Network Broadcast

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION,

PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Note	Provides additional information to emphasize or supplement important points of the main text.
 Caution	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Danger	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Contents

Chapter 1 Activate Device via Web Client

Steps

1. Change the IP address of your PC to the same subnet as the device.

Note

The default IP address of the device is 192.168.1.64.

2. Open a web browser and input the default IP address to display the activation page.

Caution

We highly recommend you create a strong password of your own choosing (the password should be between 8 and 16 characters and contain at least 2 or more of the following types: numbers, lower case letters, upper case letters, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

3. If there are multiple devices in your network, please modify the device IP address to prevent device access exception caused by conflicting IP address. After you log in to the device, you can go to **Configuration → Network → Network Configuration → TCP/IP** to modify parameters such as device IP address, subnet mask, etc.

Chapter 2 Web Client Operation Instructions

2.1 System Configuration

In the system configuration column, you can search system information, set system time, user information, etc.
Go to **Configuration → System** to complete the settings.

Basic Information

Go to **System Configuration → Basic Information** to complete the settings.
Device system information includes device name, device No., device model, device serial No., version information, etc. You can set **Device Name** and **Device No**. and click **Save**.

Time Settings

Go to **System Configuration → Time Settings** to complete the settings. You can select **Time Zone** and set **Time Synchronization Mode**.

NTP Time Sync

Select **NTP time sync** to set **Server Address**, **NTP Port**, and **Interval**. The device will sync every time according to the settings. And you can click **Test** to verify whether it takes effect.

Manual Time Sync

Select **Manual time sync** and set time. The device will perform time sync according to the set event. If you click **Sync with computer time**, the device time will be the same with the local computer time.

DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function. Check **Enable** and select the start time, end time, and DST Bias.
After configuring the parameters, click **Save** to take effect.

System Maintenance

Go to **Maintenance and Security → System Maintenance** to complete the settings.

- Reboot Device: Click **Restart** to restart the device.
- Upgrade: When the device program needs to be updated, the device can be upgraded.
  When the device needs to be upgraded, you can copy the upgrade program to the local computer, click to select the path of saving the upgrade file, and click **Upgrade** to start upgrading.

Note

After upgrading, the device will reboot automatically. Do not power off during upgrading.

- Restore parameter: Restore the device parameter to the factory settings.

  Restore

  Reset device parameters, except user information, IP parameters and video format to the default settings.

  Default

  Reset all the parameters to the factory default.

Note

- Be careful when using this function. After resetting to the factory default, all the parameters are reset to the default settings.
- Spotify function is disabled by default.

- Backup device parameter: It is used to export device parameter file. It can be used to configure device with the same parameter, but does not support network parameter backup.
  1. Click **Export**.
  2. Set encryption password to encrypt the exported device parameter file.
  3. Click **OK** to select storage path to export.
- Parameter import: Device parameter is used to import device parameter file, and it is convenient for the user to configure device with the same parameter.
  1. Click , select the storage path of the device parameter file, and click **Open**.
  2. Click **Import** to display the prompt.
  3. Click **OK**, enter encryption password, and import device parameter file.

Security Management

Go to **Maintenance and Security → System Maintenance → Security Audit Log** to complete the settings.
Enable log upload server: After you enable the enable button, you can enter **Log Server IP** and **Log Server Port** and click **Save** to upload the log to the server automatically.

Device Debugging

Go to **Maintenance and Security → System Maintenance → Device Debug** to complete the settings.

- Enable SSH: When remote debugging is required, you can swipe to enable SSH. You can log in to the device using SSH. Device remote SSH port is 22 by default, and can be edited as needed. When the device is running normally, it is recommended not to enable SSH to improve device security.
- Print Log: Click **Export** to export and print the log.
- Ping Network: Enter Ping network address. Click **Ping Network** to start the test.

Network Capture: Click **Start Capture** to capture the packet, and click **Stop** to stop capturing the packet.

User Management

Click **Configuration → System → User Management** to enter the configuration page.
You can click to change the administrator password.

