Issuing Fingerprint	
5.3 VTS Management	
5.4 IPC Setting	21
5.5 Status	23
5.6 Publish Information	23
5.6.1 Send Info	23
5.6.2 History Info	24
6 Network	
6.1 Basic	25
6.1.1 TCP/IP	25
6.1.2 Port	25
6.1.3 P2P	26
6.2 UPnP	26
6.2.1 Enabling UPnP Services	26
6.2.2 Adding UPnP Services	27
6.3 SIP Server	27
6.4 Firewall	
7 Log Management	





1 Initializing the VTO

For first-time login or after resetting the VTO, you need to initialize it on the web interface.

<u>Step 1</u> Power on the VTO.

 \square

<u>Step 2</u> Go to the default IP address (192.168.1.108) of the VTO.

Make sure that the IP address of your PC is in the same network segment as the VTO. Figure 1-1 Device initialization

Device Init				×
	1	2	— 3	
o		Тwo	Three	
	Username admi	n		
	Password			
	Low	Middle H	ligh	
Confi	rm Password			
		Next		

<u>Step 3</u> Enter and confirm the password, and then click **Next**.

- <u>Step 4</u> Enter an email address for resetting password.
- <u>Step 5</u> Click **Next**, and then click **OK**.



2 Login and Resetting Password

2.1 Login

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

<u>Step 1</u> Go to the IP address of the VTO in the browser.

 \square

For first-time login, enter the default IP (192.168.1.108). If you have multiple VTOs, we recommend changing the default IP address (**Network > Basic**) to avoid conflict.

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

Figure 2-1 Login

WEB SERVICE2.0
Username
Password
Forgot password?
Login

2.2 Resetting Password

<u>Step 1</u> On the login interface, click **Forgot Password?**, and then click **Next**.

Figure 2-2 Reset the password

Reset the password (2	/3)		×
Scan QR Code :		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.	
Enter security code :	The security code will be delivered to :		
Cancel		Next	

<u>Step 2</u> Scan the QR code, and then you will get a string of numbers and letters.



- <u>Step 3</u> Send the string to the email: support_gpwd@htmicrochip.com, and then the security code will be sent to the email address configured during initialization.
- <u>Step 4</u> Enter the security code in the input box, and then click **Next**.
 - Ш
 - If you did not set an email address during initialization, contact your supplier or customer service for help.
 - 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.
- <u>Step 5</u> Enter and confirm the new password, and then click **OK**.



3 Main Interface

Fiaure	3-1	Main	interface
inguic	5.	mann	millinace

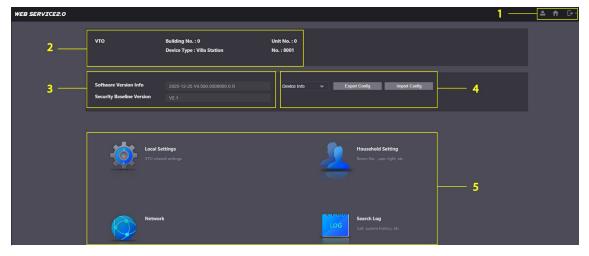


Table 3-1 Main interface introduction

No.	Function	Description		
1	General function	 Change the password and your email address. Go to the main interface. End: Go to the main interface. End: Log out, restart the VTO or restore the VTO to factor settings. If you restore the VTO to factory settings, all data except external storage will be deleted. You can format the SD card to delete the data in it. 		
2	VTO information	View the information of the VTO and the system.		
3	System information	view the information of the vio and the system.		
4	Configuration manager	Export or import VTO configuration or user information.		
5	Function	Configure parameters for different functions.		



4 Local Settings

This chapter introduces the detailed configuration of the VTO.

4.1 Basic

<u>Step 1</u>	Select Local Settings > Basic.
---------------	--------------------------------

Figure 4-1 Basic

WEB SERVICE2.0	袋Local Settings	Household Setting	Network	Search Log
Basic	Device Properties			
Video & Audio	Device Type Villa Station	▼ Center Call No		
Access Control Settings 💙	Device Name No. 8001	Calling Center Perioc Perids in which Call	5 Setting	• •
System	Group Call 🛛 🗹 Warning:Th modifying group call enable statu	can be Made e device will be rebooted after B.		
Security				
Onvif User	Events			
Update	Total SD Card Capacity 0	м		
Upload File	SD Used Capacity 0	м		
		Format		
	Auto Capture (Unlock) ON	he SD card if it can not be recognized. OFF 		
	Auto Capture (Calling) ON	OFF		
	Upload Video ON Messages	OFF		
		• OFF		

<u>Step 2</u> Configure the parameters.

