

Network Amplifier

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.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

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 . . . 1
Chapter 2 Web Client Operation Instructions . . . 2
2.1 System Configuration . . . 2
2.2 Network Configuration . . . 4
2.2.1 TCP/IP Configuration . . . 4
2.2.2 Set Port . . . 4
2.2.3 Device Access Settings . . . 4
2.3 Audio Configuration . . . 5
2.3.1 Channel Configuration . . . 5
2.3.2 Audio Configuration . . . 5
2.3.3 Speaker Test . . . 5
2.4 Bluetooth Configuration . . . 5
2.5 Broadcast Settings . . . 6
2.5.1 Material Library . . . 6
2.5.2 Scheduled Broadcast Configuration . . . 6
2.5.3 Strategy Configuration . . . 7
2.6 Alarm Configuration . . . 8
2.6.1 Alarm Input . . . 8
2.6.2 Alarm Output . . . 8
2.6.3 Audio Linkage . . . 8
Chapter 3 Operation of HikCentral Professional Web Client . . . 9
Chapter 4 Operation of HikCentral Professional Control Client . . . 10

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 **Configure → 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 **Configure → 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.

- 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 **Configure → 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 TCP/IP Configuration

Steps

1. Click **Configure → Network → Network Configuration → TCP/IP** to enter the configuration page.
2. Configure network parameters.
3. Select **NIC Type**, slide to enable **DHCP**, and 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.

Configure HTTP(s) Port

Click **Configure → 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 Device Access Settings

The device can be operated by mobile client.

Steps

1. Click **Configure → Network → Working Mode** to enter the configuration page.
2. Select platform access mode.
   - Select **ISUP** as platform access mode.
     Slide **Enable** to select **Protocol Version**.
     Configure **Server Address**, set **Port No.**, enter **Device ID,** and set **Secret Key**.
   - Select **Hik-Connect** as platform access mode.
     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.

2.3 Audio Configuration

2.3.1 Channel Configuration

Note

The device should be connected before configuring.

Click **Configure → Audio → Channel Configuration** to enter the configuration page.
Select input channels and corresponding output channels according to requirements.

2.3.2 Audio Configuration

Click **Configure → Audio → Audio** to enter the configuration page.
You can drag the slider to configure the input volume and output volume; You can also choose the acoustic fidelity mode according to your needs.

2.3.3 Speaker Test

Click **Configure → Audio → Speaker Test** to enter the configuration page.
Click **Test** to test the speaker.

2.4 Bluetooth Configuration

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

Steps

1. Click ***Configure → Bluetooth*** to enter the configuration page.
2. Select to *enable Bluetooth*.
3. Set **Bluetooth 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 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 Broadcast Settings

2.5.1 Material Library

You can add and delete broadcast material in the broadcast material library.

Steps

1. Click **Configure → 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 material library should be no more than 100 megabytes. Up to 1,000 materials can be stored. Only wav and mp3 formats are supported.

4. (Optional) Select the broadcast material to delete. Click **Delete** to delete the corresponding broadcast material.
5. (Optional) Click to edit material name.

2.5.2 Scheduled Broadcast Configuration

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

Steps

1. Click **Configure → 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 **Voice Composition**, enter voice content, 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.

2.5.3 Strategy Configuration

You can set multiple audio playing strategies through strategy settings.

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

Enable **Continue Broadcast in Next Day**. The device will continue to broadcast the broadcast at the set time of 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.

2.6 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.
4. Click **Save** to finish the settings.

2.6.2 Alarm Output

Steps

1. Click **Configuration → Alarm Configuration → Alarm Output** to enter the configuration page.
2. After any alarm output No., click to enter the editing page.
3. Set alarm type and delay time, configure the arming schedule.
4. Click **Save** to finish the settings.

2.6.3 Audio Linkage

Steps

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

Note

Please select the audio linkage channel selected in the alarm input.

3. 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.

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



UD35509B