



Panic Alarm Device

User Manual

Available Model

Product	Model
Panic Alarm Station	DS-KEP311X DS-KEP311X-G DS-KEP311X-ZJ
Panic Alarm Box	DS-KEB801X-C DS-KEB801X-CG

Contents

Chapter 1 Activation	1
1.1 Activate via SADP	1
1.2 Activate Device via Client Software	2
Chapter 2 Operation via Web Browser	4
2.1 Login	4
2.2 Overview	5
2.3 Image and Video Search	7
2.4 Configuration	8
2.4.1 Device Information	8
2.4.2 Device Time Settings	9
2.4.3 Online Users	9
2.4.4 Network Settings	9
2.4.5 Video/Audio Settings	19
2.4.6 Image Settings	21
2.4.7 Set OSD Parameter	23
2.4.8 Device Management	23
2.4.9 Storage Settings	27
2.4.10 Audio Quality Diagnosis	30
2.4.11 Alarm Parameters Settings	31
2.4.12 Intercom Settings	31
2.4.13 Audio Library Settings	36
2.5 Maintenance and Security	36
2.5.1 System Upgrade and Maintenance	36
2.5.2 Device Debugging	37
2.5.3 Set Network Diagnosis	37
2.5.4 Search and View Logs	38

2.5.5 Security Audit Log	38
2.5.6 Video&Audio Self-Test Settings	38
2.5.7 Security Settings	38
2.6 Open Source Software Licenses	39
2.7 Change Administrator's Password	39
2.8 Logout	40
Appendix A. Legal Information	41
Appendix B. Symbol Conventions	43

Chapter 1 Activation

In order to protect personal security and privacy and improve the network security level, you should activate the device the first time you connect the device to a network.

1.1 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website <http://www.hikvision.com/en/>, and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.



Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, 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.

-
4. Click **Activate** to start activation.

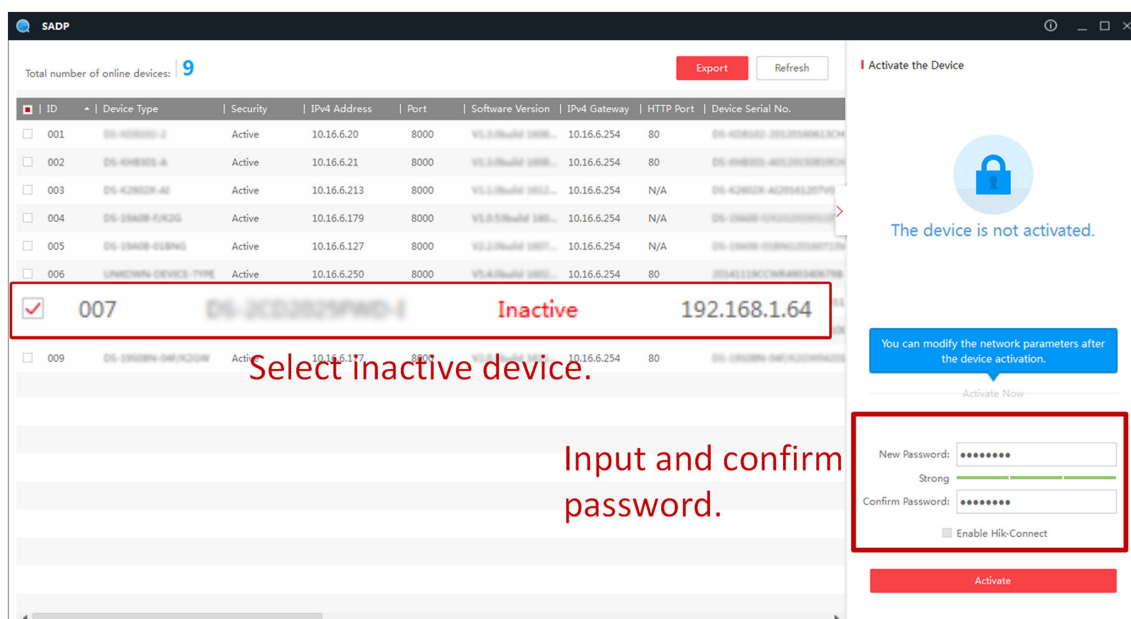


Figure 1-1 Device List

Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.

- 1) Select the device.
- 2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
- 3) Input the admin password and click **Modify** to activate your IP address modification.

1.2 Activate Device via Client Software

Before You Start

- Get the iVMS-4200 client software from the supplied disk or the official website <http://www.hikvision.com/en/> . Install the software by following the prompts.
- The device and the PC that runs the software should be in the same subnet.

Steps

1. Run the client software.
2. Enter **Device Management** or **Online Device**.
3. Check the device status from the device list, and select an inactive device.
4. Click **Activate**.
5. Create and confirm the admin password of the device.



Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, 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.

6. Click **OK** to start activation.

Device status will change to **Active** after successful activation.

7. Edit IP address of the device.

- 1) Select a device and click **Modify Netinfo** at **Online Device**.
- 2) Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking **DHCP**.
- 3) Input the admin password of the device and click **OK** to complete modification.

Chapter 2 Operation via Web Browser

2.1 Login

After logging in, you can set the device parameters including events, device management, and device status.

Before You Start

The device has been activated.



Note

Recommended browsers: IE11, Firefox 54+, or Chrome. If functionality issues occur, try Chrome or upgrade your browser version.

