

IP Speaker

User Manual

V1.03

Contents

About this Manual.....	1
1 Device Login.....	1
2 System.....	3
2.1 Basic.....	3
2.2 Time.....	3
2.3 DST.....	5
2.4 Security.....	5
2.4.1 SSH.....	5
2.4.2 HTTPS.....	5
3 Network.....	6
3.1 TCP/IP.....	6
3.2 Port.....	7
3.3 Port Mapping.....	7
3.4 SIP.....	8
4 Audio.....	10
4.1 Audio.....	10
4.2 Audio File.....	10
5 Alarm.....	10
5.1 Alarm Input.....	11
6 Broadcast.....	12
6.1 Broadcast Schedule.....	12
7 Maintenance.....	13
7.1 Diagnosis Info.....	13
7.2 Maintenance.....	13
7.3 Upgrade.....	14
Appendix: Initiative for the Proper Use of Video Products.....	14

About this Manual

Copyright Statement

©2024-2026 Zhejiang Uniview Technologies Co., Ltd. All rights reserved.

No part of this manual may be copied, reproduced, translated or distributed in any form by any means without prior content in writing from Zhejiang Uniview Technologies Co., Ltd (referred to as Uniview or us hereafter).

The products described in this manual may contain software copyrighted by us and any potential licensors. Without the permission of the relevant rights holders, no one may copy, distribute, modify, excerpt, decompile, disassemble, decrypt, reverse engineer, rent, transfer, sublicense, or engage in any other actions that infringe upon the software copyright in any form.

Disclaimer

Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

This manual is for reference only, and all statements, information, and recommendations in this manual are presented without warranty of any kind. The illustrations in this manual are for reference only and may vary depending on the version or model. The screenshots in this manual may have been customized to meet specific requirements and user preferences. As a result, some of the examples and functions featured may differ from those displayed on your monitor.

- The symbols in the following table may be found in this manual. Carefully follow the instructions indicated by the symbols to avoid hazardous situations and use the product properly.

Symbol	Description
	NOTE! Indicates useful or supplemental information about the use of product.
	CAUTION! Indicates a situation which, if not avoided, could result in damage, data loss or malfunction to product.
	WARNING! Indicates a hazardous situation which, if not avoided, could result in bodily injury or death.

1 Device Login

Login

1. Enter the device's IP address in the address bar (**192.168.1.20** by default), and then press **Enter**.



Note: DHCP is enabled by default. Please log in using the actual IP address.



2. Choose a language.
3. Enter the default username **admin** and the default password **123456**.
4. Click **Login**.
5. Follow the wizard to modify the related information.

Wizard

Change Password

Note: If IP Speaker is added to managing platform, you also need to edit the password on the platform.

Old Password*

Please enter

New Password*

Please enter

Confirm*

Please enter

Set Email

Note: It is recommended that you provide your email address; otherwise, retrieving your password will require technical support.

Email

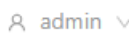
OK

 **Note:** The email address is used to retrieve the device password. If you forgot the device password without presetting an email address, you need to contact technical support (globalsupport@uniview.com) to reset the password.

- Click **OK** to return to the login page and log in with the new password.

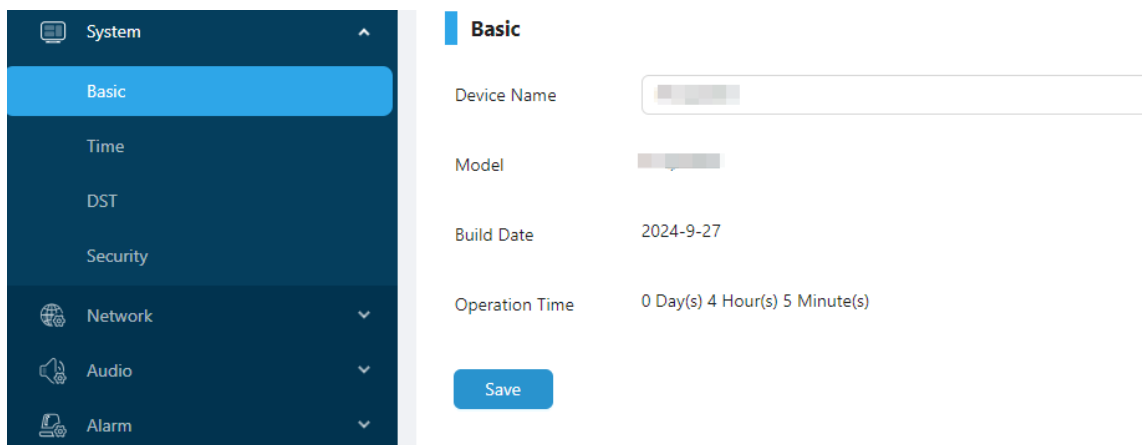
Forgot Password

If you forgot your password, you can click **Forgot Password** on the login page, and then follow the on-screen instructions to retrieve the password.

 **Note:** After login, you can click  |  in the upper-right corner to switch the language, change the password, set an email address, or log out from the account.

