Emergency Call Terminal

User's Manual



V1.0.0

Foreword

This manual introduces the configurations on the webpage of emergency call terminal. Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	October 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguard and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Operation Requirements



- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Transport, use and store the device under allowed humidity and temperature conditions.
- If the device is powered off for longer than a month, it should be placed in its original package and sealed. Make sure to keep it away from moisture, and store it under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.

Installation Requirements



- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Improper use of the battery might result in a fire or explosion.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Install the device on a stable surface to prevent it from falling.
- Install the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.

Table of Contents

Foreword I
Important Safeguard and Warnings III
1 Introduction 1
2 Structure 2
2.1 Front panel 2
2.2 Rear Panel 5
2.3 Function Cable Wiring 7
3 Installation 8
3.1 Surface Mount 8
3.2 Flush Mount 9
4 Operations on Webpage 11
4.1 Initialization 11
4.2 Logging in to the Webpage 11
4.3 Resetting Password 12
4.4 Home Page Introduction 13
4.5 Local Settings 14
4.5.1 Configuring Basic Settings 14
4.5.2 Configuring Intercom Parameters 15
4.5.3 Configuring Audio Parameters 15
4.5.4 Configuring Alarm Linkage 17
4.5.5 Power Supply Management 18
4.6 Configuring Network 18
4.6.1 Configuring TCP/IP 18
4.6.2 Configuring Port 20
4.6.3 Configuring FTP 21
4.6.4 Adding VTA 21
4.6.5 Configuring UPnP 24
4.6.6 Configuring Basic Services 25
4.7 System Management 27
4.7.1 Configuring Video Parameters 27
4.7.2 Configuring Time 32
4.7.3 Adding ONVIF User 33
4.7.4 Configuring Storage 34
4.8 Maintenance Center 35
4.8.1 One-click Diagnosis 35
4.8.2 System Information 35
4.8.3 Log 36

4.8.4 Management....37
4.8.5 Update....39
4.8.6 Advanced Maintenance....40
4.9 Searching Record....40
4.10 Searching Picture....41
4.11 Security....42
4.11.1 Security Status....42
4.11.2 Configuring System Service....44
4.11.3 Attack Defense....44
4.11.4 Configuring CA Certificate....48
4.11.5 Configuring Video Encryption....52
4.11.6 Configuring Security Warning....53
4.11.7 Configuring Security Authentication....53
Appendix 1 Cybersecurity Recommendations....55

1 Introduction

The emergency call terminal is used to call in emergency, broadcast and monitor by connecting with the platform or the alarm receiving center. It is applicable in schools, airports, factories and scenic areas where convenient methods for seeking help are necessary.

2 Structure

The appearance and ports might differ depending on the actual models. The following images are for reference only.

2.1 Front panel

VTA-2501G Series

Figure 2-1 Front panel

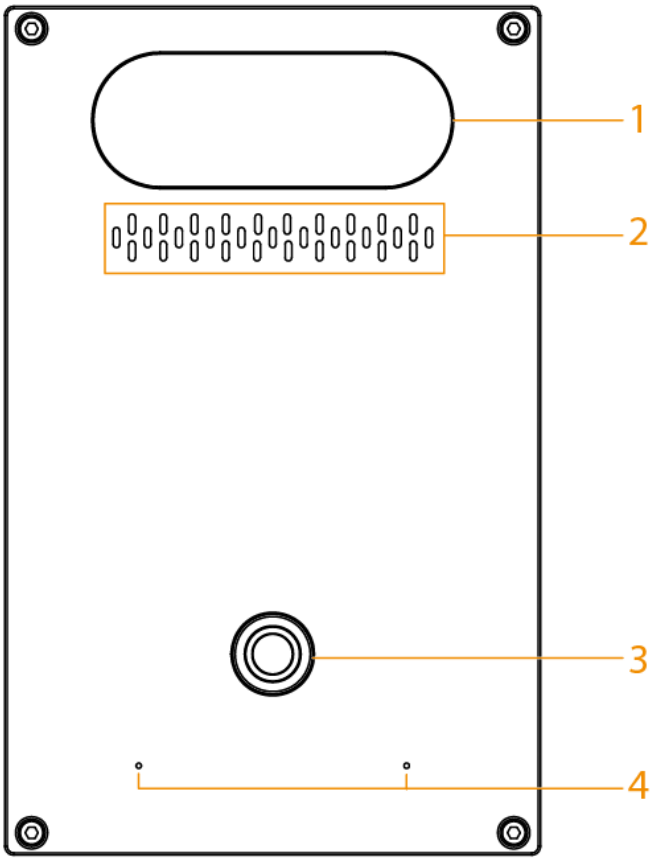


Table 2-1 Front panel description

No.	Component Name	Description
1	Camera	Collects video images.
2	Speaker	Audio output.
3	Emergency Button	Press the button to call the management center.

No.	Component Name	Description
4	Microphone	Collects audio and supports two-way voice intercom.

VTA-2502G Series (Surface Mount)

Figure 2-2 Front panel

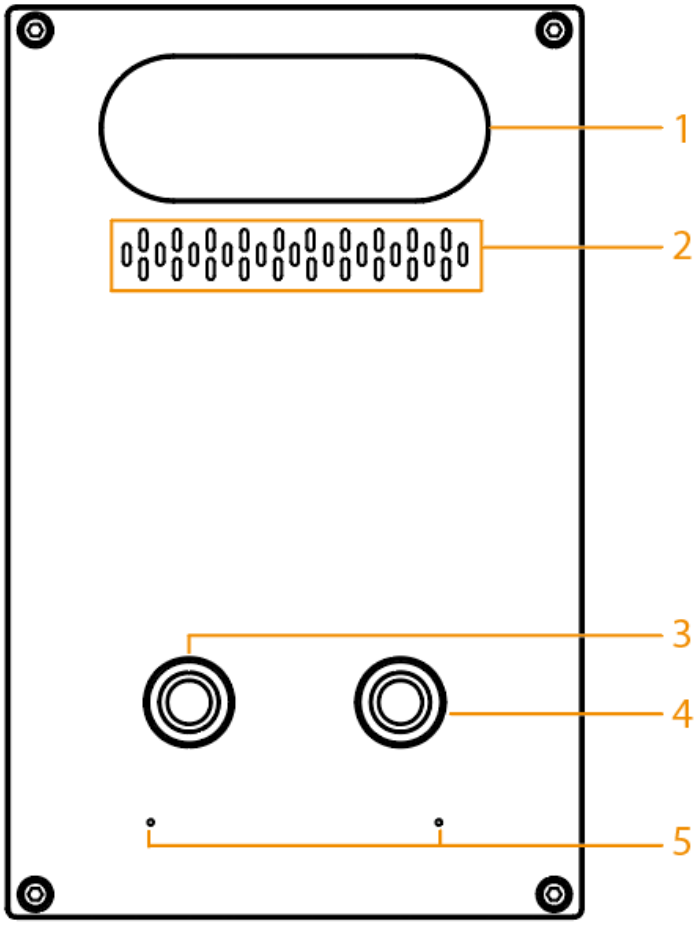


Table 2-2 Front panel description

No.	Component Name	Description
1	Camera	Collects video images.
2	Speaker	Audio output.
3	Emergency Button	Press the button to call the management center.
4	Call Button	Press the button to call the management center.
5	Microphone	Collects audio and supports two-way voice intercom.

VTA-2502G Series (Flush Mount)

Figure 2-3 Front panel

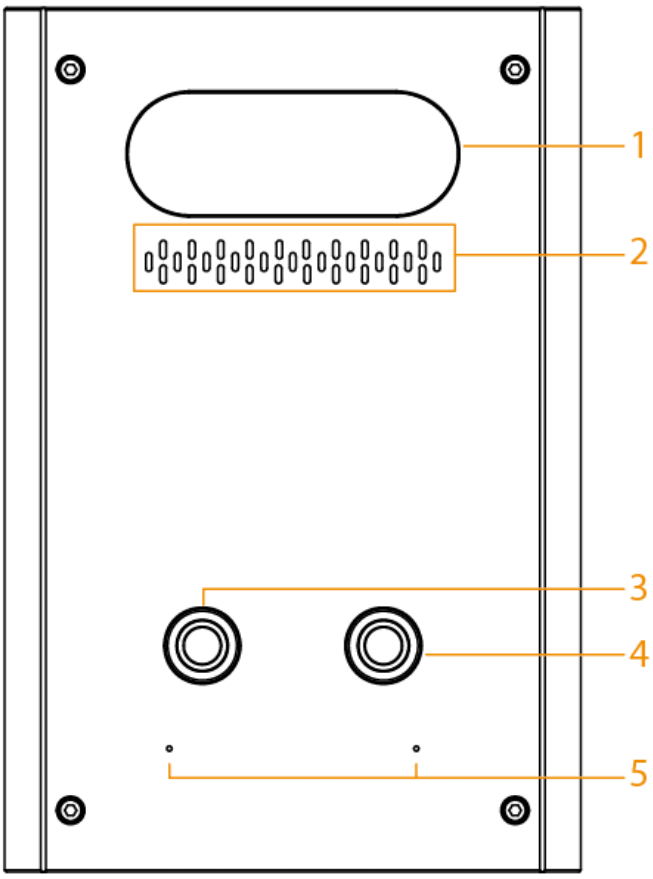


Table 2-3 Front panel description

No.	Component Name	Description
1	Camera	Collects video images.
2	Speaker	Audio output.
3	Emergency Button	Press the button to call the management center.
4	Call Button	Press the button to call the management center.
5	Microphone	Collects audio and supports two-way voice intercom.

VTA-2511G Series

Figure 2-4 Front panel

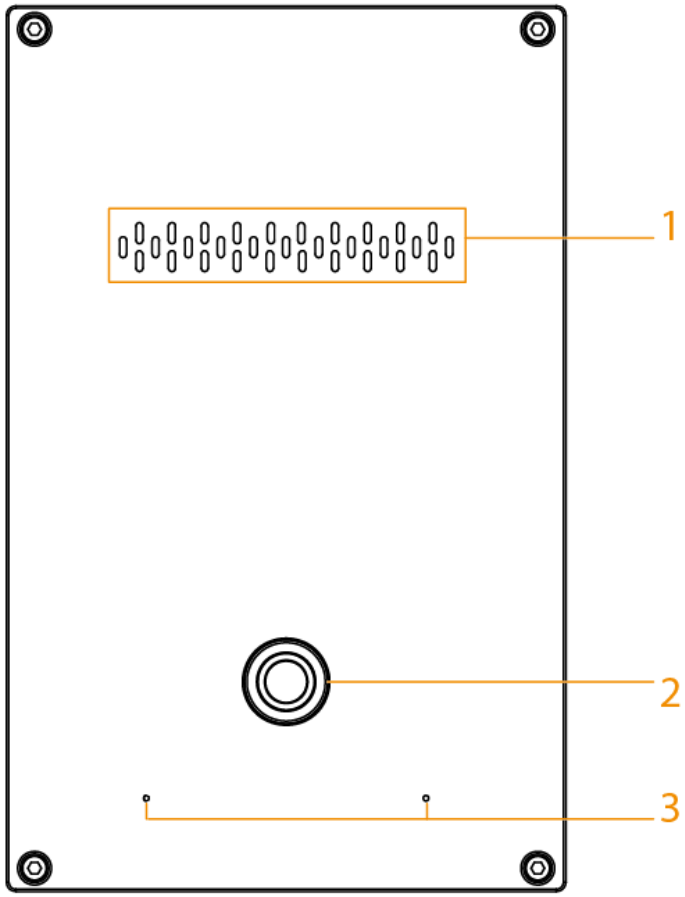


Table 2-4 Front panel description

No.	Component Name	Description
1	Speaker	Audio output.
2	Emergency Button	Press the button to call the management center.
3	Microphone	Collects audio and supports two-way voice intercom.

2.2 Rear Panel

The rear panels of different models are the same.

Figure 2-5 Rear panel

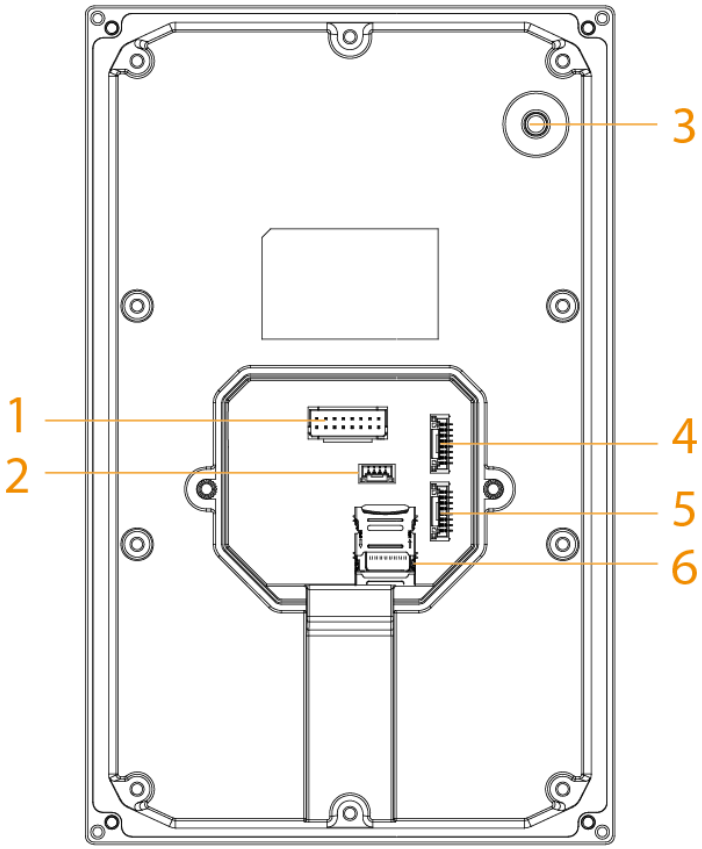


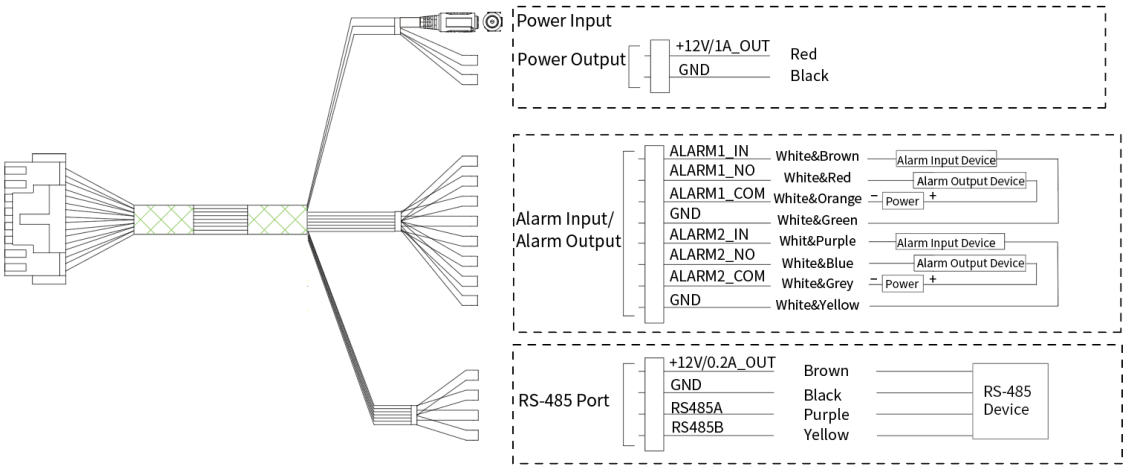
Table 2-5 Rear panel description

No.	Components and Ports	Description
1	Function Cable Port	The port includes alarm input, alarm output, power input (12 VDC), power output, and RS-485 port. Plug in the standard function cable pigtail. For more details, see "2.3 Function Cable Wiring".
2	Audio Extension Port	Audio input and output ports. Plug in the standard audio cable pigtail.
3	Tamper Button	When the device is removed from the wall, an anti-removal alarm is triggered.
4	Network Port	Plug in the standard network cable pigtail.
5	Network Port (PoE)	Standard PoE power supply. Plug in the standard network cable pigtail.

No.	Components and Ports	Description
6	SD Card Port	Insert the SD card to store video and image files. The maximum capacity is 512 GB. ⚠ Hot swapping is not supported. 📖 Only VTA250*X*G series support this function.

2.3 Function Cable Wiring

Figure 2-6 Wiring



3 Installation



- Avoid installing the emergency call terminal in bad environment, such as condensation, high temperature, oil, dust, chemical corrosion and direct sunlight environment and more.
- If there are any abnormalities after powering on the device, cut off the power supply, and then pull out the network cable. Power on the device again after troubleshooting.
- The installation and debugging of the device shall be carried out by the professional staffs. In case of device error, do not disassemble and repair it by yourself. Contact the after-sales department.

3.1 Surface Mount

Procedure

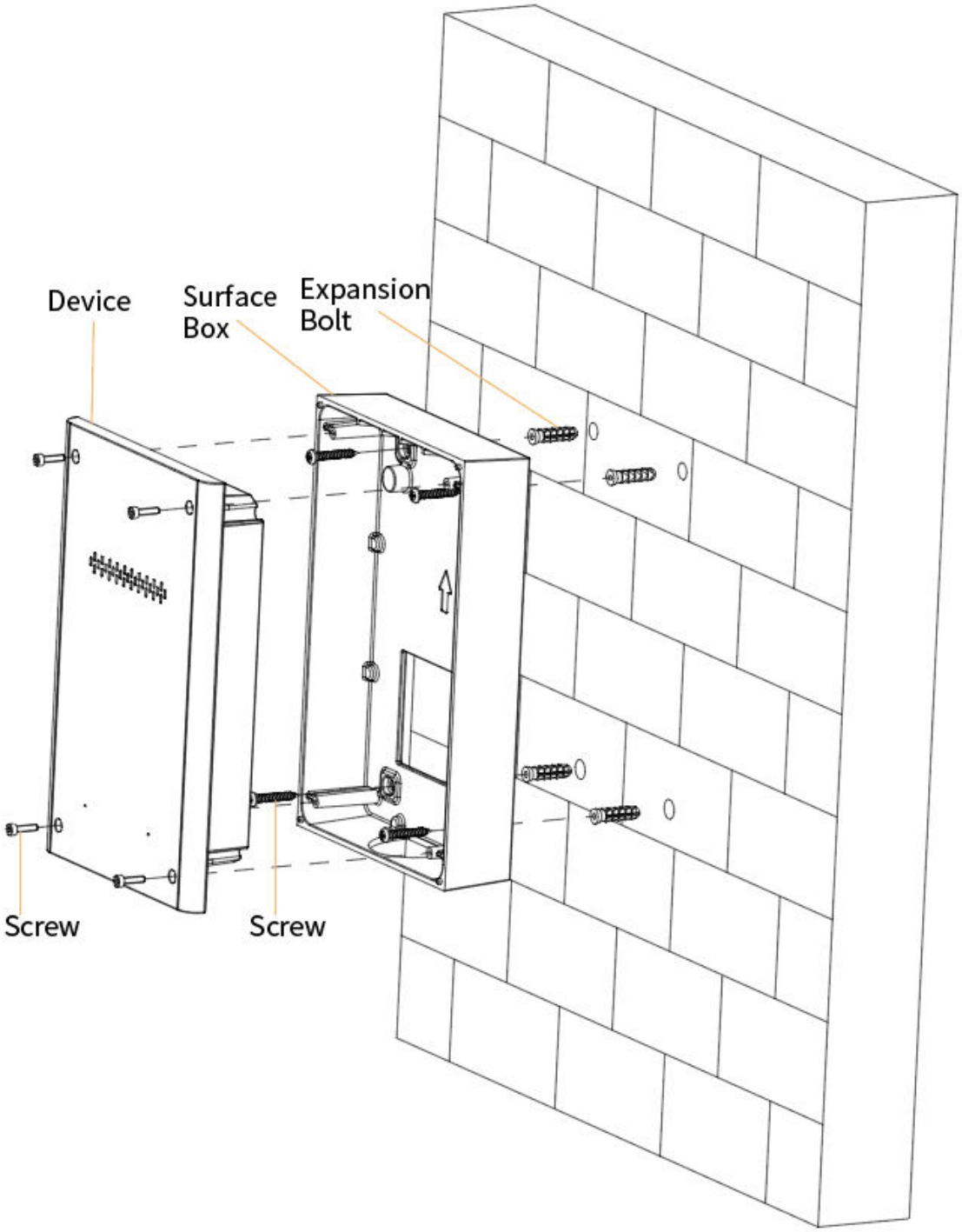
Step 1 Drill 4 holes on the wall according to the holes' position on the surface box, and then hammer in the expansion bolts.