Steps

1. Enter ***http://device_IP_address*** in the browser address bar and press Enter to access the login interface.

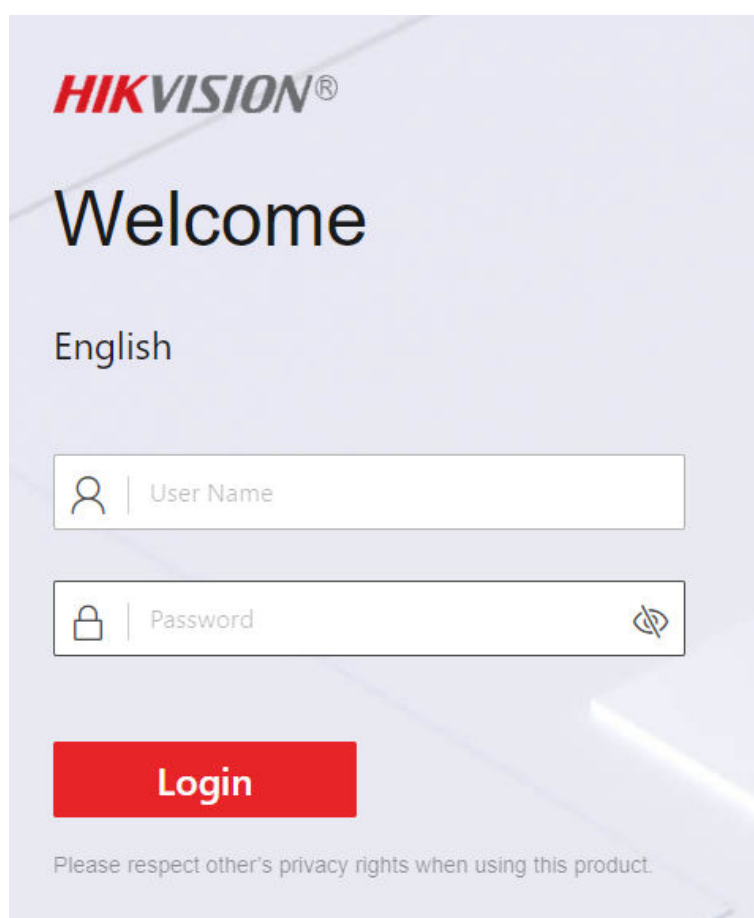


Figure 2-1 Login

2. Enter user name and password, then click **Login**.

After login, you will enter the main page.

2.2 Overview

View device-related data statistics and status overview.

After login, click **Overview**.

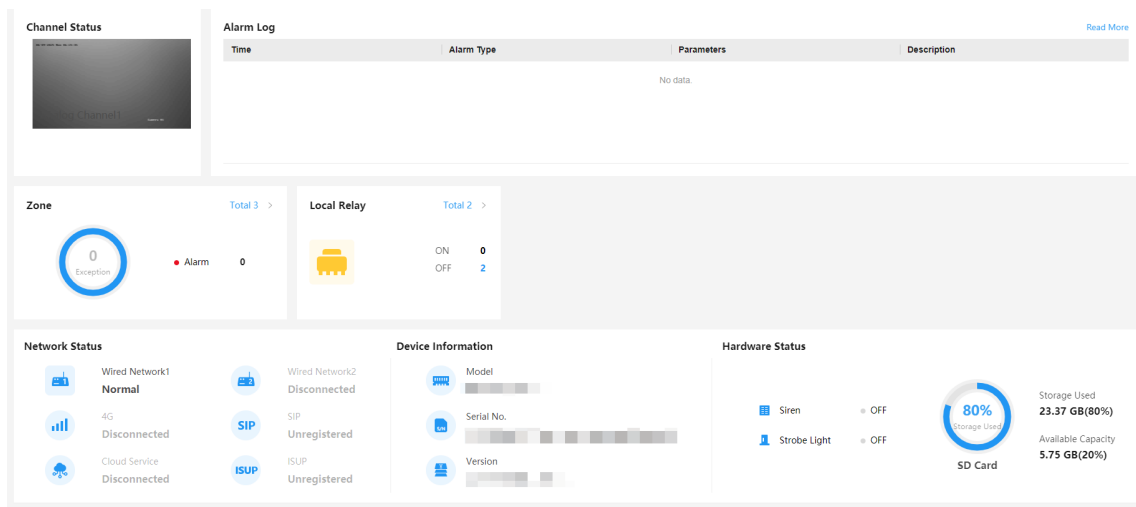


Figure 2-2 Overview

Channel Status

View device camera's live video.

Alarm Log

View alarm time, type, parameters and description. Click **Read More** to access the log interface for advanced search and viewing.

Zones

View number of zones in alarm/exception status.

Click **Total** in the upper right corner to access zone management interface.

Local Relay

View number of associated devices.

Click **Total** in the upper right corner to access management interface.

Network Status

View connection and registration status for wired, 4G, SIP, cloud service and ISUP.

Click network name or icon to access network configuration interface.

Device Information

View device model, serial number and version.

Click any area in device information section to access basic configuration interface.

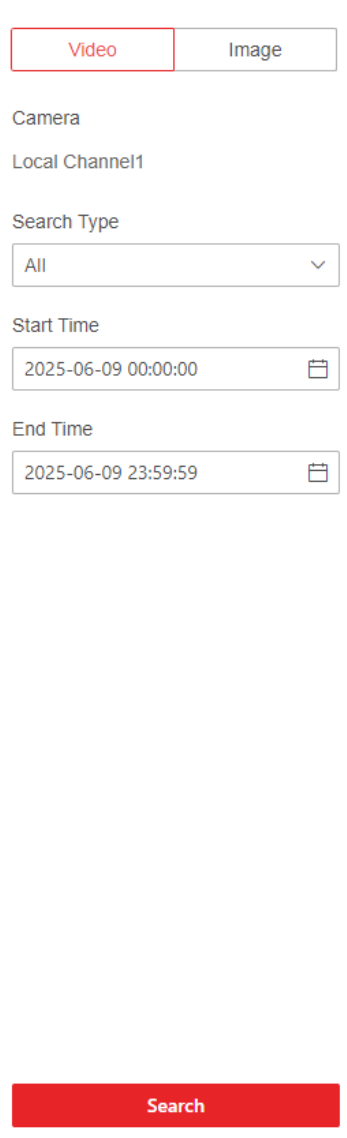
Hardware Status

View siren and strobe light status and SD card used/available capacity.

2.3 Image and Video Search

Steps

1. Enter the device address in the browser, after logging in, click **Image Search** to access the interface.



The screenshot shows a web interface for video search. At the top, there are two tabs: 'Video' (highlighted with a red border) and 'Image'. Below the tabs, the 'Camera' section is set to 'Local Channel1'. The 'Search Type' is a dropdown menu currently showing 'All'. The 'Start Time' is set to '2025-06-09 00:00:00' and the 'End Time' is set to '2025-06-09 23:59:59'. At the bottom, there is a red 'Search' button.

Figure 2-3 Video Search

2. Select the video or image category to search.
3. Select the required **Search Type**.
4. Select **Start Time** and **End Time**.
5. Click **Search** to query.

Search results are displayed in the list on the right side of the interface.

6. Optional: Click **Download** to download video or image.

2.4 Configuration

2.4.1 Device Information

Enter the device address in the browser, after logging in, click **Configuration** → **System** → **System Settings** → **Basic Information** to access the interface.

* Device Name

Device No. 255

Model

Serial No.