2 System

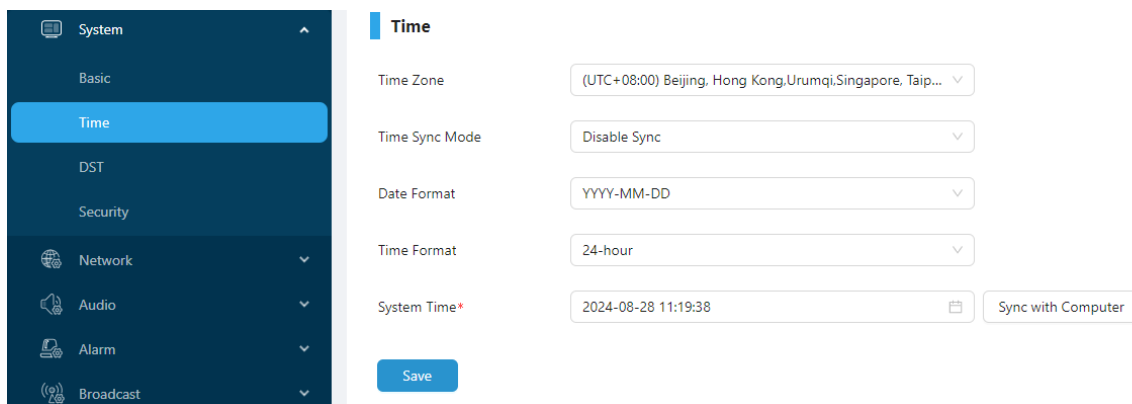
2.1 Basic



The screenshot shows the 'Basic' configuration page in a web interface. On the left is a dark sidebar with a menu: 'System' (expanded), 'Basic' (selected), 'Time', 'DST', 'Security', 'Network', 'Audio', and 'Alarm'. The main content area is titled 'Basic' and contains the following fields: 'Device Name' (text input), 'Model' (text input), 'Build Date' (2024-9-27), and 'Operation Time' (0 Day(s) 4 Hour(s) 5 Minute(s)). A blue 'Save' button is at the bottom.

Change the device name as needed, and click **Save**.

2.2 Time



The screenshot shows the 'Time' configuration page in a web interface. On the left is a dark sidebar with a menu: 'System' (expanded), 'Basic', 'Time' (selected), 'DST', 'Security', 'Network', 'Audio', 'Alarm', and 'Broadcast'. The main content area is titled 'Time' and contains the following fields: 'Time Zone' (dropdown menu showing '(UTC+08:00) Beijing, Hong Kong, Urumqi, Singapore, Taip...'), 'Time Sync Mode' (dropdown menu showing 'Disable Sync'), 'Date Format' (dropdown menu showing 'YYYY-MM-DD'), 'Time Format' (dropdown menu showing '24-hour'), and 'System Time' (text input showing '2024-08-28 11:19:38' with a calendar icon and a 'Sync with Computer' button). A blue 'Save' button is at the bottom.

Configure the time zone, date format, time format, and system time as needed. The following three ways are available.

Sync with NTP Server

- Choose **Sync with NTP Server** from the **Time Sync Mode** drop-down list.

Time

Time Zone	(UTC+08:00) Beijing, Hong Kong,Urumqi,Singapore, Taip... ▾
Time Sync Mode	Sync with NTP Server ▾
Date Format	YYYY-MM-DD ▾
Time Format	24-hour ▾
System Time*	2024-08-27 09:32:20 
NTP Server Address*	Please enter
NTP Port*	123
Update Interval	10m ▾

Save

2. Configure the NTP server address, NTP port, and update interval. The NTP port should be consistent with the NTP server port.
3. Click **Save**.

Sync with Computer

1. Click **Sync with Computer**, and the device will sync time with the computer.

Time

Time Zone	(UTC+08:00) Beijing, Hong Kong,Urumqi,Singapore, Taip... ▾
Time Sync Mode	Disable Sync ▾
Date Format	YYYY-MM-DD ▾
Time Format	24-hour ▾
System Time*	2024-08-27 09:46:51 
	<button>Sync with Computer</button>

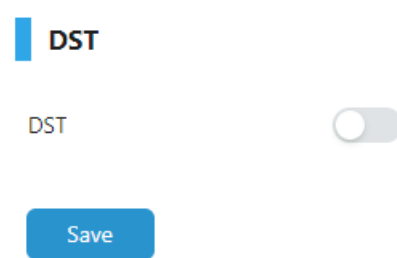
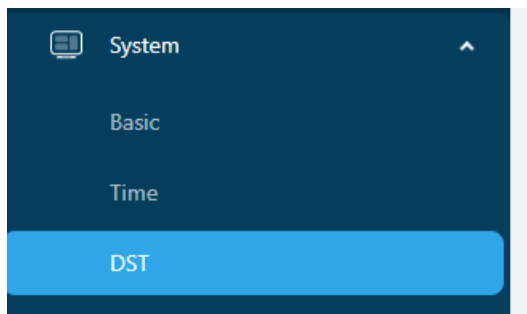
Save