Step 2 Fix the surface box on the wall with 4 screws.

Step 3 Connect the cables. For details, see "2.3 Function Cable Wiring".

Step 4 Fix the device on the surface box with 4 screws.

Figure 3-1 Surface mount



3.2 Flush Mount

Procedure

Step 1 Slot on the wall according to the dimensions of the flush box.

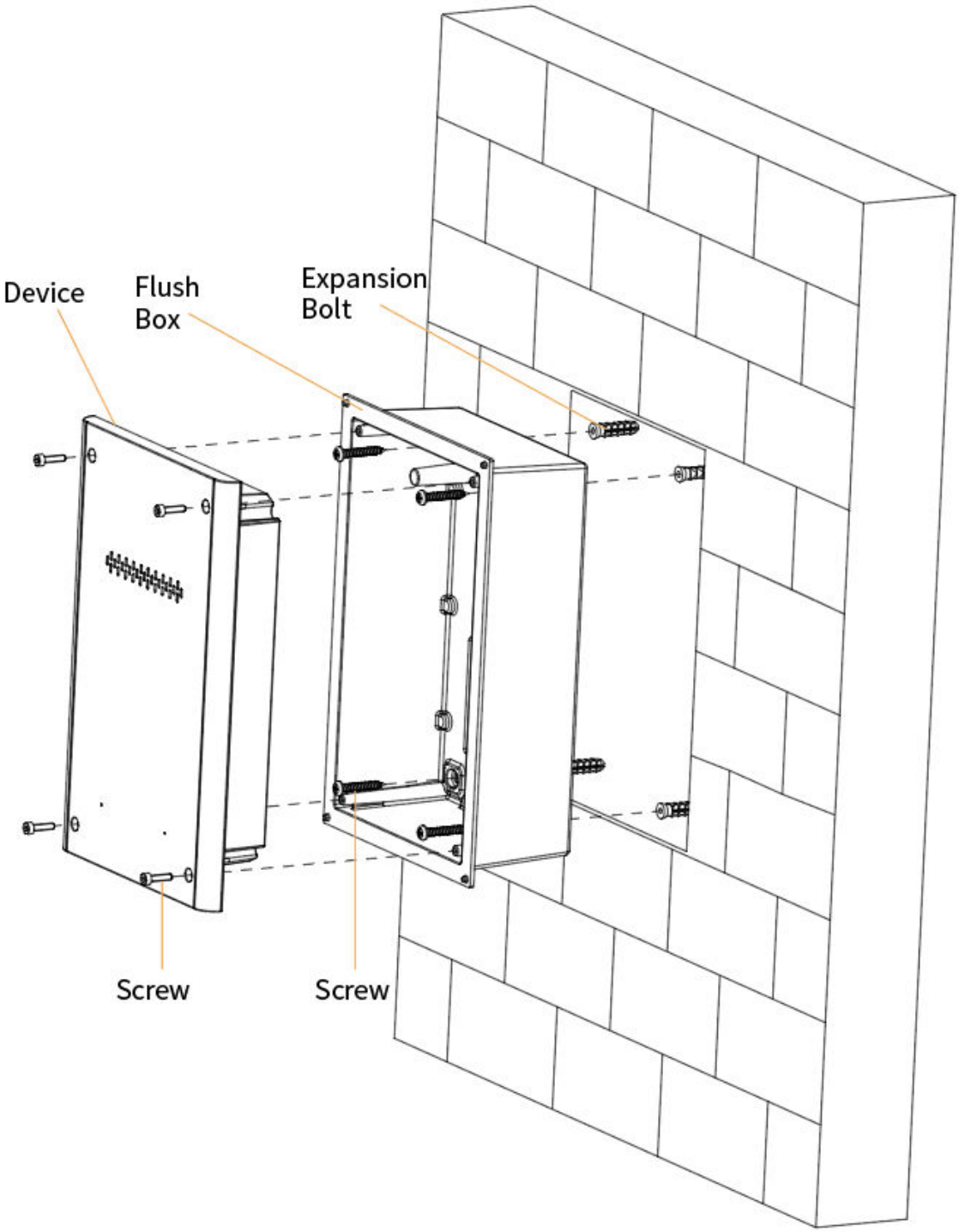
Step 2 Drill 4 holes on the slot according to the holes' position on the flush box, and then hammer in the expansion bolts.

Step 3 Fix the flush box on the wall with 4 screws.

Step 4 Connect the cables. For details, see "2.3 Function Cable Wiring".

Step 5 Fix the device on the flush box with 4 screws.

Figure 3-2 Flush mount



4 Operations on Webpage

4.1 Initialization

Initialize the device for first-time login or when you log in to the device after restoring it to factory settings.

Prerequisites

Make sure that the computer is on the same network segment as the emergency call terminal.

Procedure

Step 1 Enter the IP address of emergency call terminal in a browser, and then press the Enter key.

- The default IP address for network adapter 1 is 192.168.1.108. The default IP address for network adapter 2 is 192.168.2.108.
- We recommend you use Google Chrome with version 100 or later, or Firefox with version 100 or later.

Step 2 Select the language.

Step 3 Enter the password and email address, and then click **Done**.

- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case, lower case, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.
- Keep the password safe after initialization and change the password regularly to improve security.
- Enter the email address, and if you forget the password, you can receive the security code through the email.

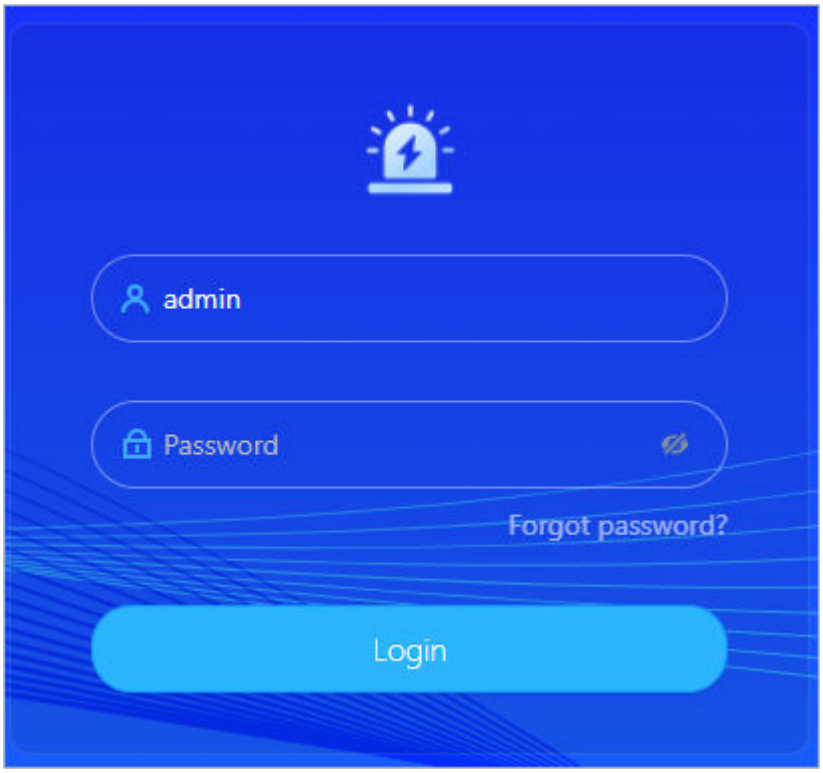
4.2 Logging in to the Webpage

Procedure

Step 1 Enter the IP address of the device in a browser, and then press the Enter key.

Step 2 Enter the username and password.

Figure 4-1 Log in



- The default username of administrator is **admin**. The default password is the password that you configured during initialization. We recommend you change the password on a regular basis.
- If you forget the password, click **Forgot password?** to reset the password. For details, see "4.3 Resetting Password".

Step 3 Click **Login**.

4.3 Resetting Password

Reset password through the email address that you bound if you forget the password.

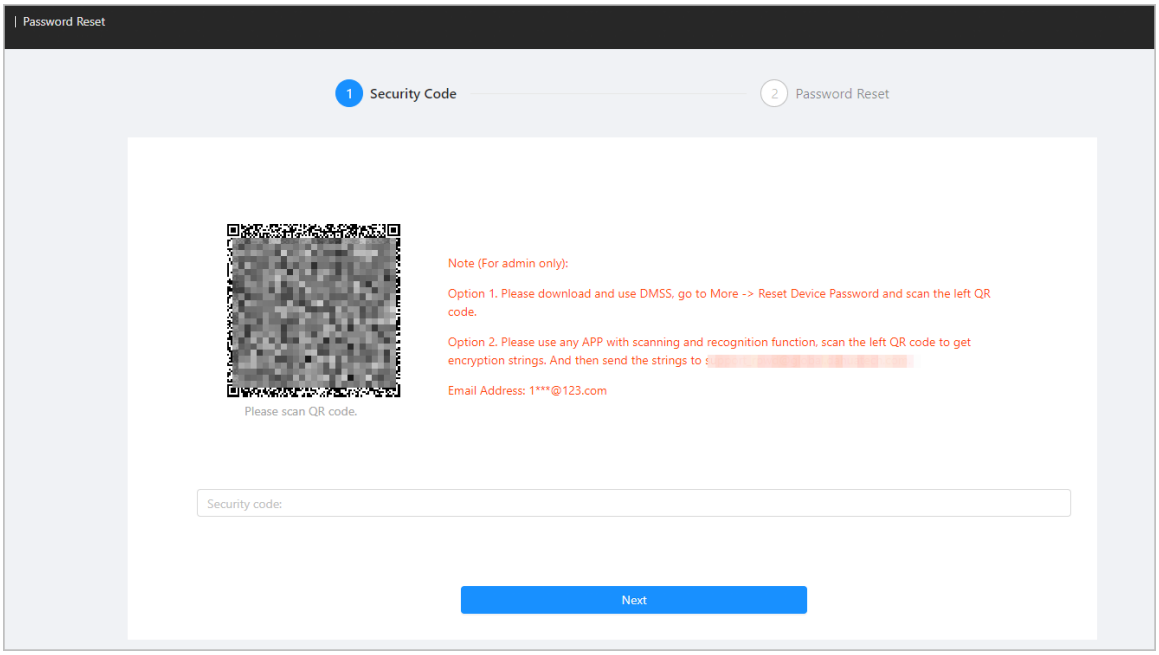
Procedure

Step 1 On the login page, click **Forgot Password?**

Step 2 Click **OK** on the pop-up window.

Step 3 Scan the QR code on the page, and then get the security code.

Figure 4-2 Get the security code



- A maximum of two security codes will be generated by scanning the same QR code. If you need to get the security code again, refresh the QR code page.
- Use the security code within 24 hours after you receive it. Otherwise the security code will become invalid.
- The account will be locked for 5 minutes if you enter the wrong security code 5 times in a row.

Step 4 Enter the security code you received.

Step 5 Click **Next**.

Step 6 Reset new password and confirm the new password.

The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among number, letter and common character (excluding space, ', ", ;, :, &).

Step 7 Click **OK**.

4.4 Home Page Introduction

The system automatically goes to the home page after you log in.

Figure 4-3 Home page

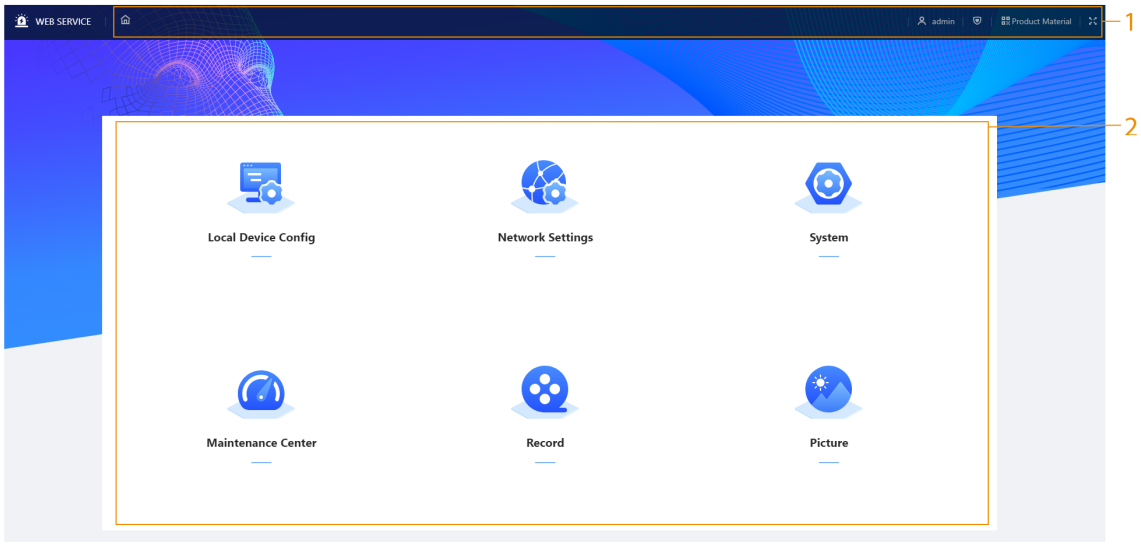


Table 4-1 Home page description

No.	Parameter and Icon		Description
1	Navigation Bar		Go to the home page.
		admin	• Click the icon. Select **Change Password** , enter the old and new password, and then click **OK**. • Click the icon. Select **Restart** to restart the device. • Click the icon. Select **Logout** to log out the account.
			Go to the security page to view the security status.
		Product Material	Click to view the QR code, and then scan the code to get the document on the product.
			Open the window in a full screen mode.
2	Function Menu		Functions configuration menu of the device. The functions may differ depending on different models.

4.5 Local Settings

4.5.1 Configuring Basic Settings

Procedure

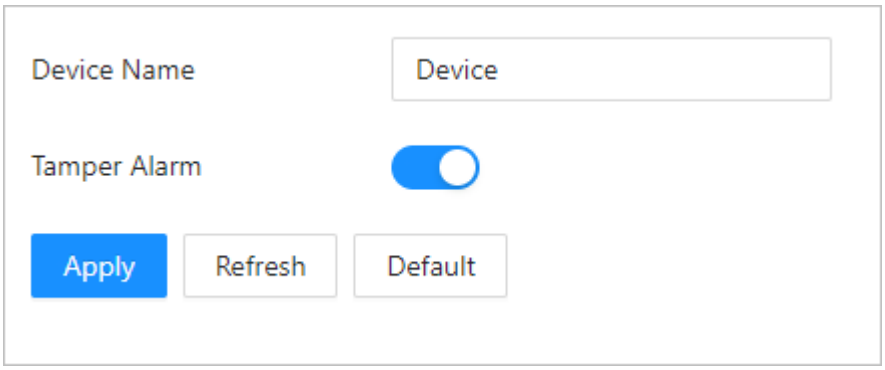
Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Basic Settings**.

Step 3 Configure the parameters, and then click **Apply**.

Tamper Alarm : When enabled, if the device is detached from the wall, an alarm is triggered.

Figure 4-4 Basic settings



4.5.2 Configuring Intercom Parameters

Procedure

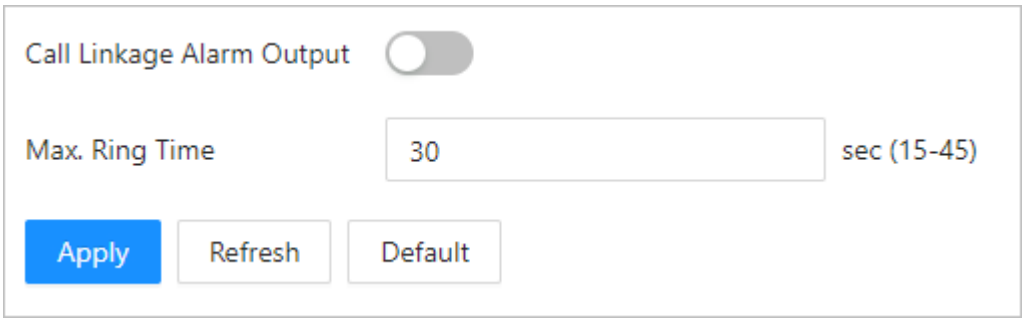
Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Intercom**.

Step 3 Configure the parameters, and then click **Apply**.

- **Call Linkage Alarm Output** : When enabled, if you press the emergency button on the device, the alarm output device connected to **ALARM1_NO** and **ALARM1_COM** ports will be linked.
- **Max. Ring Time** : Configure the ring time for calling the phone number. If there is no answer after the time expires, the device will call the next number.

Figure 4-5 Intercom



4.5.3 Configuring Audio Parameters

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Audio**.

Step 3 Configure the parameters, and then click **Apply**.