Firmware Version [Upgrade](#)

Encoding Version

Hardware Version

Web Version

Plugin Version

Number of Alarm Lights 1

Number of Sounder 1

Number of Local Zones 3

Number of Relays 2

Number of Analogue Channels 1

Number of Digital Channels 1

Number of User 1

[Save](#)

Figure 2-4 Device Information

You can edit the device name, then click **Save**.

View device model, serial number, version number, and supported device and channel number. Click **Firmware Version's Upgrade** to upgrade the firmware. See **System Upgrade and Maintenance** for details.

2.4.2 Device Time Settings

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → System → System Settings → Time Settings** to access the configuration interface.
2. Select time zone.
3. Select time synchronization method.
 - Select **NTP** to automatically sync with server time. Enter server address, NTP port number and interval.
 - Select **Manual Time Sync.** to set time manually. Set time or click **Sync with Computer**.
4. Set DST.
 - 1) Enable **DST**.
 - 2) Set the DST start time and end time.
 - 3) Set the bias time.
5. Click **Save**.

2.4.3 Online Users

View online users.

Enter the device address in the browser, after logging in, click **Configuration → System → User Management → Online Users** to access the interface.

View online user information including user name, level, IP address and operation time.

Click **Refresh** to reload the page.

2.4.4 Network Settings

Basic Network Settings

Set device TCP/IP information.

Enter the device address in the browser, after logging in, click **Configuration → Network → Network Configuration → TCP/IP** to access the configuration page.

Network Card 1 2

LAN

NIC Type Auto ▼

DHCP ☐

* IPv4 Address

* IPv4 Subnet Mask

* IPv4 Default Gateway

Mac Address

* MTU 1500

Default Route Network Card1 ▼

DNS Server

Preferred DNS Server

Alternate DNS Server

Save

Figure 2-5 Basic Network Parameter Settings

After setting parameters, click **Save** to save settings.

Network Card

Select 1 or 2 as needed.

NIC Type

Select network card type from dropdown, default is self-adaption.

DHCP

If disabled, manually configure IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway, Preferred DNS Server and Alternate DNS Server.

If enabled, system automatically assigns IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway, Preferred DNS Server and Alternate DNS Server.

MTU

Set MTU value. MTU (Maximum Transmission Unit) refers to the size of the largest packet that can be transmitted in a single network transaction (in bytes). Configure as needed.

Set Mobile Network

If the device has a SIM card inserted, you can set mobile network parameters. The device can upload alarm information to the alarm center via mobile network.

Enter the device address in the browser, after logging in, click **Configuration → Network → Network Settings → Mobile Network** to enter the configuration page.

Mobile Network ☒

Network Settings

User Name

Password

APN

* MTU

Access Number

UIM Number

Flow Limit

Enable Flow Limit ☒

* Monthly Flow Threshold MB

Start Date 1st Day of Each Month

* Flow Statistics MB [Refresh](#)

Quota SMS Reminder ☐

[Save](#) [Dialing Status Detection](#)

Figure 2-6 Mobile Network Parameters Settings

Drag the slider to enable **Mobile Network**.

Configure mobile network parameters.

Network Settings

User Name/Password/APN

Enter the user name, password and APN information after consulting your network operator.

MTU

Enter the maximum transmission unit for network data service.

Access Number

Enter the number of the inserted SIM card.

UIM Number

Enter the UIM number after consulting your network operator.

Flow Limit

Enable Flow Limit

When enabled, data usage will be limited.

Monthly Flow Threshold

Set the maximum amount of data that can be used per month. If usage exceeds this value, an alarm will be triggered and uploaded to the alarm center.

Flow Statistics

The data usage of the device for the current month will be accumulated and displayed in the text box. Click **Refresh** to update.

Quota SMS Reminder

When enabled, an SMS alert will be sent to the configured phone number when the data threshold is exceeded. You can enter the phone numbers that need to receive alerts in the list.

Dialing Status Detection

Click **Dialing Status Detection** to view dialing status. Click **Refresh** to update the status.

After configuring parameters, click **Save** to save the settings.

Port Settings

Set corresponding ports when accessing devices via network as needed.

HTTP Settings

Enter the device address in the browser, after logging in, click **Configuration → Network → Network Services → HTTP(S)** to configure HTTP ports.

HTTP Port

When logging in via browser, add the port number after the address. For example, when HTTP port is changed to 81, you need to enter `http://192.0.0.65:81`.

HTTP Listening

Device sends alarm information to target IP or domain via HTTP protocol, requiring the target IP/domain to support HTTP transmission. Enter target IP/domain, URL address and port, then select protocol type.

Click **Save** to complete configuration.

RTSP Settings

Enter the device address in the browser, after logging in, click **Configuration → Network → Network Services → RTSP** to configure and view RTSP ports.

RTSP is Real Time Streaming Protocol port. You can view and configure RTSP ports.

Click **Save** to complete configuration.

SDK Service Port Settings

Enter the device address in the browser, after logging in, click **Configuration → Network → Network Services → Service Port** to configure and view SDK service ports.

View and edit device service ports.

Click **Save** to complete configuration.

Set Port Mapping (NAT)

Set port mapping to map internal network ports to external network ports, enabling access to internal network ports from external networks.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Network → Network Services → NAT** to access the configuration page.

Enable UPnP ☒

Port Mapping Mode: Auto

Port Mapping List	Port Type	External Port	External IP Address	Internal Port	Status
	HTTP	80	0.0.0.0	80	Not Valid
	Server Port	8000	0.0.0.0	8000	Not Valid
	RTSP	550	0.0.0.0	550	Not Valid

Save

Figure 2-7 Port Mapping Configuration

2. Click the slider **Enable UPnP**.
3. Select **Port Mapping Mode**.
 - When selecting **Auto** as the mapping method, no port mapping is required on the router. Simply enable UPnP function on the router to open ports.
 - When selecting **Manual** as the mapping method, you need to fill in the mapped port number and enable UPnP function on the router to open ports. In this case, there's no need to edit the device's own ports.
4. Click **Save**.

SIP Settings

SIP server enables communication between terminals across different network segments. Without registration, only terminals within the same segment can communicate. After successful SIP server registration, terminals can dial calls using SIP IDs.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration** → **Network** → **Device Access** → **SIP** to access the interface.

Protocol Selection

☒ Private Protocol ☐ Standard SIP Protocol

Enable

☒

Enrollment Status

Not Enrolled

Server Type

☒ IPv4 ☐ Domain

* IP

10.6.120.60

* Server Port

5066

* Enrollment Password

* Device ID

176

* Device Location

176

Reuse in Device Name

☐

When enabled, the device name will automatically reuse the private SIP device location information.