Table 4-1	Basic	narameter	description
	Dasic	parameter	uescription

Parameter	Description
Device Type	Select Villa Station or Small Apartment as needed.
Center Call No.	The default phone number for the management center is 888888, and
Center Can No.	you can set it to any number with up to 9 digits.
Device Name	When other devices are monitoring this VTO, the device name will appear
Device Name	on the monitoring image.
Calling Center Period	Time period in which the management center can be called.
	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
N	by using their numbers.
No.	
	You can change the number of the VTO when it is not working as the SIP
	server.
Periods in which Calls	Configure the time if you only want to receive calls during a specific
can be Made	period.
Group Call	Enable it on the VTO that works as the SIP server, and when a main VTH



Parameter	Description			
	receives a call, all extension VTHs will also receive the call.			
Total SD Card				
Capacity	Displays the total and used capacity of the SD card. You can click Format			
SD Used Capacity	to delete all the data in the SD card.			
Format				
Auto Capture	When the door is unlocked, the VTO will take two snapshots and save			
(Unlock)	them to the SD card.			
Auto Conturo (Colling)	Take a snapshot and save it in the SD card of the VTO when the VTO is			
Auto Capture (Calling)	calling.			
	When enabled:			
	• If an SD card is inserted in both the VTH and VTO, the video message			
Upload Video	will be saved both in the SD cards of the VTH and the VTO.			
-	• If an SD card is only inserted in the VTH or the VTO, the video			
Messages	message will be saved only in the SD card of the VTH or the VTO.			
	• If no SD card is inserted in the VTH or VTO, no video message will be			
	saved.			
Auto Pocording (Call)	Take recording when the VTO is in a call, and save the recording in the SD			
Auto Recording (Call)	card of the VTO.			

Step 3 Click Save.

4.2 Video & Audio

Configure the video format and quality, and audio of the VTO. <u>Step 1</u> Select **Local Settings > Video & Audio**.



Figure 4-2 Video and audio

Video & Audio				
-	Main Stream		Sub Stream	
	Video Format 720)P 📼	Video Format	CIF 👻
1	Frame Rate 25		Frame Rate	25 👻
/-	Bitrate Rate 2M	bps 👻	Bitrate Rate	256Kbps 👻
	Status		Image	
	Scene Mode Aut	• –	Brightnes	52
06-01-2000 AGe 1-25 Thursony	Compensation Mode Dis	abled 🛛 👻	Contras	t <u> </u>
	Video Standard PAL		Hue	e <u> </u>
			Saturation	50
			Gamma	50
			Gain Adjustmen	95
			Mirror	ON OFF
			Flip	on off
			Display Time	ON OFF
				Default
	Audio Control		Volume Control	
	Voice Prompt Sound	Enable		90
	Ringback Sound	Enable		0
	Unlock	Enable		
	Alarm	Enable		
	Leave Messages	Enable		
				Default

<u>Step 2</u> Configure the parameters, which will take effect upon change.

Table 4-2 Video parameter description

Parameter		Description	
		Select different resolution as needed:	
		• 1080P : 1920 × 1080.	
	Video	• 720P : 1280 × 720.	
	Format	• WVGA : 800 × 480.	
Main/Sub	Torriat	• QVGA : 320 × 240.	
Stream		• D1 : 720 × 480.	
Stream		• CIF : 352 × 288.	
	Frame Rate	The larger the value, the smoother the video, but it requires more	
	Fidille Rate	bandwidth.	
	Bitrate Rate	The larger the value, the better the video quality, but it requires more	
		bandwidth.	
	Scene Mode	Select as needed according to the lighting condition. Auto is selected	
	Scelle Mode	by default.	
		• BLC : Back light compensation. Improve the clarity of the target in	
		the image.	
C 1 1	Compensati	• WDR : Wide dynamic range. Enhance the brightness of dark areas,	
Status	on Mode	and reduce the brightness of bright areas to improve the image.	
		• HLC: High light compensation. Reduce the brightness of the	
		strong spots to improve the overall image.	
	Video	Select PAL or NTSC according to your area.	
	Standard		



Paramete	r	Description			
		PAL is mostly used in China and Europe, and NTSC primarily in the			
		United States and Japan.			
	Brightness	The larger the value, the brighter the image.			
	Contrast	Larger value for more contrast between bright and dark areas.			
	Hue	Make the color brighter or darker. The default value is made by the			
	пие	light sensor, and we recommend keeping it default.			
	Saturation	The larger the value, the thicker the color.			
Image	Gamma	Changes the picture brightness and improves the picture dynamic			
	Gamma	range in a non-linear way. The larger the value, the brighter the image.			
	Gain	Amplify the video signal to increase image brightness. If the value is			
	Adjustment	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.			
	Display Time	Display the current time and date on the video image.			
Audio		Turn on or off each type of sound.			
Control		full of of each type of sound.			
	Microphone				
Volume	Volume	Adjust the volume as needed			
Control	Speaker	Adjust the volume as needed.			
	Volume				

4.3 Access Control Settings

This section introduces how to configure the two locks connected to the lock port or the RS-485 port of the VTO.