Figure 4-6 Audio

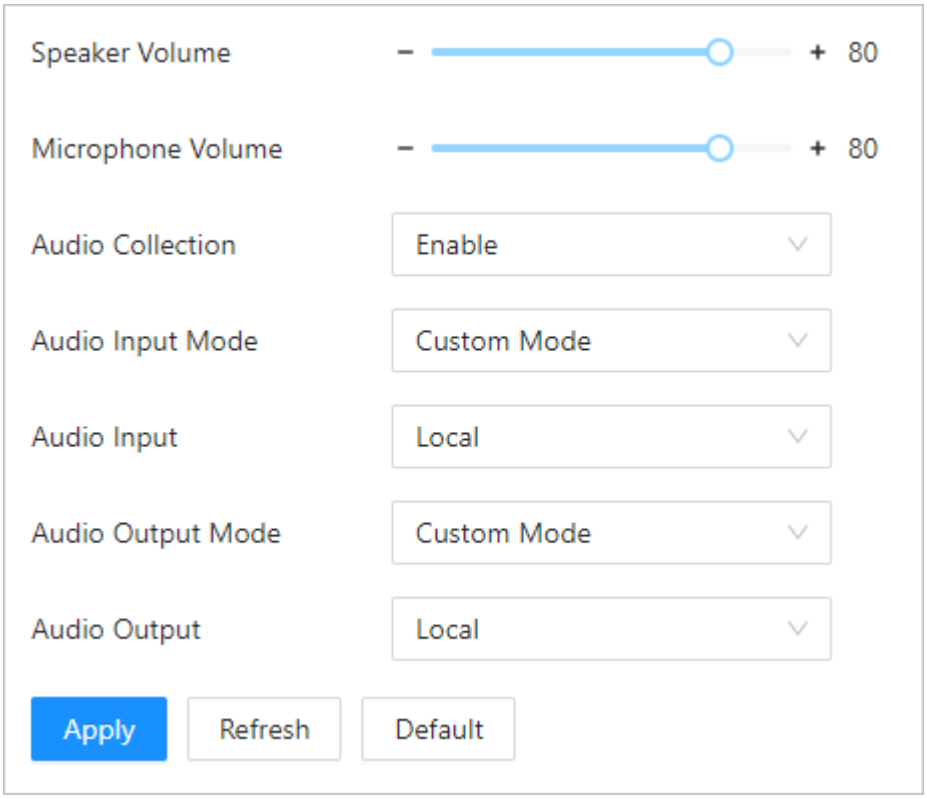


Table 4-2 Audio parameters description

Parameters	Description
Speaker Volume	Drag or click + and – to adjust the speaker volume.
Microphone Volume	Drag or click + and – to adjust the volume of collected voice.
Audio Collection	It is **Enable** by default. When enabled, the voice can be collected.
Audio Input Mode	Custom mode.
Audio Input	• **Local** : Collect the voice through the microphone on the device. • **Extended Peripheral** : Collect the voice through the extended audio device connected to 3.5 mm audio port.
Audio Output Mode	Custom mode.
Audio Output	• **Local** : Play the voice through the speaker on the device. • **Extended Peripheral** : Play the voice through the extended audio device connected to 3.5 mm audio port. • **Local and Extended Peripheral** : Play the voice through the speaker on the device and the extended audio device connected to 3.5 mm audio port at the same time.

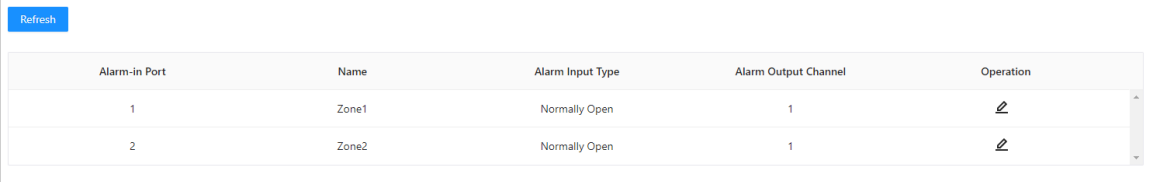
4.5.4 Configuring Alarm Linkage

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Alarm Linkage Settings**.

Figure 4-7 Alarm linkage



Step 3 Click ✎ to modify the parameters.

Figure 4-8 Modify the parameters

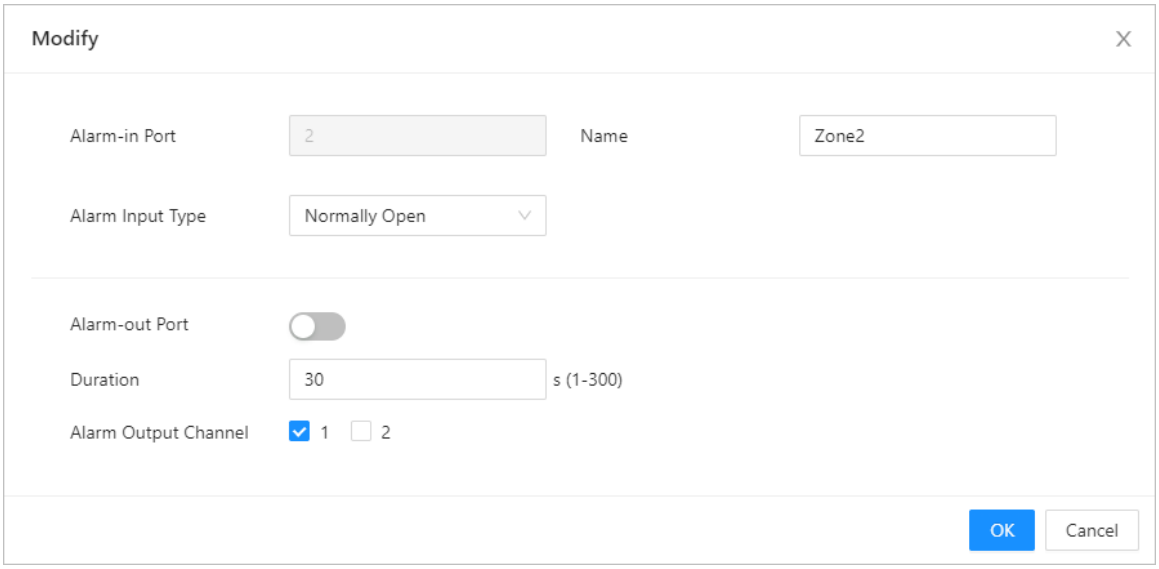


Table 4-3 Description of alarm linkage parameters

Parameter	Description
Alarm-in Port	The alarm-in port number cannot be modified.
Name	Customized.
Alarm Input Type	Select the type according to the device you purchased. • **Normally Open** : The circuit of the alarm device is normally open, and closes when an alarm is triggered. • **Normally Closed** : The circuit of the alarm device is normally closed, and opens when an alarm is triggered.
Alarm-out Port	If alarm output is enabled, the relay can generate alarm messages. Configure the alarm duration, and then select the channel according to the actual channels.
Duration	
Alarm Output Channel	

Step 4 Click **OK**.

4.5.5 Power Supply Management

If enabled, the 12 V/1 A power output is available.

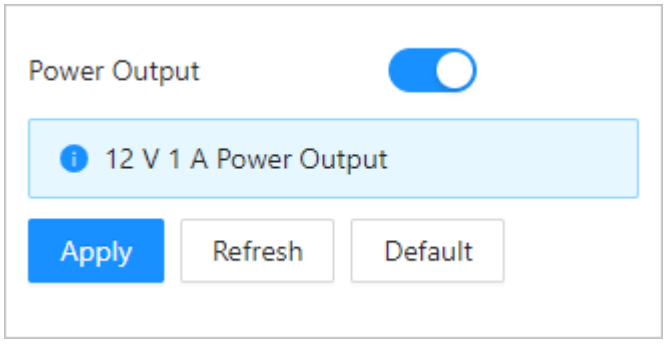
Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Power Supply Management**.

Step 3 Enable **Power Output** , and then click **Apply**.

Figure 4-9 Power output



4.6 Configuring Network

4.6.1 Configuring TCP/IP

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Network Settings** > **TCP/IP**.

Step 3 Configure the parameters.

Figure 4-10 Configure the parameters

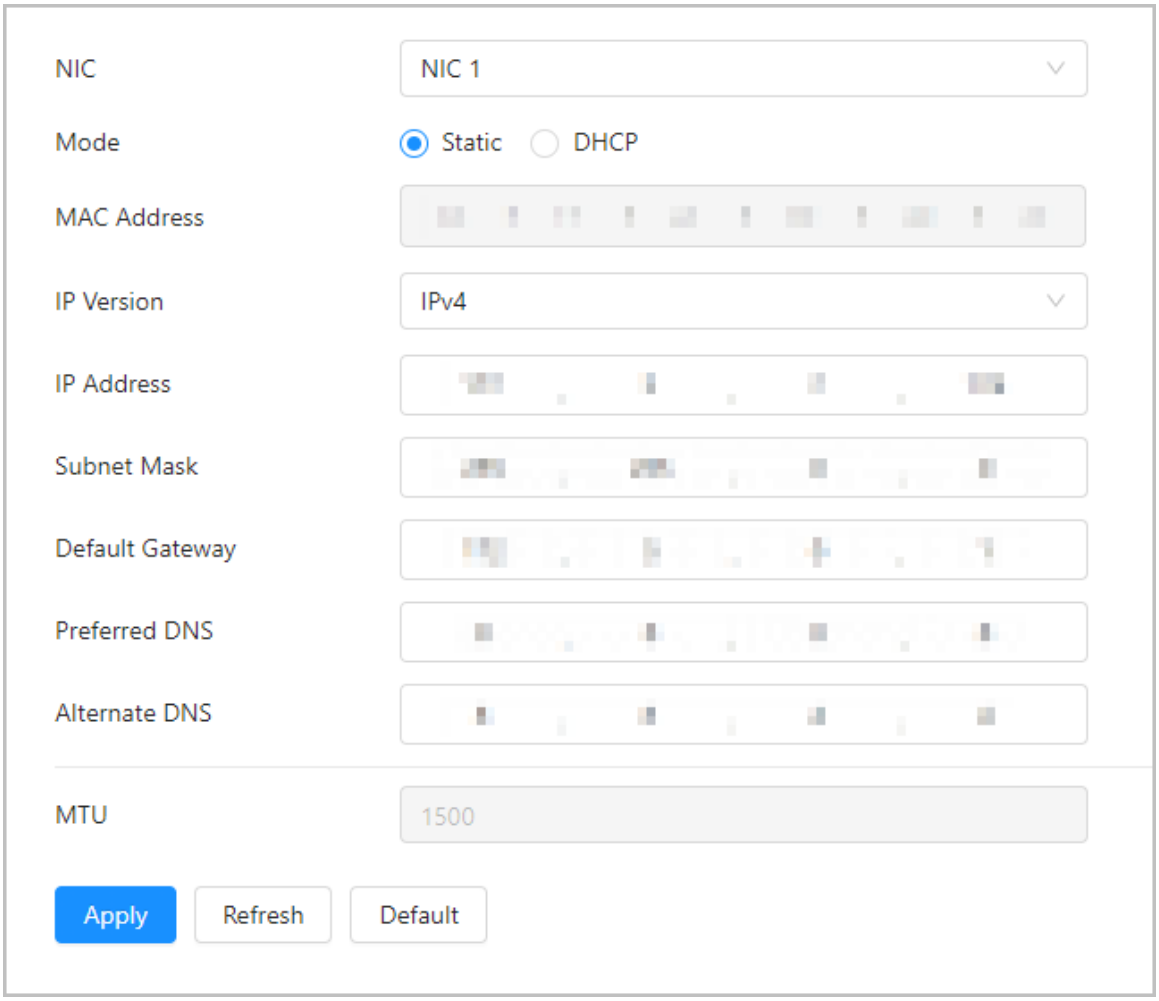


Table 4-4 Parameters description

Parameter	Description
Mode	• Static: Manually configure **IP** , **Subnet Mask** and **Default Gateway**. Click **Apply** and the webpage automatically goes to the login page of the IP that you configured. • DHCP (Dynamic Host Configuration Protocol): Select **DHCP** if there is a DHCP server. The device automatically gets a dynamic IP address.
MAC Address	MAC (Media Access Control) address of the device.
IP Version	Select from **IPv4** and **IPv6**.
IP Address	If you select **Static** in **Mode**, enter the IP address, subnet mask and default gateway according to the network planning. • There is no subnet mask in IPv6 version. • IP address and default gateway should be on the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	IP address of DNS server.
Alternate DNS	Alternate IP address of DNS server.

Parameter	Description
MTU	It is 1,500 by default.

Step 4 Click **Apply**.

4.6.2 Configuring Port

You can limit access to the emergency call terminal at the same time through webpage and desktop client, and configure port numbers of the device.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Network Settings** > **Port**.

Step 3 Configure the ports.

Except for **Max Connection** and **RTSP Port**, you need to restart the emergency call terminal to make the configurations effective after you change other parameters.

Figure 4-11 Configure ports

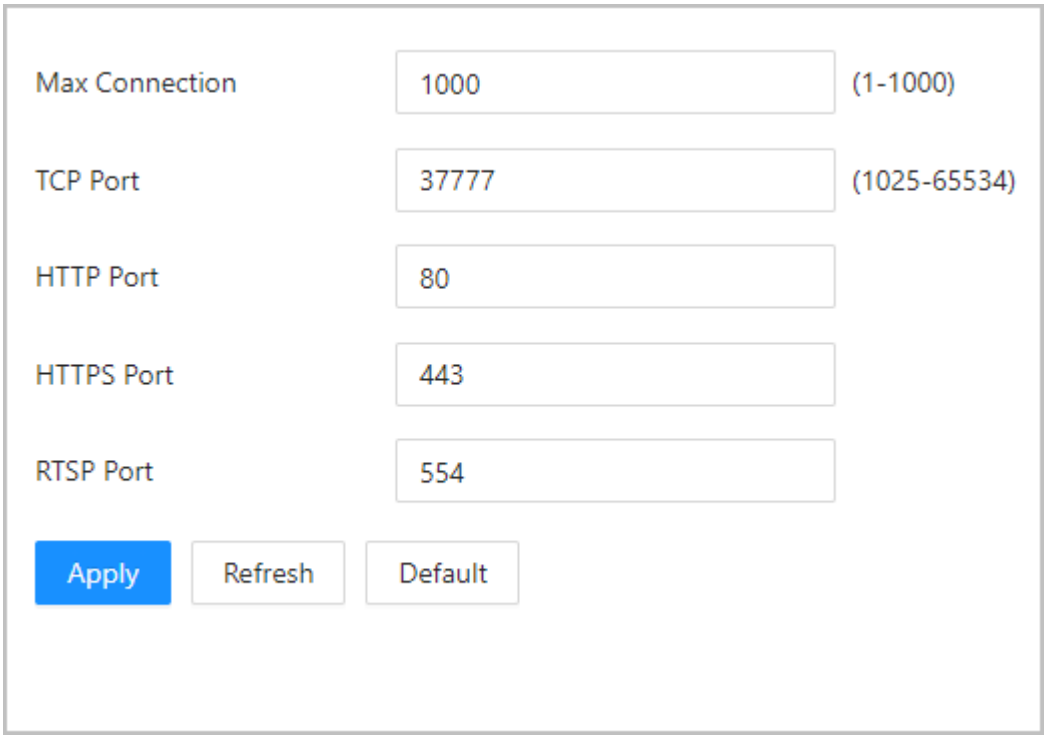


Table 4-5 Description of ports

Parameter	Description
Max Connection	Set the maximum number of clients (such as webpage and desktop client) that can access the emergency call terminal at the same time. Platform clients like SmartPSS AC are not counted.

Parameter	Description
TCP Port	Default value is 37777.
HTTP Port	Default value is 80. If you have changed the port number, add the port number after the IP address when access the webpage.
HTTPS Port	Default value is 443.
RTSP Port	Default value is 554.

Step 4 Click **Apply**.

4.6.3 Configuring FTP

Background Information

When connect the emergency call terminal with the VTS, configure the FTP parameters on the VTS, and then upload the broadcast files to the FTP server for broadcast on the emergency call terminal. After connected, the FTP configurations on emergency call terminal will synchronize with the configurations on the VTS.

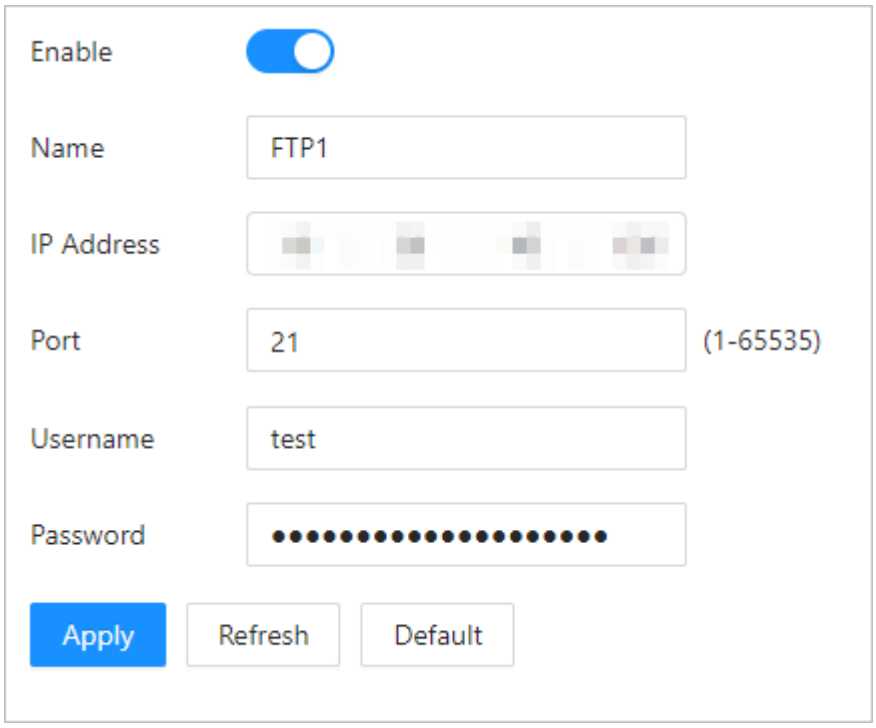
Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Network Settings** > **FTP**.

Step 3 Enable the function, configure the parameters, and then click **Apply**.

Figure 4-12 Configure FTP parameters



4.6.4 Adding VTA

4.6.4.1 Adding VTA through Auto Registration

After you enable this function, when the device is connected into Internet, it will report the current location to the specified server, such as VTS, which acts as the transit to make it easier for the client software to access the camera.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Network Settings** > **Auto Registration**.

Step 3 Click , and then configure the parameters.

Figure 4-13 Auto registration

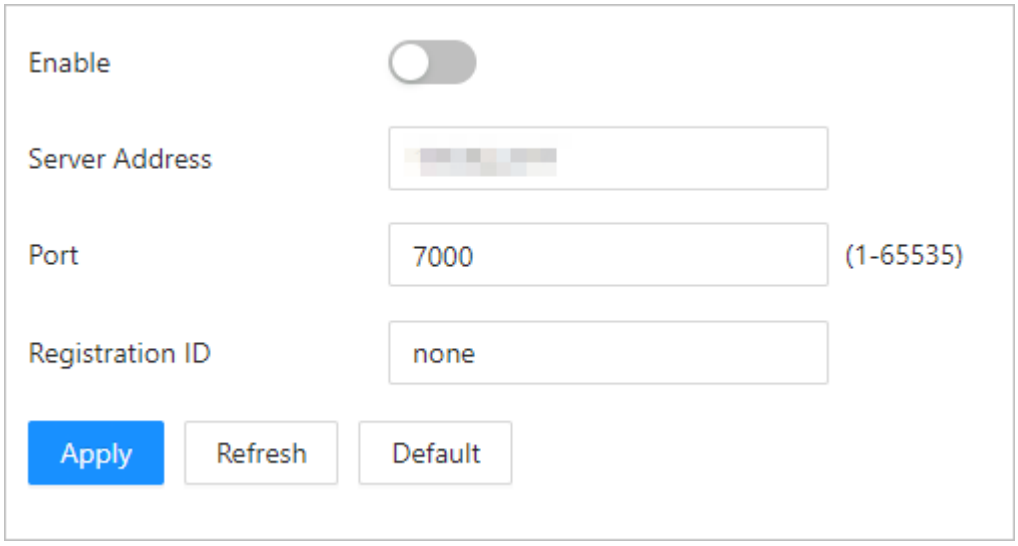


Table 4-6 Description of register parameters

Parameter	Description
Server Address	The IP address or domain name of the server to be registered. For example, the IP address of the VTS.
Port	The port number of the server to be registered. The port number of the VTS is 9050.
Registration ID	Keep consistent with the registration ID on the server. When the VTS works as the server, the registration ID is the **Device No.** on the webpage of VTS. For more details, see "4.6.4.2 Adding VTA through VTS".