2. Click **Save**.

Set Manually

1. Click  to set the system time manually.
2. Click **Save**.

2.3 DST

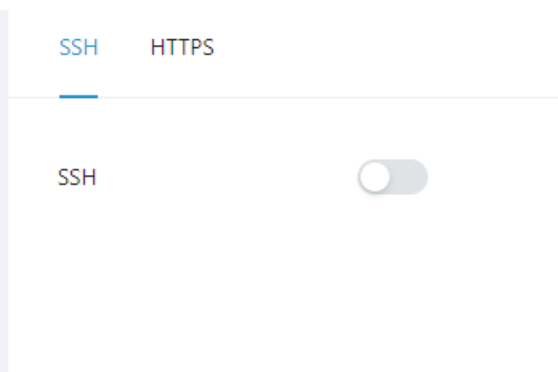
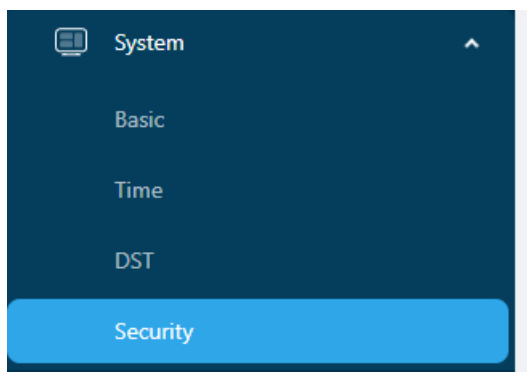


1. Click  to enable **DST**.
2. Set the DST parameters as needed.
3. Click **Save**.

2.4 Security

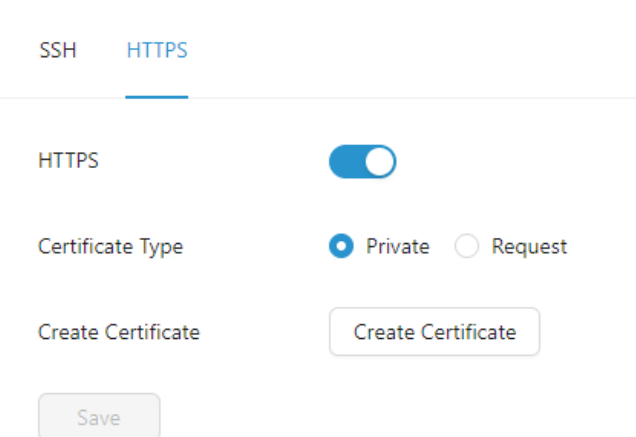
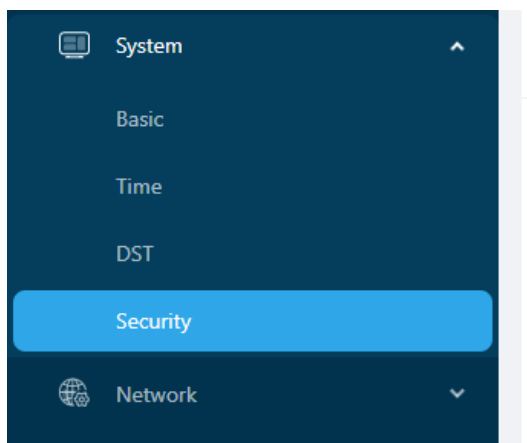
2.4.1 SSH

You can enable SSH only for device maintenance and debugging.



2.4.2 HTTPS

Use a digital certificate to encrypt the data transmission between the client (browser) and the device to ensure data security.



 **Note:** Please do not create or delete the certificate when HTTPS is enabled.

Private Certificate

A digital certificate generated by the device.

1. Click **Create Certificate**, enter the certificate information, and click **OK**.
 - Country: Abbreviation for the name of the country.
 - Hostname/IP: Device's IP address.
 - Valid Days: Supports customizing the validity period of the certificate.
2. Click  to enable **HTTPS**.
3. Click **Save**.
4. Log out from the account and log in again with `Https://IP address`, and install the certificate to the **Trusted Root Certification Authorities** folder of the browser so that you can log in normally.

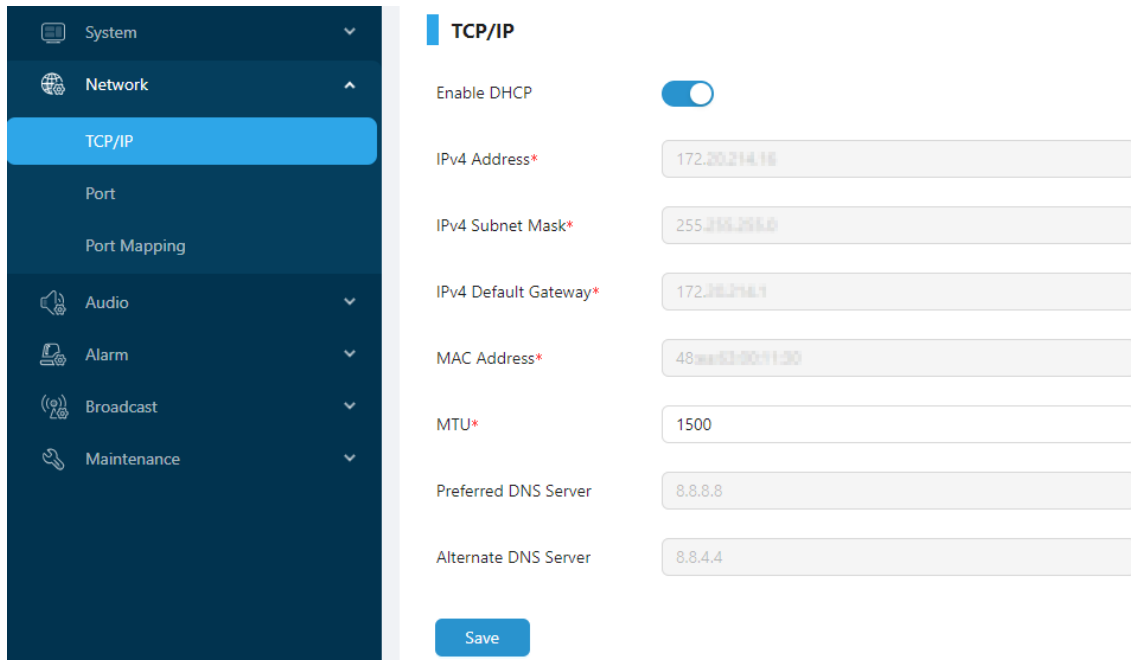
Certificate Request

A digital certificate signed by a CA authority.

