

Digital VTH (Version 4.41) Quick Start Guide

V1.0.0




Foreword

General

This document mainly introduces structure, installation process, debugging and verification process of digital VTH.

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
V1.0.0	First release	April 2020

About the Manual

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

- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

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

Operating Requirement

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

Power Requirement

- The product shall use electric wires (power wires) recommended by this area, which shall be used 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, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.
- Do not cut off power supply during device upgrade. Power supply can be cut off only after the device has completed upgrade and has rebooted.

Table of Contents









Foreword	I
Important Safeguards and Warnings	III
1 Overview.....	1
1.1 Front Panel.....	1
1.2 Rear Panel Port.....	2
1.2.1 VTH5221 Series /VTH5241 Series.....	2
1.2.2 VTH5221E-H/VTH5221EW-H	2
1.2.3 VTH15 Series Type A/Type B/Type CH.....	2
1.2.4 VTH5222CH/VTH5222CHW-2	3
1.2.5 VTH1660CH	4
1.2.6 VTH2221A/VTH2221A-S2.....	4
1.2.7 VTH2421F Series	4
2 Installation and Debugging	5
2.1 Installation	5
2.1.1 Installing with Installation Bracket	5
2.1.2 Installing with 86 Box.....	5
2.1.3 Installing with Desktop Bracket.....	6
2.2 Configuration.....	7
2.2.1 VTO Settings.....	7
2.2.2 VTH Settings.....	13
2.3 Function Verification.....	23
2.3.1 Calling VTHs from VTOs	23
2.3.2 Watching Monitoring Videos at VTHs.....	23
Appendix 1 Cybersecurity Recommendations	25

1 Overview

1.1 Front Panel

Different models of devices might have different front panel dimensions and key types, but keys or indicators with the same silkscreen or icon have the same function. See Table 1-1.

Table 1-1 Front panel button

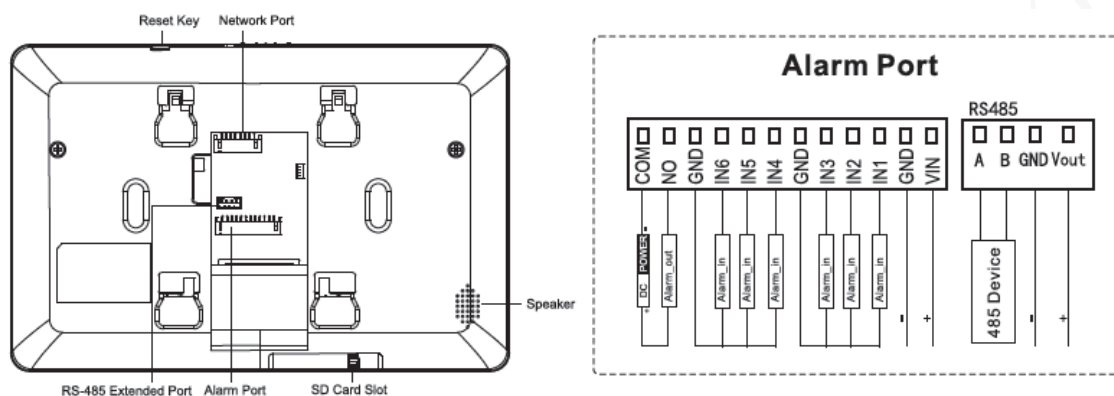
Icon or Silkscreen	Name	Description
	SOS	Tap this key to call the call center in case of emergency.
	Menu	Tap this key to return to main menu.
	Call	<ul style="list-style-type: none"> Press this key to answer the call. During talk, press this key to hang up. During monitoring, press this key to speak to unit VTO, villa VTO and fence station. During speaking, press this key to exit speaking.
	Monitor	<ul style="list-style-type: none"> In standby mode, press this key to monitor the main VTO. During monitoring, press this key to exit monitoring.
	Unlock	When there is an incoming call from a VTO, or during the call between a VTO and a VTH, or when you are watching real-time videos by a VTO, press this key, and then you can unlock the door beside the VTO.
	Message indicator	If this indicator is on, it means that there are unread messages.
	Power indicator	If this indicator is green, it means that normal power supply.
Network	Network indicator	<ul style="list-style-type: none"> If this indicator is on, it means that communication with VTO is normal. If this indicator is off, it means that communication with VTO is abnormal.
DND	DND indicator	<p>If this indicator is green, it means that DND function is enabled.</p>  <p>For DND settings, scan QR code on the front cover, and refer to the user's manual.</p>

1.2 Rear Panel Port

1.2.1 VTH5221 Series /VTH5241 Series

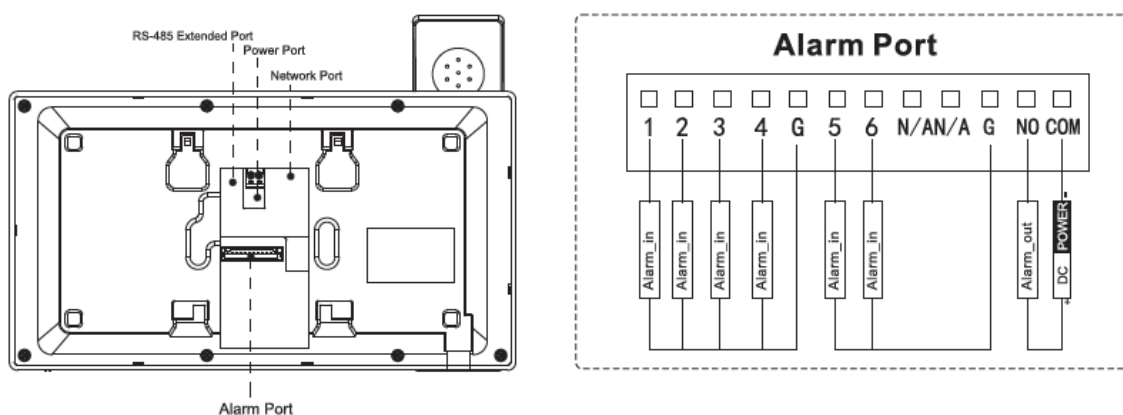
VTH5221 series and VTH5241 series have different port positions at the rear panel, but the same port provides the same function. Taking VTH5221 as an example, specific functions of ports are introduced. See Figure 1-1.