4.3.1 Local

<u>Step 1</u> Select Local Settings > Access Control Settings.



Figure 4-3 Local

WEB SERVICE2.0	¢ Local Settings	≣ Househol	d Setting	Network	Search Log	English -
Basic	Local					
Video & Audio						
	Unlock Responding Interval		Sec.			
Access Control Settings	Unlock Period		Sec.			
	Door Sensor Check Duration	30	Sec. Enable			
RS-485	First Unlock Command					
Password Management	Door Contact Type					
System	Door Sensor Enable	ON OFF				
	Fire Alarm	ON 💿 OFF				
Security	Lock	Local Second Lock				
Wiegand						
Onvif User						
	Extend Setting					
Update						
Upload File	IC Card Encryt 💿 ON	OFF				
					Save	Refresh Default

<u>Step 2</u> Configure the parameters.

Parameter	Description
Unlock	
Responding	The door can only be unlocked again after the interval.
Interval	
Unlock Period	The time during which the lock stays unlocked.
	• 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
Door Sensor	Duration , the door sensor alarm will be triggered, and the alarm will be sent to the management center.
Check Duration	 Disable it, and then the door will be locked after the Unlock Period.
	You need to install a door contact to configure this parameter.
First/Second	You can connect a third-party phone, such as a SIP phone, to the VTO, and
Unlock Command	use the command to open the door remotely.
Door Contact	• NC: Normally closed.
Туре	• NO: Normally open.
Door Sensor Enable	Synchronize door sensor status to indoor monitors (VTHs).
F : A 1	If turned on, you can connect an alarm device to the port that is originally for
Fire Alarm	the door contact, but you cannot use the door contact function.
Lock	Non-remote methods, such as password or card, will unlock the lock you
LUCK	select.
IC Card Encrypt	Access cards issued by the VTO will be encrypted and unclonable.

Table 4-3	Local access	control	parameter	description
Tuble 15	Local access	control	purumeter	acscription

Step 3 Click Save.



4.3.2 RS-485

Select **Local Settings** > **Access Control Settings**, and then configure the parameters of the lock connected through the RS-485 port. See Table 4-3 for parameter description.

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

WEB SERVICE2.0	¢ Local Settings	Household Setting	Network	Search Log	English -	♣ ♠ ⊡-
Basic	RS-485					
Video & Audio	Interface Type	Lock 👻				_ 1
Access Control Settings \land	Unlock Responding Interval Unlock Period		Sec. Sec.			
Local	Second Unlock Command		360			
RS-485	Lock	Local 💿 Second Lock				- 1
Password Management					Refresh Default	
System				Save	Refresh Default	
Security						
Wiegand						
Onvif User						
Update						
Upload File						

4.3.3 Password Management

Add a username and password used to unlock the door.

Figure 4-5 Password management

WEB SERVICE2.0	☆Local Settings	Household Setting	() Network	Search Log English -
Basic	Password Management			
Video & Audio		Username	Password	Modify
Access Control Settings		Jack	•••••	✓ ×
Local				
RS-485				
Password Management				
System				
Security				
Onvif User				
Update				
Upload File	Add Clear			∺ ≼ 1/1 ≽ ⊮ Go to +

4.4 System

Configure time parameters, NTP server, and more. <u>Step 1</u> Select **Local Settings > System**.