Step 4 Click **Apply**.

4.6.4.2 Adding VTA through VTS

Procedure

Step 1 Log in to the webpage of VTS.

Step 2 Select **Device Setting** > **Terminal Management**.

Step 3 Click **Add**, and then configure the parameters.

Figure 4-14 Add VTA

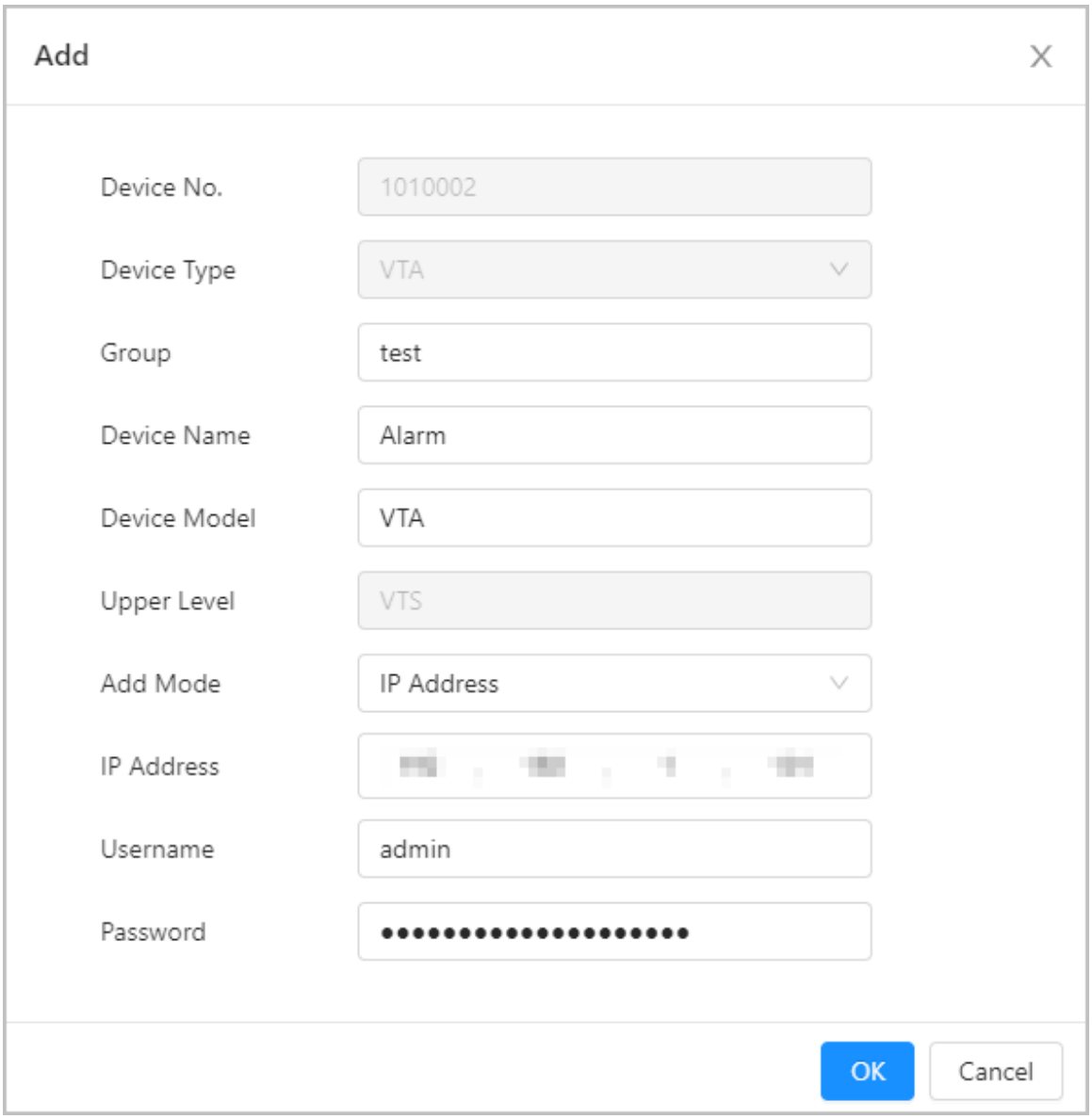


Table 4-7 Parameters description

Parameter	Description
Device No.	When the VTA is added through auto registration, the registration ID on VTA must be the same with the device number here.
Group	Select **Monitor** > **Terminal Management** on local VTS, and then you can view the devices of the group that you configured.

Parameter	Description
Device name	User-defined.
Device model	Enter the complete device model that you can get from the device label.
Add mode	You can add VTA in the following 2 ways. • IP address: Enter the IP address of the VTA. • Register: Configure the parameters for registering on the VTA.
Username	Enter the username and password of the VTA.
Password	

Step 4 Click **OK**.

4.6.5 Configuring UPnP

UPnP (Universal Plug and Play) is a protocol that establishes mapping relation between intranet and extranet. This function enables you to visit intranet device through extranet IP address.

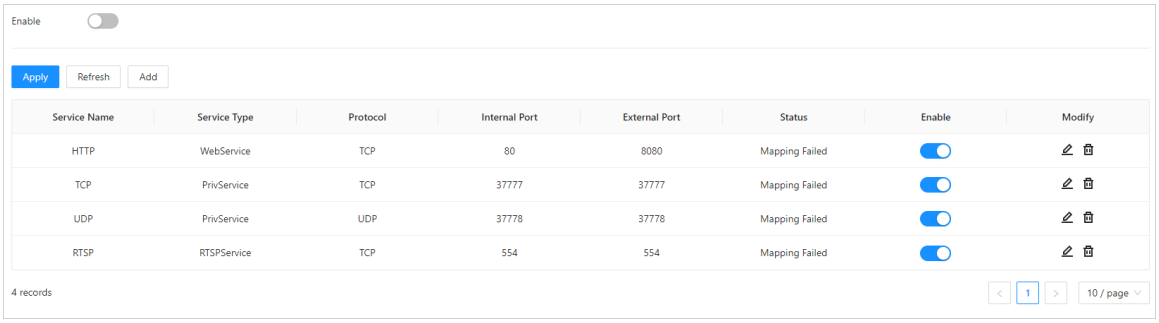
Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Network Settings** > **UPnP**.

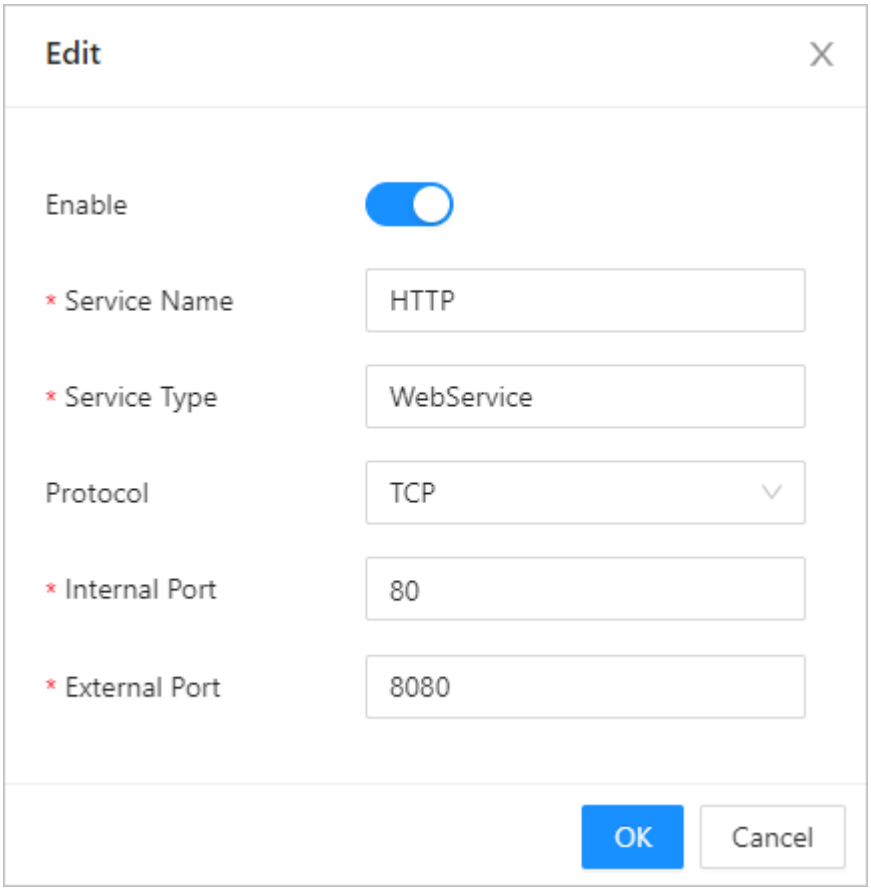
Step 3 Click next to **Enable**.

Figure 4-15 UPnP



Step 4 Click to modify the ports, and then click **OK**.

Figure 4-16 Modify the ports



Step 5 Click **Apply**.

Open a browser on the computer, enter *http:// extranet IP address: external port number*, and then you can visit the intranet device with corresponding port.

4.6.6 Configuring Basic Services

Configure the basic services to achieve the security management of the system.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Network Settings** > **Basic Services**.

Step 3 Configure the parameters, and then click **Apply**.

Figure 4-17 Basic services

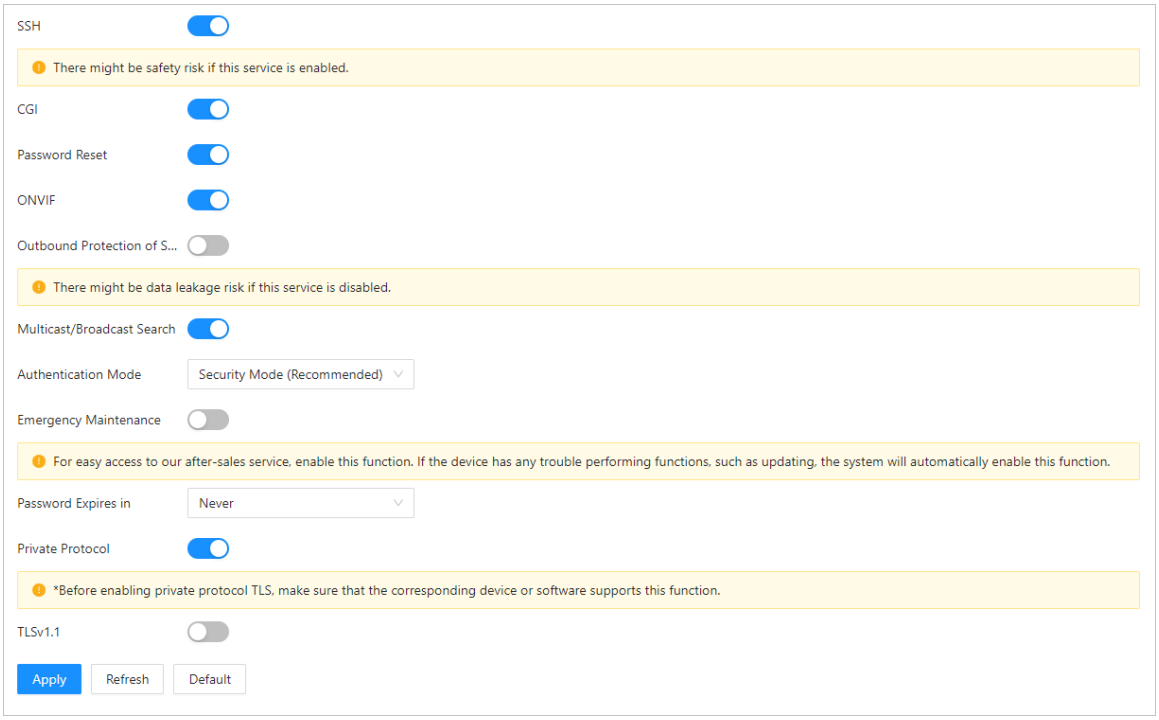


Table 4-8 Description of basic services

Service	Description
SSH	Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. If enabled, SSH provides cryptographic service for the data transmission. It is not enabled by default.
CGI	Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs similarly to console applications running on a server that dynamically generates web pages. If enabled, CGI commands can be used. The CGI is enabled by default.
Password Reset	If enabled, after configure the e-mail address, you can reset the password. This function is enabled by default.
ONVIF	Enable other devices to pull video stream of the device through the ONVIF protocol.
Outbound Protection of Service Password	If enabled, the login password of the device cannot be obtained through the protocol.
Multicast/Broadcast Search	Enable this function, and then when multiple users are previewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
Authentication Mode	• **Security Mode (Recommended)** : The mode does not support logging in with Digest, DES and plain text authentication. • **Compatibility Mode** : The mode supports logging in with Digest, DES and plain text authentication.

Service	Description
Emergency Maintenance	We recommend you enable this function for faults analysis and maintenance.
Password Expires in	Configure the time. The system will remind you to change the password before the password expires. If you select **Never**, the system never reminds you to change the password.
Private Protocol	If enabled, the platform can access to the device with private protocol.
TLSv1.1	⚠ There is security risk if you enable **TLSv1.1**.

4.7 System Management

4.7.1 Configuring Video Parameters

Log in to the webpage of the device, and then select **System** > **Video**.

📖

Only VTA250*X*G Series support this function.

Table 4-9 Parameters description

Parameter		Description
Video Standard		• PAL: The default stream frame rate is 25 fps. • NTSC: The default stream frame rate is 30 fps.
Main Stream	Compression	Select the compression mode depending on the actual bandwidth. • H.264: Main profile compression. • H.265: Main profile compression occupies smaller bandwidth than H.264 in the same image quality.
	Resolution	Select the resolution.
	Frame Rate (FPS)	The number of frames that appears within a second. Higher FPS refers to more vivid and smoother image.
Sub Stream	Compression	Select the compression mode depending on the actual bandwidth. • H.264: Main profile compression. • H.265: Main profile compression occupies smaller bandwidth than H.264 in the same image quality.
	Resolution	Select the resolution as needed.
	Frame Rate (FPS)	The number of frames that appears within a second. Higher FPS refers to more vivid and smoother image.

Bit Rate

Figure 4-18 Bit rate

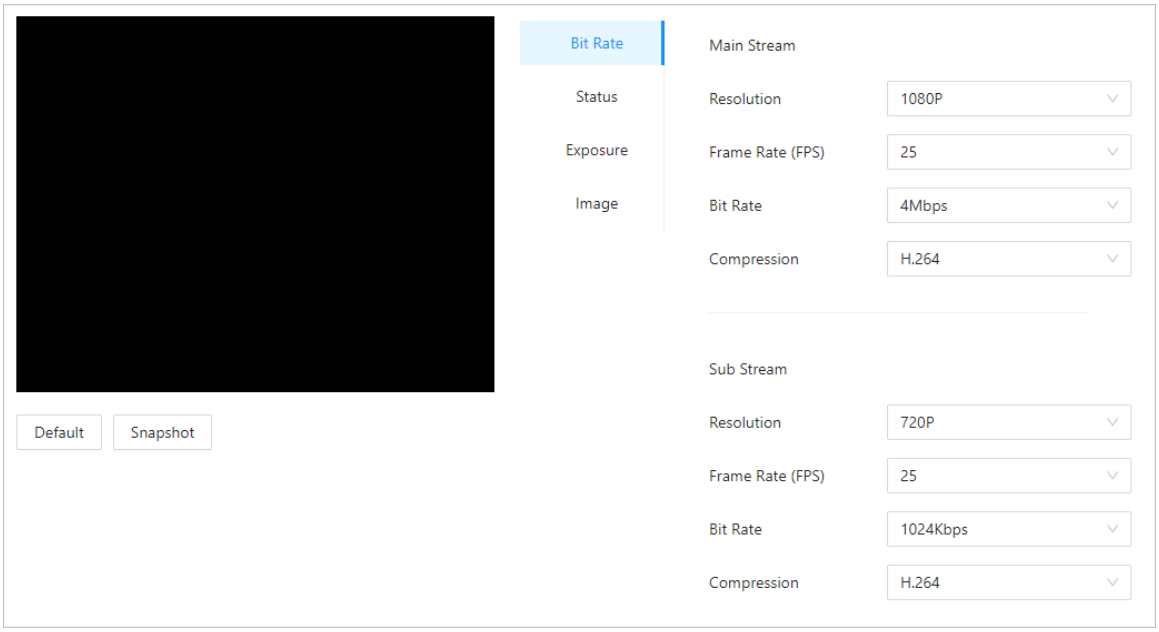


Table 4-10 Description of bit rate parameters

Parameter		Description
Main Stream	Resolution	Select the resolution. When the emergency call terminal is connected with the VTH as a VTO, the resolution is limited to 720P. If you select **1080P**, the intercom and monitoring function will be affected.
	Frame Rate (FPS)	The number of frame in one second of video.
	Bit Rate	Select the bit rate according to the actual situation.
	Compression	Select from **H.264** and **H.265**. Compared with H.264, H.265 requires smaller bandwidth.
Sub Stream	Resolution	Select the resolution.
	Frame Rate (FPS)	The number of frame in one second of video. Select from 1 to 25.
	Bit Rate	Select the bit rate according to the actual situation.
	Compression	Select from **H.264** and **H.265**. Compared with H.264, H.265 requires smaller bandwidth.