* Local Port

5060

* Enrollment Period

10

min

Communication Network

Wired Network Card1

▼

Save

Figure 2-8 SIP Settings

2. Select **Private Protocol** or **Standard SIP Protocol** according to your SIP service requirements.

3. Check **Enable**.
4. Set server type as **IPv4** or **Domain**, then enter the server's IP or domain address.
5. Set corresponding parameters based on the selected protocol type.
 - If **Private Protocol** is selected, set **Server Port**, **Enrollment Password**, **Device ID**, **Device Location**, **Local Port**, **Enrollment Period** and **Communication Network**.
 - If **Standard SIP Protocol** is selected, set **Server Port**, **User Name**, **Enrollment Password**, **Local Port**, **Communication Network** and **Target User Name**.
6. Click **Save** to complete configuration.

Set ISUP

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Network → Device Access → ISUP** to enter the configuration interface.
2. Slide the **Enable** switch to activate ISUP platform function.
3. Check the ISUP protocol version, set the server address, port and device ID.



Note

The default port number for ISUP platform is: 7660.

4. Select the communication network priority method.

Auto

The priority of the network is: Wired network first, then wireless network.

Wired Network Priority

Wired network first, then wireless network.

3G/4G/GPRS

The system will only use 3G/4G/GPRS as network.

Wired Network Card 1/Wired Network Card 2

The system will only use the specified wired network card (1 or 2) as network.

5. Enter the **Encryption Key**.
6. Click **Save**.

ONVIF Protocol Settings

When connecting devices via ONVIF protocol, configure ONVIF users as needed to enhance network security.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Network → Device Access → ONVIF** to access the interface.

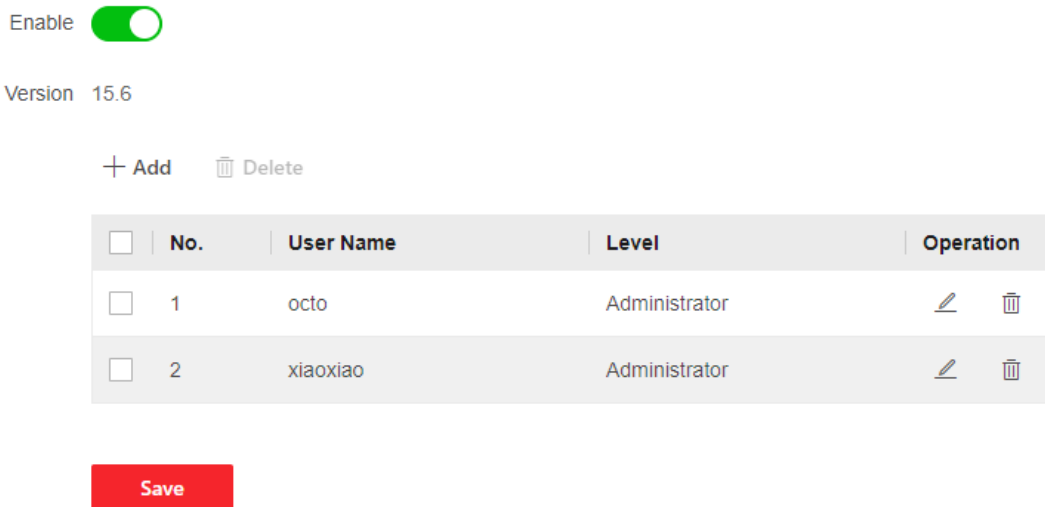


Figure 2-9 ONVIF Protocol Settings

2. Slide the **Enable** switch to activate ONVIF function.
3. Add users.
 - 1) Click **+Add**.
 - 2) Enter user name, create and confirm password.



Caution

- To better protect your privacy and improve product security, you are strongly recommended to set a more complex password according to the following rules: the password should be between 8 and 16 characters, including digits, lowercase letters, and special characters.
- 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) Select level.

Administrator

Administrator users can manage and operate the device.

- 4) Click **Confirm**.
4. **Optional:** Repeat above steps to add multiple ONVIF users as needed.
5. **Optional:** Click or to edit or delete users.
6. Click **Save**.

Protocol Compatibility Mode Settings

Enter the device address in the browser, after logging in, click **Configuration → Network → Device Access → Protocol Compatibility Mode** to enter the settings interface.

When enabled **Protocol Compatibility Mode**, it will be compatible with the user information verification method of the old version SDK client during login.

Alarm Center Settings

Set alarm center parameters to upload alarm messages to centers when triggered.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration** → **Network** → **Alarm Communication** → **Network Center** to access the interface.

The screenshot displays the 'Network Center' configuration interface. At the top, there are three tabs: 'Notify Surveillance Center', 'Wired Network1' (which is highlighted with a red border), 'Wired Network2', and 'Wireless Network'. Below the tabs, there is a toggle switch for 'Enable Wired Network1' which is currently turned on (green). Underneath, the 'Server Type' is set to 'IPv4' (selected with a red radio button) and 'Domain' (unselected with a grey radio button). The form includes several input fields: '* IP' with the value '0.0.0.0', '* Port' with the value '7200', 'Protocol' with a dropdown menu showing 'HIK Protocol', and '* User Name' with the value '000000'. At the bottom of the form is a red 'Save' button.

Figure 2-10 Network Center Interface

2. Select **Notify Surveillance Center** as **Wired Network 1**, **Wired Network 2** or **Wireless Network** as needed.
3. Check **Enable Wired Network 1/Enable Wired Network 2/Enable Wireless Network**, then set upload center parameters.

Server Type

Center server address type, select IPv4 or Domain.

IP Address/Domain

Enter server IP address or domain according to server type.

Port

Center port number. Default is 7200 for HIK protocol; set to 4001 for NAL2300 protocol.

Protocol Type

Default is HIK protocol.

User Name

Supports numbers and letters. Length range: 6 to 9 digits for HIK protocol; 6 digits for NAL2300 protocol.

4. Click **Save**.

2.4.5 Video/Audio Settings

Video Parameter Settings

Configure image parameters such as quality and resolution for device cameras.

Steps

- 1.** Enter the device address in the browser, after logging in, click **Configuration → Video/Audio → Video** to access the configuration interface.