Figure 4-6 System

Basic Date format Video & Audio Ime format Access Control Settings ^ Ime Zone Access Control Settings ^ Ime Zone System Time Jonn 0 OFF RS-485 DST ON 0 OFF Password Management Start Time Jan I The 1st Week Monday I oo : 00 System Security Maintenance Turegency I table Owif User	WEB SERVICE2.0	☆ Local Settings	Household Setting	ONetwork	Search Log	English -	≜ ♠ ⊡-
Video & Audio Time format 24 Hour NTP Server 200 1600.8 Access Control Settings Time Zone GMT+08:00 Port 123 System Time 01-12:2020 11: 49: 44 Syne with PC Interval 5 RS-485 OST ON OFF RS-485 OST Type Date Week Password Management Start Time Jan The 1st Week Monday 00: 00 System Start Time Jan The 1st Week Tuesday 00: 00 System Maintenance ruesday 00: 00 OT Security Maintenance ruesday 02: 00 Onvir User SHI Enable Dorit User Maintenance Start Time	Basic						
Access Control Settings Access Control Settings Local Dst ON OFF RS-485 Dst ON Start Time Jan The 1st Week Monday On: 00: 00 System Security Maintenance Update Update Save Research Distription Start Time Jan The 1st Week Maintenance Tuesday Onvir User Bave Research Distription Distription Research Distription Start Time Jan Research Start Time Jan The 1st Week Maintenance Tuesday Onvir User Bave Research Distription Start Time Jan Research Start Time		Date Format DD-MM-YYYY			NTP E	nable	
Access Control Settings Access Control Settings System line 0-1-2-2020 01 11 14 91 11 <t< td=""><td>Video & Audio</td><td>Time Format 24-Hour</td><td></td><td></td><td>NTP Server 200.160</td><td></td><td></td></t<>	Video & Audio	Time Format 24-Hour			NTP Server 200.160		
Local DST ON OFF RS-485 DST Type Date Week Password Management Start Time Jan ♥ The 1st Week Monday ♥ 00 0 00 End Time Jan ♥ The 1st Week Tuesday ♥ 00 0 00 Security Maintenance Tuesday ♥ 00 0 00 Viegand SSH ♥ Enable Emergency ♥ Enable Onvif User Maintenance Update Save	Access Control Settings	Time Zone GMT+08:00			Port 123		
DST ON OFF PS-485 DST Type Date Week Start Time Jan The 1st Week Monday 00 : 00 End Time Jan The 1st Week Security Maintenance Tuesday Wiegand SSH € Enable Emergency € Enable Onvif User Maintenance		System Time 01-12-2020	🖬 11 : 49 : 44 Sy	nc with PC	Interval 5	min.	
Password Management Start Time Jan * The 1st Week Monday * 00 : 00 System End Time Jan * The 1st Week Tuesday * 00 : 00 Security Maintenance Tuesday * 02 : 00 Wiegand SSH * Enable Onvif User Emergency * Enable Update Save Retresh Default	Local	DST ON	OFF				
Fastiviti Wainingement End Time Jan ▼ The 1st Week Tuesday ♥ 00 : 00 System Security Maintenance Tuesday ♥ 02 : 00 Wiegand SSH ♥ Enable Emergency ♥ Enable Onvif User Update Save	RS-485	DST Type 🔵 Date	Week				
System Security Maintenance Tuesday ♥ 02 : 00 Wiegand SSH ♥ Enable Emergency ♥ Enable Onvif User Update Savo Refresh Default	Password Management	Start Time 🛛 Jan 👻	The 1st Week Monday 👻	00 : 00			
Security Maintenance Tueaday • 02 : 00 Wiegand SSH ♥ Enable Emergency ♥ Enable Onvif User Update Save Refresh Default		End Time 🛛 Jan 🔍	The 1st Week Tuesday 👻	00 : 00			
Wiegand SSH I isolable Emergency I isolable Onvif User Update Save Refresh							
Emergency Senable Onvif User Maintenance Update Save Refresh Default	Security	Maintenance Tuesday	▼ 02 : 00				
Emergency S Enable Onvif User Update Save Refresh Default	Wingand	SSH 🔽 Enable					
Update Savo Refresh Default	Wieganu	Emergency 🔽 Enable					
Save Realized London	Onvif User	Maintenance					
Save Realized London	Undate						
Unload File	opuno				Save	Refresh D	efault
	Upload File						

<u>Step 2</u> Configure the parameters.

Table 4-4	System	parameter	description
-----------	--------	-----------	-------------

Parameter	Description	
Date Format	Select a format as needed.	
Time Format		
System Time	\triangle	
System mile	Changing system time might cause problems on video searching and information	
	publication. Turn off video recording and auto snapshot before changing it.	
Time Zone	Configure the time zone as needed.	
Sync with PC	Synchronize the VTO system time with your PC.	
DST	Daylight saving time. If it is applicable to your area, you need to enable it, and	
ונט	then configure DST type, start time and end time.	
DST Type	Select Date or Week as needed, and then configure the specific period.	
Start Time	Configure the start times and and times of DCT	
End Time	Configure the start time and end time of DST.	
NTP Enable	Enable NTP and enter the IP address of the NTP server, and then the VTO will	
NTP Server	syncronize time with the NTP server automatically.	
Port	NTP server port number.	
Interval	VTO time update cycle. 30 minutes at most.	
Maintenance	Define the time when the VTO will restrart automatically.	
SSH	You can connect debugging devices to the VTO through SSH protocol.	
221	We recommend turning it off, and turn on security mode and outbound service	
	information protection. See "4.5 Security". Otherwise, the VTO might be exposed	
	to security risks and data leakage.	
Emergency Maintenance	Enable it for fault analysis and repair.	