1. Click **Create Certificate**, enter the certificate information, and click **OK** to generate a certificate request.
 - Country: Abbreviation for the name of the country.
 - Hostname/IP: Device's IP address.
2. Click **Download** to download the certificate request and send the request to the CA authority for signature.
3. Click  , choose the signed .crt file, and click **Upload**.
4. Click  to enable **HTTPS**.
5. Click **Save**.
6. Log out from the account and log in again with `Https://IP address`.

3 Network

3.1 TCP/IP



IP Address

DHCP is enabled by default. The device may be assigned an IP address after it connects to the network. You can disable DHCP, set the IP address as needed, and click **Save**.

 **Note:** MTU (Maximum Transmission Unit): Maximum data transmission unit defined in the network protocol, maximum size of data packets that can be sent in network communication, measured in bytes. When data traverses the network, it is divided into multiple packets, with each packet's size limited by MTU.

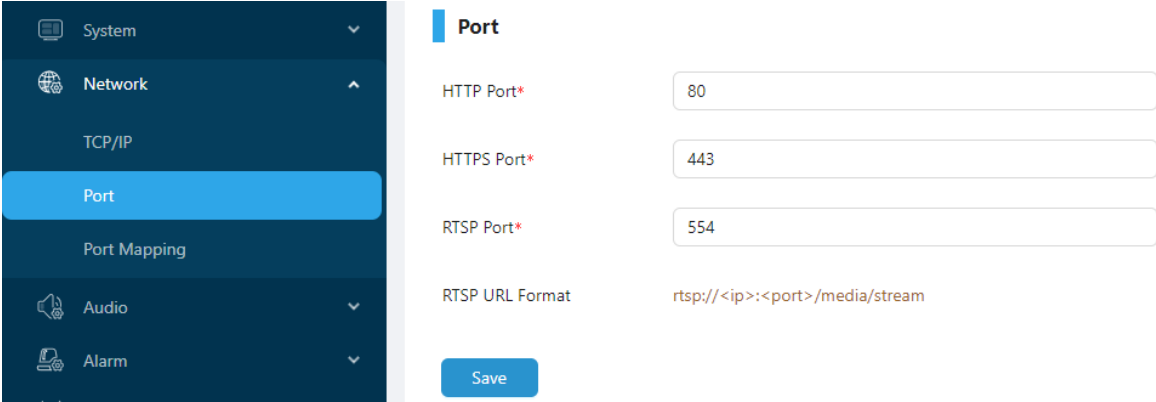
DNS

Domain name system. When a device accesses a domain name, such as cloud server, DNS can resolve the domain name to an IP address for easy access. It is recommended to use the default server.

3.2 Port

Configure internal ports including HTTP, HTTPS, and RTSP.

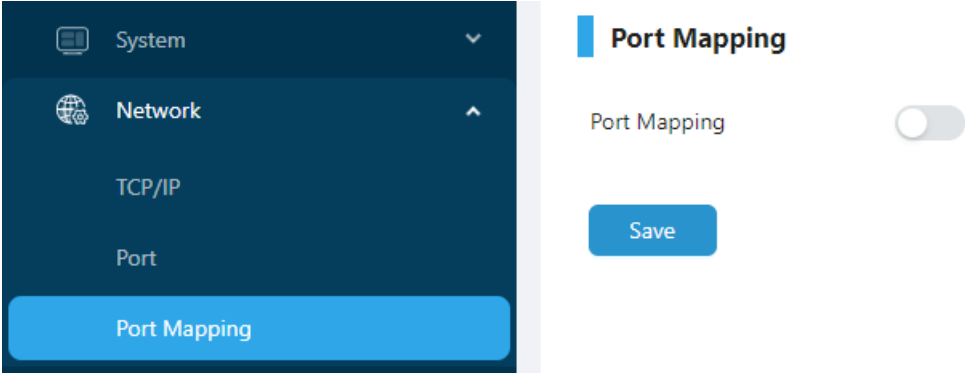
 **Note:** The internal ports are used to access the device's applications on the LAN via a LAN client (browser).



The screenshot shows the 'Port' configuration page. On the left is a sidebar menu with options: System, Network (expanded), TCP/IP, Port (selected), Port Mapping, Audio, and Alarm. The main content area is titled 'Port' and contains three input fields: 'HTTP Port*' with the value 80, 'HTTPS Port*' with the value 443, and 'RTSP Port*' with the value 554. Below these is a label 'RTSP URL Format' with the value 'rtsp://<ip>:<port>/media/stream'. A blue 'Save' button is at the bottom right.

3.3 Port Mapping

Configure a public network client (browser) to access a private network device's port.