Figure 1-1 VTH5221



1.2.2 VTH5221E-H/VTH5221EW-H

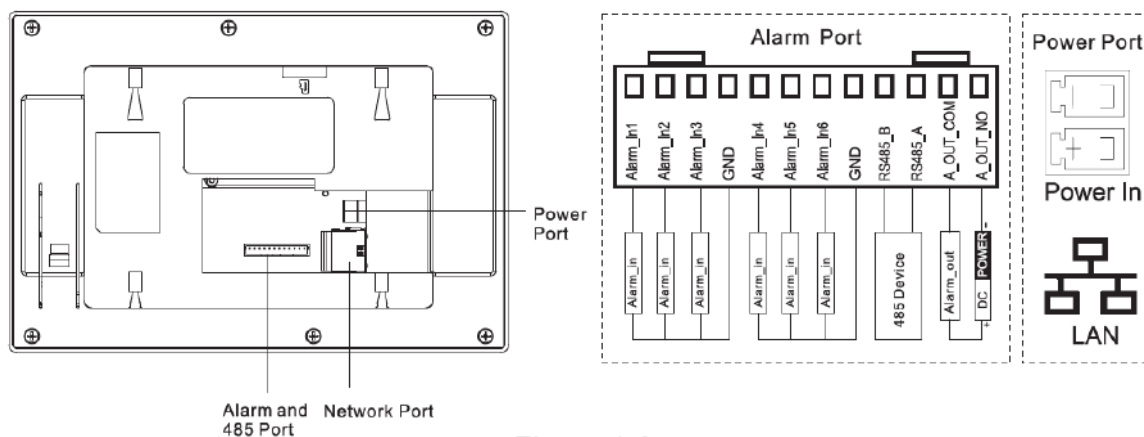
Figure 1-2 VTH5221E-H/VTH5221EW-H



1.2.3 VTH15 Series Type A/Type B/Type CH

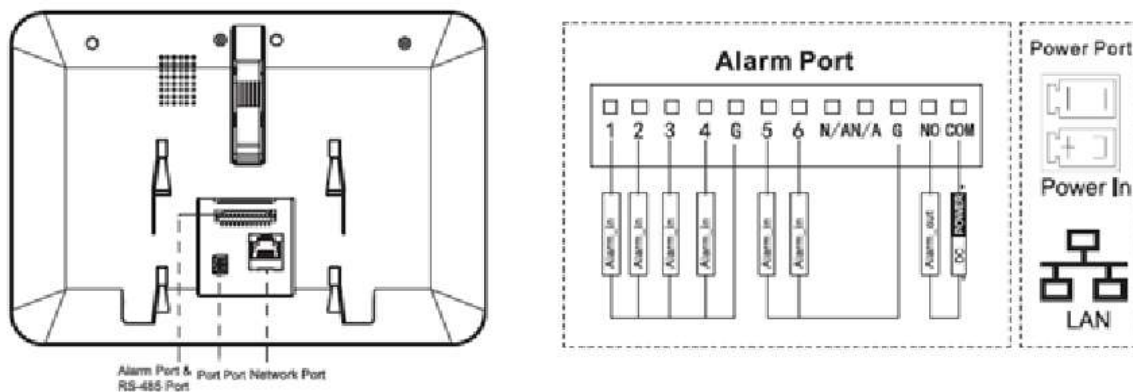
In VTH15 series, different types of digital VTH have different port positions, but the same port provides the same function. Taking VTH1550CH as an example, specific functions of ports are introduced. See Figure 1-3.

Figure 1-3 VTH1550CH



In VTH type A/type B series, different types of digital VTH have different port positions, but the same port provides the same function. Taking VTH1560B as an example, specific functions of ports are introduced. See Figure 1-4.

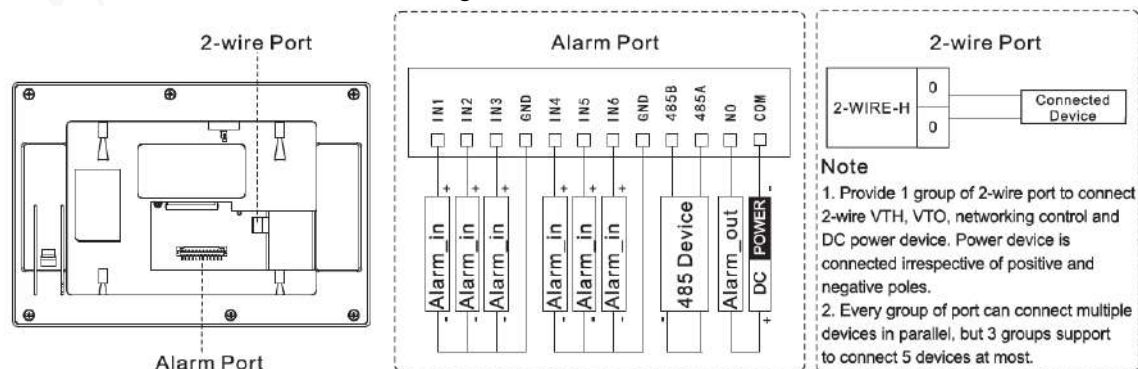
Figure 1-4 VTH1560B



1.2.4 VTH5222CH/VTH5222CHW-2

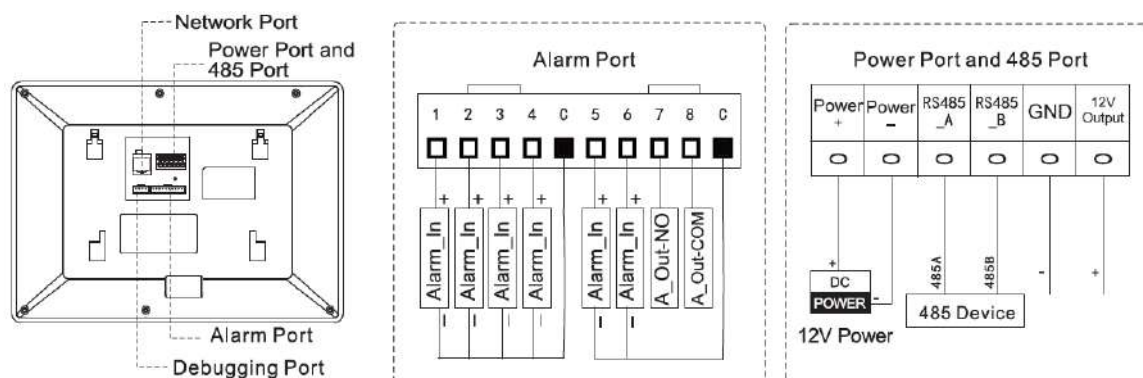
Except different numbers of 2-wire port, VTH5222CH and VTH5222CHW-2 are the same in other aspects. VTH5222CH has 1 group of 2-wire port, while VTH5222CHW-2 has 3 groups of 2-wire port. See Figure 1-5.

Figure 1-5 VTH5222CH



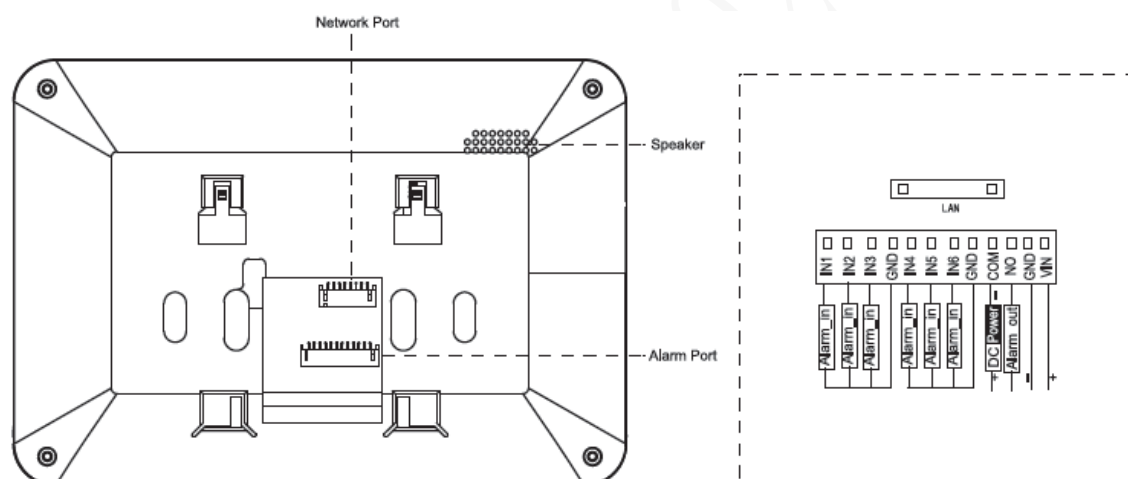
1.2.5 VTH1660CH

Figure 1-6 VTH1660CH



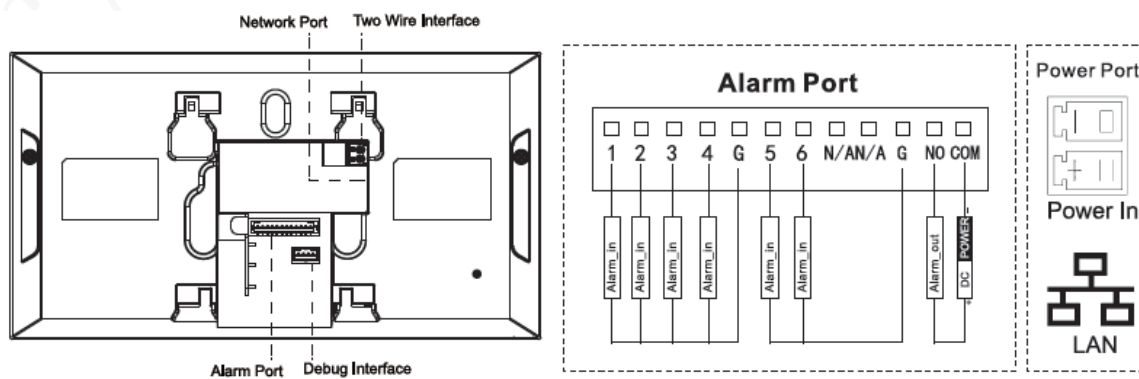
1.2.6 VTH2221A/VTH2221A-S2

Figure 1-7 VTH2221A/VTH2221A-S2



1.2.7 VTH2421F Series

Figure 1-8 VTH2421FB/VTH2421FS



2 Installation and Debugging

2.1 Installation



- Do not install VTH in environment with condensation, high temperature, stained, dusty, chemically corrosive and direct sunshine environment.
- In case of abnormality after power on, pull out network cable and cut off power supply at once. Power on after troubleshooting.
- Engineering installation and debugging shall be done by professional teams. Do not dismantle or repair arbitrarily in case of device failure. Contact after-sales department.
- It is suggested that installation height of device central point shall be 1.4cm–1.6cm above the ground.