The screenshot displays the 'Video Settings' interface. It includes the following elements:

- Camera:** A dropdown menu set to 'Analog Channel1'.
- Stream Type:** Two buttons, 'Main Stream' (highlighted with a red border) and 'Sub-Stream'.
- Video Type:** Two radio buttons, 'Mixed Flow' and 'Video Flow' (selected).
- Resolution:** A dropdown menu set to '2560*1440'.
- Bit Rate Type:** Two radio buttons, 'Constant Bit Rate' (selected) and 'Variable Bit Rate'.
- Image Quality:** A dropdown menu set to 'Medium'.
- Frame Rate:** A dropdown menu set to '25fps'.
- * Code Rate:** A text input field containing '6144' and a unit label 'kbps'.
- * I Frame Interval:** A text input field containing '25'.
- Video Encoding:** Two radio buttons, 'H.264' (selected) and 'H.265'.
- SVC Encoding:** Three radio buttons, 'ON', 'Close' (selected), and 'Auto'.
- Video Standard:** Two radio buttons, 'PAL' (selected) and 'NTSC'. Below this is a note: 'After changing the video standard, you need to restart the device'.
- Video&Audio Encoding:** Three radio buttons, 'G.711ulaw' (selected), 'AAC', and 'PCM'.
- Save:** A red button at the bottom.

Figure 2-11 Video Settings Interface

2. Set stream type, video type, resolution, bit rate type, image quality, frame rate, bit rate, code rate, I-frame interval, video encoding, SVC encoding, video standard and audio&video encoding.
3. Click **Save**.

Audio Parameter Settings

Configure device volume.

Steps

1. Enter the device address in the browser, after logging in, click **Settings → Video/Audio → Audio** to access the interface.

The screenshot displays the 'Audio Settings' interface, organized into three main sections: 'Audio Encoding', 'Audio Input', and 'Audio Output'.

- Audio Encoding:** Features a dropdown menu for 'Intercom Audio Encoding' currently set to 'G.711ulaw'.
- Audio Input:** Includes radio buttons for 'Audio Input' (selected 'micIn', unselected 'lineIn1') and a 'micIn Volume' slider set to 5.
- Audio Output:** Contains three sub-sections:
 - Broadcast Audio Output:** Has checkboxes for 'Output Type' (selected 'spkOut', unselected 'lineOut1') and sliders for 'spkOut Volume' (set to 1) and 'lineOut1 Volume' (set to 6).
 - Intercom Audio Output:** Similar to Broadcast, with 'spkOut' selected and volumes set to 1 and 6 respectively.
 - Prompt Voice Audio Output:** Also with 'spkOut' selected and volumes set to 1 and 6.

A red 'Save' button is located at the bottom center of the interface.

Figure 2-12 Audio Settings Interface

2. Set audio encoding, audio input and audio output parameters.
3. Click **Save**.

2.4.6 Image Settings

Set parameters like brightness, contrast, saturation, sharpness, day/night switch, backlight, and video adjustment for device live view.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Image → Display Settings** to access the page.

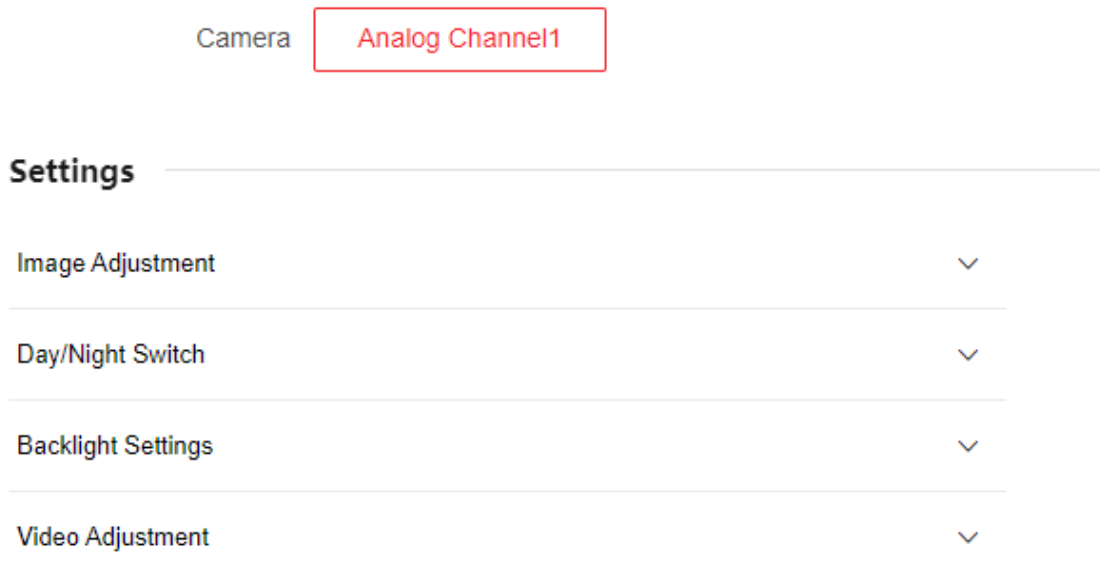


Figure 2-13 Image Settings

2. Select channel and configure parameters.

Image Adjustment

Drag sliders or input values to configure brightness, contrast, saturation and sharpness as needed.

Click **Defaults** to reset parameters.

Day/Night Switch

Set day/night switch to **Auto**, **Day**, **Night** or **Scheduled-Switch**.

Auto

Device automatically switches between day (color) and night (B/W) modes based on light intensity.

Set sensitivity and filter time required.

Day

Device live view remains in day mode (color).

Night

Device live view remains in night mode (B/W).

Scheduled-Switch

After selecting **Scheduled-Switch**, set start/end time for day mode. After end time, night mode activates.

Backlight

Enable **WDR** or **HLC** based on environment. For WDR, configure WDR level.

Video Adjustment

Set frame rate for remote live view. Device restart required after editing.

PAL

25 frames per second, applicable in Mainland China, Hong Kong (China), Middle East and Europe.

NTSC

30 frames per second, applicable in USA, Canada, Japan, Taiwan (China), South Korea, Philippines.

2.4.7 Set OSD Parameter

By setting the OSD, channel, time and other information can be displayed on live view or recorded video.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Image → OSD Settings** to access the configuration page.
2. Select a channel.
3. Check **Display Name**, **Display Date** or **Display Week** as needed. The checked items will appear on the live view.
4. Enter **Camera Name**, select **Time Format** and **Date Format**.
5. Select **OSD Mode**, **OSD Size**, **Alignment**, and **Min. Boundary**.
6. **Optional:** You can customize the display content as needed. Tap **Add**, enter the required characters.
7. Click **Save**.

