

IP Speaker

User Manual



V2.2.1

Foreword

General

This manual introduces the installation, structure, web operations of the IP speaker (hereinafter as the “speaker”). Read carefully before using the device, and keep the manual safe for future reference.

Symbols

The following symbols might appear in the manual.

Symbol	Description
 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.
 TIPS	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
V2.2.1	Deleted the product models.	April 2026
V2.2.0	Updated file management and running logs.	March 2026
V2.1.0	Update project management, maintenance center, and security, and other functions.	August 2025
V2.0.0	Update the web functions.	July 2025
V1.0.0	First release.	July 2025

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

Important Safeguards 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.

Transportation Requirements



Transport the device under allowed humidity and temperature conditions.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Installation Requirements



WARNING

- 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.
- Replace unwanted batteries with new batteries of the same type and model. Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion. Dispose of the old batteries as instructed.
- Do not expose the battery to extremely hot environments, such as direct sunlight and fire, to avoid the risk of fire and 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.
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 10 cm on the sides and 5 cm on top of the device.
- Install the device on a stable surface to prevent it from falling.
- Use an adapter or cabinet power supply provided by the manufacturer.
- 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.
- Use the power cords that are recommended for the region and conform to the rated power specifications.

- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it.
- An easily accessible safety disconnect switch must be incorporated into the external power supply circuit during installation.

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.
- Use the device 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 place an open flame on the device, such as a lit candle.
- Do not disassemble the device without professional instruction.
- Operating temperature: -20°C to +60°C (-4 °F to 140 °F).

Maintenance Requirements



WARNING

Make sure you use the same model when replacing the battery to avoid fire or explosion. Dispose the battery strictly following the instructions.



The appliance coupler is a disconnection device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the device, first disconnect the appliance coupler.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Product Overview.....	1
1.1 Introduction.....	1
1.2 Features.....	1
1.2.1 Common Features.....	1
1.2.2 Different Features.....	1
2 Web Operations.....	3
2.1 Initialization and Login.....	3
2.2 Main Page.....	4
2.3 Network Settings.....	4
2.3.1 TCP/IP.....	4
2.3.2 Port.....	6
2.3.3 SIP.....	7
2.3.4 ONVIF.....	8
2.3.5 Auto Registration.....	8
2.3.6 DDNS.....	9
2.4 Project Management.....	11
2.4.1 File Management.....	11
2.4.2 Alarm Tasks.....	12
2.4.3 Audio Parameter.....	13
2.4.4 Project Task.....	14
2.5 Maintenance Center.....	15
2.5.1 System Information.....	15
2.5.2 Update.....	17
2.5.3 Log.....	17
2.5.4 Maintenance Management.....	18
2.5.5 Account Management.....	19
2.5.6 Advanced Maintenance.....	20
2.5.7 Configurations Management.....	22
2.5.8 TF Card Storage.....	23
2.6 Security.....	24
2.6.1 System Service.....	24
2.6.2 CA Certificate.....	26
Appendix 1 Security Recommendation.....	32

1 Product Overview

1.1 Introduction

Designed with aviation aluminum, the IP speaker is a strong network speaker that features voice talk, broadcasting, and storing audio files. It supports PoE, SIP, and ONVIF protocols, and can be managed on its webpage or in batches on the platform. The IP speaker is widely used for a variety of security monitoring scenarios.



Two-way talk is available on select models.

1.2 Features

1.2.1 Common Features

IP speakers have highly similar characteristics, with common features as follows:

- Made of anti-corrosion aviation aluminum.
- With its integrated design, it has a built-in network audio decoding chip, high fidelity digital operational amplifier and horn speaker.
- Supports PoE, which is convenient for on-site installation.
- Supports the standard SIP protocol, connection to SIP platforms, SIP-based intercom, and SIP-based broadcasting.
- It has a 512 MB storage capacity, and supports uploading custom audios and using TF cards for expansion.
- Supports remote management over the network, facilitating operation and maintenance.
- Built-in one-click reset button.

1.2.2 Different Features

Different products might have different features. The key differences are listed below.

IP Speaker

- With its cone-shaped corners, it is easy to control the direction of audio broadcasts. It also supports wall mount and pole mount.
- It is not suitable for corrosion-resistant environments such as seaside and chemical factories.
- Supports device registration and intercom based on the ONVIF protocol.
- With 512 MB of storage and support for custom audio, this device can be expanded using a TF card by opening the back cover.

In-Ceiling IP Speaker

- With its cylindrical structure, it supports in-ceiling mount installation. The thickness of the mounting plate can also be adjusted when installing it in the ceiling.
- Supports device registration and broadcast based on the ONVIF protocol.

IP Column Speaker

- Designed with a column structure, suitable for wall mount installation.
- Supports device registration and broadcast based on the ONVIF protocol.
- Supports 1-channel alarm signal input and 1-channel microphone audio signal input.
- When the IP column speaker is powered through PoE, the max volume level is limited to 8. For higher volume output, connect an additional 24 VDC power supply corresponding to the product label.

2 Web Operations

You can view the basic information, upload .mp3 and .wav files, configure system settings, and more.

2.1 Initialization and Login

Procedure

Step 1 Enter the IP address of the device in the browser address bar (the IP address is 192.168.1.108, and the subnet mask is 255.255.0.0 by default), and then press the Enter key.

Step 2 Set the password for the admin user.



The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters among uppercase and lowercase letters, numbers, and special characters (excluding ' ', ' ', ' ', and '&'). The confirming password must be the same as the new password.

Step 3 Click **OK**.

Step 4 Enter the user name and password, and then click **Login**.



After 5 consecutive incorrect password attempts, the account will be locked for 30 minutes.

Figure 2-1 Login

Welcome

Username

Password

Forgot password?

Login

Related Operations

If you forgot your password, click **Forgot password?**, and then follow the instructions to reset your password.