2.1.1 Installing with Installation Bracket

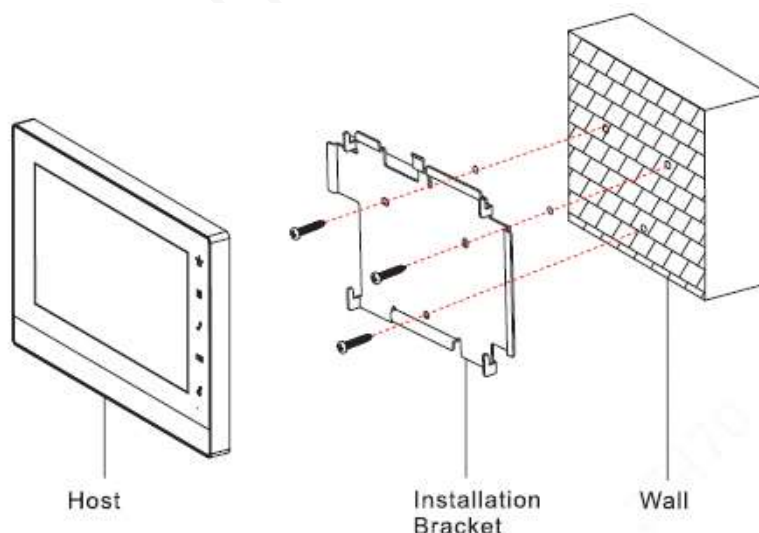
You can install the device with a bracket on a wall, which is suitable for all types of devices. Here VTH1550CH is taken as an example.

Step 1 Drill holes in the wall according to hole positions of the bracket.

Step 2 Fix installation bracket on the wall with screws.

Step 3 Hang the VTH on the installation bracket.

Figure 2-1 Installing with installation bracket



2.1.2 Installing with 86 Box

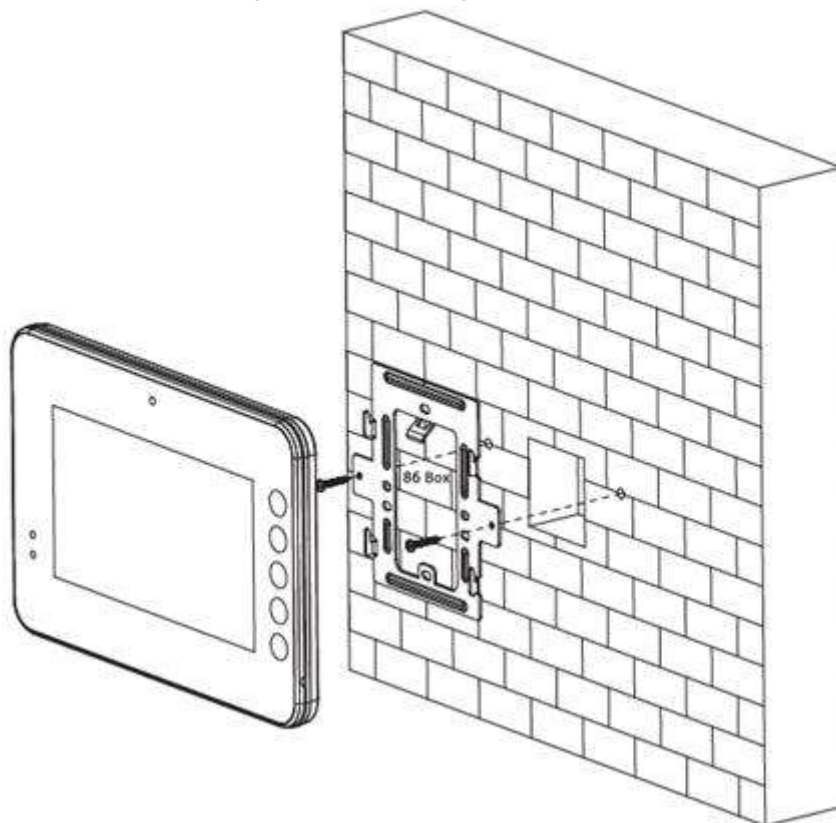
Install the device with 86 box, which is suitable for all types of devices. Take “VTH1560B/BW” for example.

Step 1 Embed 86 box into a wall at a proper height.

Step 2 Fix installation bracket on the 86 box with screws.

Step 3 Hang the VTH on the installation bracket.

Figure 2-2 Installing with 86 box



2.1.3 Installing with Desktop Bracket

Install the device with bracket on the desktop, which only applies to handset VTH. Take "VTH5221E-H" for example.

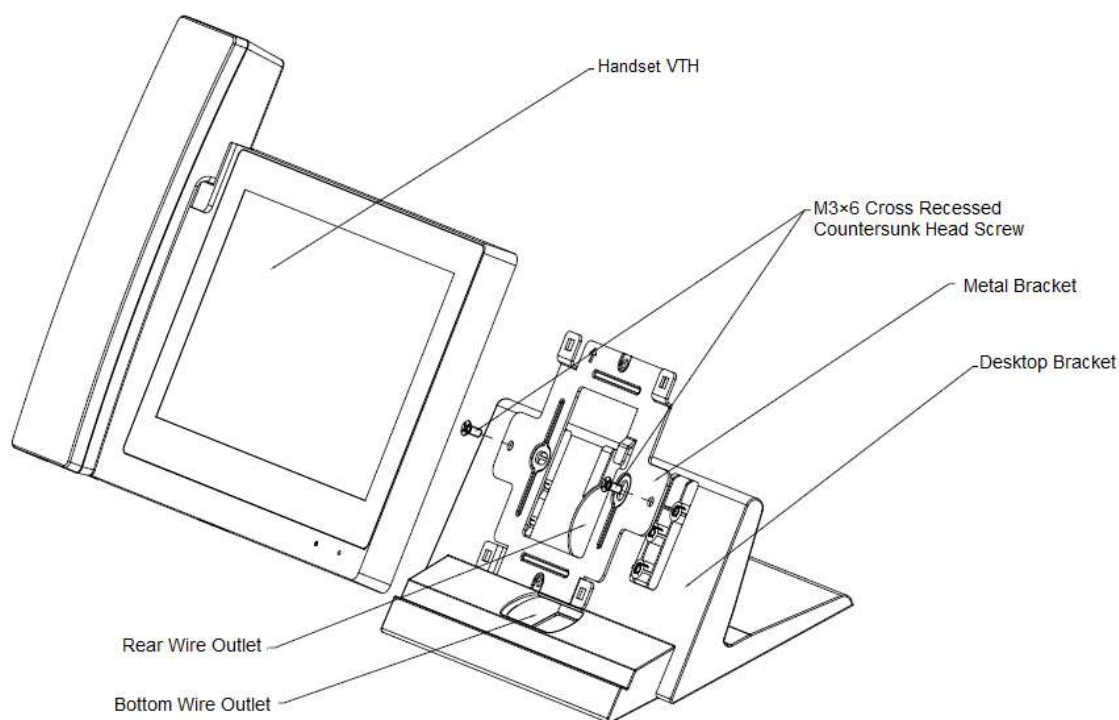
Step 1 With two M3×6 cross recessed countersunk head screws, tighten the metal bracket on the top two nuts of desktop bracket.

Step 2 Connect cables (see "1.2.2 VTH5221E-H/VTH5221EW-H").

Step 3 Thread the cable through the rear cable outlet or bottom cable outlet.

Step 4 Hang the VTH on the metal bracket.

Figure 2-3 Installing with desktop bracket



2.2 Configuration



Before configuration, check whether the following work has been completed or not.

- Check whether there is short circuit or open circuit. Power on the device only after the circuit is normal.
- IP addresses and No. of every VTO and VTH have been planned.
- Scan QR code on the cover for details.

Set VTO info and VTH info at web interface of every VTO, set VTH info, network info and VTO info on every VTH so that video and voice communication can be realized.