The screenshot shows the 'Port Mapping' configuration page. The sidebar menu is the same as in the previous screenshot, but 'Port Mapping' is now selected. The main content area is titled 'Port Mapping' and features a 'Port Mapping' toggle switch, which is currently turned off. A blue 'Save' button is located below the toggle.

Manual

Configure external ports manually.

 **Note:** The external ports are used to access the device's applications of the device on the LAN via a public network client (browser).

Port Mapping

Port Mapping ☒

Mapping Mode Manual

HTTP Port* 80

RTSP Port* 554

HTTPS Port* 443

Save

UPnP

UPnP is short for Universal Plug and Play. UPnP-enabled network address translation (NAT) can perform automatic port mapping to enable computers on the public network to access the device on the private network.

Note:

- This function requires router support. You need to enable UPnP on the router before starting configuration on the DEVICE.
- External IP Address: The IP address of the router's WAN port.
- Device IP: The speaker's IP address.

UPnP Mapping	Description																												
Auto	The device automatically assigns external port numbers, which are usually the same as the internal port numbers.																												
Manual	Port Mapping Port Mapping ☒ Mapping Mode UPnP UPnP Mapping Manual <table><tr><th>Port Type</th><th>External Port</th><th>External IP Address</th><th>Internal Port</th><th>Device IP</th><th>Enable</th><th>Status</th></tr><tr><td>HTTP Port</td><td> 80 </td><td>N/A</td><td>80</td><td>172.20.210.212</td><td>Yes</td><td> Inactive </td></tr><tr><td>RTSP Port</td><td> 554 </td><td>N/A</td><td>554</td><td>172.20.210.210</td><td>Yes</td><td> Inactive </td></tr><tr><td>HTTPS Port</td><td> 443 </td><td>N/A</td><td>443</td><td>172.20.210.210</td><td>Yes</td><td> Inactive </td></tr></table> Save Choose Manual from the UPnP Mapping drop-down list, configure the external port as needed, and click Save. Note: After the port mapping is configured, you can enter the IP address of the WAN port of the router in the browser: HTTP external port number to log in to the web interface of the device. For example: If the external IP address of the router is 10.2.2.10 and the external port of HTTP is 82, enter http://10.2.2.10:82 in the address bar of the browser.	Port Type	External Port	External IP Address	Internal Port	Device IP	Enable	Status	HTTP Port	80	N/A	80	172.20.210.212	Yes	Inactive	RTSP Port	554	N/A	554	172.20.210.210	Yes	Inactive	HTTPS Port	443	N/A	443	172.20.210.210	Yes	Inactive
Port Type	External Port	External IP Address	Internal Port	Device IP	Enable	Status																							
HTTP Port	80	N/A	80	172.20.210.212	Yes	Inactive																							
RTSP Port	554	N/A	554	172.20.210.210	Yes	Inactive																							
HTTPS Port	443	N/A	443	172.20.210.210	Yes	Inactive																							

3.4 SIP

SIP (Session Initiation Protocol) is an application layer protocol for establishing, modifying, and terminating multimedia sessions. By configuring the device to access a SIP server, audio intercom and audio broadcast can be implemented between the device and platforms, IP phones, and other SIP terminals.

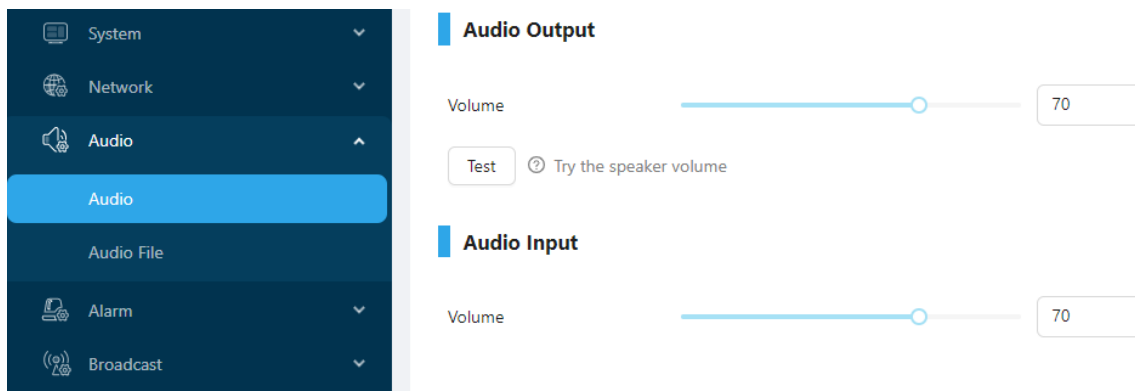
1. Use the default **Account**.
2. Configure SIP parameters.

Parameter	Description
Device Status	Displays the SIP registration status of the current account, which cannot be edited. Online: Successfully registered to the SIP server. Offline: Not registered to the SIP server.
Username	The user account registered on the SIP server.
Auth Username	The user ID used for Digest authentication on the SIP server.
Auth Password	The user password used for Digest authentication on the SIP server. Some servers do not require authentication, so this parameter can be left unconfigured.
Server Address	The IP address or domain name of the SIP registration server.
Server Port	The port of the SIP registration server.
SIP Transport Protocol	The transport layer protocol used for SIP communication: UDP, TCP, TLS.
Timeout(s)	The validity period of SIP registration, that is, the registration keep-alive period. Before expiration, the device will send a registration request again to maintain the online status.