Caution

- The admin is the default user. The user name cannot be edited. Only its password can be edited.
- To ensure the security of account information, it is recommended to set a password between 8 and 16 characters, including at least digits, lowercase letters, uppercase letters, and special characters (!"#$%&'()*+,-./:;<=>?@@[\\]^_`{|}~. space) and cannot contain user name.
- Password length should be less than 8 characters. Password should contain only 1 type of character. Password should be the same as user name, or the password should be the reverse of user name. The above types of passwords are risky. To better protect your privacy and improve product security, it is recommended to change the risky password to high-intensity.
- Password strength rule:
  1. If the password contains 3 or more types (digits, lowercase letters, uppercase letters, and special characters), the password security strength is strong.
  2. If the password is a combination of digits and special characters, lowercase letters and special characters, uppercase letters and special characters, lowercase letters and uppercase letters, the password security

strength is medium.
3. If the password is a combination of digits and lowercase letters, digits and uppercase letters, the password security strength is weak.

2.2 Network Configuration

2.2.1 Set TCP/IP

Steps

1. Click **Configuration → Network → Network Configuration → TCP/IP** to enter the configuration page.
2. Configure network parameters.
3. Select **NIC Type**, slide to enable **DHCP**, or manually enter **IPv4 Address**, **IPv4 Subnet Mask**, **IPv4 Default Gateway**, **MTU**, **Preferred DNS Server** address, and **Alternate DNS Server** address.

Note

Click **Test** to test if IPv4 address is used.

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

2.2.2 Set Port

Port configuration parameters include HTTP port and HTTPS port. Set corresponding port as needed.

Set HTTP(s) Port

Click **Configuration → Network → Network Service → HTTP(S)** to configure HTTP port and HTTPS port.

HTTP Port

When you log in with a browser, you need to add the modified port number after the address. If HTTP port No. is changed to 81, you can enter http://192.0.0.65:81 when you log in via browser.

HTTPS Port

Configure HTTPS port for browser access, and certificate verification is required.

Click **Save** to complete the configuration.

2.2.3 Set RTSP

RTSP (Real Time Streaming Protocol) is an application-layer controlling protocol for streaming media.

Steps

1. Go to **Configuration → Network → Network Service → RTSP**.
2. Enter **Port No**.
3. Click **Save**.

2.2.4 Set Cloud Service

The device can be operated by mobile client.

Steps

1. Click **Configuration → Network → Cloud Service** to enter the configuration page.
2. Slide **Enable** to enable the mode, check **Custom** after server address and enter the address. Configure the **Verification Code**.

   Note

   Verification code should contain 6 to 12 letters or digits, and it is case sensitive. To ensure device security, it is recommended to set a combination of uppercase letters, lowercase letters, and digits with more than 8 characters.

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

2.2.5 Set ISUP

When the device is registered on ISUP platform (formerly called Ehome), you can visit and manage the device, transmit data, and forward alarm information over public network.

Steps

1. Go to **Configuration** → **Network** → **Platform Access** → **ISUP**.
2. Optional: Select an access center.
3. Check **Enable**.
4. Select a protocol version and enter related parameters.
5. Click **Save**.
   Register status turns to **Online** when the function is correctly set.

2.2.6 Set Open Network Video Interface

If you need to access the device through Open Network Video Interface protocol, you can configure the user settings to enhance the network security.

Steps

1. Go to **Configuration** → **Network** → **Platform Access** → **Open Network Video Interface**.
2. Check **Enable**.
3. Select an authentication mode.
   - If you select **Digest**, the device only supports digest authentication.
   - If you select **Digest&ws-username token**, the device supports digest authentication or ws-username token authentication.
4. Click **Add** to configure the Open Network Video Interface user.
5. Click **Save**.
6. Optional: Repeat the steps above to add more Open Network Video Interface users.
7. Optional: Manage the user.
   - Click to delete the selected Open Network Video Interface user.
   - Click to modify the selected Open Network Video Interface user.