If you did not enter your email address during initialization, contact your local dealer or technical support for help.

2.2 Main Page

Figure 2-2 Main page

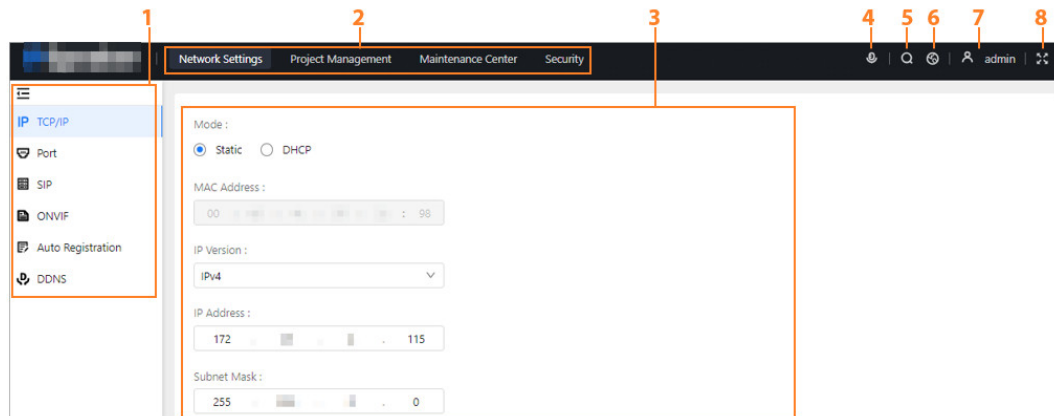


Table 2-1 Main page description

No.	Description
1	Supported functions of each function module.
2	Function module.
3	Parameters of each supported function.
4	Start talking.  This function is only available in HTTPS, and you need to plug in a microphone.
5	Quick search. Click the icon, enter the function that you want to configure, and then it will go to the page for configuring that function.
6	Language. Chinese and English (default) are supported.
7	Log out of the webpage.
8	Full-screen display. Click the icon again, or press the Esc key to exit full screen.

2.3 Network Settings

2.3.1 TCP/IP

Set the IP address, DNS server and other parameters of the IP speaker to make sure that the IP speaker can connect to other devices on the network.

Procedure

Step 1 Select **Network Settings** > **TCP/IP**.

Figure 2-3 TCP/IP

Mode :

☒ Static ☐ DHCP

MAC Address :

00 : [] [] [] [] [] : 4f

IP Address :

172 . [] [] [] []

Subnet Mask :

255 . [] [] [] []

Default Gateway :

172 . [] [] [] []

Preferred DNS :

8 . [] [] [] []

Alternate DNS :

8 . [] [] [] []

Step 2 Configure the parameters.

Table 2-2 TCP/IP parameters

Parameter	Description
Mode	Select a network mode. ● Static : Manually assign a fixed IP address, subnet mask and gateway. It provides consistent and predictable access. This option is useful if you have specific requirements for port forwarding or network settings. ● DHCP : Automatically obtains the IP address, subnet mask and gateway from a DHCP server. This simplifies network setup and eliminates the need for manual configuration. It allows the IP speaker to adapt to changes in the network, such as IP conflicts or changes in the DHCP server.
IP Address	Enter IP address of the IP speaker.
Subnet Mask	Specify the mask for the subnet that the camera is located on. The subnet prefix is a number in the range from 1 to 255. The subnet prefix identifies a specific network link and usually contains a hierarchical structure.
Default Gateway	Set a default gateway on the same network segment as the IP address as needed.
Preferred DNS	IP address of preferred DNS and alternate DNS.
Alternate DNS	 When the preferred DNS server failed to respond, the alternate DNS server will work.

Step 3 Click **Apply**.

2.3.2 Port

Ports allow the IP speaker to establish network connections and transfer data between the IP speaker and other devices on the network.

Procedure

Step 1 Select **Network Settings > Port**.

Figure 2-4 Port

The screenshot shows a configuration window titled 'Port'. It contains four input fields, each with a label, a value, and a range in parentheses:

- Max Connection :** 128 (1-128)
- TCP Port :** 37777 (1-65534)
- HTTP Port :** 80 (1-65534)
- RTSP Port :** 554 (1-65534)

At the bottom of the window are three buttons: **Apply** (blue), **Refresh** (light blue), and **Default** (light blue).

Step 2 Configure port parameters.

Table 2-3 Description of port parameters

Parameter	Description
Max Connection	The maximum number of concurrent connections that a server, application, or service can handle at any given time. The value is 128 by default.
TCP Port	Transmission Control Protocol (TCP) helps direct traffic for specific applications or services on a computer or network. The value is 37777 by default.
HTTP Port	Hypertext transfer protocol port. The value is 80 by default.
RTSP Port	Real time streaming protocol port, and the value is 554 by default.

Step 3 Click **Apply**.

2.3.3 SIP

Session Initiation Protocol (SIP) is a signaling protocol widely used for initiating, maintaining, and terminating real-time sessions that include voice, video, and messaging applications over IP networks.

Procedure

Step 1 Select **Network Settings** > **SIP**.

Figure 2-5 SIP

Enable : ☒

Mode : ☒ IP Address ☐ Domain

SIP Server IP :

SIP Server Port : (1-65534)

SIP Server Username :

SIP Server Password :

Step 2 Configure the parameters.

Table 2-4 SIP parameters

Parameter	Description
Mode	Select IP Address or Domain mode, which means devices communicate through SIP using IP address or domain.
SIP Server IP	Enter the IP address of SIP server when IP Address mode is selected.

Parameter	Description
SIP Server Domain Name	Enter the domain name of SIP server when Domain mode is selected.
SIP Server Port	The port of SIP server.
SIP Server Username	The user name for logging in to the SIP server.
SIP Server Password	The password for logging in to the SIP server.