3. Click **Save** to complete the configuration.

4 Audio

4.1 Audio



Audio Output

Volume 70

Test ⓘ Try the speaker volume

Audio Input

Volume 70

Audio Output

Adjust the volume of device test and two-way audio. Click **Test** to try the volume on the IP speaker.

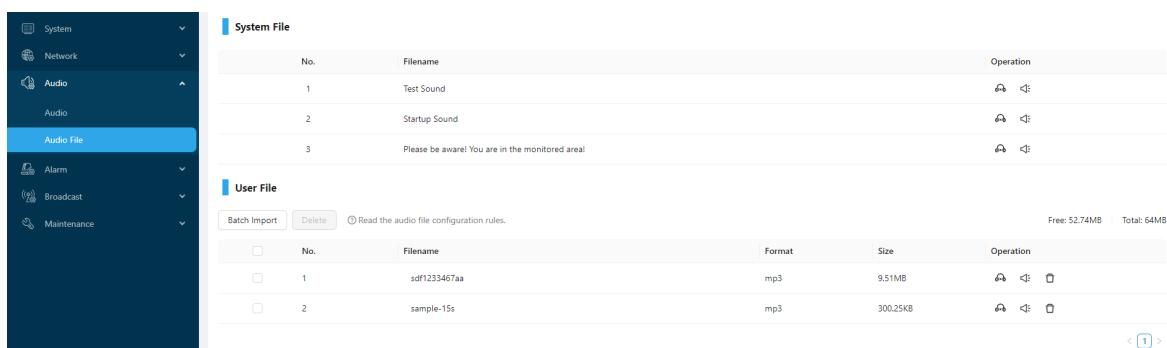
 **Note:** If the volume set in [Broadcast Schedule](#) is inconsistent with audio output volume, please adjust the audio output volume to match the volume set for the broadcast before test.

Audio Input

Adjust the volume of the device on the NVR or app. That is, the volume of the audio played on the NVR or app during the two-way audio.

4.2 Audio File

The audio file includes system audio and custom audio, which can be used for broadcasting and sound alarm.



System File

No.	Filename	Operation
1	Test Sound	 
2	Startup Sound	 
3	Please be aware! You are in the monitored area	 

User File

ⓘ Read the audio file configuration rules.

Free: 52.74MB Total: 64MB

No.	Filename	Format	Size	Operation
1	sdf1233467aa	mp3	9.51MB	   
2	sample-15s	mp3	300.25KB	   

< 1 >

System File

- : Click to play audio on your PC.
- : Click to play audio on the local device.

User File

Click **Batch Import** to import the custom audio.

5 Alarm

5.1 Alarm Input

Configure the alarm mode, arming schedule, and alarm-triggered actions for external alarm input devices connected to the IP speaker via the ALARM IN interface. For example, access control devices, doorbells, etc.

The screenshot shows the 'Alarm Input' configuration page. The left sidebar has a menu with 'System', 'Network', 'Audio', 'Alarm', 'Broadcast', and 'Maintenance'. The 'Alarm' section is expanded, showing 'Alarm Input', 'Alarm Sound', and 'Alarm Output'. The 'Alarm Input' configuration form includes the following fields:

- Alarm Input No.: A dropdown menu showing 'A<-1'.
- Alarm Input Name: A text input field.
- Alarm Type: A dropdown menu showing 'N.O.'.
- Alarm Input: A toggle switch.

Below the form is a 24-hour arming schedule grid. The grid has tabs for 'Arming Schedule' and 'Alarm Sound'. The 'Arming Schedule' tab is active, showing a 24-hour timeline from 0 to 24, with days of the week listed on the left. A 'Save' button is at the bottom left. On the right, there are 'Armed' and 'Disarmi...' buttons.

1. Set other parameters as needed.

- **Alarm Input No.:** The hardware interface of the IP speaker to which the alarm input device is connected. A<-1 means that the alarm input device is connected to the IP speaker via the ALARM IN 1 interface.
- **Alarm Input Name:** Set the name as needed.
- **Alarm Type**
 - **N.O.:** Choose this option if the alarm input device is normally closed. The normally closed alarm device opens the circuit to input an alarm, triggers the device to open the alarm circuit and generate an alarm.
 - **N.C.:** Choose this option if the alarm input device is normally opened. The normally opened alarm device closes the circuit to input an alarm, triggers the device to close the alarm circuit and generate an alarm.

2. Enable **Alarm Input**.

3. Set the arming schedule. A 24/7 normal recording schedule is enabled by default. To change the arming schedule, you can cancel all arming schedules first and reset the arming schedule as needed. The following mainly introduces the arming method. To disarm the schedule, click **Disarming**, and follow the steps below.

- **Set a schedule:** Set the arming schedule in minutes. You can only set the arming schedule for one day at a time.

(1) Click **Armed**.

- (2) Click any time cell of the day you want to set, and the cell becomes blue. Move the mouse away from the blue cell, and hover it again until the setting box appears.

The screenshot shows the 'Arming Schedule' grid with a time selection box open. The grid has tabs for 'Arming Schedule' and 'Alarm Sound'. The 'Arming Schedule' tab is active, showing a 24-hour timeline from 0 to 24, with days of the week listed on the left. A time selection box is open over the grid, showing '5:00' and '6:00' with a clock icon. A 'Save' button is at the bottom left. On the right, there are 'Armed' and 'Disarmi...' buttons.