2.2.7 Set SDK Service

If you want to add the device to the client software, you should enable SDK Service.

Steps

1. Go to **Configuration → Network → Platform Access → SDK Service**.
2. Enter **Service Port**.
3. Click **Save**.

2.3 Audio Configuration

2.3.1 Algorithm Configuration

Note

For professional debugging use only. Features may vary by model, please refer to the actual device.

Click **Configuration → Audio → Algorithm Configuration** to enter the configuration page.

Noise Reduction	When enabled, set the **Noise Reduction Level** as needed.
Equalizer	Click **Configure** to adjust equalizer parameters. Supports high/low-pass filters and high/low-shelf filter adjustments to modify the frequency, bandwidth, and gain of the output signal.
Automatic Gain Control	When enabled, it controls the gain of the output signal. Set the Target, Mode, Output Noise, Maximum Gain, and Adjustment Speed as required.

Note

Click **Restore Default** to reset algorithm configuration parameters to their default values.

2.3.2 Audio Configuration

Note

Only certain models support the function.

Click **Configuration → Audio → Audio** to enter the configuration page.
You can drag the slider to configure the input volume and output volume.
You can click **Speaker Test** to test the speaker, and adjust the speaker test volume by dragging the slider.
You can click **Microphone Test** to test the microphone.
You can configure the prompt volume by dragging the slider, which controls the volume of the prompts, including prompts for wireless connection, wireless disconnection, and device power-on.

Note

- The speakers should be connected.
- Click **Restore Default** to reset audio configuration parameters to their default values.

2.3.3 Other Settings

Click **Configuration → Audio → Other Settings** to enter the configuration page.
You can choose the **Acoustic Fidelity Mode** ,**Listening Audio Encoding** and **Scene Mode** according to your needs.

2.4 Bluetooth Configuration

Enable Bluetooth function of the device to match with smart device.

Note

Only certain models support the function.

Steps

1. Click ***Configuration → Bluetooth*** to enter the configuration page.
2. Slide **Enable** to enable Bluetooth.
3. Set **Device Name** and **Paired Password**.

Note

- It is applicable to network cabinet speakers and network ceiling speakers, please refer to the actual device. Bluetooth default name is HIK-Audio- and default password is 2345.
- The default password of Bluetooth is 2345.
- Pairing password should be 4 characters.

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

2.5 SIP Configuration

2.5.1 SIP Registration

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

Steps

1. Click **Configure → SIP → SIP Registration** to enter the configuration page.
2. Enable this function and set the parameters.
3. Click **Save**.
4. Register device on SIP server.
5. Refresh the window and check whether the device has been registered or not.

2.5.2 SIP Call

Steps

1. Click **Configure → SIP → SIP Call** to enter the configuration page.
2. Select the desired **Encoding/Decoding Format** as needed, and drag to sort the formats.
3. Enable **Allowed Call** as required and set the **Max. Call Duration**. When an alarm input is triggered, the system will automatically call the preset SIP terminal to establish two-way audio intercom, enabling remote alarm confirmation and real-time communication.
4. Click **Save**.

2.5.3 DTMF

DTMF (Dual-Tone Multi-Frequency) is a signaling technology used in telephone systems, which represents keys (such as 0-9, *, #, etc.) by simultaneously transmitting two specific frequency tones.

Steps

1. Click **Configure → SIP → DTMF** to enter the configuration page.
2. Add DTMF。
   1) Click **Add**.
   2) Slide to enable DTMF.
   3) Enter a custom name to distinguish different DTMF configurations.
   4) Enter the button, which specifies the key identifier that triggers the DTMF function.
   5) Select an audio file to be played when triggered.
   6) Set the volume for audio file playback.
   7) Set the times of playing, specifying how many times the audio file will be played consecutively.
   8) Click Save to complete the setup.
3. (Optional) Click to modify the audio file playback volume.
4. (Optional) Click to modify DTMF information.