Step 3 Click **Apply**.

2.3.4 ONVIF

ONVIF is enabled by default, which allows network devices from other manufacturers to connect to your device.

Procedure

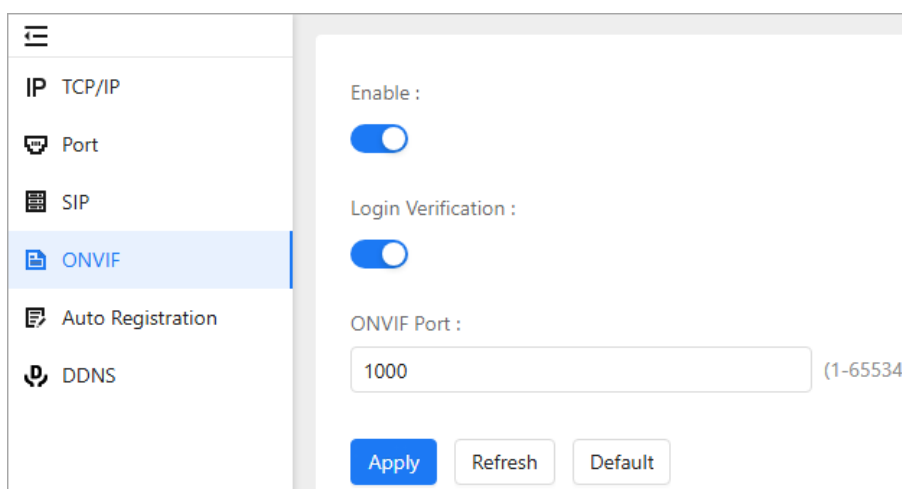
Step 1 Select **Network Settings** > **ONVIF**.

Step 2 Click  next to **Login Verification**, to ensure secure and authorized access by validating the identity of devices or systems trying to interact with ONVIF services.

Step 3 Enter the port for communication of ONVIF devices.

Step 4 Click **Apply**.

Figure 2-6 ONVIF



2.3.5 Auto Registration

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

Procedure

Step 1 Select **Network Settings** > **Auto Registration**.

Step 2 Click  to enable the function, and then configure the parameters.

Figure 2-7 Auto registration

Table 2-5 Parameter description

Parameter	Description
Server Address	The IP address or domain name of the server to be registered.
Port	The port for registration.
Sub-Device ID	The custom ID for the IP speaker.

Step 3 Click **Apply**.

2.3.6 DDNS

Properly configure DDNS, and then the domain name on the DNS server matches your IP address and the matching relation refreshes in real time. You can always visit the device with the same domain name no matter how the IP address changes.

Procedure

Step 1 Select **Network Settings** > **DDNS**.

Step 2 Enable DDNS.



- After enabling the DDNS function, third-party server might collect your device information.
- Register and log in to the DDNS website, and then you can view the information of all the connected devices in your account.

Figure 2-8 DDNS

Type :

NO-IP DDNS

Enable :

☒

After enabling DDNS function, third-party server may collect your device info.

Server Address :

dyn[REDACTED].com

Port :

80

(1-65534)

Domain Name :

none

Test

Username :

none

Password :

●●●●●●●●●●●●●●●●

Interval :

1440

min (1440-2880)

Apply

Refresh

Default

Step 3 Configure DDNS parameters.

Table 2-6 Description of DDNS parameters

Parameter	Description
Type	The name and web address of the DDNS service provider, see the matching relationship below. ● CN99 DDNS web address: www.3322.org. ● NO-IP DDNS web address: dynupdate.no-ip.com. ● Dyndns DDNS web address: members.dyndns.org.
Server Address	
Port	

Parameter	Description
Domain Name	The domain that you registered on the DDNS website.
Test	Click Test to check whether the domain name registration is successful.
Username	Enter the user name and password that you got from the DDNS server provider. You need to register an account (includes user name and password) on the DDNS server provider's website.
Password	
Interval	The update cycle of the connection between the device and the server.

Step 4 Click **Apply**.

2.4 Project Management

You can upload and manage the audio files, adjust the volume of microphone and speaker, view project tasks, and more.

2.4.1 File Management

You can upload audio files, play the audio file, and delete the files.

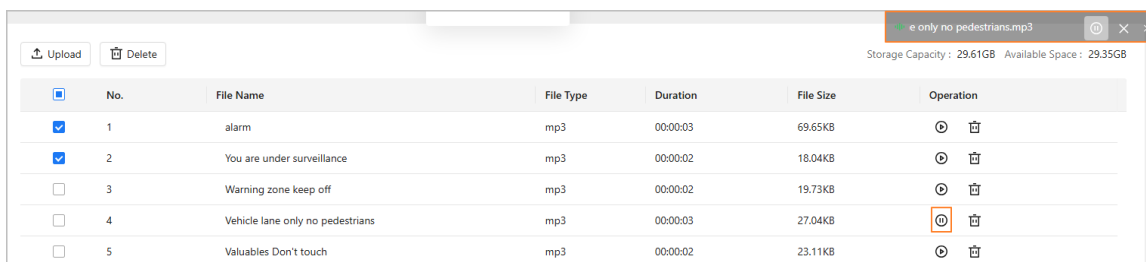
Procedure

Step 1 Select **Project Management** > **File Management**.



The page might vary depending on the product model. Refer to the actual page for details.

Figure 2-9 File management



Step 2 Click **Upload** to upload .mp3 or .wav files.



You can select multiple audio files to upload them quickly.

Step 3 Click  to play the audio file.

You can play one audio file at one time. The file being played has its status displayed in the upper-right corner of the page.

Related Operations

- Rename the audio file: Double-click the file name, and then rename it.
- Delete audio files: Click  to delete the audio file, or select files, and then click **Delete** to delete them in batches.



You cannot delete the audio file being played.