Parameter	Description
	This function will occupy 8088 and 8087 ports.

Step 3 Click Save.

4.5 Security

Configure functions that involve device security.

<u>Step 1</u> Select Local Settings > Security.

Figure 4-7 Security

WEB SERVICE2.0	¢ Local Settings	≣ Household Setting	ONetwork	Search Log	English -	🐥 🔶 🕞 -
Basic	Security					
Video & Audio	CG	I Enable				
Access Control Settings		bile Push Notifications				
Local		ssword Reset dio/Video Transmission Encryption				
RS-485		IVIF On				
Password Management		SP Over TLS tbound Service Information Protection				
System		ilticast/Broadcast Search				
Security	Authen	itication Mode 💿 Security Mode (Re	commended) Compatibl	le Mode		
Wiegand				Save	Refresh	Default
Onvif User						
Update						
Upload File						

Parameter	Description		
	Enable the use of CGI command.		
CGI Enable			
	We recommend turning it off. Otherwise, the VTO might be exposed to		
	security risks and data leakage.		
	Send information to the app on the smartphone.		
Mobile Push Notification			
Notification	We recommend turning it off if you do not need this function. Otherwise,		
	the VTO might be exposed to security risks and data leakage.		
Password Reset	If turned off, you will not be able to reset password.		
	Encrypt all data during voice or video call.		
Audio/Video	\wedge		
Transmission			
Encryption	We recommend turning it on. Otherwise, the VTO might be exposed to		
	security risks and data leakage.		
ONVIF On	Allow third-party to pull video stream of the VTO through the ONVIF		



Parameter	Description				
	protocol.				
	\triangle				
	We recommend turning it off. Otherwise, the VTO might be exposed to security risks and data leakage.				
	Output encrypted bit stream through RTSP.				
RTSP Over TSL	\triangle				
	We recommend turning it on. Otherwise, the VTO might be exposed to security risks and data leakage.				
	Protect your passwords.				
Outbound Service Information	\triangle				
Protection	We recommend turning it on. Otherwise, the VTO might be exposed to				
	security risks and data leakage.				
	Enable it and the VTO will be found by other devices.				
Multicast/Broadcast Search	\triangle				
Search	We recommend turning it off. Otherwise, the VTO might be exposed to				
	security risks and data leakage.				
	• Security Mode (recommended): Support logging in with Digest				
	authentication.				
Authentication	Compatible Mode: Use the old login method.				
Mode					
	We recommend the security mode. Compatible mode might expose the				
	VTO to security risks and data leakage.				

Step 3 Click Save.

4.6 Wiegand

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



Figure 4-8 Wiegand

WEB SERVICE2.0	☆ Local Settings	≣ Household Se	tting 💿 Network	k Search Log	English -	🌲 🕇 🕞 -
Basic	Wiegand					
Video & Audio	Transmission Mode	34bit Trans 🔍 👻				
Access Control Settings 🔷		1000				
Local				Save	Refresh	Default
RS-485						
Password Management						
System						
Security						
Onvif User						
Update						
Upload File						

4.7 Onvif User

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



If you delete an account, it cannot be undone.

<u>Step 1</u> Select Local Settings > Onvif User.

Step 2 Click Add.

Figure 4-9 Add an ONVIF user

Add				x
Username				
Password				
	Weak	Medium	Strong	
Confirm				
			Save	Cancel

<u>Step 3</u> Enter the information, and then click **Save**.

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



4.8 Upload File

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

<u>Step 1</u> Select Local Settings > Upload File.

<u>Step 2</u> Select an audio type, and then click **Browse** to select the audio file as needed.

Figure 4-10 Change the sound prompt

WEB SERVICE2.0	ঞ্চLocal Settings	Household Setting	(e) Network
Basic	Upload File		
Video & Audio	Audio Types Unlocked		
Access Control Settings 💙	Local Upload	B I files, and the file size cannot exceed 20 Kb	rowse Upload
System	No.		Audio Types
Security			
Onvif User			
Update			
Upload File			
			No data

Step 3 Click **Upload**.



5 Household Setting

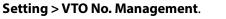
This chapter introduces how to add, modify, and delete VTO, VTH, VTS, and IPC, and how to send messages from the SIP server to VTOs and VTHs when the VTO works as the SIP server. If you are using other servers as the SIP server, see the corresponding manual for details. Ш

To configure SIP server parameters, see "6.3 SIP Server" for details.