2.5 Broadcast Settings

2.5.1 Material Library

Click **Configuration → Broadcast Settings → Material Library** to enter the configuration page.

Set Material Library

- Add custom audio folder: Click +, enter the custom folder name, click **OK** to save the settings.
- Delete custom audio folder: Select the custom audio folder, click to delete the corresponding folder.
- Edit custom audio folder: Select the custom audio folder, click to modify the corresponding folder name.

Set Audio Folder

Steps

1. Click **Configuration → Broadcast Settings → Material Library** to enter the configuration page.
2. Click **Batch Import** to go to local file.
3. After selecting the local file, click **Open** to import the broadcast material in the file to the broadcast material library.

Note

The file size of material library should not exceed 100M, and can store up to 1000 files. It only supports mp3, MP3, wav, WAV, aac, AAC, mp2 and MP2 formats.

4. (Optional) Select the broadcast material and click **Delete** to delete the corresponding broadcast material.
5. (Optional) Click to edit material name.
6. (Optional) Listen broadcast material: Click , the computer and the remote speaker will play the broadcast file. mp2 and MP2 audio files do not support listening.
7. (Optional) Play broadcast material: Click , the remote speaker plays the audio file, and the built-in microphone captures the live sound and returns it to the WEB for playback.
8. (Optional) Select the audio file, click **Convert Text to Audio**, configure the voice conversion rules. Set **File Name**, input **Audio Content**, choose **Language Type**, and select **Audio Type** for broadcasting. Click **Save** to finish the settings.

Note

The following rules apply to the content of voice text:

- Punctuation mark will affect the semantics of pronunciation. Please use punctuation mark correctly. Please view the help for using rules of numbers, Chinese and English.
- Number Reading Settings [n1][n2]: The default setting is active judgement. Adding [n1] before a number reads as a number, and adding [n2] before a number reads as a numerical value.
- Word Pronunciation Settings [h1][h2]: The default setting is active judgement. Adding [h1] before a word reads as letters of the word, and adding [h2] before a word reads as the word.
- English Pronunciation Settings for Number 0[o0]/[o1]: The default [o1] number 0 is pronounced as zero in English. Adding [o0] before the sentence reads as o. The number 0 will only take effect when read as a number, i.e. marking as [n1]. When processed as a numerical value 0, marking as [n2], it will be affected by the marking n， and read as a numerical value.

Set Alarm Linkage/TTS/Custom Audio Library

Note

The built-in alarm linkage and TTS audio libraries cannot be edited or deleted. Please refer to the actual device for details.

Steps

1. Click **Batch Add**.
2. Select the audio material files, click **Add** to add the broadcast materials to the selected audio library.
3. (Optional) Select the broadcast material and click **Delete** to delete the corresponding broadcast material.

4. (Optional) Click to edit material name.
4. (Optional) Listen broadcast material: Click , the computer and the remote speaker will play the broadcast file. mp2 and MP2 audio files do not support listening.
6. (Optional) Play broadcast material: Click , the remote speaker plays the audio file, and the built-in microphone captures the live sound and returns it to the WEB for playback.
7. (Optional) Select the audio file, click **Convert Text to Audio**, configure the voice conversion rules. Set **File Name**, input **Audio Content**, choose **Language Type**, and select **Audio Type** for broadcasting. Click **Save** to finish the settings.

Note

The following rules apply to the content of voice text:

- Punctuation mark will affect the semantics of pronunciation. Please use punctuation mark correctly. Please view the help for using rules of numbers, Chinese and English.
- Number Reading Settings [n1][n2]: The default setting is active judgement. Adding [n1] before a number reads as a number, and adding [n2] before a number reads as a numerical value.
- Word Pronunciation Settings [h1][h2]: The default setting is active judgement. Adding [h1] before a word reads as letters of the word, and adding [h2] before a word reads as the word.
- English Pronunciation Settings for Number 0[o0]/[o1]: The default [o1] number 0 is pronounced as zero in English. Adding [o0] before the sentence reads as o. The number 0 will only take effect when read as a number, i.e. marking as [n1]. When processed as a numerical value 0, marking as [n2], it will be affected by the marking n， and read as a numerical value.