2.4.2 Alarm Tasks

When the alarm-in port generates an alarm signal, the system performs alarm linkage actions.

Background Information

This function is available on select models.

Procedure

Step 1 Select **Project Management** > **Alarm Tasks**.

Figure 2-10 Alarm tasks

Enable : ☒

Alarm-in Port :

Alarm File :

Alarm Mode :

Times Looped : time(s) (1-50)

Step 2 Click ☐ to enable the alarm task function.

Step 3 Configure the alarm parameters.

Table 2-7 Alarm parameters

Parameter	Description
Alarm-in Port	The port that generates alarms.
Alarm File	Select the audio file that will be played when an alarm is triggered. You can upload and manage the audio files from Project Management > File Management .  The selected audio file cannot be deleted but can be replaced.

Parameter	Description
Alarm Mode	• Times Looped : The alarm repeats according to the defined Times Looped. • Alarm Duration : The alarm lasts within the defined duration.

Step 4 Click **Apply**.

2.4.3 Audio Parameter

Procedure

Step 1 Select **Project Management** > **Audio Parameter**.



The audio parameter page might vary, depending on the IP speaker model.

Figure 2-11 Adjust audio parameters (IP speaker)

Microphone Volume :

Speaker Volume :

Audio Format :

Audio Sampling Rate :

Apply Refresh Default

Figure 2-12 Adjust audio parameters (IP column speaker)

Speaker Volume :

1

(0-10)

Audio Format :

G711U

Audio Sampling Rate :

8kHz

Apply

Refresh

Default

- Step 2** Move the slider of microphone or speaker to adjust the volume of microphone or speaker. The greater the value, the higher the volume.



Microphone volume adjustment is available on select models.

- Step 3** Select the audio format from the drop-down list. The default audio format is G711U.

- Step 4** Select the audio sampling rate when the **Audio Format** is set **AAC-LC**.

Audio sampling rate refers to how often per second an audio signal is sampled during analog-to-digital conversion.

- Step 5** Click **Apply**.

2.4.4 Project Task

You can view the project tasks sent from NVR.

Background Information



This function is available on select models. Please refer to the actual page.

Procedure

- Step 1** Select **Project Management** > **Project Task**.

Figure 2-13 Project task

Refresh										
No.	Status	Task Name	Task Type	Day	Start Date	Start Time	End Time	Times Looped	End Date	Operation
1	Disable	new program1	Use Once		2025-07-01	10:05:12	10:06:12		2025-07-08	🔊
2	Disable	new program2	Use Once		2025-07-01	10:07:16		1	2025-07-08	🔊
3	Enable	new program3	Use Everyday		2025-07-01	10:15:10	10:16:10		2025-07-08	🔊
4	Enable	new program4	Use Everyday		2025-07-01	10:20:00		1	2025-07-08	🔊
5	Disable	new program5	Use Once		2025-07-01	10:26:19		3	2025-07-08	🔊
6	Enable	new program6	Use Everyday		2025-06-18	15:20:00	15:30:00		2025-06-25	🔊
7	Enable	new program7	Use Every Week	Wed	2025-07-01	14:00:17	14:01:17		2025-07-08	🔊

- Step 2** View the project tasks.

- Click **Refresh** to refresh the task list.
- Click  to view the file list.

2.5 Maintenance Center

The maintenance center supports one-click diagnosis of the device status, so that technical supports can easily track and troubleshoot device issues.

2.5.1 System Information

You can view various information of the camera, including version, logs and online users, running status, and legal information.

2.5.1.1 Basic Settings

Select **Maintenance Center** > **System Info** > **Basic Settings**, and then you can rename the device.
Click **Apply** to make the settings take effective.

2.5.1.2 Version

Select **Maintenance Center** > **System Info** > **Version** to view different information of the IP speaker, including device model, serial number, web version, system version, software version, and security baseline version.

2.5.1.3 Online User

Select **Maintenance Center** > **System Info** > **Online User** to view all the online users logging in to the webpage.
Click **Refresh** to get the latest status.

2.5.1.4 Legal Information

Select **Maintenance Center** > **System Info** > **Legal Info** to view open source software notice.

2.5.1.5 Date & Time

You can configure date and time format, time zone, current time, DST (Daylight Saving Time) or NTP server.

Procedure

- Step 1 Select **Maintenance Center** > **System Info** > **Date & Time**.
- Step 2 Configure the parameters.

Figure 2-14 Date & time

Date :
2025-07-01 Tuesday

Time :
20:08:48

Time :
☒ Manual Settings ☐ NTP

System Time :
 2025-07-01 20:08:48 [Sync PC](#)

Time Format :
 YYYY-MM-DD 24-Hour

Time Zone :
 (UTC+08:00) Beijing

DST

Enable :
☐

Type :
☐ Date ☒ Week

Start Time :
 Jan Item 1 Monday 00:00

End Time :
 Jan Item 1 Tuesday 00:00

[Apply](#) [Refresh](#) [Default](#)

Table 2-8 Parameter description

Parameter	Description
Time	Select the way of setting the time from Manual Settings and NTP .
System Time	When selecting Manual Settings , you need to configure the system time. Click Sync PC , and the system time changes to the computer time.
Server	When selecting NTP , you need to enter the IP address and port number of the server, and the interval that the device will synchronize time with.
Port	
Interval	
	You can click Manual Update to update the NTP server information manually.
Time Format	Configure the time format. You can select from 12-Hour or 24-Hour .
Time Zone	Configure the time zone that the camera is at.
DST	Enable DST as needed. Click , and configure start time and end time of DST with Date or Week .

Step 3 Click **Apply**.