5.1 VTO No. Management

You can add VTOs 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



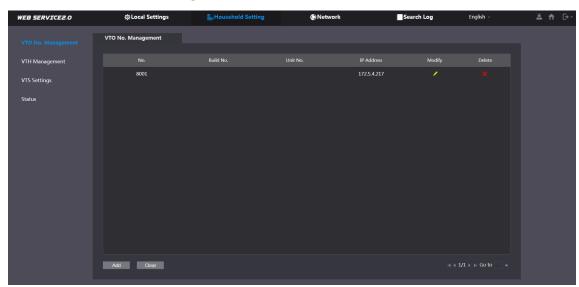


Figure 5-1 VTO management

Step 2 Click Add.



Figure 5-2 Add VTO

Add	(Int No.	×
No.		
Registration Password	····· ~~	
Build No.		
Unit No.		
IP Address	127.0.0.1	
Username		
Password		
	Save	Cancel

<u>Step 3</u> Configure the parameters.

\sim	~	_	~
п.	- 1		n.
н.	- 1		н.
н.	- 1		н.
L-	_	_	4

The SIP server must be added.

Parameter	Description		
No.	The VTO number you configured. See Table 4-1 for details.		
Registeration	Koop it default		
Password	Keep it default.		
Build No.	Available only when other convers work as the SID conver		
Unit No.	Available only when other servers work as the SIP server.		
IP Address	IP address of the VTO.		
Username	Wah interface login username and password of the VTO		
Password	Web interface login username and password of the VTO.		
Step 4 Click Save.			

Click 🔽 or X to modify or delete a VTO, or **Clear** to delete all added VTOs, but the one

that you have logged in to cannot be modified or deleted.

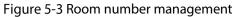
5.2 VTH Management

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.

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





	5			5		
WEB SERVICE2.0	众Local Settings	Household Settin		Network	Search Log	English -
VTO No. Management	VTH Management					
	Room No.	First Name	Last Name	Nick Name	Registration Mode	Modify
VTS Settings	9901#0				public	
Status	9901#1				public	2×
	9901#2				public	
	9901#3				public	× ×
	9901#4				public	
	9901#5				public	× ×
	9901#6				public	
	9901#7				public	× ×
	9901#8				public	
	9901#9				public	× ×
	Add Refresh Cle	3ar				



Figure 5-4 Add a room number

Add					×
First Name		Username	Card No.	Modify	
Last Name					
Nick Name					
Room No.					
Registration Mode	public 💌				
Registration Password					
Registration Password			No data		
				Issue Card	
				Save	Cancel
				Save	

<u>Step 3</u> Configure the parameters.

Parameter	Description	
First Name		
Last Name	Enter the information you need to differentiate each room.	
Nick Name		
Room No.	Enter a room number, and then configure the number on a VTH to connect	
noom no.	to connect it to the network.	
Registeration Type	Select public .	
Registeration	Koop it default	
Password	Keep it default.	
Stop A Click Sava		

Step 4 Click Save.



Click 🔽 or 📕 to modify or delete a room number.

5.2.2 Issuing Access Card

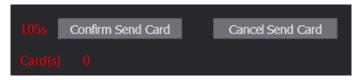
Issue an access card to unlock the door of a room.

Ш

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

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

Figure 5-5 Countdown notice



<u>Step 2</u> Swipe the card on the VTO.

Figure 5-6 Issue card

Issue Card		×
Card No.		
Room No.	201#0	
Username		
	Save	Cancel

<u>Step 3</u> Enter the username, click **Save**, and then click **Confirm Send Card**. Figure 5-7 Issued access card

Username	Card No.	Modify
mm	22.2	

Other Operations

- Click 🖬 to set it as the main card, and then the icon changes to 🖪. 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 changes to 🖪. The lost card cannot be used to open the door.
- Click do r do r control of the username or delete the card.

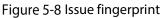


5.2.3 Issuing Fingerprint

Issue fingerprints to unlock the door of a room.

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

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



Add		×
Username		
Room No.	101	
Unlock Permission	🗹 Lock 1 🛛 🗹 Lock 2	
		Save Cancel

<u>Step 2</u> Enter a username, assign unlock permission as needed, and then click **Save**.<u>Step 3</u> Press your fingerprint on the 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.

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

WEB SERVICE2.0	ঞ্চLocal Settings	Household Setting	Network	Search Log	English -	≛ ≜ ⊡-
VTO No. Management	VTS Settings					
VTH Management			IP Address	Modify	Delete	
VTS Settings						
Status						
Status						
			No data			
	Add				1/1 ▶ ⊮ Go to →	

Figure 5-9 VTS management

Step 2 Click Add.



Figure 5-10 Add VTS

Add	5.11 <u>9</u> .11	×
VTS No.		
Registration Password	×-	
IP Address	127.0.0.1	
	Save	Cancel

<u>Step 3</u> Configure the parameters.