(3) Set the start time and end time.

(4) Click **OK**.

- **Draw a schedule:** Draw the arming schedule in hours. You can draw the arming schedule for multiple days at a time.

(1) Click **Armed**.

- (2) Right-click or drag on the schedule to select the time cells you want to enable arming.

(3) Click **OK**.

 **Note:** You can draw the arming schedule roughly, and then set the precise period.

- Set the alarm sound.

Item	Description
Enable	Click  to enable alarm sound.
Audio	Choose an alarm audio.
Volume	The volume at which the alarm audio is played.
Play Mode	By Play Count: The number of times that the alarm audio is played. By Duration: The duration that the alarm audio is played.
Play Count	Set it as needed.
Duration	Set it as needed.

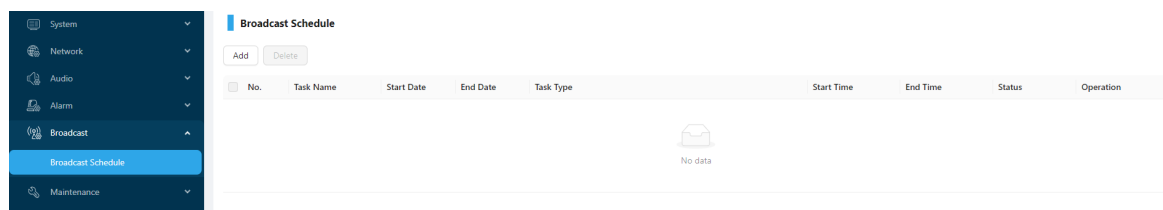
- Click **Save**.

6 Broadcast

6.1 Broadcast Schedule

Configure the play time of the broadcast file.

 **Note:** The time periods of different schedules cannot overlap.



- Click **Add**.
- Configure the basic information.

Basic Info	Description
Task Name	Set it as needed.
Start/End Date	The start/end date of the schedule.
Task Type	Daily: Play the broadcast during the schedule time every day. Weekly: Play the broadcast during the schedule time every week.
Repeat Day(s)	Repeated days of the weekly schedule.
Start/End Time	Play time every day or on the specified day(s) according to the schedule.
Play Mode	Repeat: Play broadcast repeatedly during the schedule. If there are multiple audio files, all audio files will be played in a single loop. By Play Count: Play audio based on the set times during the schedule. If there are multiple audio files, all audio files will be played in a single loop.
Play Count	Set it as needed.  Note: If the set play count reaches but the end time has not reached, the audio will stop.
Volume	The volume of the current file played by the device.  Note: To try the volume of the broadcast task, adjust the audio output volume to the volume set by the current task before test.

3. Configure the audio file.

(1) Click **Add**, and choose the desired audio file(s).

(2) Click **OK**.



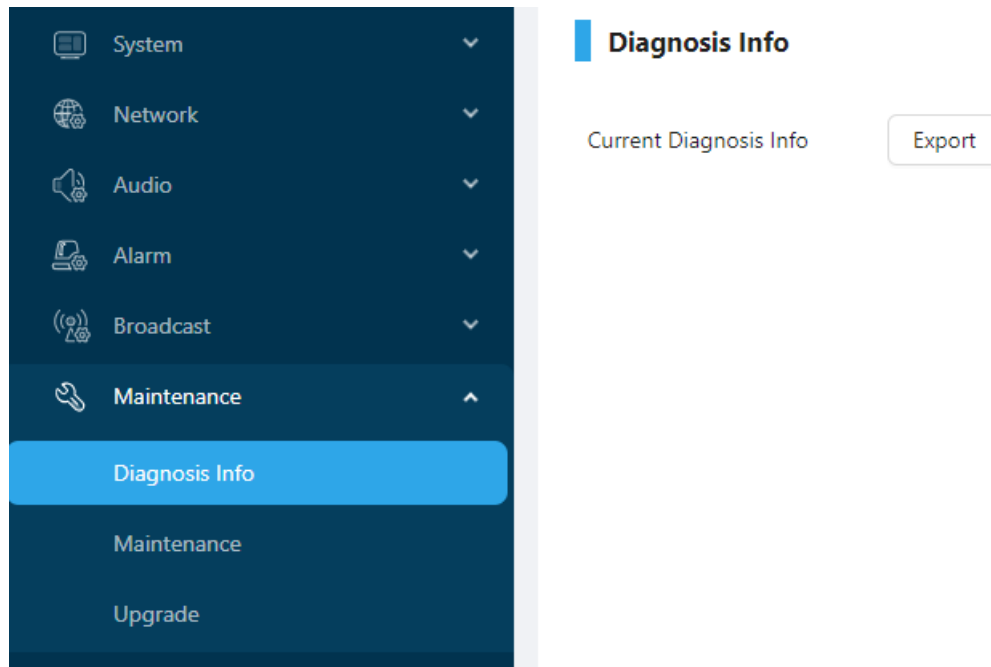
Note:

Click to delete the audio file.

Click and drag to sort the audio file.