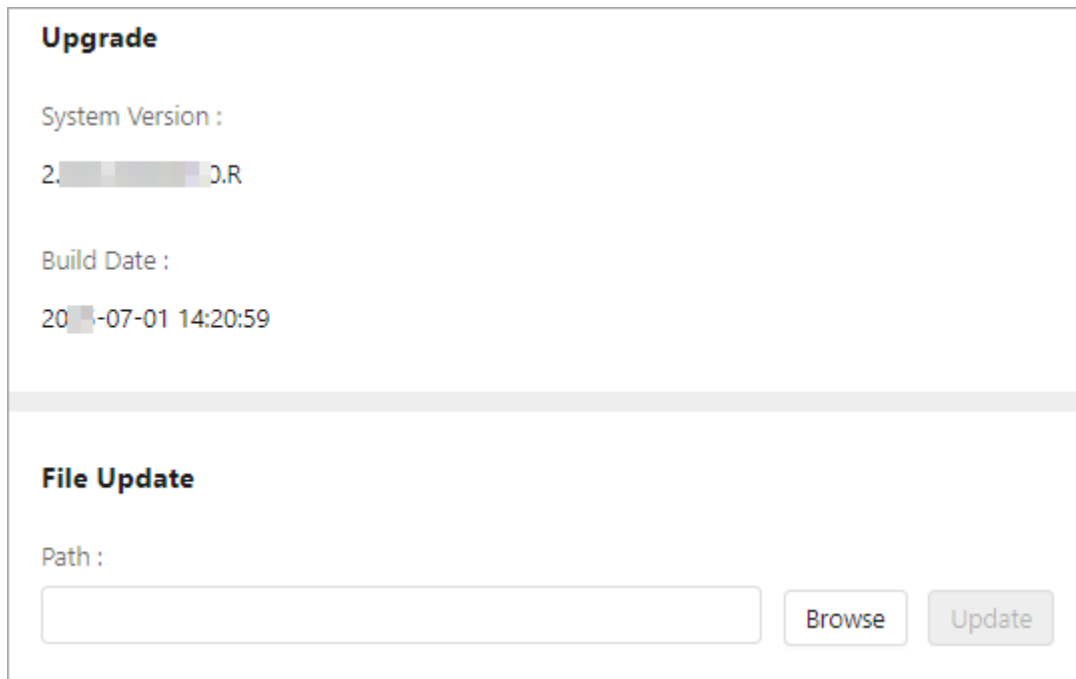
2.5.2 Update

Update the device to the latest version to improve its stability and functions. If wrong update file has been used, restart the device; otherwise some functions might not work properly.

Procedure

Step 1 Select **Maintenance Center** > **Update**.

Figure 2-15 Update



Upgrade

System Version :
2.0.0.R

Build Date :
2017-07-01 14:20:59

File Update

Path :

Step 2 Click **Browse**.

Step 3 Select the update file in .bin format.



If you use an incorrect update file and the update is in progress, restart the device manually. Otherwise, certain functions might not work properly.

Step 4 Click **Update**.

2.5.3 Log

You can search for and back up logs on the device.

Procedure

Step 1 Select **Maintenance Center** > **Log**.

Step 2 Configure the search time range, and then select the log type, which includes system, configuration, account, alarm, and file operation.



Alarm logs are available on select models.

Step 3 Click **Search**.

The search results are displayed.

Figure 2-16 Logs

Start and End Time : 2025-07-01 00:00 → 2025-07-01 23:59		Type : All	Encrypt Log Backup : ☒			Search	Backup
No.	Time	Username	Type	Operation			
1	2025-07-01 20:19:06	admin	Login				
2	2025-07-01 20:09:07	admin	Play				
3	2025-07-01 20:04:40	admin	Play				
4	2025-07-01 20:04:36	admin	Play				
5	2025-07-01 20:04:26	admin	Play				
6	2025-07-01 20:03:31	admin	Login				

Step 4 (Optional) Click or click a log, and then you can view the detailed information in the **Details** area.

Step 5 (Optional) Click **Backup**, and then you can back up all the logs that are searched for to your computer.



Enable **Encrypt Log Backup**, and then set a password to protect the log file. The password must be used when accessing the log file.

2.5.4 Maintenance Management

You can restart the device, and restore settings of the device to the default status.

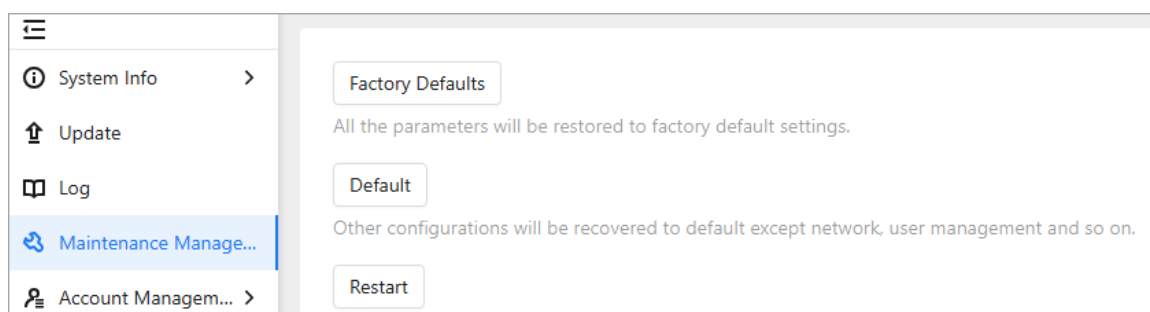
Procedure

Step 1 Select **Maintenance Center > Maintenance Management**.

Step 2 Restart the device, or restore to default settings.

- Click **Factory Defaults**, and then enter the login password. All the configurations will be restored to factory default settings.
- Click **Default**, and then all the configurations (except network, user management, and more) are restored to default settings.
- Click **Restart** to restart the device.

Figure 2-17 Maintenance management



2.5.5 Account Management

2.5.5.1 User

2.5.5.1.1 Adding User

The user is admin by default. You can add users, and configure different permissions.

Background Information

Supports up to 20 users.