2.2.1 VTO Settings

VTHs and VTOs are always used together so you need to configure VTO parameters in advance to ensure the communication between VTHs and VTOs.

2.2.1.1 Initialization

Before using the VTO, initialize the device and modify the login password.



Make sure that default IP addresses of PC and VTO are in the same network segment. Default IP address of VTO is 192.168.1.110.

Step 1 Power on the device.

Step 2 Enter default IP address of VTO at the address bar of PC browser.

Figure 2-4 Device initialization

Device Init

1 — 2 — 3
One Two Three

Username admin

Password

Low Middle High

Confirm Password

Next

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

Step 4 Enter an email address.



This email address is used to reset the password.

Step 5 Enter default address in the browser to login web interface.



Default username is admin. Password is the one set during initialization.

2.2.1.2 Network Setting

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

Figure 2-5 Network setting

WEB SERVICE 2.0 Local Setting Household Setting **Network Setting** Log Management

Basic

FTP

SIP Server

Active Reg.

IP Permissions

TCP/IP

IP Addr.

MAC Addr.

Subnet Mask 255.255.0.0

Gateway

Preferred DNS 8.8.8.8

Alternate DNS 8.8.8.8

Step 2 Enter the planned IP Address, subnet mask, and gateway.

Step 3 Click **OK**.

After modification is completed, VTO reboots automatically. There are two occasions:

- If PC is in the planned network segment, web interface will go to a new IP login interface automatically.
- If PC is not in the planned network segment, the log in will fail. Modify PC IP to make PC IP is in the planned network segment and login web interface again.

2.2.1.3 Selecting SIP Servers

The Session Initiation Protocol (SIP) is used for signaling and controlling multimedia communication sessions in applications of voice and video calls. A SIP server is an application provides information or direction to a user agent.

- When this VTO or another VTO works as SIP server, select **VTO** from the **Server Type** drop-down list. It applies to a scenario where there is only one building.
- When the platform (Express/DSS) works as SIP server, select **Express/DSS** from the **Server Type** drop-down list. It applies to a scenario where there are multiple buildings or multiple units.

Step 1 Log in the web page.

Step 2 On the homepage, select **Local Setting > Basic**.

Figure 2-6 Device properties

The screenshot shows the 'WEB SERVICE 2.0' interface with the 'Local Setting' tab selected. Under the 'Basic' sub-tab, the 'Device Properties' section is active. It contains the following fields:

- Device Type:** Unit Door Station (dropdown)
- System Type:** TCP/IP (dropdown)
- Centre Call No.:** 888888 (text field)
- Building No.:** 0 (text field)
- Unit No.:** UNIT1 (text field with a blue checkmark icon)
- VTO No.:** 80001 (text field)

- 1) Select **TCP/IP** from the **System Type** drop-down list.



Default system type is analogue system and shall be changed to TCP/IP.

Otherwise, it will fail to connect VTH.

- 2) Click **OK** to save the settings.
- 3) Reboot the device manually, or wait for auto reboot to make the settings effective.

Step 3 Log in to web interface again.

Step 4 Select **Network Setting > SIP Server**.

Figure 2-7 SIP server (1)

The screenshot shows the 'WEB SERVICE 2.0' interface with the 'Network Setting' tab selected. Under the 'SIP Server' sub-tab, the settings are as follows:

- SIP Server:** Enabled (checkbox)
- Server Type:** VTO (dropdown)
- IP Addr.:** (empty text field)
- Port:** 5060 (text field)
- Username:** UNIT1@80001 (text field)
- Password:** (empty text field)
- SIP Domain:** (empty text field)
- SIP Server Username:** 80001 (text field)
- SIP Server Password:** (empty text field)

A warning message at the bottom reads: "Warning! The device needs reboot after modifying the SIP server settings." Buttons for 'Save', 'Refresh', and 'Default' are at the bottom right.

Step 5 Select a SIP server.

VTO as SIP server

Step 1 Select **Enable** behind **SIP Server**.

Step 2 Select **VTO** from the **Server Type** drop-down list

Step 3 Configure parameters (see Table 2-1 for details).

Step 4 Click **Save**.

The VTO will reboot automatically.

Platform (Express/DSS) as a SIP server

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

Figure 2-8 SIP server (2)

The screenshot shows the 'SIP Server' configuration page in the WEB SERVICE2.0 interface. The left sidebar contains navigation links: Basic, FTP, SIP Server (highlighted), Active Reg., and IP Permissions. The main content area is titled 'SIP Server' and includes the following fields:

- SIP Server:** A toggle switch set to 'Enable'.
- Server Type:** A dropdown menu set to 'Express/DSS'.
- IP Addr.:** A text input field.
- Port:** A text input field set to '5060'.
- Username:** A text input field set to 'UNIT1#0001'.
- Password:** A password input field.
- SIP Domain:** A text input field.
- SIP Server Username:** A text input field set to 'admin'.
- SIP Server Password:** A password input field.
- Alternate IP Addr.:** A text input field.
- Alternate Username:** A text input field set to 'admin'.
- Alternate Password:** A password input field.
- Alternate VTS IP Addr.:** A text input field.
- Alternate Server:** A toggle switch set to 'Enable'.

At the bottom of the form, there is a red warning message: 'Warning! The device needs reboot after modifying the SIP server settings.' Below the warning are three buttons: 'Save', 'Refresh', and 'Default'.

Step 2 Select **Express/DSS** from the **Server Type** drop-down list.

Step 3 Set parameters according to Table 2-1.

Table 2-1 SIP server parameter description

Parameter	Description
IP Address	IP address of SIP server.
Port	<ul style="list-style-type: none"> It is 5060 by default when another VTO works as SIP server. It is 5080 by default when the platform works as SIP server.
Username/Password	Use default value.
SIP Domain	<ul style="list-style-type: none"> It shall be VDP when another VTO works as SIP server. It can be null or keep default value when the platform works as SIP server.
Login Username/ Password	Username and password to login SIP server.
Alternate IP Addr.	IP address of the alternate server.
Alternate Username	Username and password for logging in the alternate server.
Alternate Password	
Alternate VTS IP Addr.	IP address of the alternate VTS.
Alternate Server	After entering alternate IP address, username, password, and VTS IP address, you need to select the Enable checkbox to enable the alternate server.

Step 4 Click **OK** to save the configuration.

The VTO will reboot automatically.



When the platform works as SIP server, if it is necessary to set Building No. and Building Unit No., enable **Support Building** and **Support Unit** first.

2.2.1.4 Household Setting

You need to set VTO, No, room No for VTOs, because when you call VTHs from VTOs, VTH No. (same as room No.) is needed.

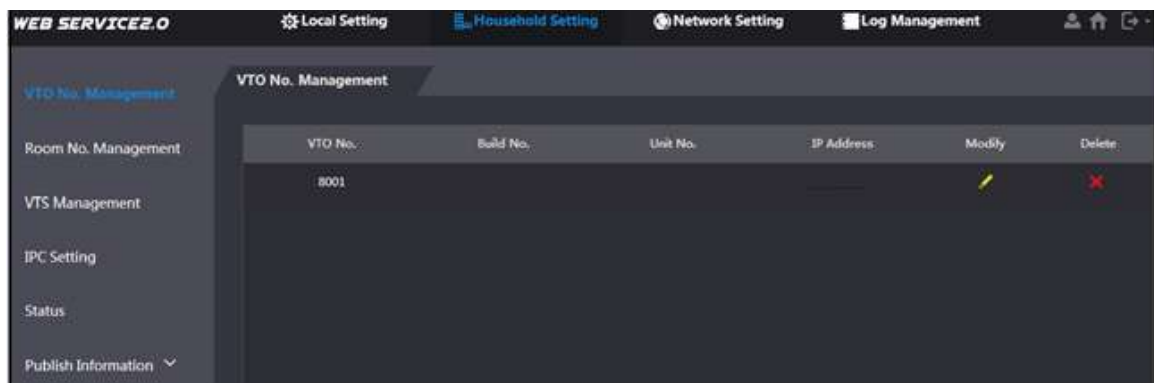
VTO No. Management

Step 1 (Optional) Log in to web interface again.

Step 2 Select **Household Setting > VTO No. Management**.

The **VTO No. Management** is displayed. See Figure 2-9.

Figure 2-9 VTO No. management



Step 3 Click **Add**, and then set VTO parameters.