Parameter	Description		
VTS No.	ne number of the VTS.		
Registeration 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 VTO working as the SIP server, and then all the connected VTHs can monitor them.

 \square

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

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



Figure 5-11 IPC setting

VEB SERVICE2.0	ঞ্চ Local	Setting	≣ Househo	ld Setting	Netw	vork Setting	_ L	og Managemen	t	
VTO No. Management	IPC Setting	3								
Room No. Management	IPC Name	IP Addr.	Username	Port No	Protocal	Stream	Channel	Device Type	Modify	Delete
VTS Management			admin	554	Local	Main		IPC	1	
		0.0.0.0	admin	554	Local	Extra1		IPC	1	
		0.0.0.0	admin	554	Local	Extra1		IPC	1	
Status		0.0.0.0	admin	554	Local	Extra1		IPC	1	
		0.0.0.0	admin	554	Local	Extra1		IPC	1	
Publish Information 🗡		0.0.0.0	admin	554	Local	Extra1		IPC	1	
		0.0.0.0	admin	554	Local	Extra1		IPC	1	
		0.0.0.0	admin	554	Local	Extra1		IPC	1	
		0.0.0.0	admin	554	Local	Extra1		IPC	1	
		0.0.0.0	admin	554	Local	Extra1		IPC	1	
		0.0.0.0	admin	554	Local	Extra1		IPC	1	
		0.0.0.0	admin	554	Local	Extra1		IPC	1	
		0.0.0.0	admin	554	Local	Extra1		IPC	1	
		0.0.0.0	admin	554	Local	Extra1		IPC	1	
					Import Cor	nfig Exp	ort Config	Refresh		efault

Step 2 Click

Figure 5-12 Add IPC

Modify			×
1 - CSSA			
IPC Name			
IP Address	0.0.0.0		
Username	admin		
Password			
Port	554		
Protocol	Local		
Stream Type	Extra1	-	
Channel	1		
Device Type	IPC	-	
MediaEncrypt	🔵 on 💿 off		
		Save	Cancel

<u>Step 3</u> Configure the parameters.

Table 5-4 Add IPC configuration

Parameter	Description
IPC Name	Enter the name that identifies the IPC.
IP Address	IP address of the IPC.



Username	Web interface login ucorname and password of the device			
Password	Web interface login username and password of the device.			
Port	Keep it default.			
Protocol	Select Local or Onvif.			
Charles Trans	• Main: Better video quality but requires more bandwidth.			
Stream Type	• Extra1 : Smoother video with poorer quality, but requires less bandwidth.			
Channel	The number of the channels that a device supports.			
Device Type	Select the one as needed.			
MediaEncrypt	Select ON if the IPC to be added is encrypted.			

Step 4 Click Save.

Other Operations

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

5.5 Status

You can view the online status and IP addresses of all the connected devices.

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

Figure 5-13 Status

WEB SERVICE2.0	袋 Local Setting	Househo	ld Setting 🔘 Network	Setting Log Manage	ement
VTO No. Management	Status				
Room No. Management	Room No.	Status	IP:Port	Reg Time	Off Time
	201#0	Online		2018-10-09 02:01:58	
VTS Management	201#1	Online		2018-10-09 02:02:11	
IPC Setting		Online		2018-10-09 02:02:15	
Status		Online		2018-10-09 02:06:20	
Publish Information 💙					⊯ ∢ 1/1 ⊳ ⊮ Go to 🛛 ⇒

5.6 Publish Information

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

5.6.1 Send Info

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



Figure 5-14 Send information

WEB SERVICE2.0	햤 Local Setting	s ∎Hous	ehold Setting	(i) Network	Search Log	English -
VTO No. Management	Validity Period 200	0-01-16 🖬 23:59:59	o			
VTH Management	Send to		All devices			
VTS Settings	Contents					
Status Announcement						
History Info						Confirm Refresh

- <u>Step 2</u> Specify the **Validity Period** that the message will be valid.
- <u>Step 3</u> Enter the VTO number or VTH number, 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**.