Procedure

- Step 1 Select **Maintenance Center > Account Management > User**.
- Step 2 Click **Add**.
- Step 3 Configure the parameters.

Table 2-9 Description of user parameters

Parameter	Description
Username	The name that identifies the user.
Password	Enter password and confirm it again.
Confirm Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

- Step 4 Click **Apply**.

The user is displayed in the user name list.

Related Operations

- Click  to edit password, group, memo or authorities.


For admin account, you can only edit the password.

- Click  to delete the added users. Admin user cannot be deleted.


The admin account cannot be deleted.

2.5.5.1.2 Resetting Password

Enable the function, and you can reset password by clicking **Forget password?** on the login page.

Procedure

- Step 1 Select **Maintenance Center > Account Management > User**.
- Step 2 Click  next to **Password Reset**.


- Enter the email address, and then when you forgot your password, you can receive the security codes through the email address in advance to reset the password.
- If the function is not enabled, you can only reset the password by resetting the device.

Step 3 Click **Apply**.

You can now reset the password of users on the login page by clicking **Forgot password?**.

2.5.5.2 ONVIF User

ONVIF user is created by default after initialization. Only 1 ONVIF user is supported. You can edit and delete the ONVIF user.

Procedure

Step 1 Select **Maintenance Center > Account Management > ONVIF User**.

Step 2 Manage the ONVIF user.

- Click  to edit the password.
- Click  to delete the user.

2.5.6 Advanced Maintenance

It provides maintenance services for tracking and troubleshooting of network connection issues.



It is mainly used by technical support engineers for troubleshooting and other tech support.

2.5.6.1 Ping

Test whether the network can be accessed.

Procedure

Step 1 Select **Maintenance Center > Advanced Maintenance > Ping**.

Step 2 Enter the destination address, that is, the address to which a packet of data is sent over a network.

Step 3 Click **Test** to perform the network test.

Step 4 Check the test results in **Test Result**.

The following figure shows that the network is normal. If it shows **timeout**, means that the network cannot be accessed.

Figure 2-18 Network test results

Destination Address :

172 . . 115

[Test](#)

Test Result

72 bytes from 172 . . 115: icmp_seq=1 ttl=255 time< 1 ms
72 bytes from 172 . . 115: icmp_seq=2 ttl=255 time< 1 ms
72 bytes from 172 . . 115: icmp_seq=3 ttl=255 time< 1 ms
72 bytes from 172 . . 115: icmp_seq=4 ttl=255 time< 1 ms
--- 172 . . 115 ping statistics ---

Average Delay: 1ms,Packet Loss Rate: 0.00%,Network Status: OK

2.5.6.2 Running Logs

You can view the logs of device abnormality and maintenance.

Background Information



The page might vary by device model. Please refer to the actual page.

Procedure

Step 1 Select **Maintenance Center** > **Advanced Maintenance** > **Running Logs**.

Step 2 Click ☐ to enable this function.

Step 3 Select the log level, and then click **Apply**.

The following log levels are available.

- **Error** : Critical failures requiring attention.
- **Warn** : Unexpected but non-breaking issues.
- **Info** : Routine operational messages.
- **Trace** : Granular event tracing (lowest severity).
- **Debug** : Diagnostic details for developers.

Step 4 Click **Search**, and then it searches for the logs of the selected level.



Click **History Files**, and it will display the history logs that you have searched.

Figure 2-19 Running logs

Step 5 (Optional) Click to download the log.

2.5.6.3 Packet Capture

You can examine network traffic by capturing IP packets to investigate network issues and detect security threats.

Procedure

- Step 1** Select **Maintenance Center > Advanced Maintenance > Packet Capture**.
- Step 2** (Optional) Enter the specified IP and port.
- Step 3** Click to perform a packet capture. A packet sniffer backup will be uploaded automatically after you click to end the capture.

Figure 2-20 Packet capture

NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Capture Data Size	Operation
eth0	192.168.1.31	Optional	Optional	Optional	Optional	0.00MB	
lo	127.0.0.1	Optional	Optional	Optional	Optional	0.00MB	

2.5.7 Configurations Management

- Export the configuration of the IP speaker in a file to your computer for backup.
- Import a configuration file to quickly configure the IP speaker.

Procedure

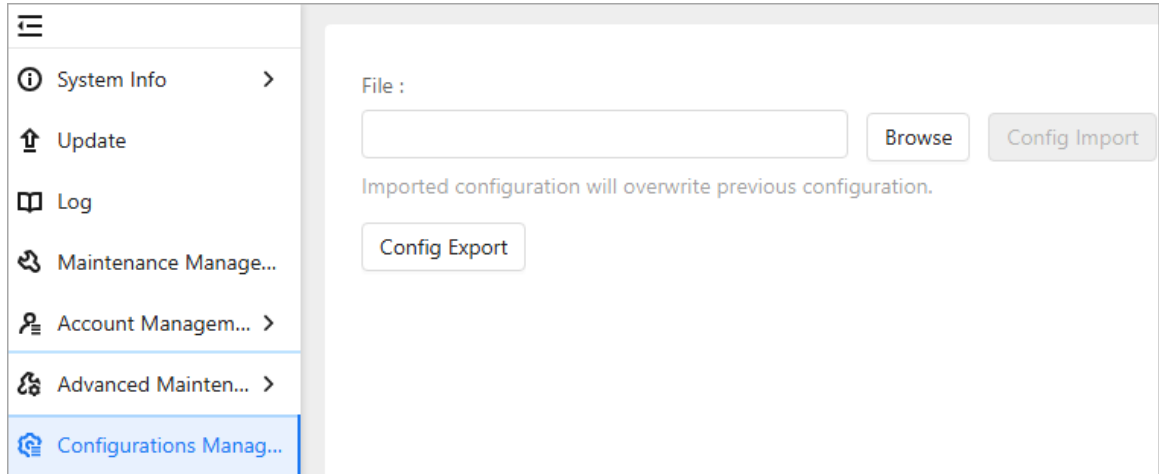
- Step 1** Select **Maintenance Center > Configurations Management**.
- Step 2** Import or export the file.
 - Import: Click **Browse** to select the configuration file on your computer, and then click **Config Import** to import it to the device.