2.4.8 Device Management

Zone Settings

Connect detectors to realize arming/disarming by configuring zones.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Device → Zone → Local Zone** to access the interface.

No.	Name	Zone Type	Sensitivity	Zone Status	Operation
1	zone1	Disabled	500ms	Normal	
2	zone2	Disabled	500ms	Normal	
3	zone3	Emergency Help Zone	500ms	Normal	

Figure 2-14 Zone Management

All zone information can be viewed in the list.

2. Select the zone to configure, click  to open the zone parameter settings window.
3. You can edit zone parameters including **Name**, **Detector Type**, **Zone Type**, and **Audio File**.

Zone type descriptions:

Instant

Enters alert status after system arming, triggers immediate alarm when activated.

Suitable for IR detectors, commonly installed in supermarkets, etc.

Fire

24-hour monitoring with fixed alarm sound linkage (voice/siren).

Typically used for smoke/heat detectors in fire-prone areas.

24-hour Silent Zone

24-hour monitoring without alarm sound linkage (voice/siren).

Used for silent alarms (e.g., bank emergency buttons) and cannot be bypassed.

Emergency Help Zone

24-hour monitoring. Typically used for panic buttons, smoke detectors, and glass break detectors.

4. **Optional:** Set **Upload Restored Alarm**. When enabled, alarm restored reports will be sent to the center.
5. Set linkage for **Siren**, **Strobe Light**, **Relay**, **Channel**, **Recording**, and **Capture**. When triggered, linked devices will activate.
6. Click **Save**.
7. **Optional:** Click **Copy To** to duplicate configurations to other zones.

Siren Settings

Enable the siren to sound when alarm events occur.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Device → Siren** to access the page.

2. Enable or disable **Sounder Switch** as needed. When enabled, the associated siren will sound upon alarm trigger.
3. Click **Save**.

Strobe Light Settings

Configure strobe lights to flash when alarm events occur.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Device → Strobe Light** to access the page.

Strobe Light Name Strobe Light1

Strobe Light Switch ☐

Advanced

Scheduled Flashing

Scheduled Flashing ☐

Flashing Schedule

Flashing Schedule ☐

Control Operation Priority

Priority Settings	Priority	Control Method
Priority1	☒ Schedule Template of Strobe	☐ Alarm Control Strobe ☐ Manual Control Strobe
Priority2	☐ Schedule Template of Strobe	☒ Alarm Control Strobe ☒ Manual Control Strobe
Priority3	☐ Schedule Template of Strobe	☐ Alarm Control Strobe ☐ Manual Control Strobe

Save

Figure 2-15 Strobe Light

2. Enable or disable **Strobe Light Switch** as needed. When enabled, linked strobe lights will flash.
3. Configure advanced alarm light parameters.

Scheduled Flashing

After enabling **Scheduled Flashing**, set the flashing duration by configuring **Lighting Duration** and **Lighting off Duration**.

Flashing Schedule

Enable **Flashing Schedule** and use the brush tool on the timeline to set flashing periods. The alarm light will flash during configured time periods.

4. Configure operation priority. The device controls alarm lights according to the checked items in priority order.
5. Click **Save**.

Relay Settings

When an event occurs, you can link a relay output if it is required.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Device → Relay → Local Relay** to access the configuration interface.

☺ ON ☹ OFF

☐	No.	Name	Status	Output Delay(s)	Operation
☐	1	AlarmOut1	OFF	0	
☐	2	AlarmOut2	OFF	0	

Figure 2-16 Relay Management

All relay information can be viewed in the list.

2. Select a relay to configure, click to open the relay parameters settings interface.
3. You can edit relay parameters including **Name** and **Output Delay**.
4. **Optional:** Enter the **Output Delay** time.



Note

The relay will start output after the configured time. Output delay can be set from 1 to 600 seconds.

5. **Optional:** Enable **Close When Relay Connected** as needed. When enabled, the relay turns off when the triggered call is answered; if disabled, the relay turns off after the call ends.
6. Click **OK**.



Note

Multiple relays can be associated with the same wireless output module.

7. **Optional:** Check relays in the list and click **ON/OFF** to manually control relays.

Key Backlight Settings

You can set the activation method for key backlight.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Device → Button Backlight → Button Backlight** to access the interface.
2. Slide the switch to enable the required configuration items.

Close All The Time

When enabled, the button backlight remains off.

Close When Free

The button backlight remains off when the device is idle.

Stay On During Two-Way Audio

The button backlight stays on when the device is in two-way audio mode.

Stay On During Calling

The button backlight stays on when the device is making a call.

3. Click **Save**.

2.4.9 Storage Settings

SD Card Management

View SD card capacity information and format SD card.

Steps

1. Insert the SD card into the device.
2. Enter the device address in the browser, after logging in, click **Configuration → Storage → Storage Management → SD Card Management** to access the configuration interface.
3. View the current status and capacity of the SD card.
4. **Optional:** Click **Format** to format the current SD card. All content on the SD card will be erased after formatting.
5. Set storage parameters including storage mode, recording quota percentage and material quota percentage.
6. Click **Save**.

Recording Schedule Settings

Set the device's automatic recording schedule.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Storage → Schedule Settings → Recording Schedule** to access the configuration interface.

Enable ☒

Recording Schedule Sche... Event... Zone ... Panic... Clear ...

	00	02	04	06	08	10	12	14	16	18	20	22	24
Monday													
Tuesday													
Wednesday													
Thursday													
Friday													
Saturday													
Sunday													

Advanced ^

Video Coverage ☒

Record Audio ☒

Stream Type ☒ Main Stream ☐ Sub-Stream

Pre-Recording Time ☐ No Pre-Recording ☒ 5 s

Recording Delay ☒ 5 s ☐ 10 s

Save

Figure 2-17 Recording Schedule Interface

- Slide the **Enable** switch to activate the recording schedule function.
- Select the recording schedule brush and drag on the timeline to mark the required recording periods.
- Optional:** Click **Advanced** to expand advanced configuration options.

Video Coverage

When enabled, recordings will overwrite oldest files when SD card is full.

Record Audio

When enabled, audio will be recorded along with video.

Stream Type

Select main stream or sub-stream as needed.

Pre-Recording Time

Set the pre-recording duration before scheduled recording starts.

Recording Delay

Set the extended recording duration after scheduled recording ends.

- Click **Save**.

Set Capture Schedule

Set the automatic capture schedule for the device.

Steps

1. Enter the device address in the browser, log in, and click **Configuration** → **Storage** → **Schedule Settings** → **Capture Schedule** to access the configuration interface.

