Network Control Keyboard User Manual

Manual Version: V1.00

Disclaimer and Safety Warnings

Copyright Statement

©2022 Zhejiang Uniview Technologies Co., Ltd. All rights reserved.
No part of this manual may be copied, reproduced, translated or distributed in any form or by any means without prior consent in writing from Zhejiang Uniview Technologies Co., Ltd (referred to as Uniview or us hereafter).
The product described in this manual may contain proprietary software owned by Uniview and its possible licensors. Unless permitted by Uniview and its licensors, no one is allowed to copy, distribute, modify, abstract, decompile, disassemble, decrypt, reverse engineer, rent, transfer, or sublicense the software in any form or by any means.

Trademark Acknowledgements

unv uniarch are trademarks or registered trademarks of Uniview.
All other trademarks, products, services and companies in this manual or the product described in this manual are the property of their respective owners.

Export Compliance Statement

Uniview complies with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abides by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described in this manual, Uniview asks you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

Privacy Protection Reminder

Uniview complies with appropriate privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information. Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

About This Manual

- This manual is intended for multiple product models, and the photos, illustrations, descriptions, etc, in this manual may be different from the actual appearances, functions, features, etc, of the product.
- This manual is intended for multiple software versions, and the illustrations and descriptions in this manual may be different from the actual GUI and functions of the software.
- Despite our best efforts, technical or typographical errors may exist in this manual. Uniview cannot be held responsible for any such errors and reserves the right to change the manual without prior notice.
- Users are fully responsible for the damages and losses that arise due to improper operation.
- Uniview reserves the right to change any information in this manual without any prior notice or indication. Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

Disclaimer of Liability

- To the extent allowed by applicable law, in no event will Uniview be liable for any special, incidental, indirect, consequential damages, nor for any loss of profits, data, and documents.
- The product described in this manual is provided on an "as is" basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. Uniview strongly recommends that users take all necessary measures to enhance the protection of network, device, data and personal information. Uniview disclaims any liability related thereto but will readily provide necessary security related support.
- To the extent not prohibited by applicable law, in no event will Uniview and its employees, licensors, subsidiary, affiliates be liable for results arising out of using or inability to use the product or service, including, not limited to, loss of profits and any other commercial damages or losses, loss of data, procurement of substitute goods or services; property damage, personal injury, business interruption, loss of business information, or any special, direct, indirect, incidental, consequential, pecuniary, coverage, exemplary, subsidiary losses, however caused and on any theory of liability, whether in contract, strict liability or tort (including negligence or otherwise) in any way out of the use of the product, even if Uniview has been advised of the possibility of such damages (other than as may be required by applicable law in cases involving personal injury, incidental or subsidiary damage).
- To the extent allowed by applicable law, in no event shall Uniview's total liability to you for all damages for the product described in this manual (other than as may be required by applicable law in cases involving personal injury) exceed the amount of money that you have paid for the product.

Network Security

Please take all necessary measures to enhance network security for your device.

The following are necessary measures for the network security of your device:

- **Change default password and set strong password:** You are strongly recommended to change the default password after your first login and set a strong password of at least nine characters including all three elements: digits, letters and special characters.
- **Keep firmware up to date:** It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit Uniview's official website or contact your local dealer for the latest firmware.

The following are recommendations for enhancing network security of your device:

- **Change password regularly:** Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.
- **Enable HTTPS/SSL:** Use SSL certificate to encrypt HTTP communications and ensure data security.
- **Enable IP address filtering:** Allow access only from the specified IP addresses.
- **Minimum port mapping:** Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- **Disable the automatic login and save password features:** If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- **Choose username and password discretely:** Avoid using the username and password of your social media, bank, email account, etc, as the username and password of your device, in case your social media, bank and email account information is leaked.
- **Restrict user permissions:** If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- **Disable UPnP:** When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage. Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.
- **SNMP:** Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.
- **Multicast:** Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- **Check logs:** Check your device logs regularly to detect unauthorized access or abnormal operations.
- **Physical protection:** Keep the device in a locked room or cabinet to prevent unauthorized physical access.
- **Isolate video surveillance network:** Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.

Learn More

You may also obtain security information under Security Response Center at Uniview's official website.

Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

Storage, Transportation, and Use

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Protect the device from liquid of any kind.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.
- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting Uniview first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.
- Always disconnect the device from power before attempting to move the device.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.

Power Requirements

- Install and use the device in strict accordance with your local electrical safety regulations.
- Use a UL certified power supply that meets LPS requirements if an adapter is used.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded.