2.5.2 Live Broadcast Configuration

Steps

1. Click **Configuration → Broadcast Settings → Live Broadcast** to enter the configuration page.
2. Enable **Bell Reminder.** When enabled, the bell reminder will be played before real-time broadcasting.
3. Click **Start Speaking** to start real-time speaking, and click to stop speaking.

2.5.3 Scheduled Broadcast Configuration

Add scheduled broadcast task. The device will broadcast according to schedule.

Steps

1. Click **Configuration → Broadcast Settings → Scheduled Broadcast** to enter the configuration page.
2. Click **+ Add** to create scheduled broadcast task.
3. Select **Output Channel.**
3. Slide the Enable button.
4. Enter scheduled **Task Name**.
5. Select **Task Type**.
   - **Day Schedule**: broadcast task will be played at a fixed time every day.
   - **Weekly Schedule**: broadcast task will be played every week.
6. Configure broadcast rule.
   1) Select **Broadcast Rule**.

      Audio File

      Drag and drop the blue bar on the time line, click **Advanced Configuration**, select **Audio File**, and

click **+** to add audio source file in the material library to play.

Speech Synthesis

Drag and drop the yellow bar on the time line, click **Advanced Configuration**, select **Speech Synthesis**, enter the audio content (which can be saved as a template) or directly select a template, and select the parameters to broadcast to male or female.

Note

The following rules apply to the content of voice text:

- Punctuation mark will affect the semantics of pronunciation. Please use punctuation mark correctly. Please view the help for using rules of numbers, Chinese and English.
- Number Reading Settings [n1][n2]: The default setting is active judgement. Adding [n1] before a number reads as a number, and adding [n2] before a number reads as a numerical value.
- Word Pronunciation Settings [h1][h2]: The default setting is active judgement. Adding [h1] before a word reads as letters of the word, and adding [h2] before a word reads as the word.
- English Pronunciation Settings for Number 0[o0]/[o1]: The default [o1] number 0 is pronounced as zero in English. Adding [o0] before the sentence reads as o. The number 0 will only take effect when read as a number, i.e. marking as [n1]. When processed as a numerical value 0, marking as [n2], it will be affected by the marking n， and read as a numerical value.

2) Slide to adjust volume. Volume range is from 0 to 200. If the volume is over 100, volume gain will be expanded.

3) Adjust **Broadcast Ratings**.

Note

Broadcast ratings should be between 0 and 15.

4) Select **Play Mode**.

Play Once

Play in the order of audio list. Each audio will be played only once.

Loop

Repeat in order.

Note

When selecting task type as week schedule, you need to select cycle period.

5) Click **Save** to finish the configuration.

7. Select **Start Date** and **End Date**.
8. Click **Save** to complete the configuration.
9. (Optional) Copy broadcast task. Click to copy the current day's audio broadcast schedule to the rest of the week.

2.5.4 Strategy Configuration

You can set multiple audio playing strategies through strategy settings.

Click **Configuration → Broadcast Settings → Strategy Settings** to enter the configuration page.

Enable **Continue Broadcast in Next Day**. The device will continue to play the next audio in the list at the set time in the next day. Click **Save** to save the settings.

Enable **Resume Play**. The device will replay the audio file, which is played before power-off, after restarting when the function is enabled. Click **Save** to save the settings.

2.5.5 Broadcast Priority

You can set the priority of the broadcasts. Priority range: 0 to 15. The higher the value, the higher the priority. You can set the mixing audio volume. When the device performs multiple broadcast tasks simultaneously, it is sorted according to broadcast priority and supports mixing volume adjustment for low priority broadcast tasks.

2.5.6 Set Audio Template

Steps

1. Click **Configuration → Broadcast Settings →Audio Template** to enter the configuration page.
2. Click **Add Template**, input **Audio Content** and click **Save** to finish the settings.