Capture Schedule

Enable ☐

Capture Parameters

Schedule

Scheduled Capture ☒

Resolution 1280*720

Image Quality ☐ Low ☐ Medium ☒ High

* Capture Interval Millisecond ▾

Event

Event Capture ☒

Resolution 1280*720

Image Quality ☐ Low ☐ Medium ☒ High

* Capture Interval Millisecond ▾

Capture Number ⬆ ⬇ ⬆

Save

Figure 2-18 Capture Schedule Interface

2. Slide **Enable** to activate the capture schedule function.
3. Select the capture schedule brush and drag it on the timeline to mark the time periods for capture.
4. set other capture parameters.

Scheduled Capture

When enabled, you can set the **Image Quality** and **Capture Interval**. The device will capture pictures at the configured interval.

Event Capture

When enabled, the device will capture pictures based on the configured **Image Quality**, **Capture Interval**, and **Capture Number** when an event is triggered.

5. Click **Save**.

2.4.10 Audio Quality Diagnosis

Set audio rules and diagnostic methods.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration** → **Event** → **Exception Detection** → **Audio Quality Diagnosis** to access the configuration interface.

Select Channel **Analog Channel**

Setting Rule

Settings

Sound Sudden Increase ☐

Sound Sudden Decrease ☐

Arming Schedule

Arming Schedule **Audio Detection** **Clear** ...

	00	02	04	06	08	10	12	14	16	18	20	22	24
Monday													
Tuesday													
Wednesday													
Thursday													
Friday													
Saturday													
Sunday													

Linkage Settings

Alarm Output ☐ Select All

☐ A->1 ☐ A->2

Save

Real-time Volume

100
80
60
40
20
0

now

Figure 2-19 Audio Quality Diagnosis Interface

2. Set parameters.

Select Channel

By default, **Analog Channel** is selected.

Sound Sudden Increase

When enabled, sets the sensitivity and threshold for sudden sound increase. Higher sensitivity makes triggering easier; higher threshold requires stronger sound to trigger.

Sound Sudden Decrease

When enabled, set the sensitivity for sudden sound decrease. Higher sensitivity makes triggering easier.

Arming Schedule

Select the arming time brush and draw time periods on the timeline. Audio quality diagnosis will be performed during the drawn time periods. When the sound intensity exceeds the threshold, an alarm will be triggered.

Alarm Output

Select the alarm output method. When the sound intensity exceeds the threshold, alarm linkage will be triggered.

3. Click **Save**.

2.4.11 Alarm Parameters Settings

Set tampering alarm. When enabled, the device will trigger an alarm if forcibly dismantled.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Alarm Settings → Alarm Parameters** to access the interface.
2. Enable **Tampering Alarm** as needed.
3. Click **Save**.

2.4.12 Intercom Settings

Call Settings

Set related parameters for calling and receiving calls.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Intercom → Call Settings** to enter the interface.
2. Set calling-related parameters.

Call Ends Upon Rejection

When enabled, if any receiver rejects the call after the device initiates a call, the call will be ended. When disabled, after the device initiates a call, it will wait until all receivers reject the call or any receiver accepts the call before ending the call.

Call Timeout

If the call duration exceeds the set duration, it will be considered as a timeout, and the user needs to call again.

Call Extension Time

You can set the call extension time. If no one answers after exceeding the extension time, it will be considered as a timeout, and the user needs to call again.

3. Set called-related parameters.

Speak

If a management device calls this device, you can choose **Auto Answer** or **Manual Answer** to answer the call from the management device.

Alarm Terminal Call

If another alarm terminal calls this device, you can choose **Auto Answer** or **Manual Answer** to answer the call from other alarm terminals.

GSM Call

If a GSM phone calls this device, you can choose **Auto Answer** or **Manual Answer** or **Disabled** to answer.

Called Waiting Time

When another terminal calls this device and the calling device is set to non-auto answer, you can set the waiting time. If no one answers after the waiting time ends, the call will be hung up.

Auto Answer Time

When another terminal calls this device and the calling device is set to auto answer, you can set the auto answer time. After the set time ends, this device will automatically answer.

Voice Prompt Settings

Set device prompt tones and mute schedules.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Intercom → Voice Prompts** to access the configuration interface.

Call Waiting Tone ☐ Mute ☐ Male Prompt Tone ☒ Female Prompt Tone

Reject Tone ☐ Mute ☐ Male Prompt Tone ☒ Female Prompt Tone

Two-way Audio End Tone ☐ Mute ☐ Male Prompt Tone ☒ Female Prompt Tone

Emergency Help Tone

Called Prompt Sound

Mute Schedule

Mute Schedule ☐

Save

Figure 2-20 Voice Prompt Settings Interface

2. Set prompt tones.

Call Waiting Tone

Played when the device button is pressed while waiting for answer.

You can select **Mute**, **Male Prompt Tone** or **Female Prompt Tone**.

Reject Tone

Played when the call is rejected after button press.

You can select **Mute**, **Male Prompt Tone** or **Female Prompt Tone**.

Two-way Audio End Tone

Played after intercom ends with administrator.

You can select **Mute**, **Male Prompt Tone** or **Female Prompt Tone**.

Emergency Help Tone

Played when panic button is pressed.

Select **Mute** or other ringtones from dropdown.



Note

Configure ringtones in **Audio Library Settings** .

Called Prompt Sound

Played when receiving calls from main station, alarm terminals or GSM.

Select **Mute** or other ringtones from dropdown.

 Note

Configure ringtones in ***Audio Library Settings*** .

3. Set mute schedule. Device will be muted during configured periods.
 - 1) Enable **Mute Schedule**.
 - 2) Select mute brush and draw mute periods on timeline.
 - 3) **Optional**: Click **Clear** then click unwanted periods to remove.
 - 4) **Optional**: Click  to copy day's schedule to other days.
4. Click **Save**.

Key Settings

Set the call content for device keys.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Intercom → Key Settings** to access the interface.

Call Type

☒ GSM or LAN ☐ Panic Alarm Device

Network Mode

Wired Network

▼

①

VoLTE HD Call

☐

Telephone Number1

137*****634



Telephone Number2

192*****634



Telephone Number3

000*****000



Telephone Number4

000*****000



①

Ring

☐

Save

Figure 2-21 Key Settings Interface

2. Set **Call Type**.
GSM or LAN

Calls can be made via GSM or wired network. When a person presses the key, the configured phone number will be dialed.

Network Mode

Select the required network from the dropdown list.