Table 2-2 VTO parameter

Parameter	Description
VTO No.	VTO number.
Register Password	Signaling interactive use in SIP system. Adopt default value.
Build No.	Number of the building where VTO is located.
Unit No.	Number of the unit where VTO is located.
IP Address	IP address of VTO.
Username/Password	Username and password to log in to web interface of this VTO.

Step 4 Click **OK** to save the configurations.

Step 5 Repeat this step to add other VTOs in the group.

Room No. Management

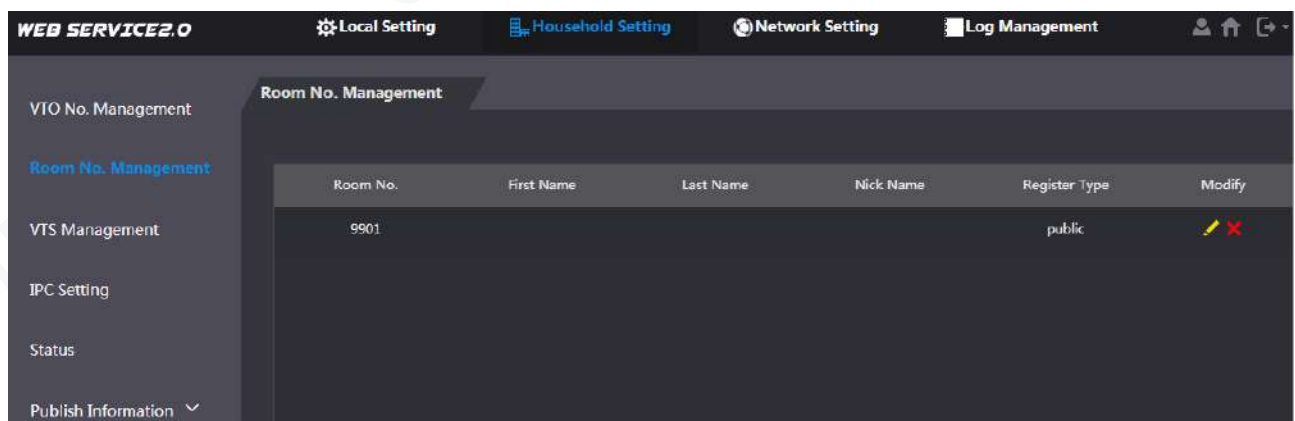
Step 1 (Optional) Select **Household Setting > Room No. Management**.

Room No. Management interface is displayed. See Figure 2-10.



When there are master VTH and extension, both shall be added.


Figure 2-10 Room No. management



Step 2 Click the yellow pencil to set VTH parameters.

Table 2-3 Room No. parameters

Parameter	Description
Family Name	Set VTH username and nickname to tell one VTH from another.
First Name	

Parameter	Description
Nick Name	
Room No.	<p>Set VTH room number.</p>  <ul style="list-style-type: none"> VTH room number consists of 1–6 numbers, which may include number and “#”. It should be the same as room number configured at VTH. When there are master VTH and extensions, to realize group call function, master VTH short No. shall end with “#0”, whereas extension VTH short no. shall end with #1, #2 and #3. For example, if master VTH is 101#0, extensions will be 101#1, 101#2...
Register Type	Signaling interactive use in SIP system. Adopt default value.
Register Password	

Step 3 Repeat these steps to add more VTHs in the group.

2.2.1.5 Adding VTH and VTO

You need to add other VTHs and VTOs to the VTH so that voice calls and video calls can be made. For details, see the user's manual.

2.2.2 VTH Settings

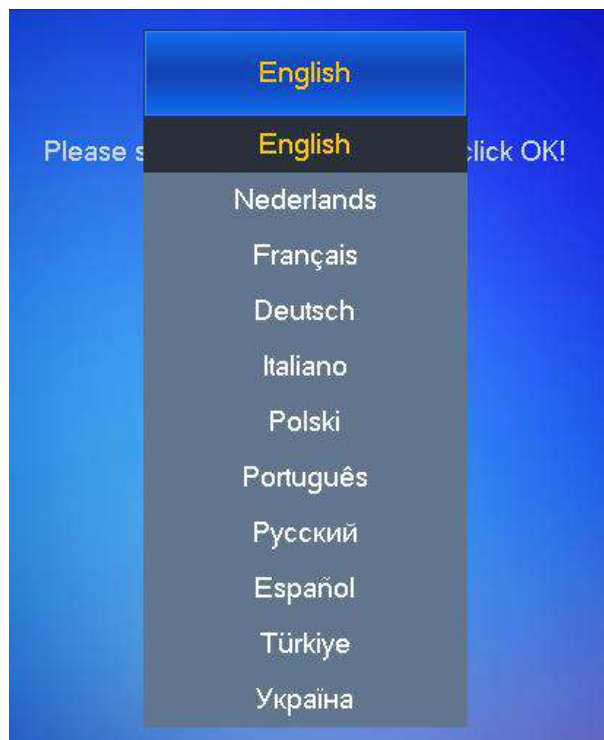
When the VTH is used for the first time, you need to select a language that you prefer, initialize the VTH to get a password to enter project setting interface and an email to reset your password. In addition, you need to configure parameters for all door stations (VTO) and VTH that are found on the VTH you are operating.

2.2.2.1 Quick Configuration for VTH (For Villa)

Step 1 Power on the device.

The language selection interface is displayed.

Figure 2-11 Select a language

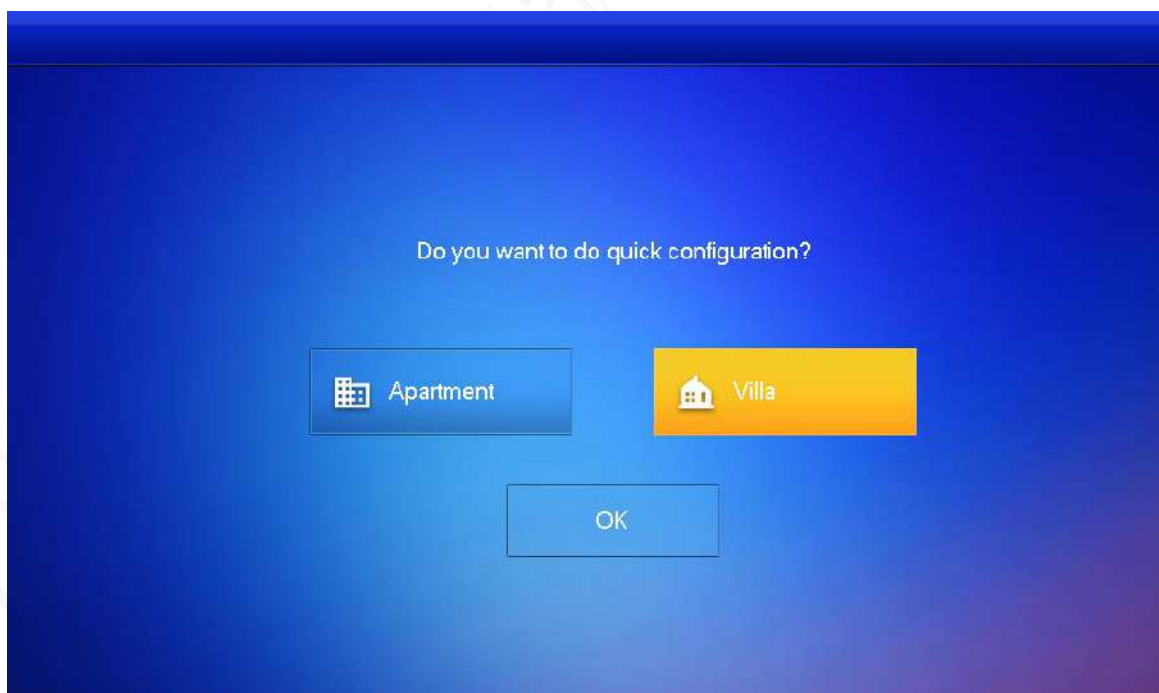


Step 2 Select a language that you prefer.

Step 3 Tap **OK**.

Welcome is displayed, and then the message **Do you want to do quick configuration?** appears.

Figure 2-12 Select apartment or villa



- Apartment: Select **Apartment** when the door stations and indoor monitors are installed in apartments. Quick configuration is not available when you select apartment.
- Villa: Select **Villa** when the door stations and indoor monitors are installed in villas. Quick configuration is available when you select villa.

Step 1 Select **Villa**.