After importing the file, the original configurations will be overwritten. Please be advised.

- Export: Click **Config Export** to export the configuration of the device in a file to your computer.

Figure 2-21 Configurations management



2.5.8 TF Card Storage

You can view the TF card information, and format the card if necessary.

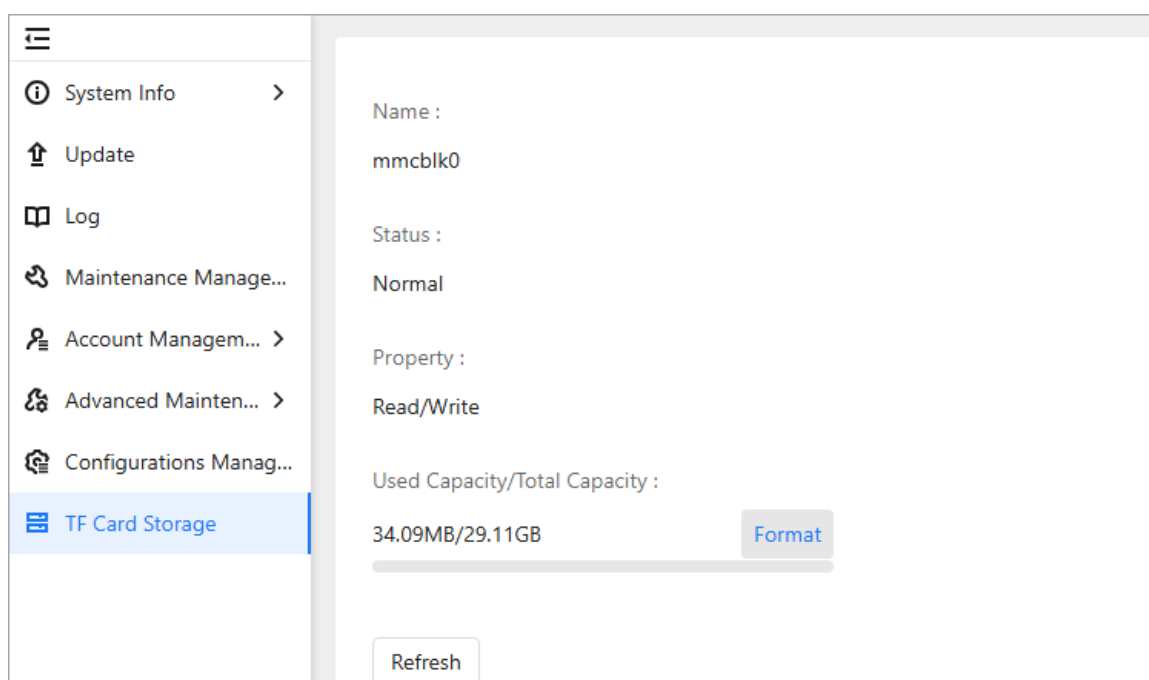
Procedure

- Step 1 Select **Maintenance Center** > **TF card Storage**.
- Step 2 View the TF card name, status, property, and capacity.



You can click **Format** to format the TF card, or click **Refresh** to refresh the card status.

Figure 2-22 TF card storage



2.6 Security

2.6.1 System Service

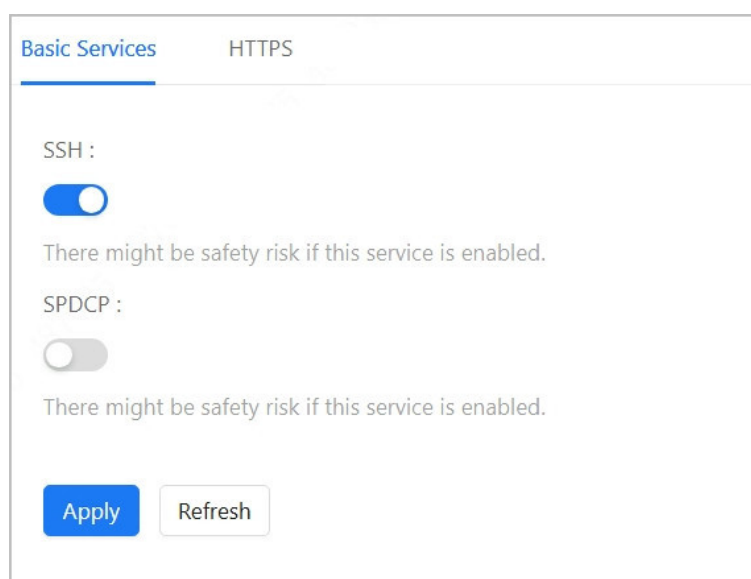
2.6.1.1 Basic Services

Configure the IP hosts (devices with IP address) that are allowed to visit the device. Only the hosts in the trusted sites list can log in to the webpage. This can enhance network and data security.

Procedure

Step 1 Select **Security** > **System Service** > **Basic Services**.

Figure 2-23 Basic services



Step 2 Enable the basic services according to the actual needs.

Table 2-10 Description of basic service parameters

Function	Description
SSH	You can enable SSH authentication to securely access and manage network devices or servers over untrusted networks.  There might be safety risk if this service is enabled.
SPDCP	It is not enabled by default. Enable SPDCP, and then the device can be matched with the earlier versions of NVR and DSS Pro.  There might be safety risk if this service is enabled.

Step 3 Click **Apply**.

2.6.1.2 HTTPS

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

Procedure

Step 1 Select **Security** > **System Service** > **HTTPS**.