VoLTE HD Call

When enabled, calls can be made via VoLTE. VoLTE (Voice over LTE) is an IP-based data transmission technology. Enabling VoLTE provides shorter connection time, higher call quality, and better voice/video call performance.



Note

This feature requires a SIM card with activated VoLTE service.

Telephone Number 1/2/3/4

Enter the phone number to call.

Ring

When enabled, plays "Start calling alternative phone number N" voice prompt before playing the configured call tone for the triggered key.

3. Click **Save**.

Allowed Number Settings

Set the allowed call-in list, only phone numbers in the list can call the device.

Enter the device address in the browser, after logging in, click **Configuration** → **Intercom** → **Allowed Number List** to access the interface.

Enable ☒

When enabled, only numbers within the list are allowed to call in.

[+ Add](#) [Delete](#)

☐	No.	Number	Operation
No data.			

[Save](#)

Figure 2-22 Allowed Call-in List Interface

After enabling this function, click **Add** to input phone numbers, then click **Save**.

Click **Delete** to delete.

2.4.13 Audio Library Settings

Configure voice prompts and ringtones.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → Custom → Audio Library** to enter the configuration interface.
2. Click **Import** to import audio files into the device.



Note

Supports importing audio files smaller than 2 MB in WAV or MP3 format, with a maximum of 16 files allowed.

2.5 Maintenance and Security

2.5.1 System Upgrade and Maintenance

You can reboot the device, restore device settings, upgrade the device, and back up device settings.

Reboot Device

Click **Maintenance & Security → Maintenance → Reboot** to enter the page.

Manual Reboot

Click **Reboot**, and the device will begin rebooting.

Auto Reboot

Slide **Auto Reboot** and set the auto restart day and time. The device will automatically reboot at the set time.

Upgrade Device

Click **Maintenance & Security → Maintenance → Upgrade** to enter the page.

Select the upgrade type from the drop-down list, click  to select the upgrade file from local storage, and then click **Upgrade**. The device will automatically upload the upgrade file and begin upgrading.



Note

The upgrade process takes approximately 1to10 minutes. Do not power off the device during the upgrade. The device will automatically reboot after completing the upgrade.

Restore Settings

Click **Maintenance & Security → Maintenance → Backup and Reset** to enter the page.

Restore to Default Settings

Click **Restore** and the device will retain only network settings and user accounts. All other data will be cleared.

Restore to Factory Settings

Click **Restore** and all device functions and settings will be completely restored to factory defaults. The device will need to be reactivated before it can be used again.

Device Parameters Import/Export

Click **Maintenance & Security** → **Maintenance** → **Backup and Reset** to enter the page.

Parameters Export

Click **Export** to export device settings.



Note

The exported device settings can be imported to another device.

Parameters Import

Click  to select the file to be imported from your computer, then click **Import** to perform the settings import operation.

2.5.2 Device Debugging

Enable SSH for maintainers' debugging.

Click **Maintenance & Security** → **Maintenance** → **Device Debugging** to access the interface.

Enable SSH

SSH is typically used for remote debugging. When not needed, it's recommended to disable SSH to enhance device security.

Print Log

Click **Export** to export printed device logs.

Network Packet Capture

Set packet capture duration and captured packet size. Set filtering condition. Click **Capture** to begin packet capture.

2.5.3 Set Network Diagnosis

Enter the device IP address or domain name, you can perform PING settings. Debug the network according to the PING result.

Go to **Maintenance and Security** → **Maintenance** → **Network Diagnosis** .

Enter the device IP for PING operation, select the network connection mode, PING duration, and Ping data package size (default parameter is recommended.) Click **Diagnose**. The result will displayed in **PING Result**.

2.5.4 Search and View Logs

Search and view device logs.

Click **Maintenance & Security → Maintenance → Log** to access the interface.

Select log major type and sub type, set start/end time, click **Search**. Log information will display in list including: No., Time, Major Type, Sub Type, Local/Remote User, Remote Host IP, Parameters and Description.

2.5.5 Security Audit Log

You can upload device log information to a specified server.

Click **Maintenance & Security → Maintenance → Security Audit Log** to access the interface.

Slide **Enable Log Upload Server** and set the server IP and port.

Click  to select a certificate from local storage, then click **Import**.

Click **Save**.

2.5.6 Video&Audio Self-Test Settings

Set auto or manual self-test for video and audio.

Steps

1. Enter the device address in the browser, after logging in, click **Configuration → System Maintenance → Audio&Video Self-Test** to access the interface.
2. Set auto or manual self-test.
 - Automatic self-test: Slide **Auto Test** and set detection time, device will start self-test at scheduled time.
 - Manual self-test: Click **Test**, results will display in **Results**. Click **Stop Checking** to abort.

2.5.7 Security Settings

To enhance network security, you can set IP address filtering function and user lock parameters.

IP Address Filter

The device supports setting both a blocked IP address list and an allowed IP address list for communication. The device will not communicate with IP addresses in the block list. If an allow list is added, the device only communicates with IP addresses in the allowed list.

Enter the device address in the browser, after logging in, click **Maintenance & Security → Security → IP Address Filter** to access the configuration interface.

Slide the **Enable** switch. Select **Block List** or **Allow List**, click **Add**, enter the IP address, and click **OK**. Click **Save**.

Locking User

Enter the device address in the browser, after logging in, click **Maintenance & Security → Security → Locking User** to access the configuration interface.

Slide **Enable Locking**.

Set **Max. Failure Attempts** and **Locking Duration**. When incorrect user name/password attempts reach the maximum number, the IP will be locked. After exceeding the configured lock duration, the IP will be unlocked automatically.



Note

Admin users can manually unlock.

Click **Save**

Click **Unlock** or **Unlock All** to unlock locked IPs.

2.6 Open Source Software Licenses

You can view open source software licenses.

Click  → **Open Source Software Statement** on the upper-right corner to view the licenses.

2.7 Change Administrator's Password

change the administrator login password (device activation password).

Steps

1. Click **admin → Modify Password** in the upper right corner of the interface to enter the page.
2. Enter the old password, create and confirm the new password.



Caution

- To better protect your privacy and improve product security, you are strongly recommended to set a more complex password according to the following rules: the password should be between 8 and 16 characters, including digits, lowercase letters, and special characters.
 - 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. Click **Save**.

The device password will be edited, and you need to log in to the web page again.

2.8 Logout

Log out the account.

Click **admin** → **Logout** → **OK** to logout.

Appendix A. 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.

Appendix B. Symbol Conventions

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

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



See Far, Go Further