Step 2 Tap **OK**.

The **Set local password** interface is displayed.

Figure 2-13 Set local password

STEP1/3 Set local password

Password 6 digits password

Confirm Pwd 6 digits password

Email This email is used to reset the password

OK

Step 3 Enter password, confirm password, and email for the VTH you are to initialize.

Step 4 Tap **OK**.

Figure 2-14 Set another device password

STEP2/3 Set another device password

Device Type	SN	MAC	IP	Status	Operation
VTO	4G017E1YAZ37516			Initialized	Initialize
VTO	3E04030YAZ00018			Initialized	Initialize
VTH	3c:ef:8c:0b:4d:27			Initialized	Initialize
VTH	PZZ4LN058W00004			Initialized	Initialize
VTO	ASDFGZXCVBQWERT			Uninitialized	Initialize

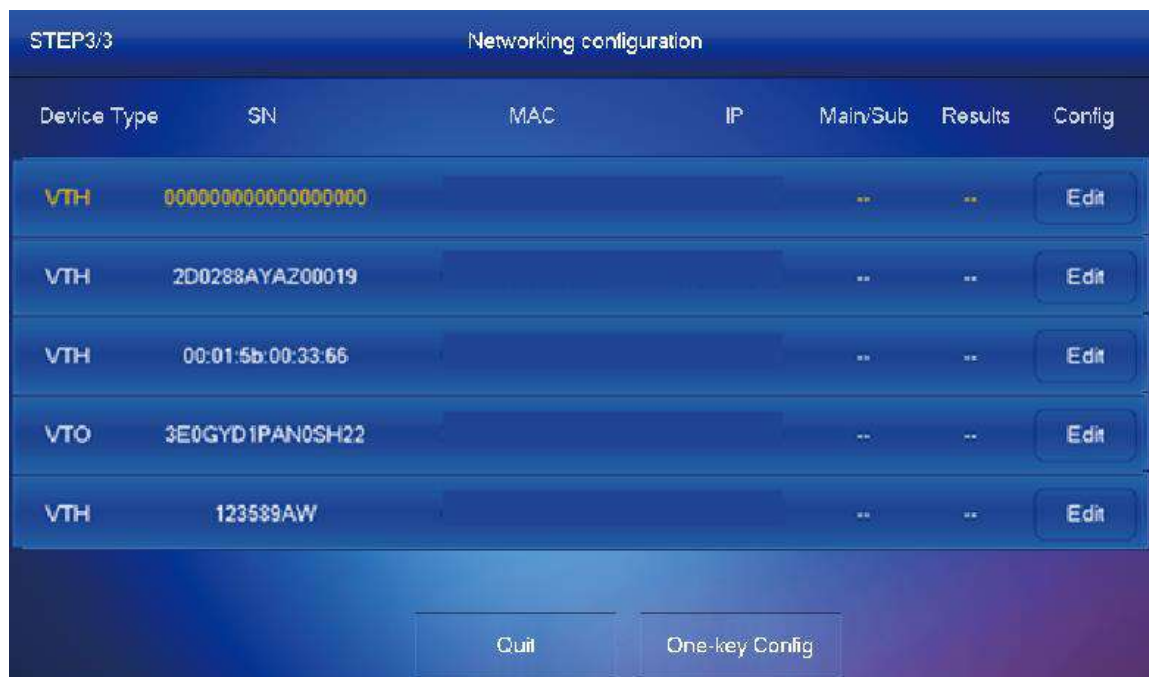
Refresh Next

< >

Step 5 Tap **Refresh**, and then tap **Next**.

The **Networking configuration** interface is displayed.

Figure 2-15 Networking configuration



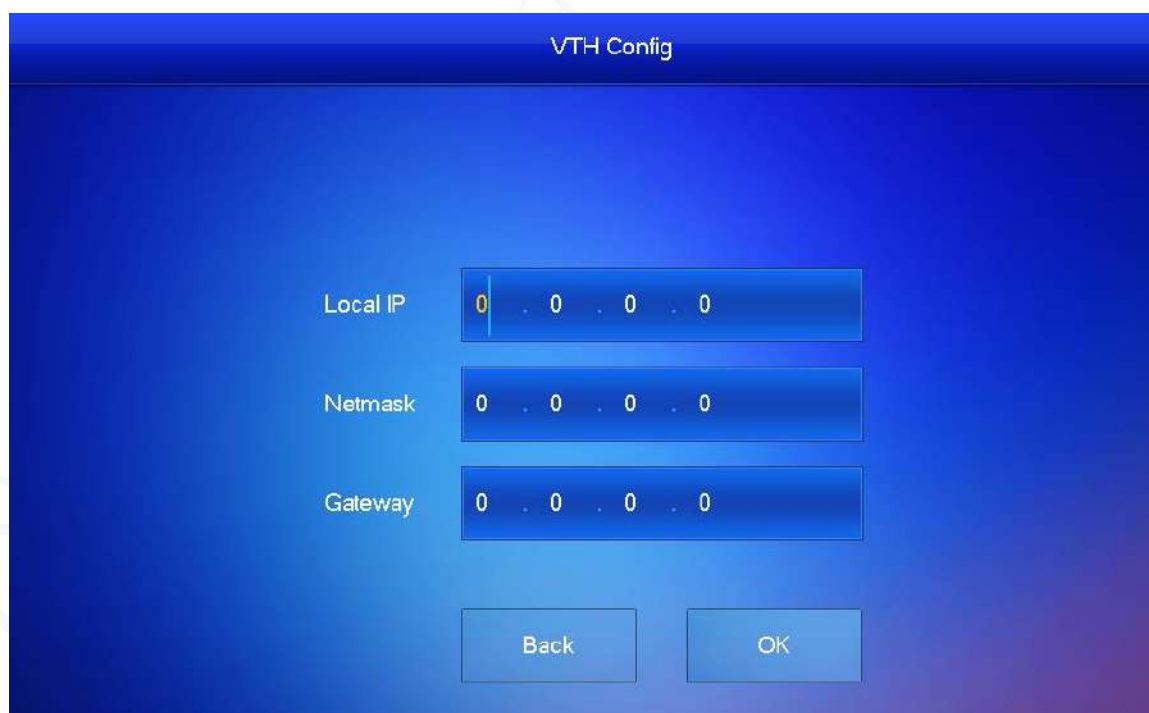
Step 6 Tap **Edit** behind each device to do configurations.

- Configure VTH.

1) Select a VTH.

The **VTH Config** interface is displayed.

Figure 2-16 VTH config



2) Enter local IP, Network, and gateway.

3) Tap **OK**.

The VTH configuration is completed.

- Configure Main VTO and Sub VTO. There must be only one main VTO and one or more sub VTOs.



If there are no sub VTOs, then you do not need to do sub VTO configurations.

- 1) Select a VTO.

The **VTO Config** interface is displayed. See Figure 2-17.

Figure 2-17 VTO config

- 2) Select **Main** or **Sub**.

Enter local IP, Network, gateway; select video standard, date format, time format; set date and time.

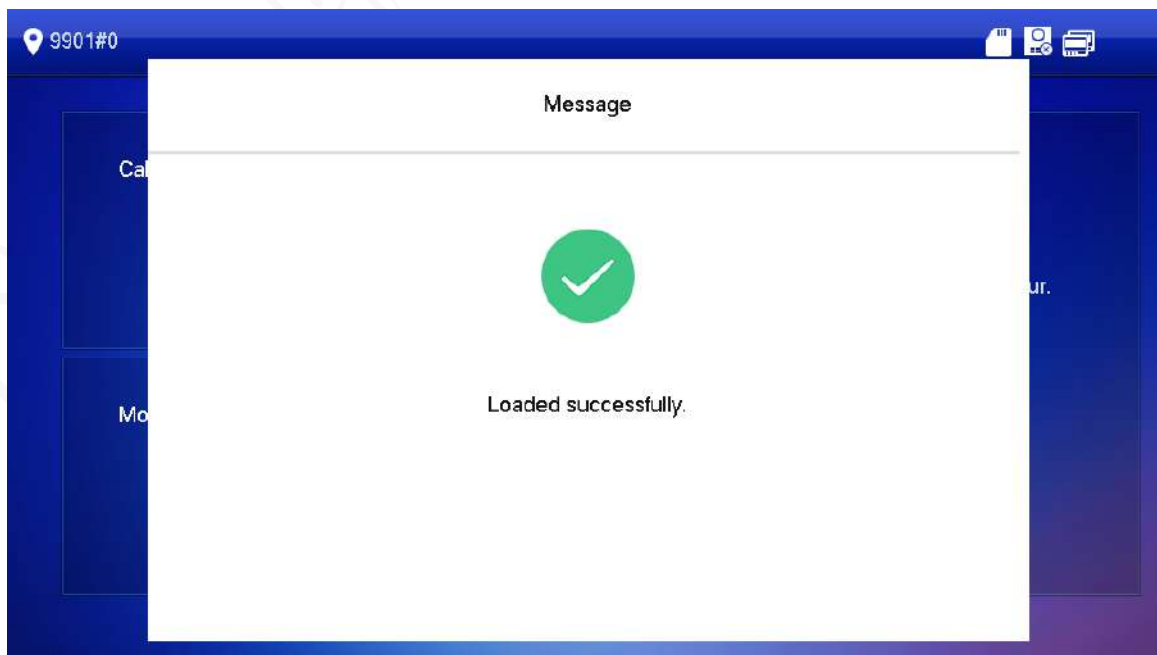
- 3) Tap **OK**.