Status

Figure 4-19 Status

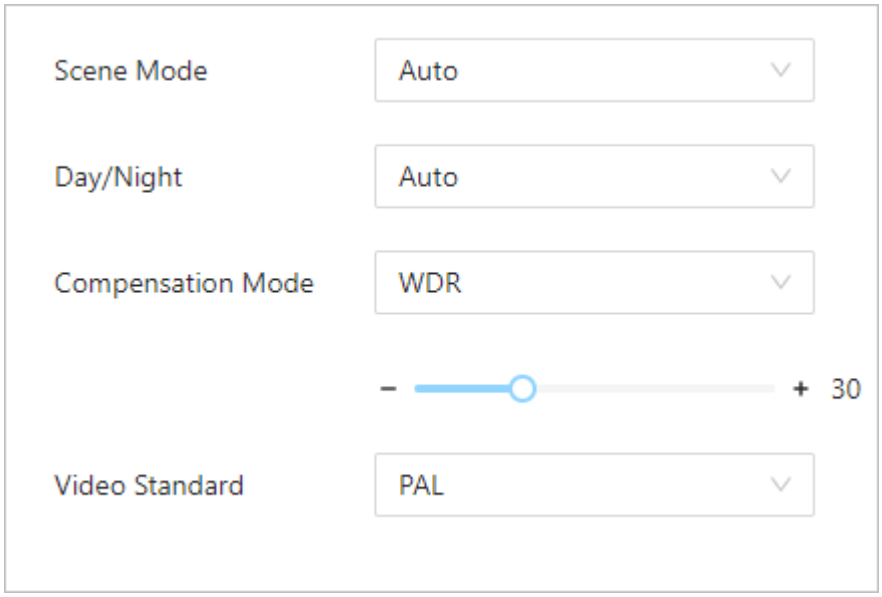


Table 4-11 Description of status parameters

Parameter	Description
Scene Mode	Different modes determine the color tone. It is **Auto** by default. • **Disable** : The mode is not configured. • **Auto** : Adjust the scene mode to display the image according to the actual situation. • **Sunny** : The image color is darker. • **Night** : The image color is lighter.
Day/Night	• **Auto** : The system switches between color and black-and-white according to actual situation. • **Color** : The system displays the image in color. • **B/W** : The system displays black-white image.
Compensation Mode	• **Disable** : There will be no backlight. • **BLC** : The system gets a clearer image of the dark areas on the target when shooting against light. • **WDR** : The system dims bright areas and compensates for dark areas to ensure the clarity of all areas. • **HLC** : The system dims strong lights, and reduce the size of Halo zone to lower the brightness of the whole image. We recommend you select **WDR** for backlight.
Video Standard	Select from **PAL** and **NTSC**.

Exposure

Figure 4-20 Exposure

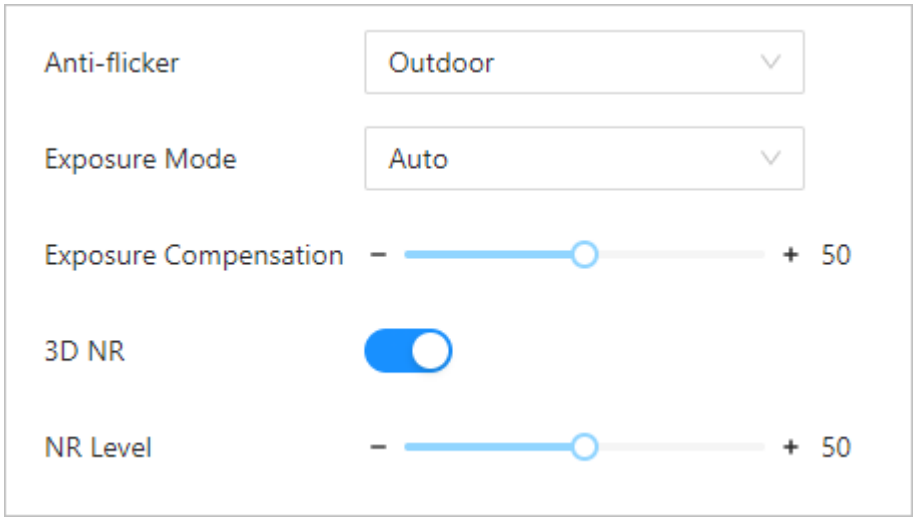


Table 4-12 Description of exposure parameters

Parameter	Description
Anti-flicker	• **50Hz** : The system adjusts the exposure according to ambient light automatically to ensure that stripes do not appear. • **60Hz** : The system adjusts the exposure according to ambient light automatically to ensure that stripes do not appear. • **Outdoor** : If you select **Outdoor**, the exposure mode can be adjusted to display the image.
Exposure Mode	• **Auto** : Exposure is automatically adjusted according to scene brightness if the overall brightness of images is in the normal exposure range. • **Shutter Priority** : Configure the **Shutter** value. The device will adjust according to the configure value. • **Manual** : You can adjust the **Gain** and **Shutter** value manually. 📖 • If the **Anti-flicker** is set as **Outdoor**, you can select **Shutter Priority**. • Different devices support different exposure modes.
Exposure Compensation	You can set the exposure compensation value. The higher the value is, the brighter the image will be.
3D NR	Reduce the noise of multiple-frame (at least two frames) images by using inter-frame information between two adjacent frames in a video. The higher the level is, the lower the noise will be, and the larger the trailing smear will be.
NR Level	

Image

Figure 4-21 Image

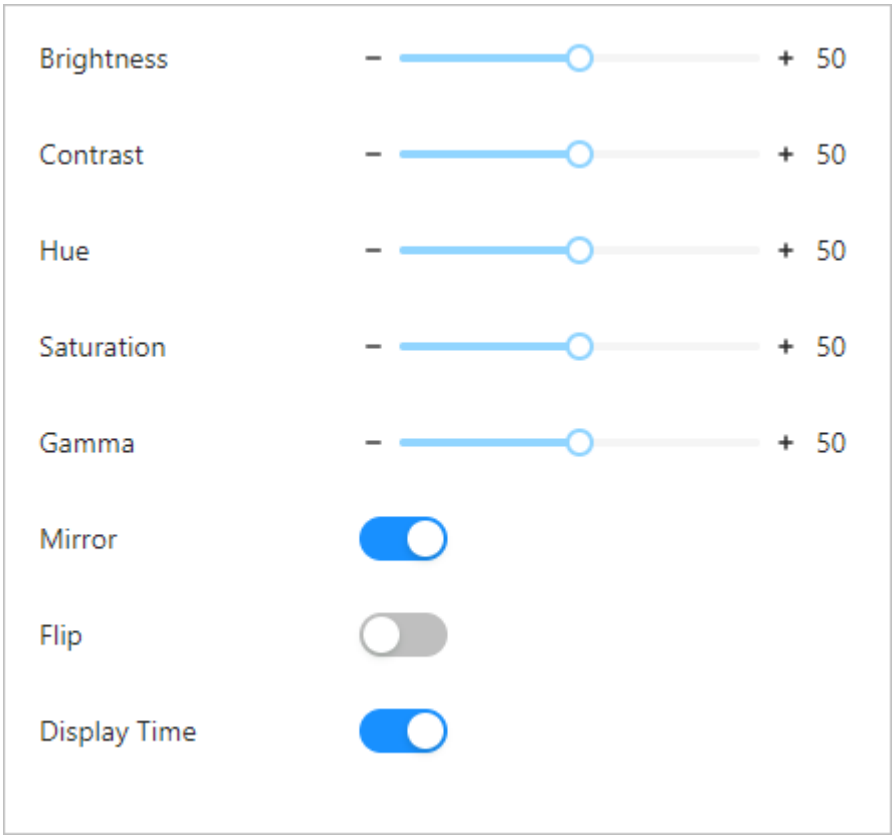


Table 4-13 Description of image parameters

Parameter	Description
Brightness	Change the overall brightness of the image. The higher the value, the brighter the image.
Contrast	Change the contrast of the image. The higher the value, the greater the contrast between bright and dark areas. If the value is too big, the dark area will be too dark and the bright area will be more vulnerable to overexposure.
Hue	Makes the color deeper or lighter. The default value is made by the light sensor, and it is recommended.
Saturation	Set the intensity of colors. The higher the value, the deeper the color. Saturation value does not change image brightness.
Gamma	Change the image brightness and contrast in a non-linear way. The higher the value, the brighter the image.
Mirror	If enabled, the image flips left and right.
Flip	If enabled, the image flips up and down.
Display Time	If enabled, the current time displays on the video image.

4.7.2 Configuring Time

You can configure date, time zone, and NTP (Network Time Protocol) server.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **System** > **Time**.

Step 3 Configure the parameters.

Figure 4-22 Configure time

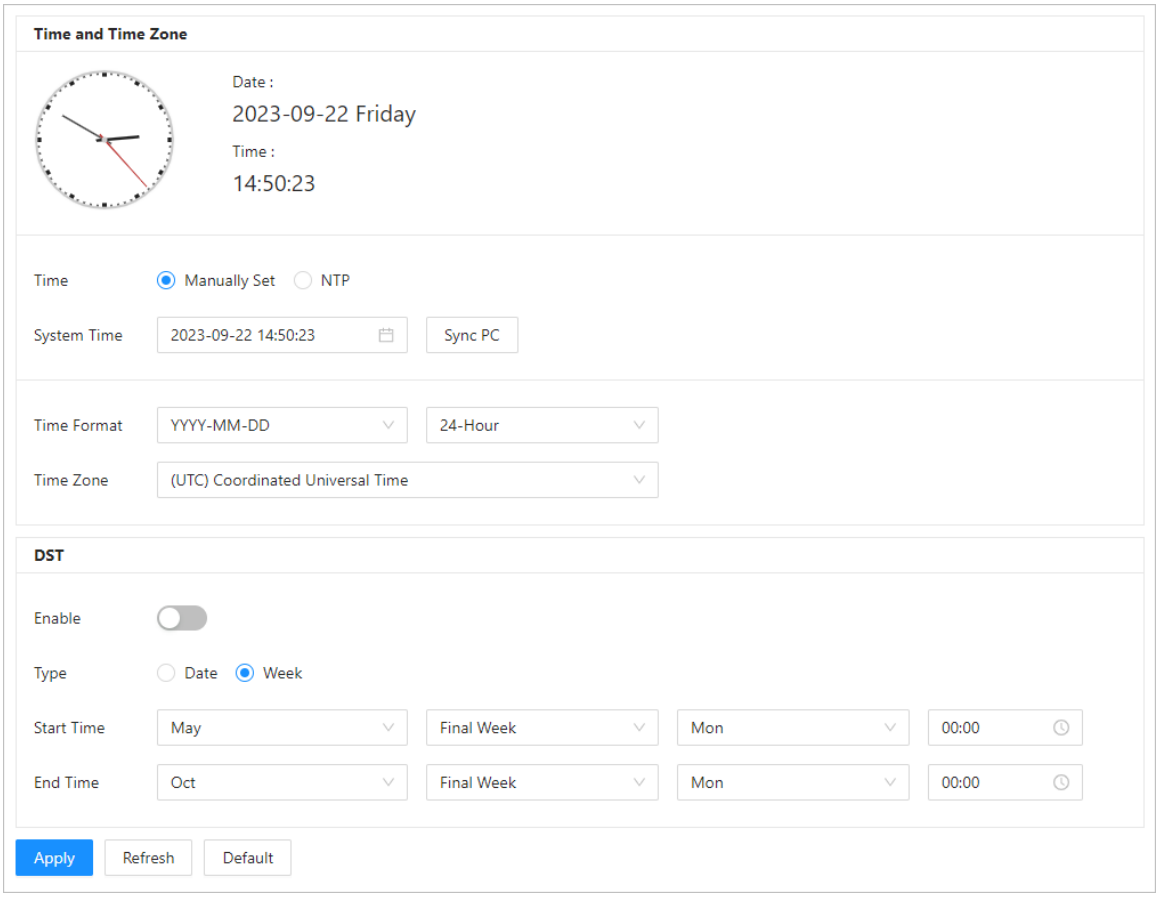


Table 4-14 Description of date and time parameters

Parameter		Description
Time and Time Zone	Time	Select **Manual Set** or **NTP**.
	System Time	If you select **Manual Settings**, configure the system time manually. Click **Sync PC**, and the system time changes to the PC time.
	Server	If you select **NTP**, the system then syncs time with the internet server in real time. You can also enter the IP address, port, and interval of a PC running NTP server to use NTP.
	Port	
	Interval	

Parameter		Description
	Time Format	Select the time format.
	Time Zone	Configure the time zone that device is at.
DST	Enable	If the area where the device is at use DST, enable it.
	Type	Select the type from **Date** and **Week**, and then configure the start time and end time for DST.
	Start Time	
	End Time	

Step 4 Click **Apply**.

4.7.3 Adding ONVIF User

ONVIF users are used for ONFVIF protocol.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **System** > **ONVIF User**.

Step 3 Click **Add**, and then configure the parameters.

Figure 4-23 Add ONVIF user

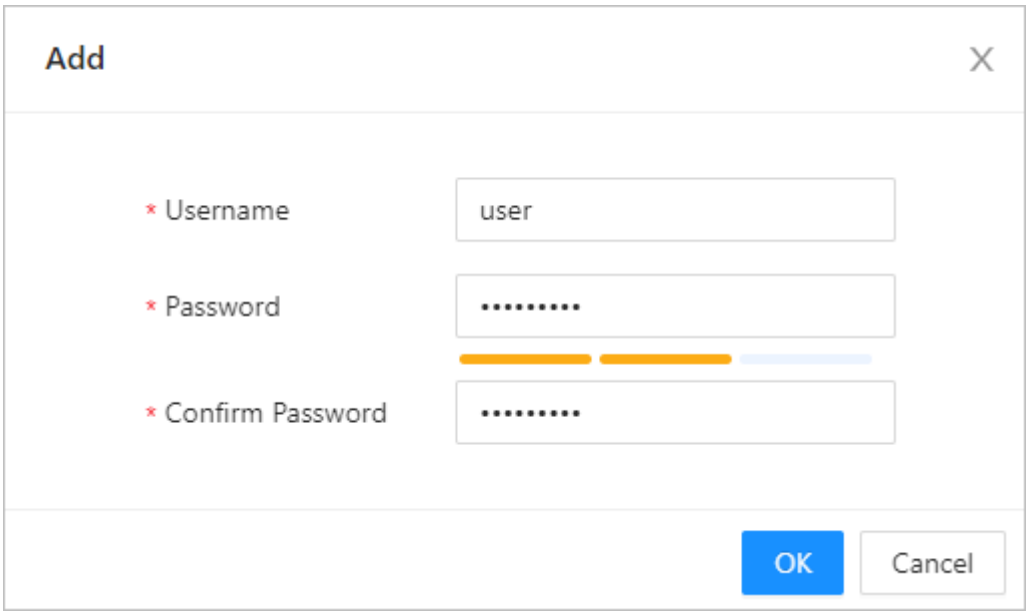


Table 4-15 Description of ONVIF user parameters

Parameter	Description
Username	The user name is unique. Username consists of up to 31 characters, including numbers, letters, underlines, dots and @.
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case, lower case, numbers, and special characters (excluding ' " ; : &).
Confirm Password	

Step 4 Click **OK**.

The added ONVIF user is displayed in the list.

Related Operations

- Click to modify the username, password and the group.
- Click to delete the ONVIF user.

4.7.4 Configuring Storage

Background Information

Only VTA250*X*G Series support this function.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **System** > **Storage**.

View the status and capacity of the inserted SD card.

Step 3 (Optional) If the inserted SD card cannot be recognized, click **Format Storage Card**.

Step 4 Configure the parameters, and then click **Apply**.

Figure 4-24 Storage

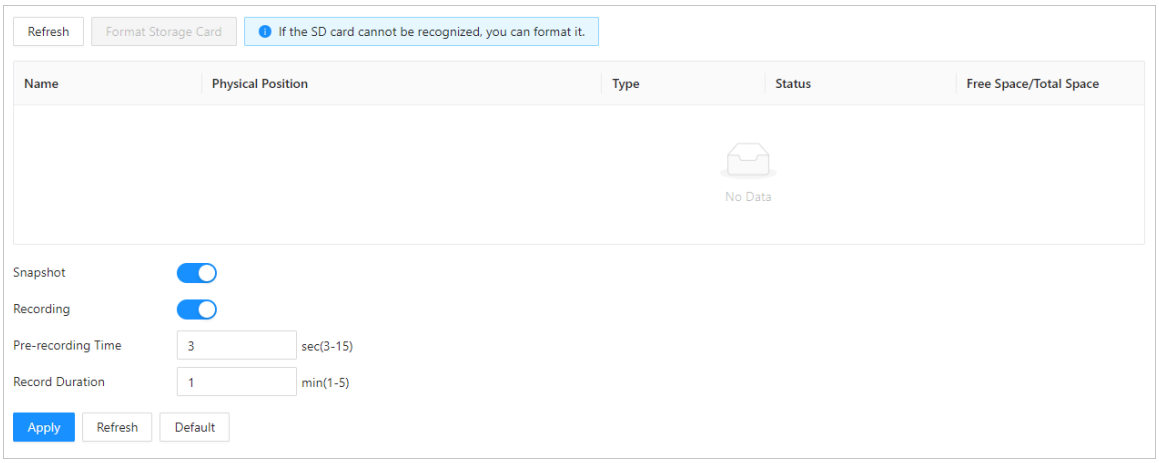


Table 4-16 Storage parameters description

Parameter	Description
Snapshot	If enabled, when the alarm is triggered, the device takes the snapshot. When the event occurred, the device takes one snapshot.
Recording	If enabled, when the alarm is triggered, the device starts recording. When the event occurred, the device starts recording.
Pre-recording Time	The value is 3 s by default. The device starts recording 3 s before the event is detected.

Parameter	Description
Record Duration	The value is 1 min by default. Each recording time will be within 1 min.

4.8 Maintenance Center

4.8.1 One-click Diagnosis

Detect the configurations and status of the device to improve the performance.

Procedure

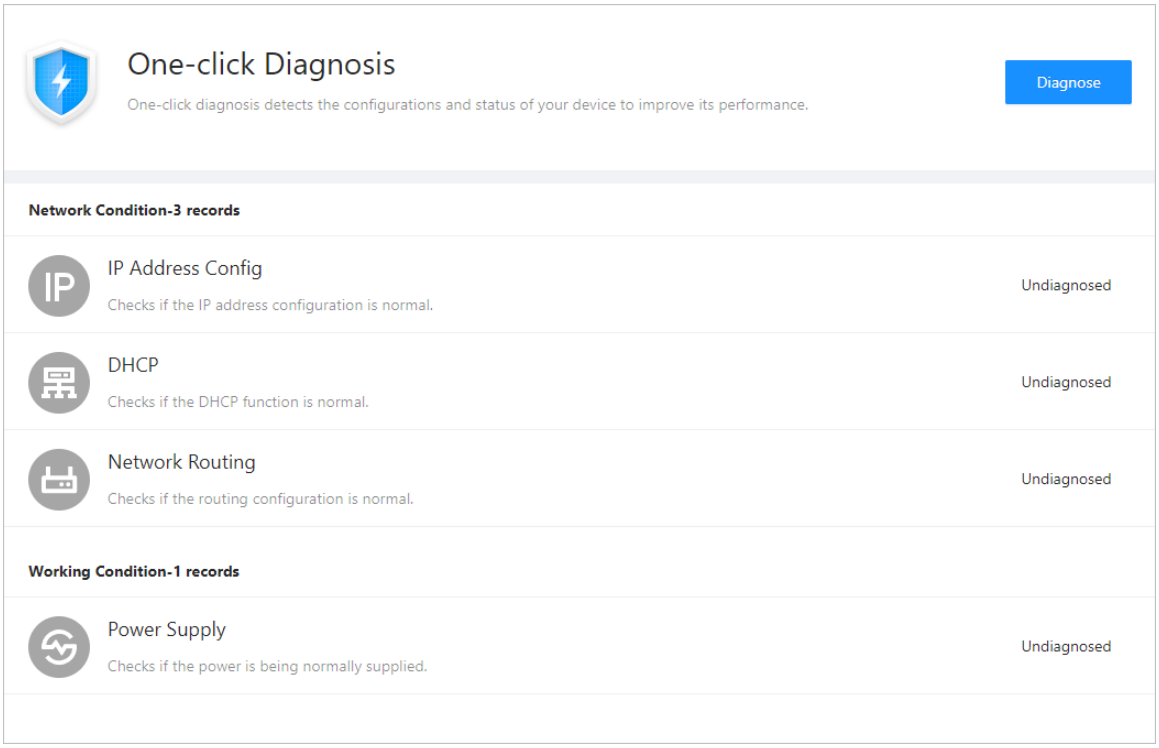
Step 1 Log in to the webpage of the device.