Note

The following rules apply to the content of voice text:

- Punctuation mark will affect the semantics of pronunciation. Please use punctuation mark correctly. Please view the help for using rules of numbers, Chinese and English.
- Number Reading Settings [n1][n2]: The default setting is active judgement. Adding [n1] before a number reads as a number, and adding [n2] before a number reads as a numerical value.
- Word Pronunciation Settings [h1][h2]: The default setting is active judgement. Adding [h1] before a word reads as letters of the word, and adding [h2] before a word reads as the word.
- English Pronunciation Settings for Number 0[o0]/[o1]: The default [o1] number 0 is pronounced as zero in English. Adding [o0] before the sentence reads as o. The number 0 will only take effect when read as a number, i.e. marking as [n1]. When processed as a numerical value 0, marking as [n2], it will be affected by the marking n， and read as a numerical value.

3. (Optional) Check the audio content to be deleted and click **Delete** to remove the corresponding audio content.

2.6 Alarm Configuration

2.6.1 Alarm Input

Steps

1. Click **Configuration → Alarm Configuration → Alarm Input** to enter the configuration page.
2. After any alarm input No., click ✎ to enter the editing page.
3. Set alarm type, alarm name and enable alarm input handling, configure the arming schedule and linkage method.

Note

Audio and SIP cannot be enabled at the same time.

4. Click **Save** to finish the settings.

2.6.2 Set Audio Exception Alarm

Audio exception alarm function detects the abnormal sound in the scene, such as the sudden increase/decrease of the sound intensity, and some certain actions can be taken as response.

Steps

1. Go to **Configuration** → **Event** → **Event and Detection** → **Audio Exception Detection**.
2. Select one or several audio exception detection types.

Sudden Increase of Sound Intensity Detection

Detect sudden increase of sound intensity. **Sensitivity** and **Sound Intensity Threshold** are configurable.

Note

- The lower the sensitivity is, the more significant the change should be to trigger the detection.
- The sound intensity threshold refers to the sound intensity reference for the detection. It is recommended to set as the average sound intensity in the environment. The louder the environment sound, the higher the value should be. You can adjust it according to the real environment.

Sudden Decrease of Sound Intensity Detection

Detect sudden decrease of sound intensity. **Sensitivity** is configurable.

3. Configure the arming schedule and linkage methods.
4. Click **Save**.

2.6.3 Audio Linkage

Steps

1. Click **Configuration → Alarm Configuration → Audio Linkage** to enter the configuration page.
2. Select **Trigger Source**.

Note

Please select the audio linkage trigger source selected in the alarm input.

3. Select **Audio Type**. Set audio file or audio content. Please refer to the chapter of Broadcast Settings for detailed settings.
4. Set broadcast rule, including broadcast ratings, volume and play mode.
5. Configure the arming schedule.
6. Click **Save** to finish the settings.

2.6.4 Alarm Server

The device can send alarms to destination IP address or host name through HTTP or ISUP protocol. The

destination IP address or host name should support HTTP or ISUP data transmission.

Set Alarm Server

Steps

1. Go to **Configuration** → **Event** → **Alarm Setting** → **Alarm Server**.
2. Click **Add**, and enter **Destination IP or Host Name**, **URL**, and **Port**.
3. Select **Protocol Type**.
4. Click **Test** to check if the IP or host is available.
5. Click **OK**.

Chapter 3 Operation of HikCentral Professional Web Client

You can refer to the **Chapter 2 Login** and **Chapter 34 Broadcast Management** after scanning the following QR code for the detailed operation of HikCentral Professional Web Client.

Figure 3-1 QR Code of Web Client User Manual

Chapter 4 Operation of HikCentral Professional Control Client

You can refer to the **Chapter 2 Login** and **Chapter 30 Broadcast** after scanning the following QR code for the detailed operation of HikCentral Professional Control Client.

Figure 4-1 QR Code of Control Client User Manual


See Far, Go Further