The **Networking configuration** interface (Figure 2-15) is displayed.

- 4) Tap **One-key Config**.

The VTO configuration will be completed in a few seconds.

Figure 2-18 Making the configuration effective



2.2.2.2 Normal Configuration for VTH (For Apartment)

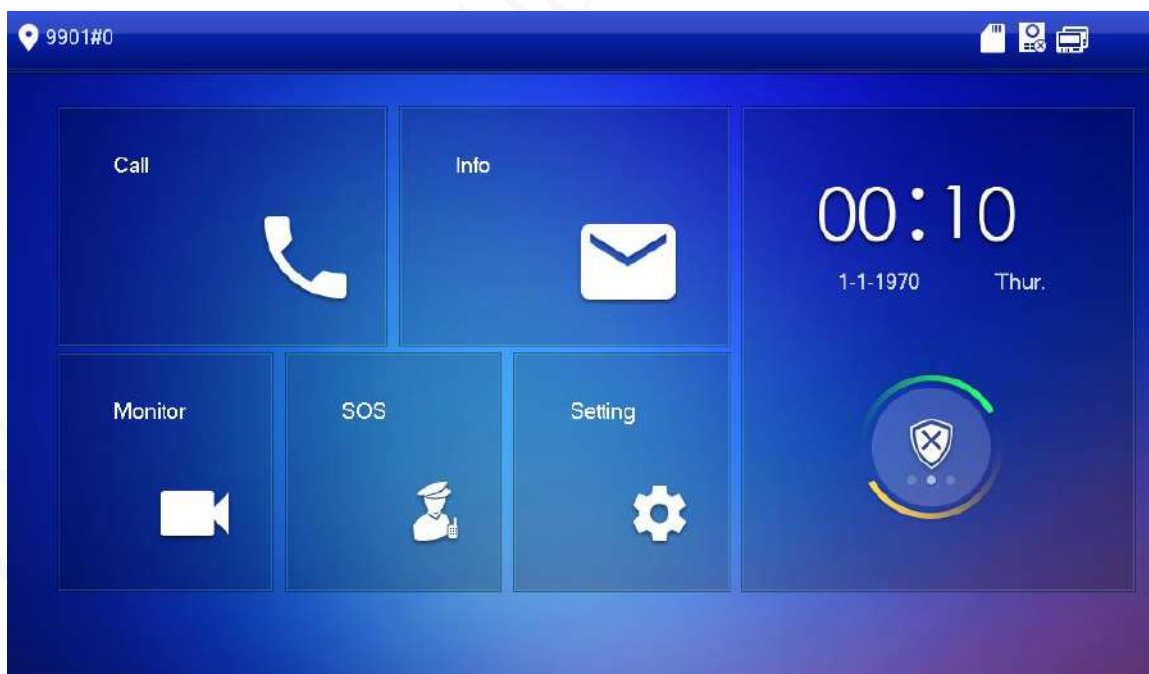
Step 1 Tap **Apartment** on Figure 2-12.

The **Device Init** interface is displayed.

Figure 2-19 Device initialization

Step 2 Enter password, confirm Pwd, and email, and then press **OK**.

Figure 2-20 Homepage



Step 3 Press **Setting** for more than 6 seconds, enter the password set during initialization, and click **OK**.

Step 4 Tap **Network**.



IP addresses of VTH and VTO shall be in the same network segment. Otherwise, VTH will fail to obtain VTO info after configuration.

Figure 2-21 Network (1)

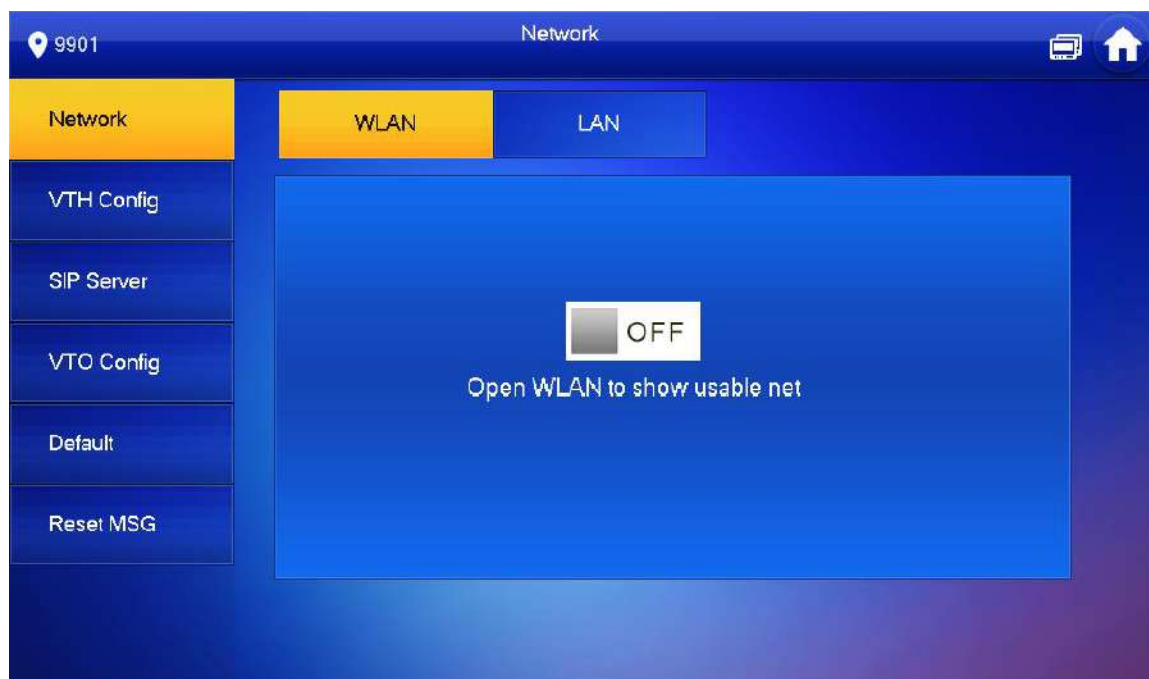


Figure 2-22 Network (2)



- LAN

Enter local IP, subnet mask and gateway, press **OK**. Or press ☐ OFF to enable DHCP function and obtain IP info automatically.

- WLAN

- 1) Press ☐ OFF to enable Wi-Fi function.

List of available Wi-Fi is displayed, see Figure 2-23.

Figure 2-23 WLAN



2) Connect Wi-Fi.

The system has two access ways.