Step 2 Select **Maintenance Center** > **One-click Diagnosis**.

Step 3 Click **Diagnose**.

Click **Diagnose Again** if it is not the first time to diagnose.

Figure 4-25 Diagnose



4.8.2 System Information

Log in to the webpage of the device. Select **Maintenance Center** > **System Info**. Click **Legal Info** to view the software license agreement, privacy policy and open source software notice. Click **System Info** to view the basic information of the device, including device model and version information.

4.8.3 Log

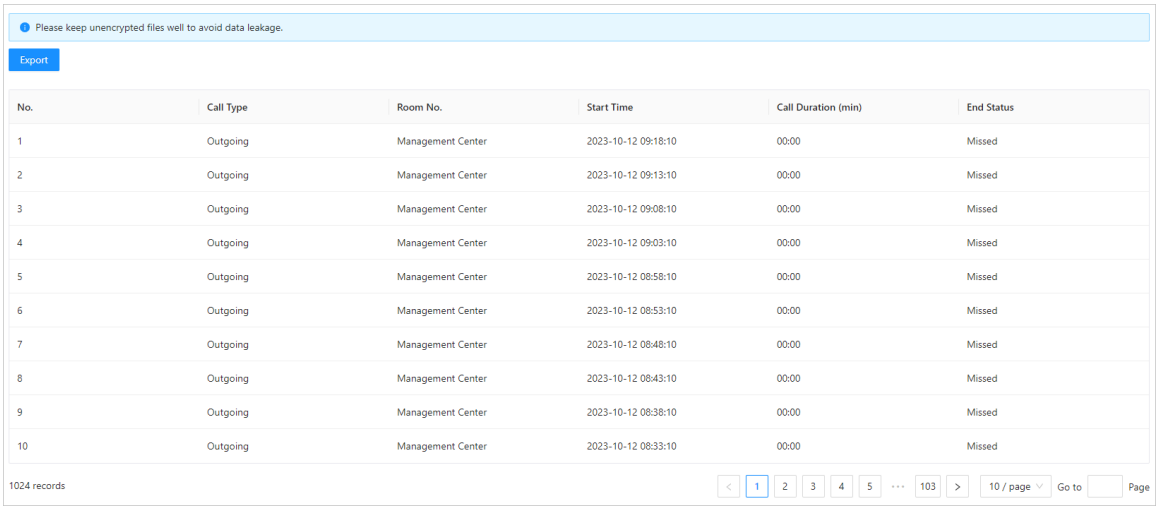
4.8.3.1 Viewing the Call History

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Maintenance Center** > **Log** > **Call History** to view the call records.

Figure 4-26 Call history



Step 3 (Optional) Click **Export** to export the call records.

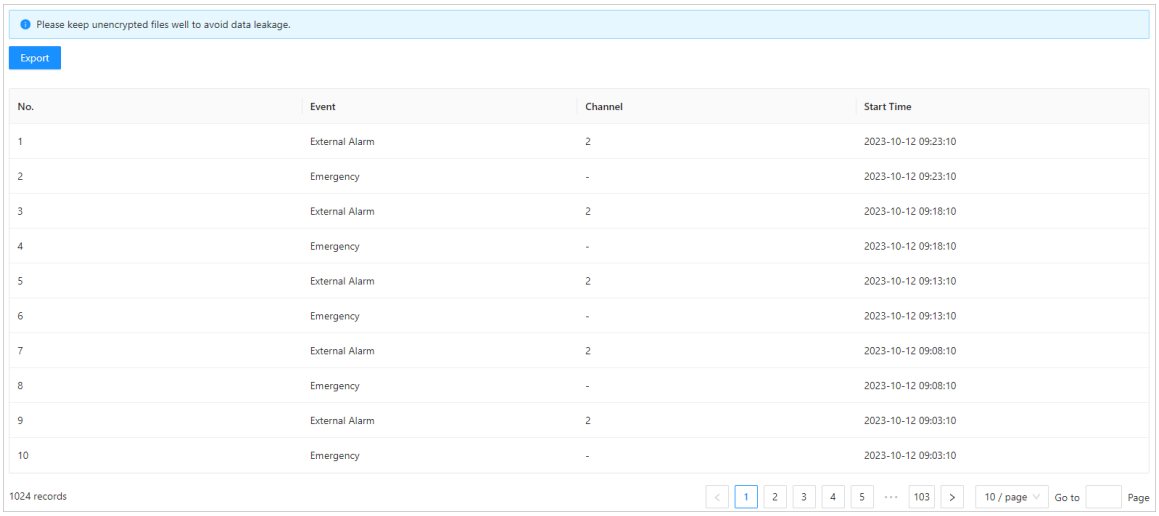
4.8.3.2 Viewing the Alarm Logs

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Maintenance Center** > **Log** > **Alarm Logs**.

Figure 4-27 Alarm log



Step 3 (Optional) Click **Export** to export the alarm records.

4.8.3.3 Viewing the System Logs

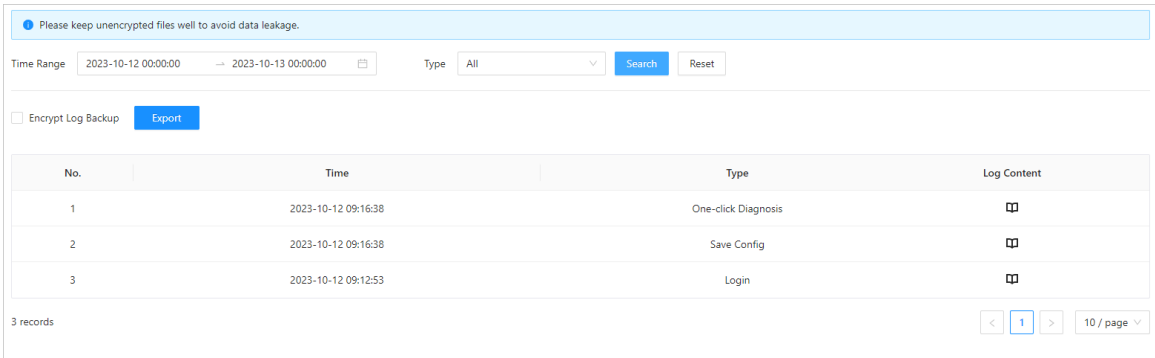
Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Maintenance Center** > **Log** > **Log**.

Step 3 Select the time range and the log type, and then click **Search**.

Figure 4-28 System log



Related Operations

- Click **Export** to download the results to your computer.

  If you enable **Encrypt Log Backup** and enter the password before you export the log, you need to enter the password to open the exported file.

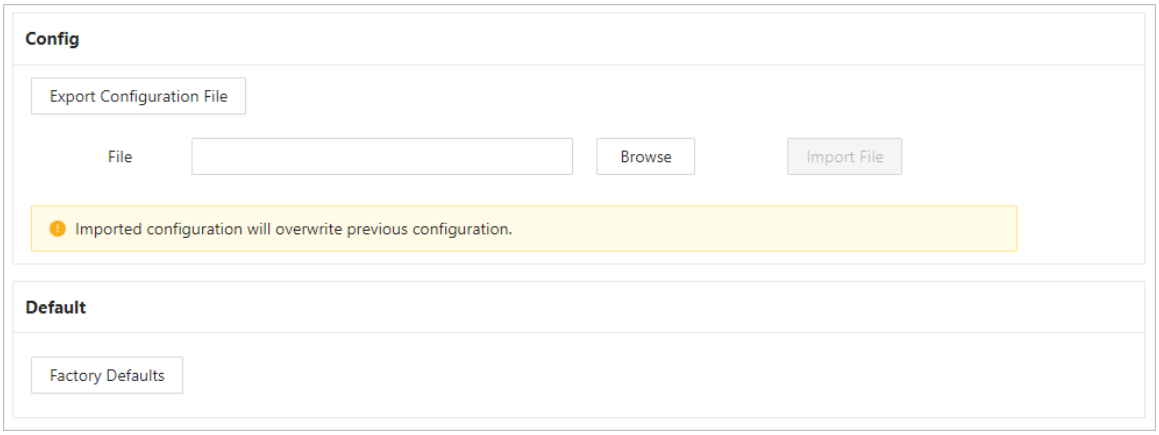
- Click  to view the details of the log.

4.8.4 Management

4.8.4.1 Configuration

Log in to the webpage of the device. Select **Maintenance Center** > **Manager** > **Config**.

Figure 4-29 Configuration



4.8.4.1.1 Exporting/Importing the Configuration File

Export or import the configuration file. When you need the same configurations on many devices, you can use the exported configuration file.

Export Configuration File

Click **Export Configuration File**, download the file to your computer.



The IP address will not be exported.

Import Configuration File

1. Click **Browse**, select the configuration file.
2. Click **Import File**.



The configuration file must be imported to the devices with the same model. After importing, the device restarts.

4.8.4.1.2 Restoring to Factory Defaults



Restoring the device to default configurations will cause data loss. Please be advised.

Click **Factory Defaults** , enter the login password, and then click **OK**. Restore all settings to default except for IP address.

4.8.4.2 Maintenance

Configure the time for automatic restart to maintain the device performance.

Procedure

Step 1 Log in to the webpage of the device.

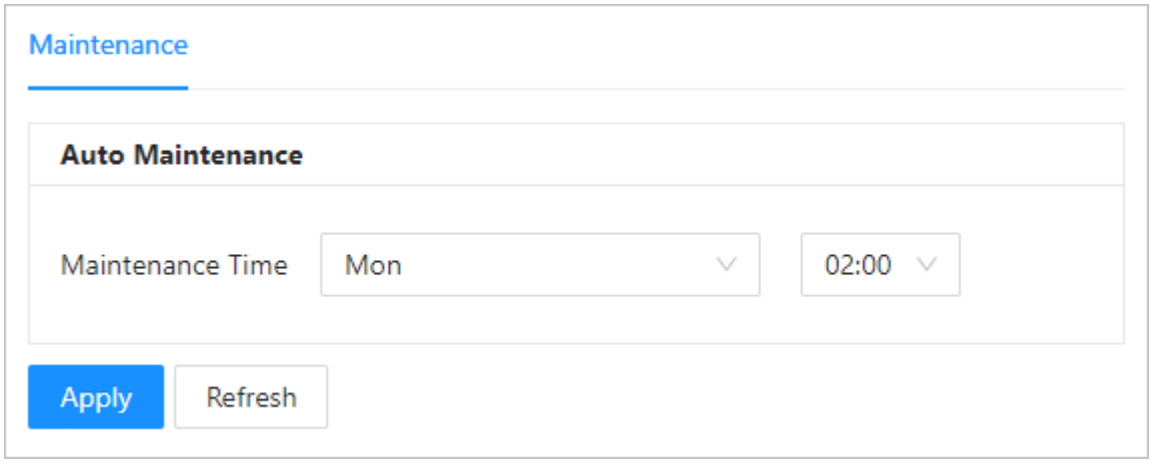
Step 2 Select **Maintenance Center** > **Manager** > **Maintenance**.

Step 3 Select the maintenance time, and then click **Apply**.



The default maintenance time is 2:00 every Tuesday.

Figure 4-30 Maintenance



4.8.5 Update

- Do not disconnect the power supply or network, or restart or shut down the device during the update.
- Use the correct update file. Make sure that you get the correct update file from the technical support.
- Rollback to lower versions will cause potential security risk. Please be cautious.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Maintenance Center** > **Update**.

Step 3 Select the update type.

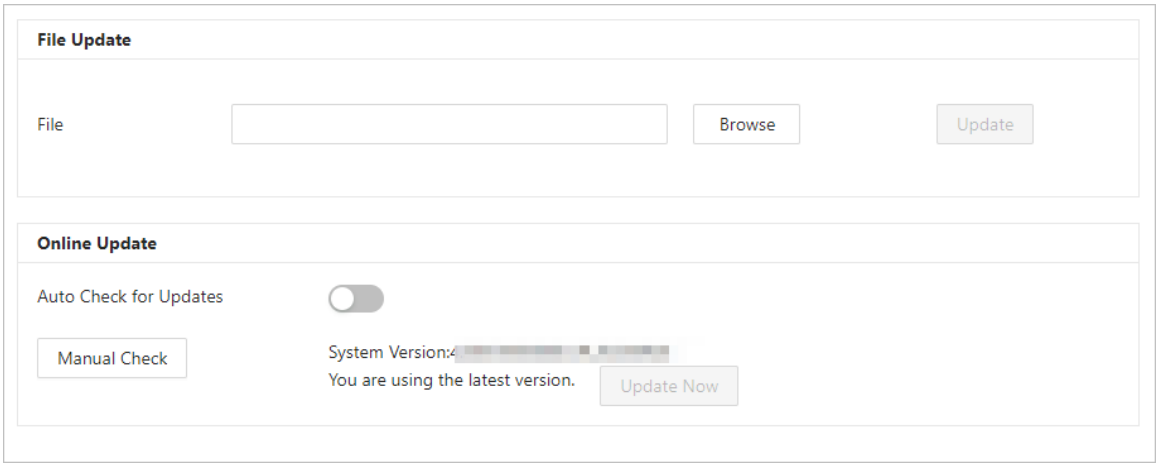
- File update
  1. Click **Browse**, and then select the update file.

     The update file should be a .bin file.
  2. Click **Update**.
- Online update

  Check the new version automatically or manually, and then click **Update**.
  - **Auto Check for Updates** : If enabled, the system checks the version every day. There will be prompt if the system detects the new version.

    In order to inform you of updating automatically, we will collect the IP address, device name, serial number, firmware version and other information. The information is only used for verification and update notification.
  - **Manual Check** : Click **Manual Check** to detect the new version.

Figure 4-31 Update



4.8.6 Advanced Maintenance

Get the device information and packet data for troubleshooting.

Export

Log in to the webpage of the device, select **Maintenance Center** > **Advanced Maintenance** > **Export**, and then click **Export** to export the serial number, firmware version, device operation logs and configuration information.

Packet Capture

1. Log in to the webpage of the device.
2. Select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.
3. Enter the IP address, and then click ▶.

   The icon becomes ⏸.
4. After you get the data, click ⏸.
5. The data will be automatically saved to your computer.

Figure 4-32 Packet capture



4.9 Searching Record

Only VTA250*X*G Series support this function.

Procedure

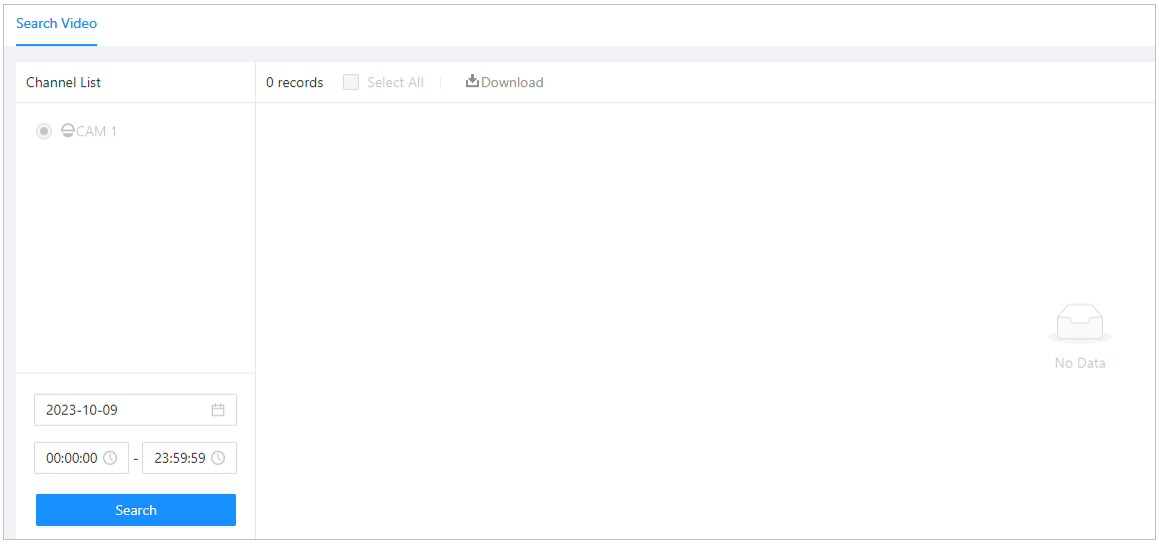
Step 1 Log in to the webpage of the device.

Step 2 Click **Record**.

Step 3 Select the time, and then configure **Search**.

You can only view the daily records.

Figure 4-33 Record



Related Operations

- Select the files, and then click **Download** to save the files to your computer.
- Click **Select All** , and then click **Download** to download all files.

4.10 Searching Picture

Only VTA250*X*G Series support this function.

Procedure

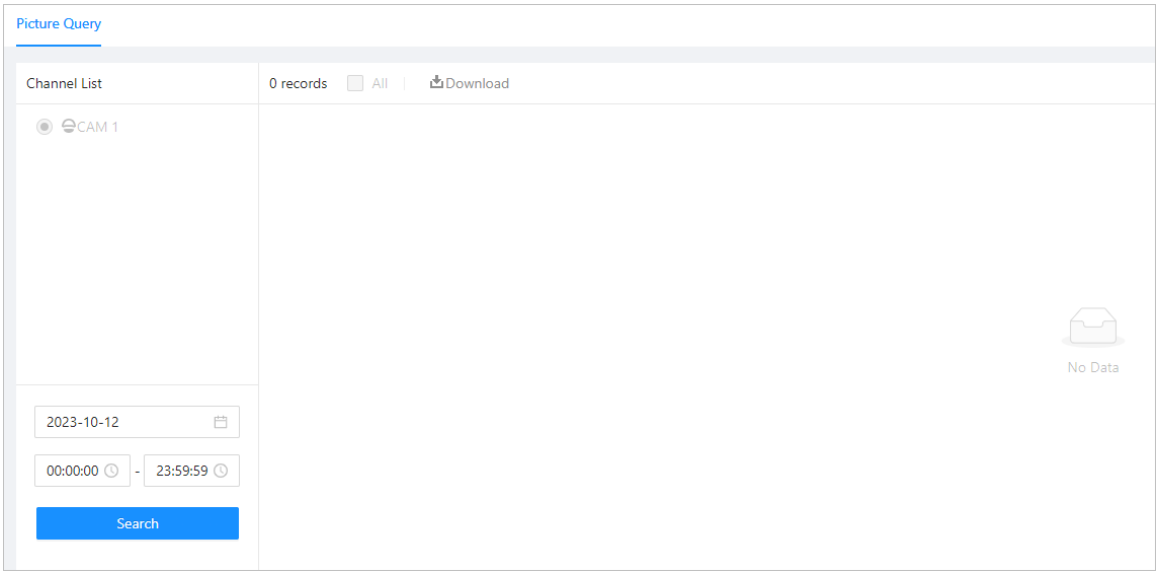
Step 1 Log in to the webpage of the device.