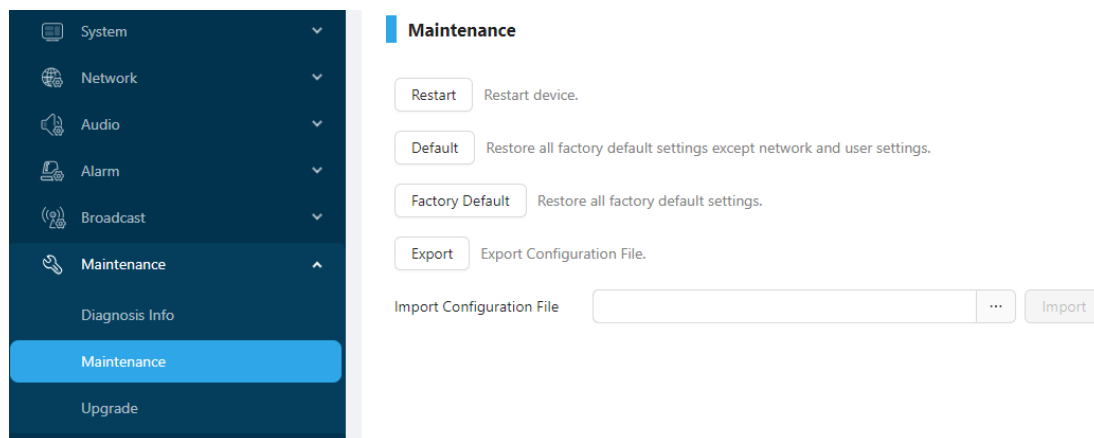
7 Maintenance

7.1 Diagnosis Info



Click **Export** to export the current diagnosis information.

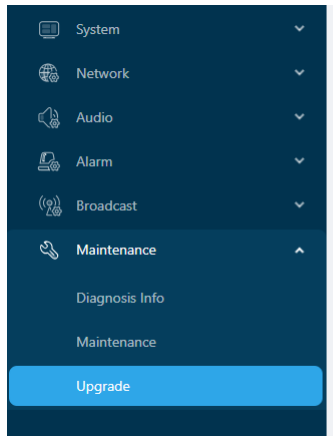
7.2 Maintenance



Click , choose the configuration file, and click **Import** to import the configurations of other speakers to the current device.

 **Note:** The software version of the device to which the configuration file resides must be the same as that of the device to which the configuration file is imported.

7.3 Upgrade



- Local upgrade: Click  or blank area in the text box, choose the upgrade file, and then click **Upgrade** to start upgrade.
- Cloud upgrade: Click **Check for Update**. If the page shows a new version is available, click **Upgrade** to start the cloud upgrade.

Appendix: Initiative for the Proper Use of Video Products

Thank you for choosing our products.

As technology advances, its applications have a profound impact on every aspect of our lives. As a high-tech company, we have an increasingly deep understanding of the contributions of technology in enhancing efficiency and improving the quality of life. At the same time, we are also aware that the misuse of technology can cause harm. For instance, video surveillance products, due to their ability to record real, complete, and clear images, have significant value in tracing and reconstructing facts. However, improper dissemination, use, and processing of image records can also lead to issues that infringe upon the legitimate rights and interests of others. To continuously promote technology for good, we advocate that every user should use technology and video products responsibly. This includes not only adhering to legal and regulatory requirements but also following the constraints of moral customs, to jointly establish and maintain a positive social environment and atmosphere.

Please read the following proposals carefully:

- Everyone has a reasonable expectation of privacy, and the installation of video products should not violate the reasonable privacy expectations of an individual. When installing video surveillance products in public places, it should be done in a reasonable and effective manner with clear indications of the surveillance area. When installing video products in non-public places, one should not infringe upon the rights and interests of others, including but not limited to not installing video surveillance products without the consent of the stakeholders, or installing highly covert video surveillance products.
- During the use of video products, real activities within specific time and space frames will be recorded under certain conditions. Users should reasonably define the rights they have within that specific range to avoid infringing upon the portrait, privacy, or other legal rights of others.
- During the use of video products, a continuous stream of video image data originating from real-life scenes, including a large amount of biometric data (such as facial data), will be generated. This data can be applied or further processed for various purposes. The video products themselves are not capable of distinguishing between good and bad uses of data. The outcomes of data usage depend on the actions of the data controllers, their intentions, and purposes. Data controllers should adhere to legal requirements and norms, as well as respect international conventions, local customs, societal ethics, public order, and moral standards.

- all non-mandatory regulations. It is essential for data controllers to respect individuals' privacy, likeness, and other rights during data usage.

- Considering the ongoing generation of video image data by video products, which carries the rights protection requirements, value claims, or other demands of various stakeholders, it is crucial to ensure the security of the product and its data. Users of the product and data controllers should take reasonable and necessary measures to ensure network and data security, to prevent data leaks or improper use. This includes, but is not limited to, carefully allocating the use and management permissions of the product, and establishing and continuously optimizing the security systems of various networks, such as the Internet and local area networks, that the product connects to, in conjunction with the product's usage scenarios.
- Video products have made significant contributions to enhancing societal security, and we believe these products will continue to play a positive role in more aspects of social life. Any use of these products to infringe upon human rights or engage in illegal activities is contrary to the original intent of technological innovation and product development. Therefore, we encourage every user to establish an assessment and tracking mechanism to ensure that the product is used properly, reasonably, and in good faith.