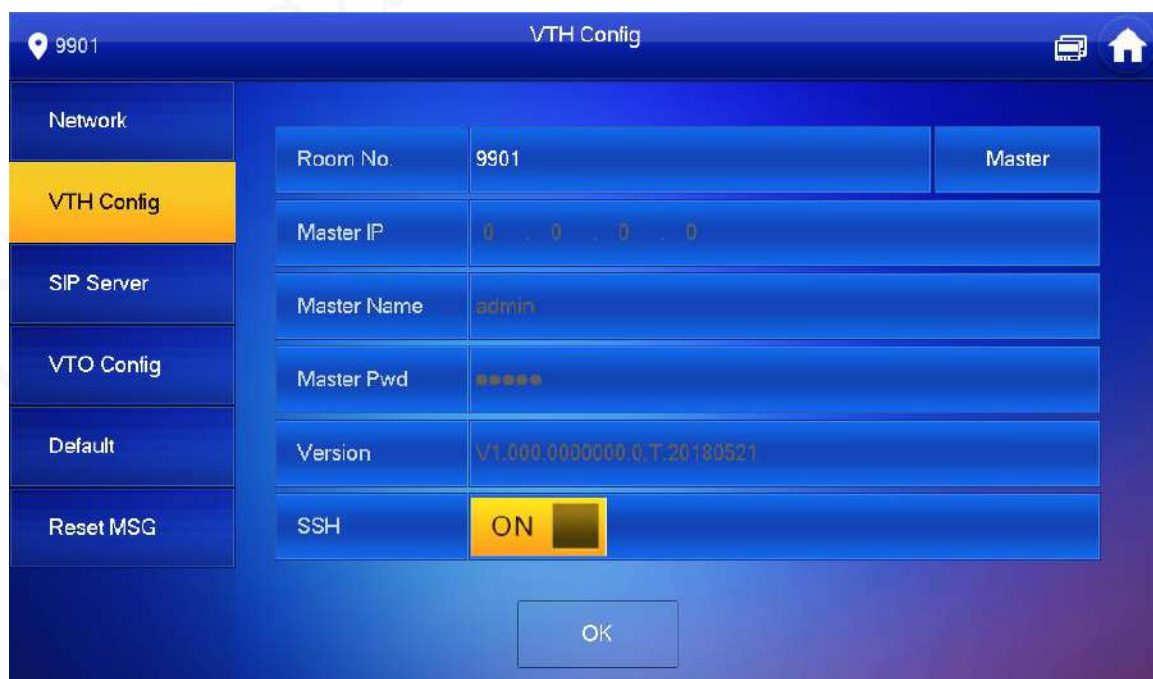
- ◇ On **WLAN** interface, select a Wi-Fi, click **Wireless IP** to enter local IP, subnet mask and gateway, and then press **OK**.
- ◇ On **WLAN** interface, select a Wi-Fi, click **Wireless IP**, press ☐ OFF to enable DHCP function and obtain IP info automatically.



To obtain IP info with DHCP function, use a router with DHCP function.

Step 5 Tap **VTH Config**.

Figure 2-24 VTH config



- Be used as a master VTH.

Enter Room No. (such as 9901 or 101#0) and press **OK** to save.



- Room no. shall be the same as VTH Short No., which is set when adding VTH at web interface. Otherwise, connecting VTO to VTH will fail.
 - In case of extension VTH, room no. shall end with #0. Otherwise, connecting VTO to VTH will fail.
 - Be used as an extension VTH.
- 1) Tap **Master** and **Master** will be changed to **Extension**.
 - 2) Enter room No. (such as 101#1) and master IP (IP address of master VTH).



- Master name and master Pwd are the user name and password of master VTH.
 - Default user name is admin, and the password is the one set during device initialization.
- 3) Press **OK** to save settings.

Step 6 Tap **SIP Server**.

Figure 2-25 SIP server

- 1) Set parameters of SIP server.

Table 2-4 SIP server parameter description

Parameter	Description
Server IP	<ul style="list-style-type: none"> • When the platform works as SIP server, server IP is IP address of the platform. • When VTO works as SIP server, server IP is IP address of the VTO.
Network Port	<ul style="list-style-type: none"> • When the platform works as SIP server, network port is 5080. • When VTO works as SIP server, network port is 5060.
User Name	Use default value. If you enabled custom name, you can customize a username.
Register Pwd	
Domain	Registration domain of SIP server, which can be null. When VTO works as SIP server, registration domain of SIP server

Parameter	Description
	shall be VDP.
User Name	User name and password to log in to SIP server.
Login Pwd	

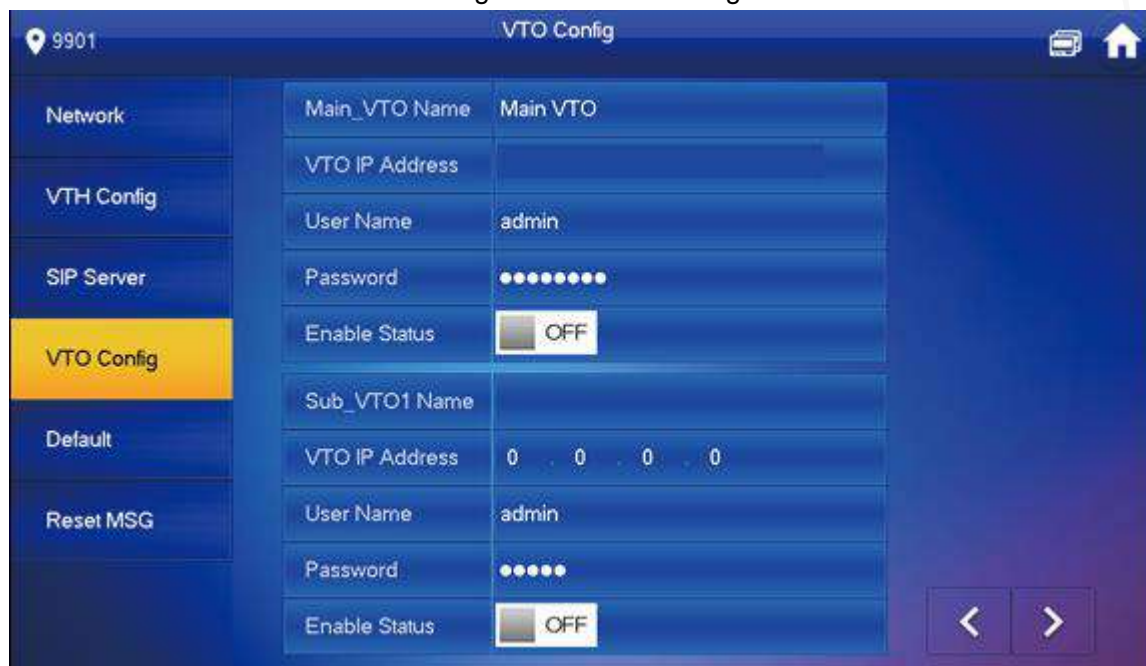
- 2) Set **Enable Status** to be .

The SIP server function is enabled.


- 3) Press **OK** to save settings.

Step 7 Tap **VTO Config**.

Figure 2-26 VTO config




Step 8 Add VTO or fence station.



- Add main VTO.
 - 1) Enter main VTO name, VTO IP address, user name and password.
 - 2) Switch the **Enable Status** to be .



User name and password entered here shall be the same as VTO web login user name and password. Otherwise, VTO cannot be connected to the VTH.

- Add sub VTO or fence station.
 - 1) Enter sub VTO/fence station name, sub VTO/fence station IP address, user name and password.
 - 2) Switch the **Enable Status** to be .



Press   to turn over pages and add more sub VTO/fence stations.

2.3 Function Verification

2.3.1 Calling VTHs from VTOs

Dial VTH room No. (such as 101) at VTO to call VTH. The monitoring image and operating icons are displayed, see Figure 2-27. It represents successful debugging.



The following figure means that SD card has been inserted into VTH. If SD card is not inserted, recording and snapshot icons are gray.

Figure 2-27 Calling VTHs from VTOs



2.3.2 Watching Monitoring Videos at VTHs

You can watch monitor places where VTO, fence station or IPC are installed. Here VTO will be taken as an example.

Step 1 Select **Monitor > Door**.

Step 2 Select a VTO to watch monitoring videos, see Figure 2-29.



The following figure means that SD card has been inserted into VTH. If SD card is not inserted, recording and snapshot icons are gray.

Figure 2-28 Door



Figure 2-29 Monitoring video



Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic equipment network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

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

2. Update Firmware and Client Software in Time

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

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

1. Physical Protection

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

2. Change Passwords Regularly

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

3. Set and Update Passwords Reset Information Timely

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

4. Enable Account Lock

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

5. Change Default HTTP and Other Service Ports

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

6. Enable HTTPS

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

7. Enable Whitelist

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

8. MAC Address Binding

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

9. Assign Accounts and Privileges Reasonably

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

10. Disable Unnecessary Services and Choose Secure Modes

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

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

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

11. Audio and Video Encrypted Transmission

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

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

12. Secure Auditing

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

13. Network Log

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

14. Construct a Safe Network Environment

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

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

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