Step 2 Click **Picture**.

Step 3 Select the time, and then configure **Search**.

You can only view the daily pictures.

Figure 4-34 Picture



Related Operations

- Select the files, and then click **Download** to save the files to your computer.
- Click **Select All** , and then click **Download** to download all files.

4.11 Security

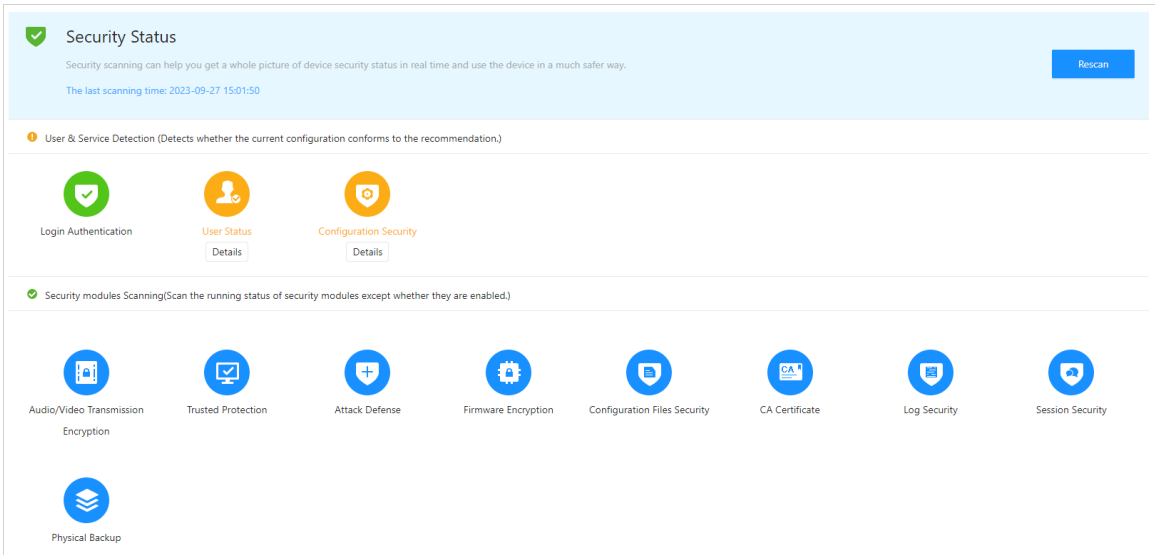
4.11.1 Security Status

Detect and check the security status of the device.

Log in to the webpage of the device. Select > **Security Status**. Click **Scan** to scan the security status of the device.

Click **Rescan** if it is not the first time to scan.

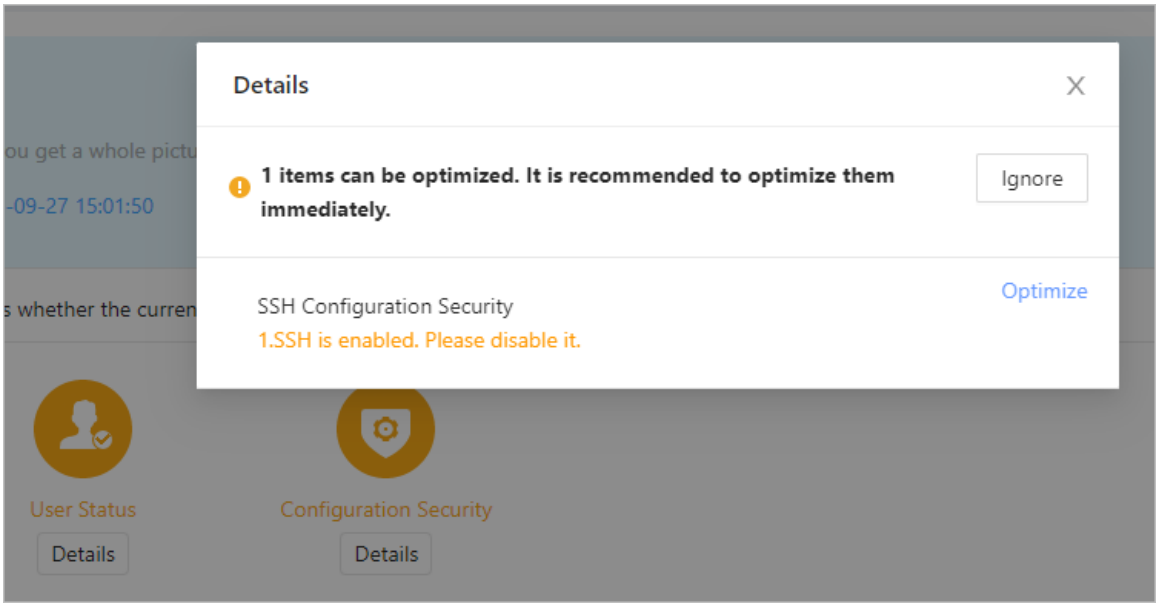
Figure 4-35 Security status



User & Service Detection

- If the configuration of the detection item conforms to the recommendation, the icon is green.
- If the detection item needs to be optimized, the icon is yellow. Click **Details** to view the details of the scanning result. Click **Ignore** to ignore the exception, and it will not be scanned in next scanning.

Figure 4-36 Details



- If the detection item will not be scanned, the icon is grey. Click **Start Detection** to include the detection item in next scanning.

Hover over the detection item to view the configuration of the current detection.

Security Modules Scanning

Hover over the security module icon to view the operating status.

4.11.2 Configuring System Service

Background Information

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with your PC. The HTTPS can protect page authenticity on all types of websites, secure accounts, and keep user communications, identity, and web browsing private.

We recommend you enable the HTTPS. Otherwise, the device data may be leaked.

Procedure

Step 1 Log in to the webpage of the device.

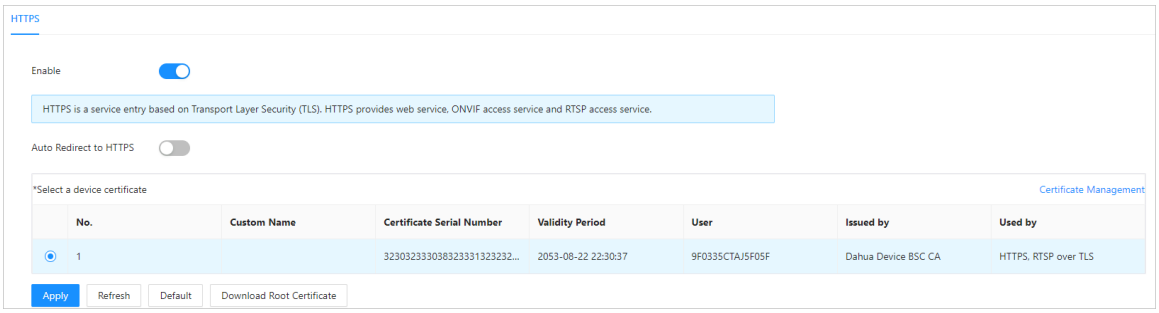
Step 2 Select > **System Service**.

Step 3 Click to enable HTTPS.

Step 4 Select the certificate.

If there is no certificate in the list, click **Certificate Management**. For details, see "4.11.4 Configuring CA Certificate".

Figure 4-37 HTTPS



Step 5 Click **Apply**.

Results

Enter https://*IPaddress: https port* in the browser.

- If you have already installed the certificate, the normal login page will be displayed.
- If you have not installed the certificate, the browser displays a certificate error message.

4.11.3 Attack Defense

4.11.3.1 Configuring Firewall

Configure firewall to limit access to the device.

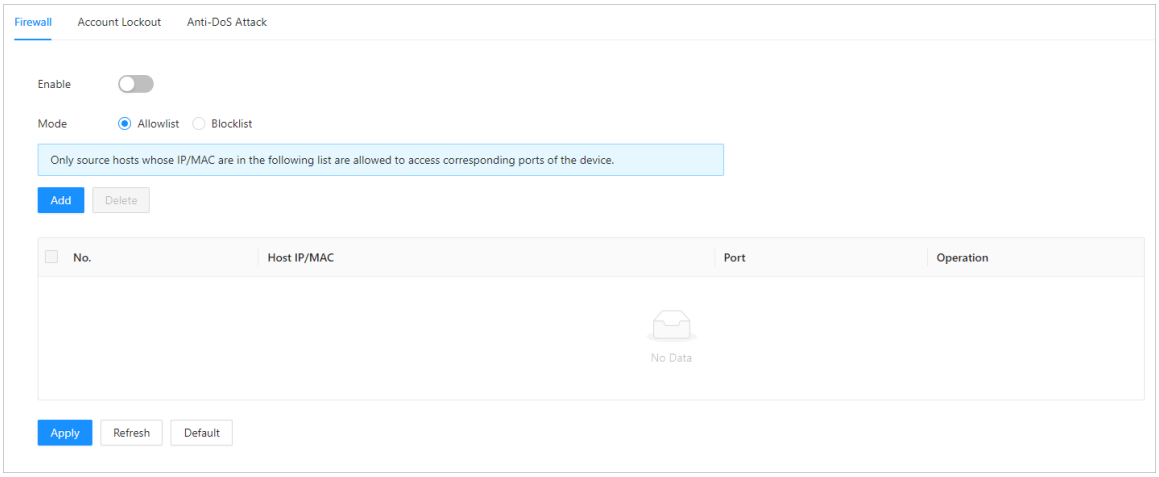
Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select > **Attack Defense** > **Firewall**.

Step 3 Click to enable the firewall function.

Figure 4-38 Firewall

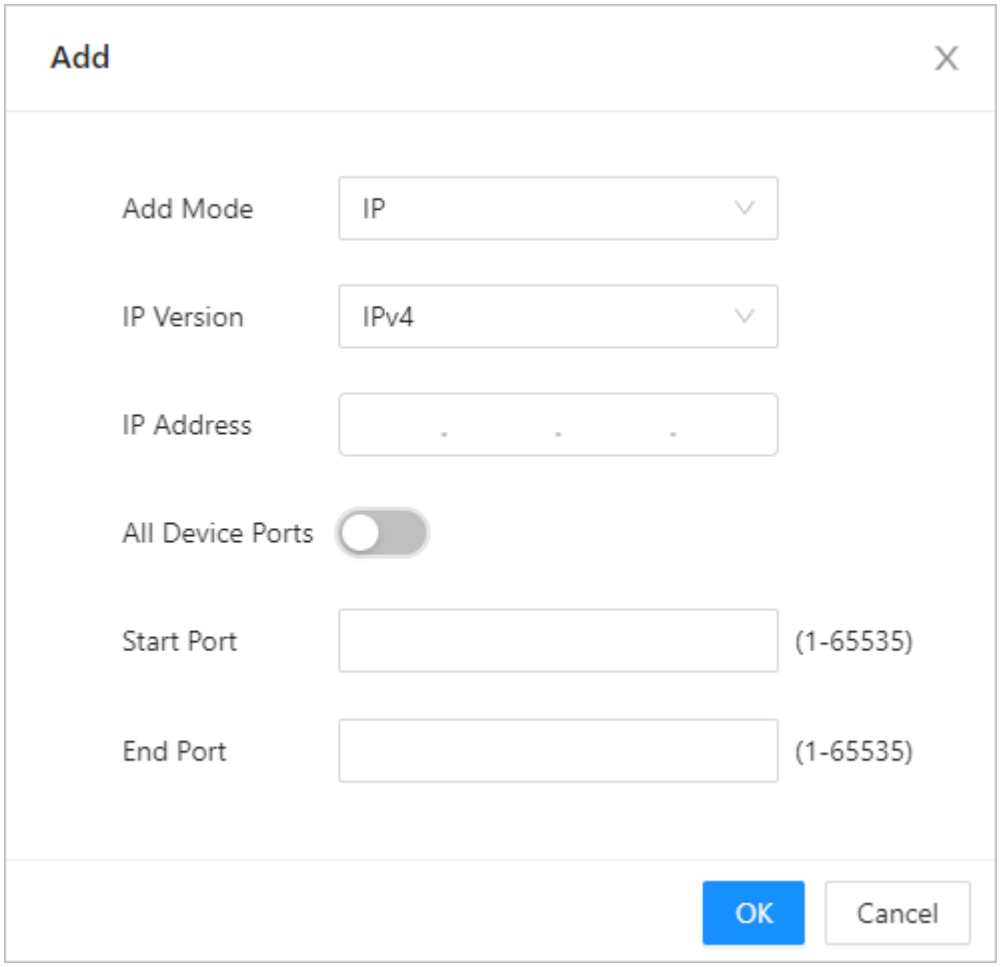


Step 4 Select **Allowlist** or **Blocklist** as the mode.

- Allowlist: Only when the IP/MAC address of your PC is in the allowlist, can you access the device. Ports are the same.
- Blocklist: When the IP/MAC address of your PC is in the blocklist, you cannot access the device. Ports are the same.

Step 5 Click **Add** to add the host IP/MAC address to **Allowlist** or **Blocklist**, and then click **OK**.

Figure 4-39 Add the address



Step 6 Click **Apply**.

Related Operations

- Click to edit the host information.
- Click to delete the host information.

4.11.3.2 Configuring Account Lockout

If you consecutively enter a wrong password more than the configured value, the account will be locked.

Procedure

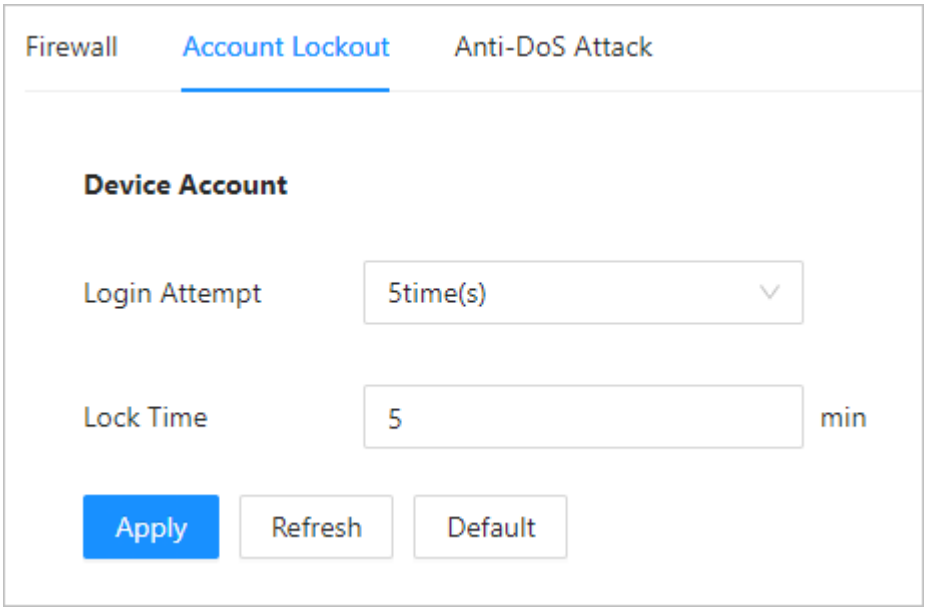
Step 1 Log in to the webpage of the device.

Step 2 Select > **Attack Defense** > **Account Lockout**.

Step 3 Configure the login attempt and lock time for device account and ONVIF user.

- Login attempt: Upper limit of login attempts. If you consecutively enter a wrong password more than the defined value, the account will be locked.
- Lock time: The period during which you cannot log in after the login attempts reaches upper limit.

Figure 4-40 Account lockout



Step 4 Click **Apply**.

4.11.3.3 Configuring Anti-DoS Attack

You can enable **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to defend the device against DoS (Denial of Service) attack.

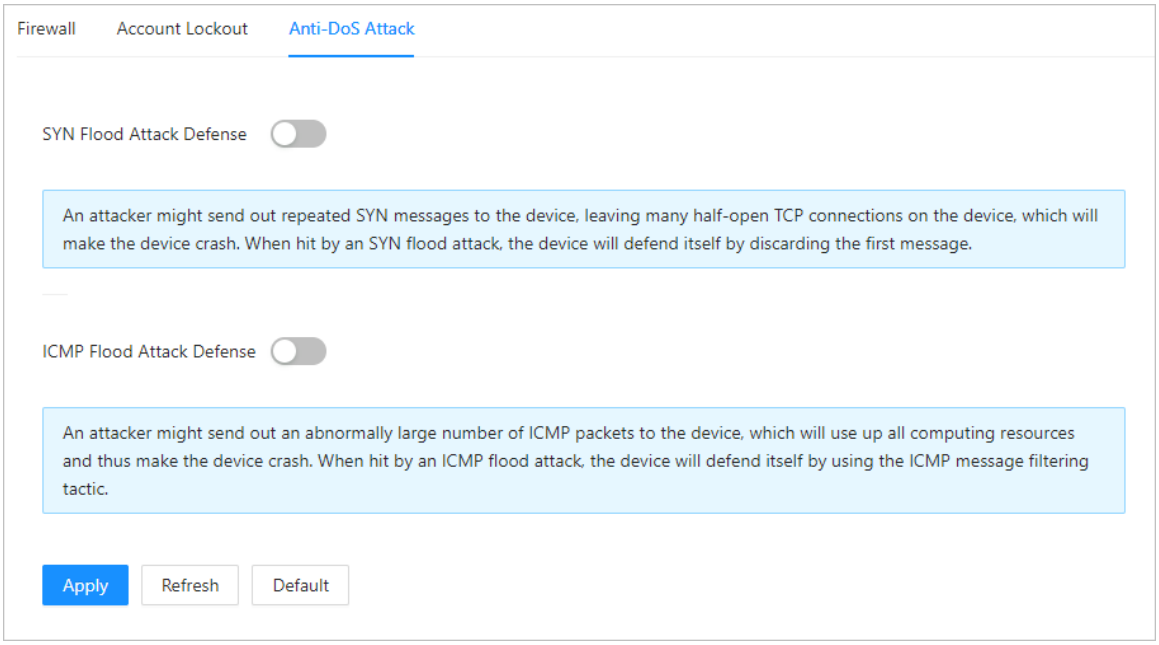
Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select > **Attack Defense** > **Anti-DoS Attack**.

Step 3 Enable **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to defend the device against DoS (Denial of Service) attack.

Figure 4-41 Anti-DoS Attack



Step 4 Click **Apply**.

4.11.4 Configuring CA Certificate

4.11.4.1 Installing Device Certificate

Create a certificate or upload an authenticated certificate, for example when you log in through HTTPS with your PC, you need to verify device certificate.