Contents

1 Overview 1
2 Login 1
3 System Settings 3
3.1 User 3
3.2 Wired Network 4
3.3 Date & Time 6
3.4 Language 6
3.5 Sound 7
3.6 Restart 7
3.7 System Maintenance 8
4 Keyboard Operations 10
4.1 Resource Management 11
4.1.1 Encoding/Decoding Devices 12
4.1.2 Sequence Resources 16
4.2 Live View 19
5 Platform Operations 23
5.1 Platform Login 23
5.2 Platform Operations 24

1 Overview

This product is a new generation of Android touch-screen network keyboard. With a capacitive touch screen and a user-friendly GUI, users can view live video on the touch screen or mirror video to an HDMI-connected display device. It can be applied to scenarios where multiple IPCs and NVRs are installed, such as streets, schools, communities, factories, etc., to realize unified control of ONVIF devices in the LAN.

2 Login

The keyboard shows the login screen by default after startup.

1. On the login screen, enter the username and password, and then tap **LOGIN**.

NOTE!
The default username/password is admin/123456.

Figure 2-1 Login Screen

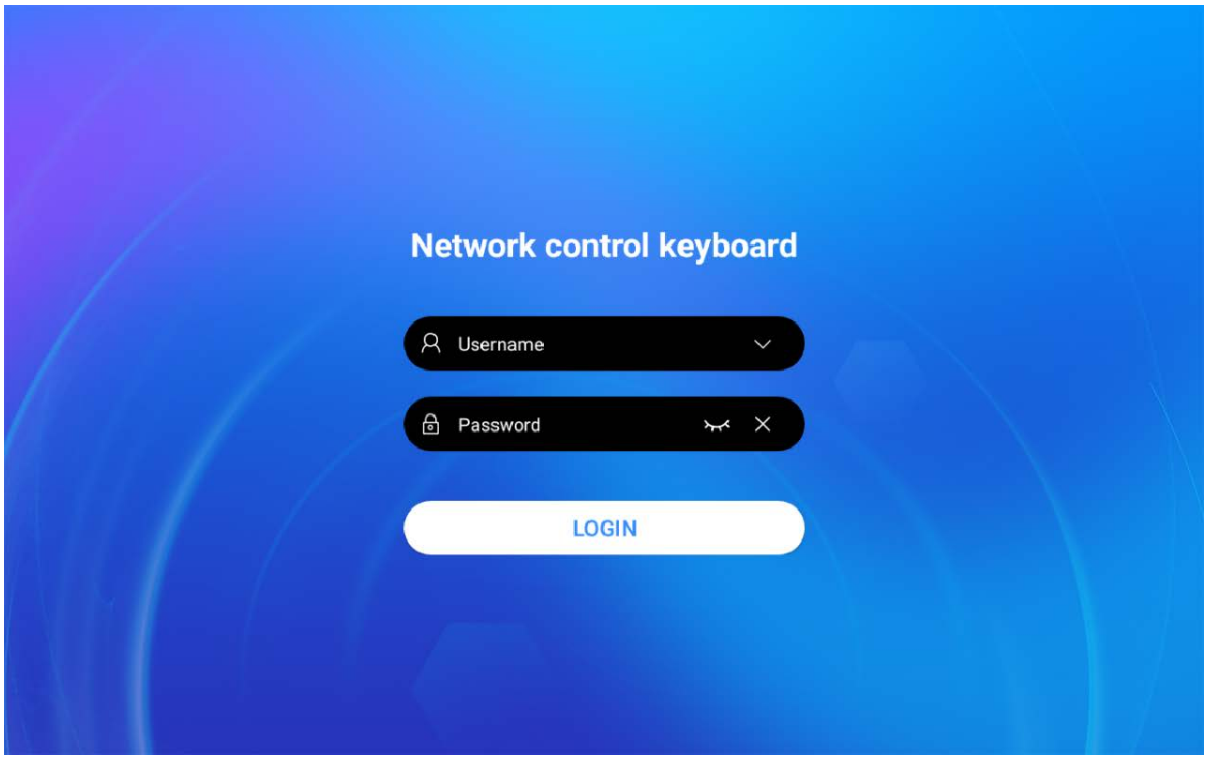
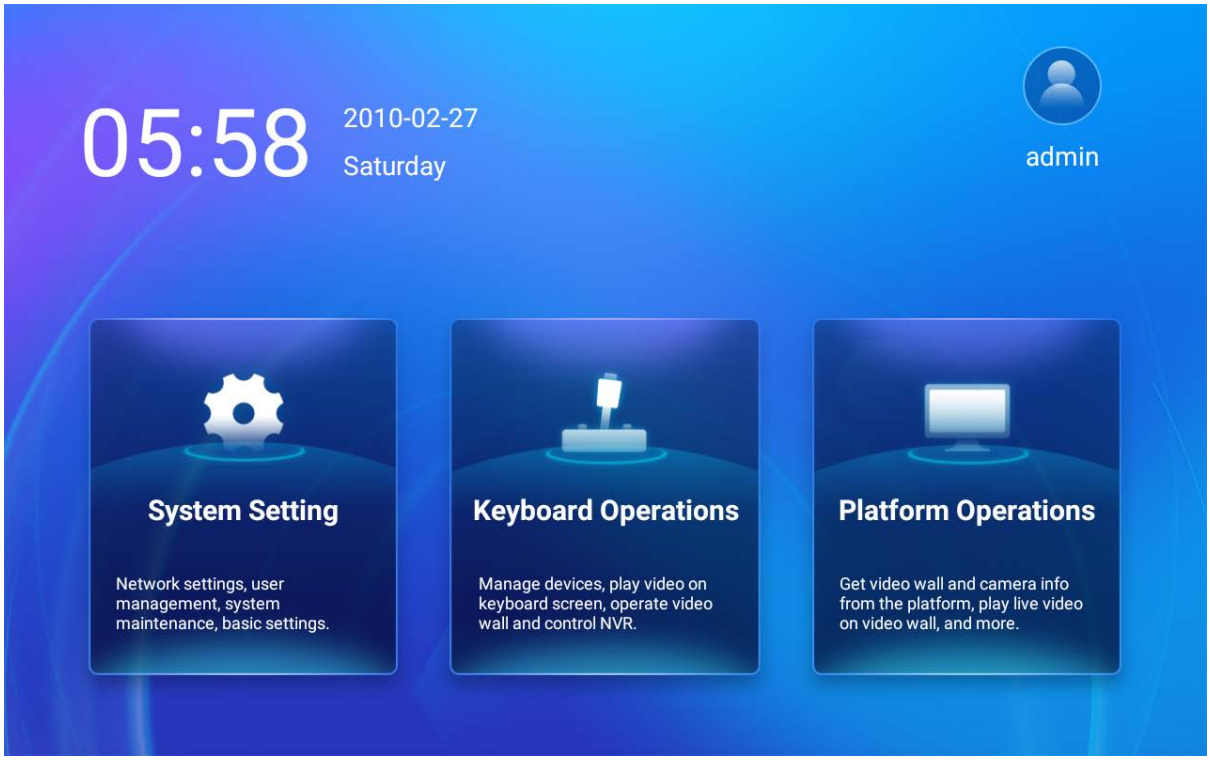
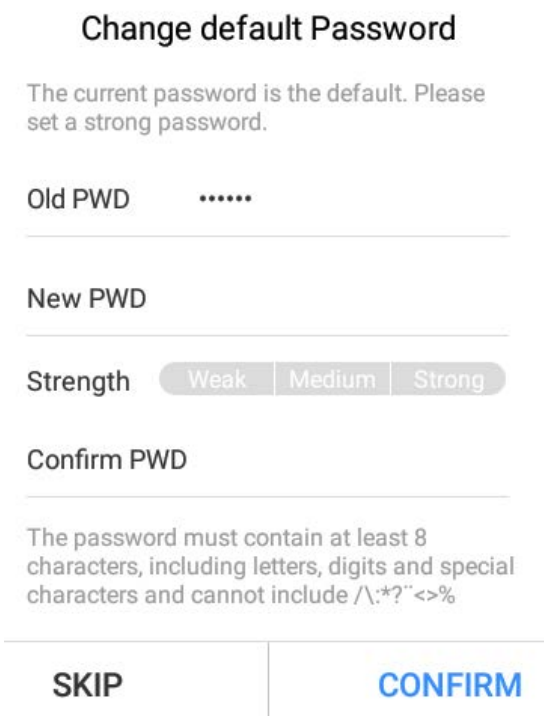


Figure 2-2 Home Screen



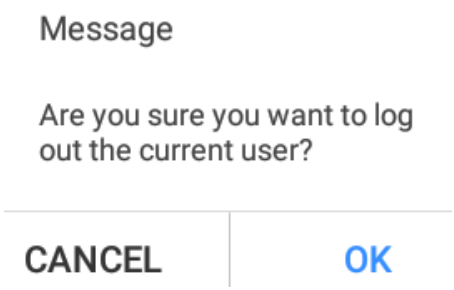
2. The **Change Default Password** dialog box appears after you log in with the default password. You can change the password as needed. To keep the default password, tap **SKIP**.



NOTE!

The **Change Default Password** dialog box appears every time you log in with the default password.