Step 2 Click  to enable the function.

Step 3 Select the certificate.



If there is no certificate in the list, click **Certificate Management** to configure one.

Figure 2-24 HTTPS

Enable ☒

HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access service and RTSP access service.

Auto Redirect to ... ☐

*Select a device certificate [Certificate Management](#)

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
☒ 1			2054-04-09 18:11:11		General Device ITC CA	HTTPS, RTSP over TLS

Step 4 Click **Apply**.

2.6.2 CA Certificate

2.6.2.1 Installing Device Certificate

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with your computer.

2.6.2.1.1 Creating Certificate

Create certificate in the device.

Procedure

- Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.
- Step 2 Click **Install Device Certificate**.
- Step 3 Select **Create Certificate**, and click **Next**.
- Step 4 Enter the certificate information.

Figure 2-25 Certificate information

Step 2: Fill in certificate information.

Custom Name :

* IP/Domain Name :

172.115

Organization Unit :

Organization :

* Validity Period :

Days (1~9999)

* Region :

Province :

City Name :

Back

Create and install certificate

Cancel

Step 5 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**, you can edit the custom name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

2.6.2.1.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the camera.

Procedure

- Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.
- Step 2 Click **Install Device Certificate**.
- Step 3 Select **Apply for CA Certificate and Import (Recommended)** , and then click **Next**.
- Step 4 Enter the certificate information.

Figure 2-26 Certificate information

Step 2: Fill in certificate information. [X]

* IP/Domain Name :
172.115

Organization Unit :
[]

Organization :
[]

* Region :
[]

Province :
[]

City Name :
[]

[Back] [Create and Download] [Cancel]

- Step 5 Click **Create and Download**, and then save the request file to your computer.
- Step 6 Use the request file to apply for a CA certificate with a third-party certificate authority.
- Step 7 Click **Browse**, and then open the CA certificate.

Figure 2-27 Import a CA certificate

Step 3: Import the signed certificate. [X]

Custom Name :

Certificate Path :

Step 8 Click **Import and Install**.

Related Operations

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

2.6.2.1.3 Installing Existing Certificate

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

Procedure

Step 1 Select **Security > CA Certificate > Device Certificate**.

Step 2 Select **Install Device Certificate**.

Step 3 Select **Install Existing Certificate**, and then click **Next**.

Step 4 Click **Browse** to open the CA certificate and private key, and then enter the private key password.

Figure 2-28 Certificate and private key

Step 2: Select certificate and private key. X

Custom Name :

Certificate Path :
 Browse

Private Key :
 Browse

Private Key Password :

Back Import and Install Cancel

Step 5 Click **Import and Install**.

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.

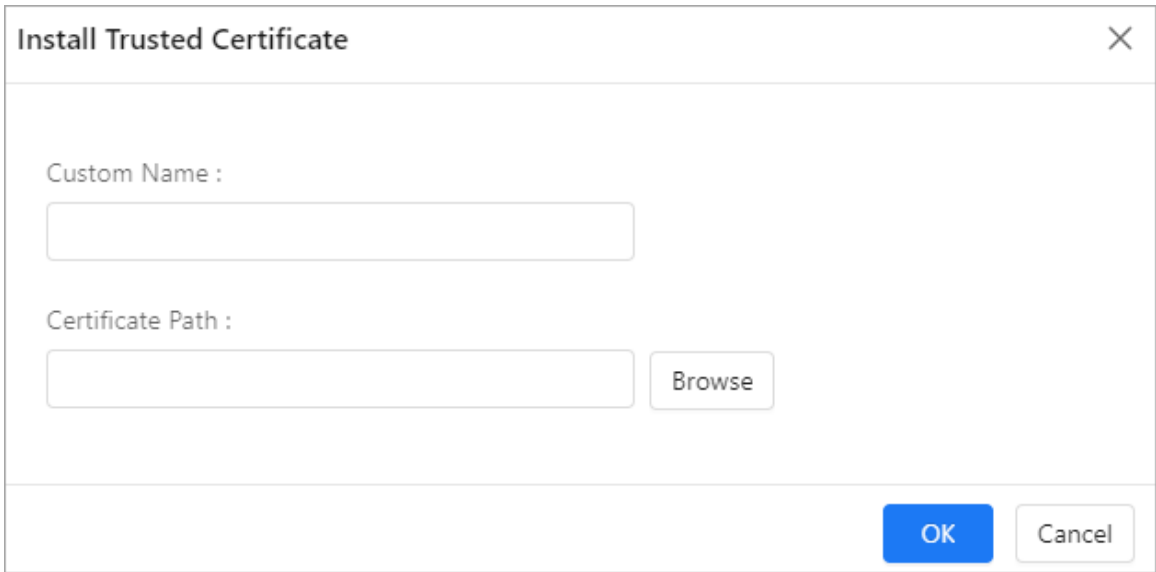
2.6.2.2 Installing Trusted CA Certificate

A 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 Select **Security** > **CA Certificate** > **Trusted CA Certificates**.
- Step 2 Select **Install Trusted Certificate**.
- Step 3 Click **Browse** to open the certificate.

Figure 2-29 Install trusted certificate

A dialog box titled "Install Trusted Certificate" with a close button (X) in the top right corner. It contains two input fields: "Custom Name :" and "Certificate Path :". The "Certificate Path :" field has a "Browse" button next to it. At the bottom right, there are "OK" and "Cancel" buttons.

Install Trusted Certificate

Custom Name :

Certificate Path :

Browse

OK Cancel

Step 4 Click **OK**.

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

Related Operations

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

Appendix 1 Security Recommendation

Account Management

1. Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account logout function

The account logout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access web services through secure channels.

2. Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

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

4. Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.

2. **MAC address binding**

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. **Build a secure network environment**

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

It is recommended to check online users regularly to identify illegal users.

2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).