4.11.4.1.1 Creating Certificate

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select > **CA Certificate** > **Device Certificate**.

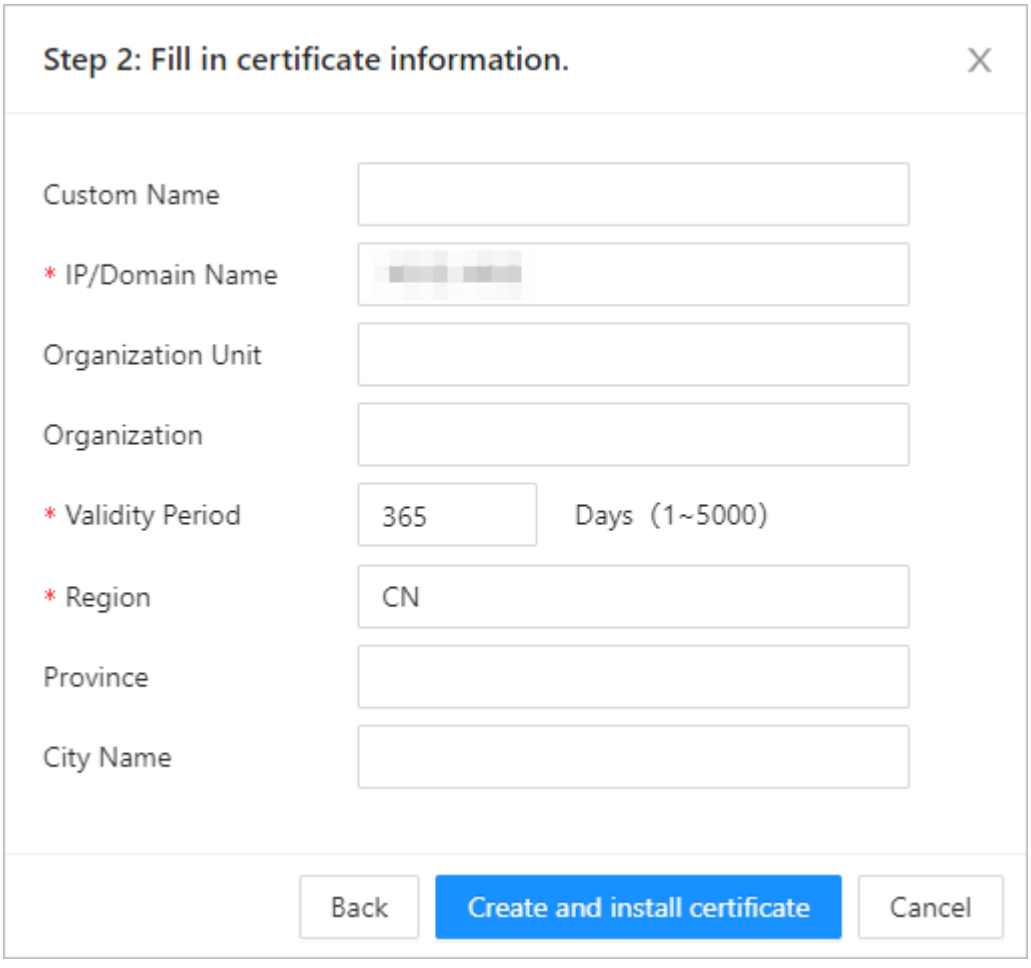
Step 3 Click **Install Device Certificate**.

Step 4 Select **Create Certificate** , and then click **Next**.

Step 5 Enter the certificate information.

IP or domain name of the device is automatically entered in **IP/Domain Name**.

Figure 4-42 Certificate information



Step 6 Click **Create and install certificate**.

After the certificate is created successfully, you can view the created certificate on the **Device Certificate** page.

Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

4.11.4.1.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the device.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select > **CA Certificate** > **Device Certificate**.

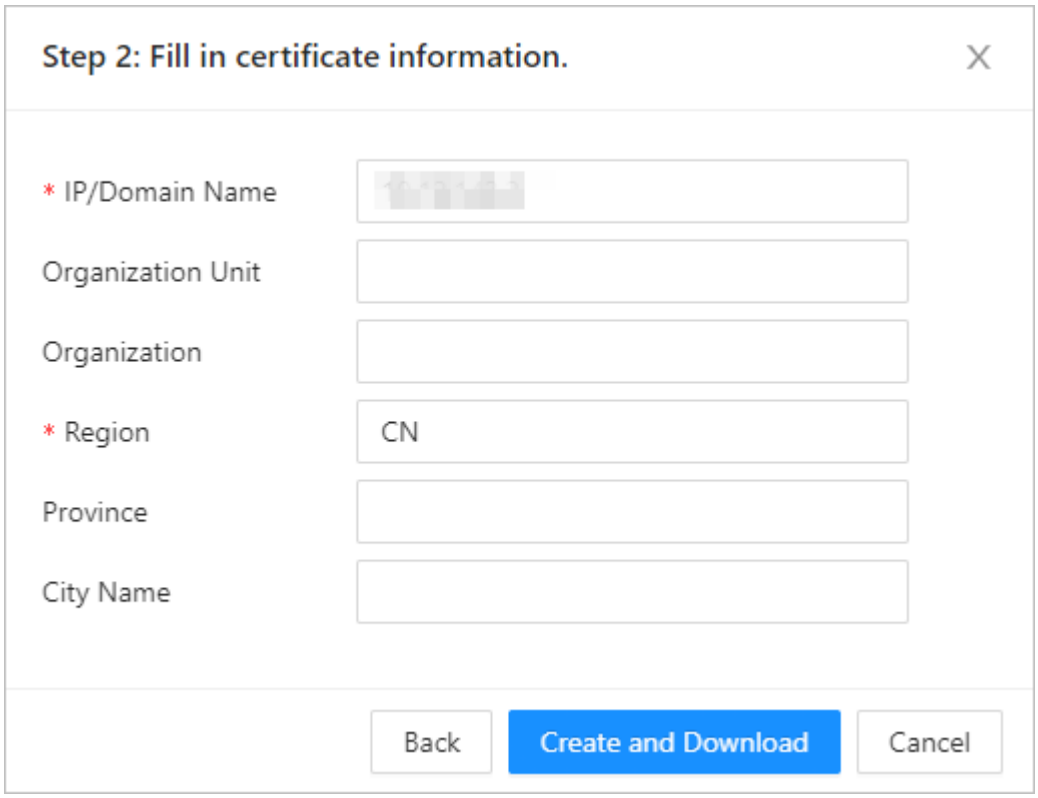
Step 3 Click **Install Device Certificate**.

Step 4 Select **Apply for CA Certificate and Import (Recommended)** , and then click **Next**.

Step 5 Enter the certificate information.

IP or domain name of the device is automatically entered in **IP/Domain Name**.

Figure 4-43 Certificate information



Step 6 Click **Create and Download**.

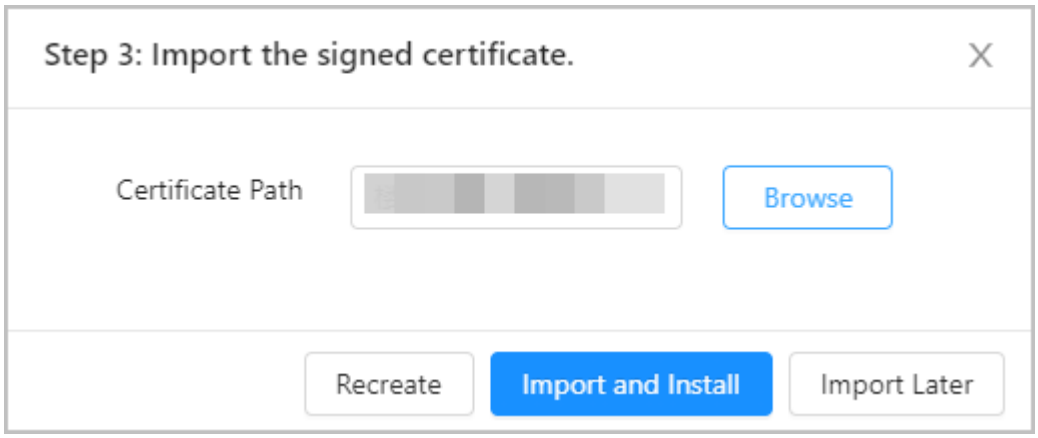
Save the request file to your PC.

Step 7 Apply for the CA certificate from the third-party certificate authority.

Step 8 Import the signed CA certificate.

1. Save the CA certificate to the PC.
2. Select **Install Device Certificate** , click **Apply for CA Certificate and Import (Recommended)**, and then click **Next**.
3. Click **Browse** to select the signed CA certificate.

Figure 4-44 Import the signed CA certificate



4. Click **Import and Install**.

   After the certificate is created successfully, you can view the created certificate on the **Device Certificate** page.

   - Click **Recreate** to create the request file again.
   - Click **Import Later** to import the certificate next time.

Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

4.11.4.1.3 Installing Existing Certificate

Import the existing third-party certificate to the device. When apply for the third-party certificate, you also need to apply for the private key file and private key password.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select > **CA Certificate** > **Device Certificate**.

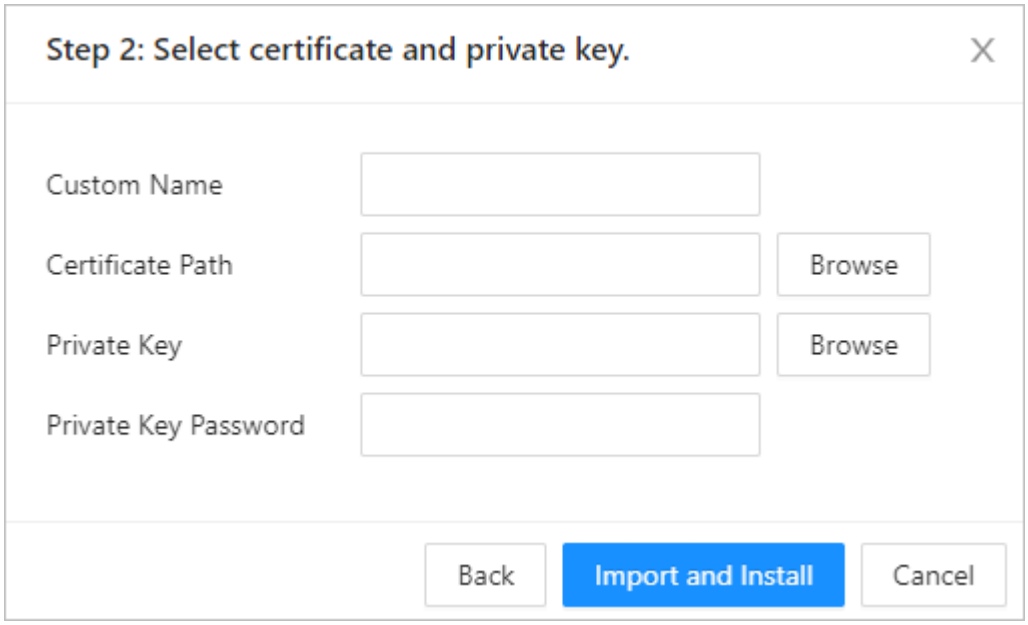
Step 3 Click **Install Device Certificate**.

Step 4 Select **Install Existing Certificate** , and then click **Next**.

Step 5 Click **Browse** to select the certificate and private key file.

Enter the private key password if the private key file is encrypted.

Figure 4-45 Certificate and private key



Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

4.11.4.2 Installing Trusted CA Certificate

CA certificate is a digital certificate for the legal identity of the camera. For example, when the camera accesses the LAN through 802.1x, the CA certificate is required.

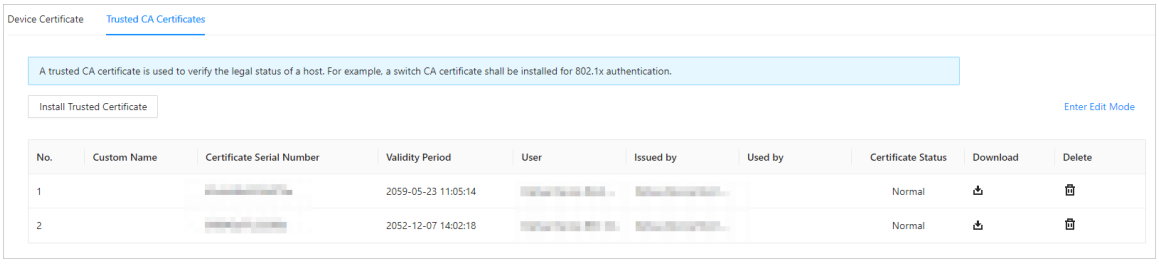
Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select > **CA Certificate** > **Trusted CA Certificate**.

Step 3 Click **Install Trusted Certificate**.

Figure 4-46 Install trusted certificate



Step 4 Click **Browse** in the pop-up window to select the certificate.

Step 5 Click **OK** to import the trusted certificate.

After the certificate is imported successfully, you can view the imported certificate on the **Trusted CA Certificate** page.

Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.

- Click to download the certificate.
- Click to delete the certificate.

4.11.5 Configuring Video Encryption

The device supports audio and video encryption during data transmission.

Background Information

We recommend you enable video encryption function. There might be safety risk if this function is not enabled.

Only VTA250*X*G Series support this function.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select > **Video Encryption**.

Step 3 Configure the parameters, and then click **Apply**.

Figure 4-47 Video encryption

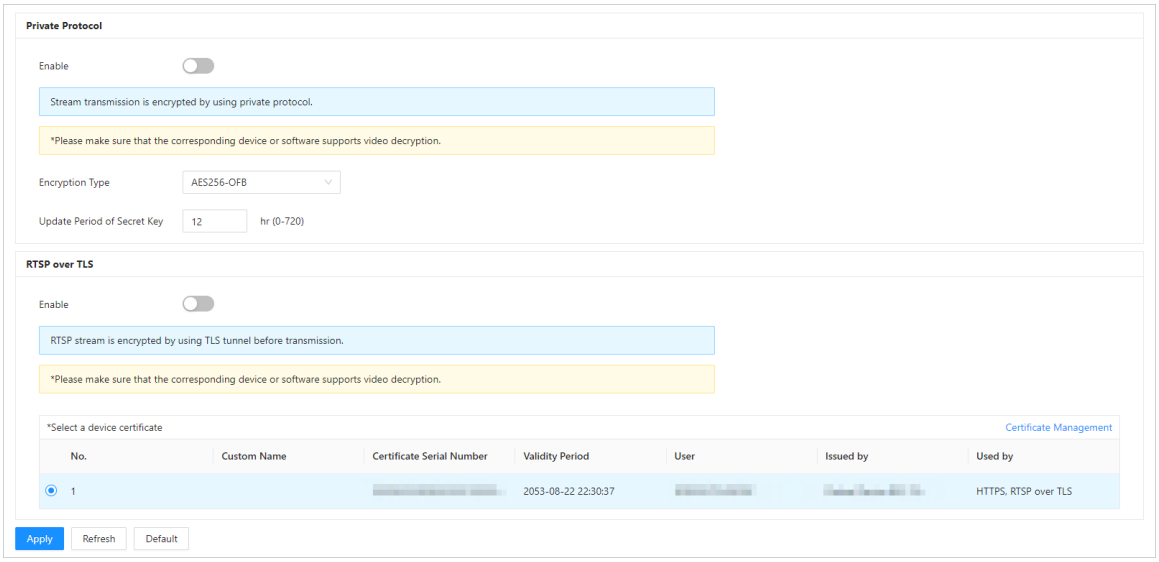


Table 4-17 Description of video encryption parameters

Area	Parameter	Description
Private Protocol	Enable	Enable stream frame encryption by using private protocol. Click to enable audio and video encryption during data transmission. Select the encryption type, and then configure update period of secret key. • **Encryption Type** : Use the default setting. • **Update Period of Secret Key** : Value range is 0–720 hours. 0 means never update the secret key.
	Encryption Type	
	Update Period of Secret Key	

Area	Parameter	Description
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. Click , and then select a device certificate from certificate list.
	Certificate Management	For details about certificate management, see "4.11.4 Configuring CA Certificate". Created certificate of imported certificate are displayed in **Select a device certificate** list.

4.11.6 Configuring Security Warning

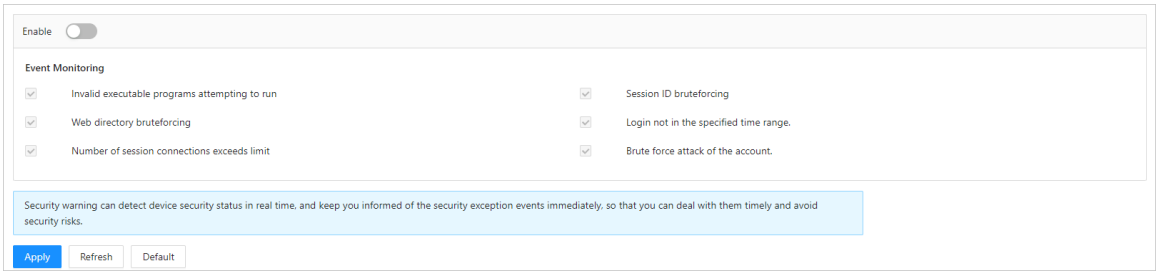
Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select > **Security Warning**.

Step 3 Enable the warning function, select the events, and then click **Apply**.

Figure 4-48 Security warning



4.11.7 Configuring Security Authentication

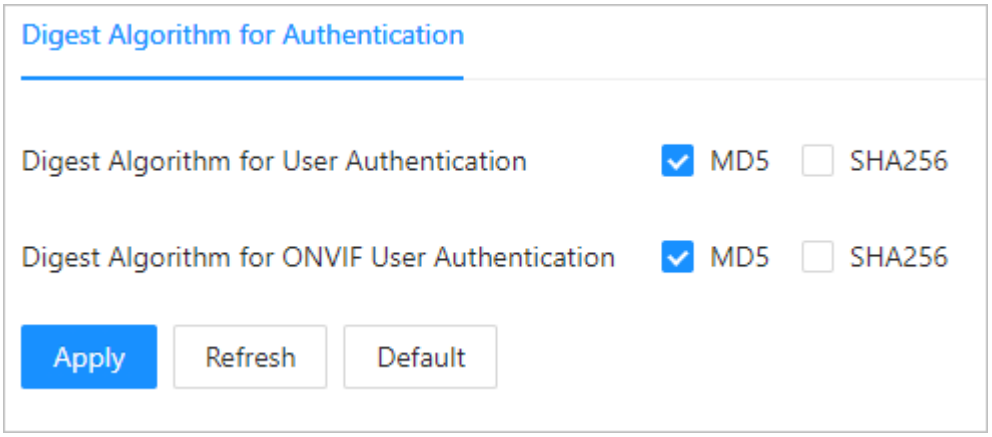
Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select > **Security Authentication**.

Step 3 Select the digest algorithms, and then click **Apply**.

Figure 4-49 Security authentication



Appendix 1 Cybersecurity Recommendations

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, 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 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, 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.

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.