WEB SERVICE2.0	✿ Local Setting	Household Setting	Network Setting	Log Management	2
VTO No. Management	IssueTime	Period of validity		Delete	
Room No. Management	2018-10-09 16:52:31	2018-10-09 16:54:00			
VTS Management	2018-10-09 16:52:31	2018-10-09 16:53:00			
IPC Setting	2018-10-09 03:15:38	2018-10-09 16:52:00			
Status					
Publish Information \land					
Send Info					
History Info					
				i∈i ⊲i 1/1 ⊳ i⊨i Go to	

Figure 5-15 History information



6 Network

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. <u>Step 1</u> Select **Network > Basic**.

		i iguic o i i			
WEB SERVICE2.0		¢Local Settings	Household Setting	Network	
	тс	P/IP			
UPnP	IP Address				
SIP Server	Subnet Mask Default Gateway				
Firewall	MAC Address				
	Preferred DNS Alternate DNS				
	P	ort			
	Port	80		TCP Port	37777
	HTTPS Port	443	Enable	UDP Port	37778
		Compatible with TLSv1.	1 and earlier versions.		
	Certificate Manag	ement Create Server Certific Details	ate Download Root CERT Delete		
		2P			
	Status			QR Code	EXECUTE
					255
					69632

Figure 6-1 TCP/IP and port

Step 2Configure the parameters, and then click Save.The VTO will restart, and you need to modify the IP address of your PC to the same networksegment as the VTO to log in again.

6.1.2 Port

Parameter	Description
Port	80 by default. If already used, choose any number from 1025 to 65535 as
FUIL	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 <i>https://VTO IP address:HTTPS Port</i> to log in to the VTO.
TCP/UDP Port	Used for accessing the VTO with devices in other networks. See "6.2 UPnP" for details.
Create Server Certificate	The unique digital identification of VTO for the SSL protocol. For first time use or after changing the IP address of the VTO, you need to go through this process. If you delete the certificate that has been created, it cannot be undone.
Download Root CERT	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.

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.

Preparation

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

6.2.1 Enabling UPnP Services

- <u>Step 1</u> Select **Network > UPnP**.
- <u>Step 2</u> Enable the services listed as needed.
- Step 3 Select Enable.
- Step 4 Click Save.



6.2.2 Adding UPnP Services

- <u>Step 1</u> Select **Network > UPnP**.
- Step 2 Click Add.
- <u>Step 3</u> Configure the parameters as needed.

Figure 6-2 Add a UPnP service

Add	2 mail: d	x
(Art)		
	ON OFF	
Service Name		
Service Type		
Protocol	ТСР 👻	
	TCP	
Internal Port		
External Port		
	Save	Cancel
	Save	Cancer

Table 6-2 Parameter description

Parameter	Description				
Service Name					
Service Type	Enter the information as needed.				
Protocol	Select TCP or UDP as needed.				
Internal Port	Use port number from 1024 through 5000.				
External Port	• Do not use port number 1–1023 to avoid conflict.				
	• If you need to configure this function for multiple devices, make sure				
	that the ports are not the same.				
	• The port number you use must 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 connected VTOs and VTHs to call each other. You can use a VTO or other servers as the SIP server.

<u>Step 1</u> Select **Network > SIP Server**.



Figure 6-3 SIP Server

WEB SERVICE2.0	袋 Local Settings	Household Setting	Network	Search Log	English - 💄 🕇	[→ -
Basic						
	SIP Server 🗹 En	able				
UPnP	Server Type VTO					
	IP Address					
	Port 5080					
Firewall	Username 800					
	Password					
	SIP Domain VDF					
	SIP Server Username adm					
	SIP Server Password					
				Save	Refresh Default	

<u>Step 2</u> 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 "5 Household Setting".

Ш

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

If another VTO works as the SIP server:
 Do not enable SIP server. Set Server Type to VTO, configure the parameters, and then click Save.

Parameter	Description		
IP Addr.	VTO IP address.		
Port	• 5060 by default when VTO work as SIP server.		
	• 5080 by default when the platform works as SIP server.		
Username	- Keep it default.		
Password			
SIP Domain	VDP.		
SIP Server Username	 Web interface login username and password of the VTO. 		
SIP Server Password			

Table 6-3 SIP server configuration

• If other servers work as the SIP server:

Select the **Server Type** as needed, and then see the corresponding manual for details.

6.4 Firewall

You can enable different firewall types to control network access to the VTO. <u>Step 1</u> Select **Network > Firewall**.



Figure 6-4 Firewall

WEB SERVICE2.0	☆ Local Settings	Household Setting	Network	Search Log	English ~	🐥 🔶 🕞
Basic	Firewall					
UPnP	Type Network Access					
SIP Server	Enable Default Refresh	Confirm				
	Delault Nellesi	Committee				

<u>Step 2</u> Select one or more firewall types, and then enable them.

<u>Step 3</u> Configure the parameters.

Table 6-4 Firewa	Ill type description
	in type description

Туре	Description		
	Select either Allowlist or Blocklist, and then add an IP address or segment		
Network Access	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**. You can search for different logs, and export them to your PC as needed.

À

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 enabling 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.

ENABLING A SAFER SOCIETY AND SMARTER LIVING