3. To log out, tap  on the home screen and tap **OK**.

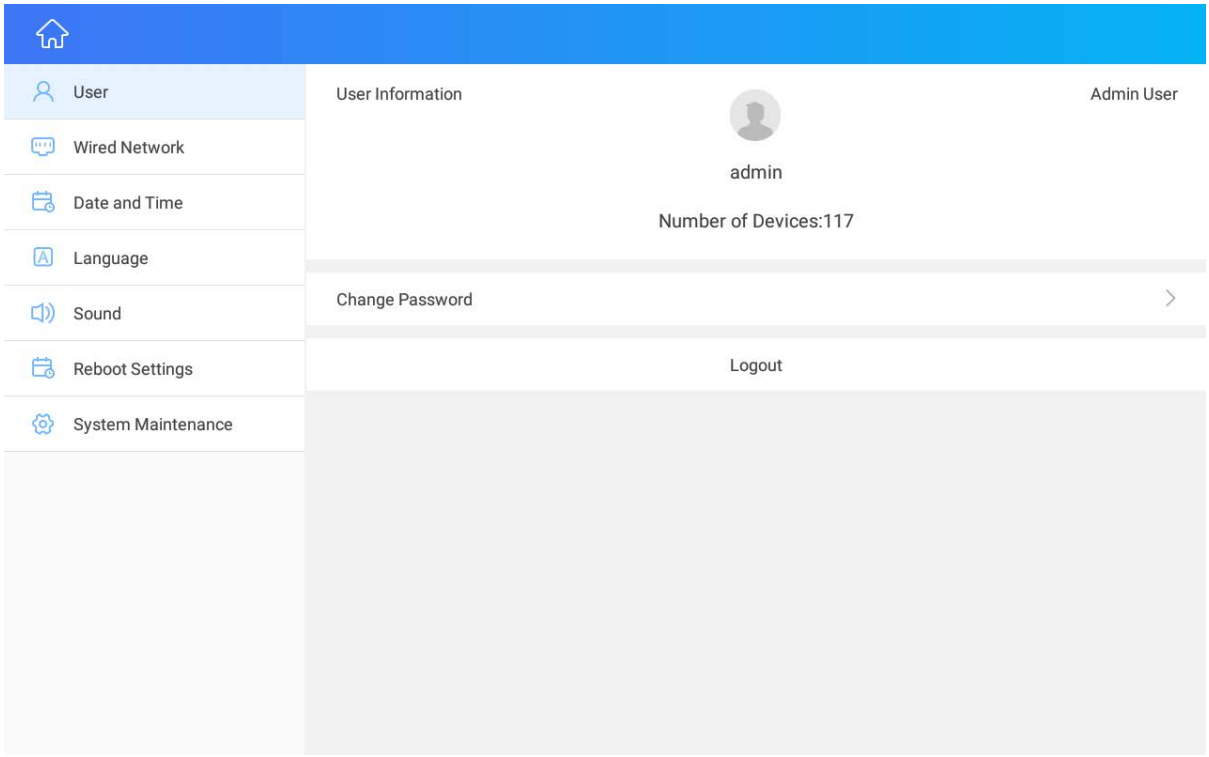


3 System Settings

Tap **System Setting** on the home screen to configure network, user management, system maintenance, etc. To return to the home screen, tap .

3.1 User

View user information, change login password, and log out.

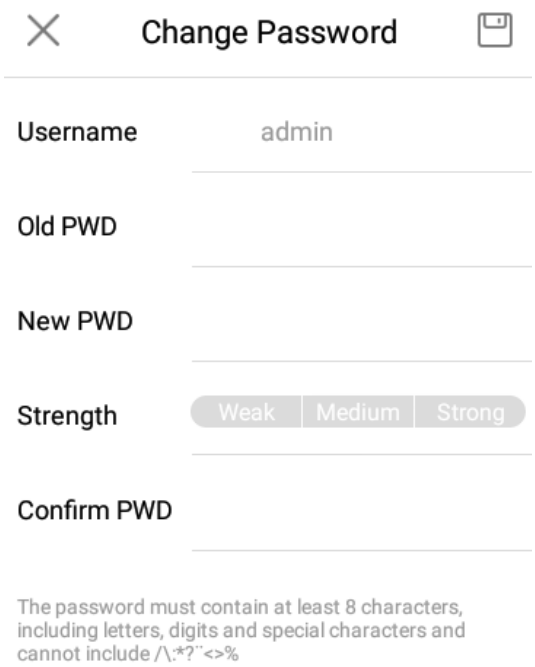


1. User Info

View the current user, user role, and number of devices (including all added encoding and decoding devices).

2. Change Password

1. Tap **Change Password**.



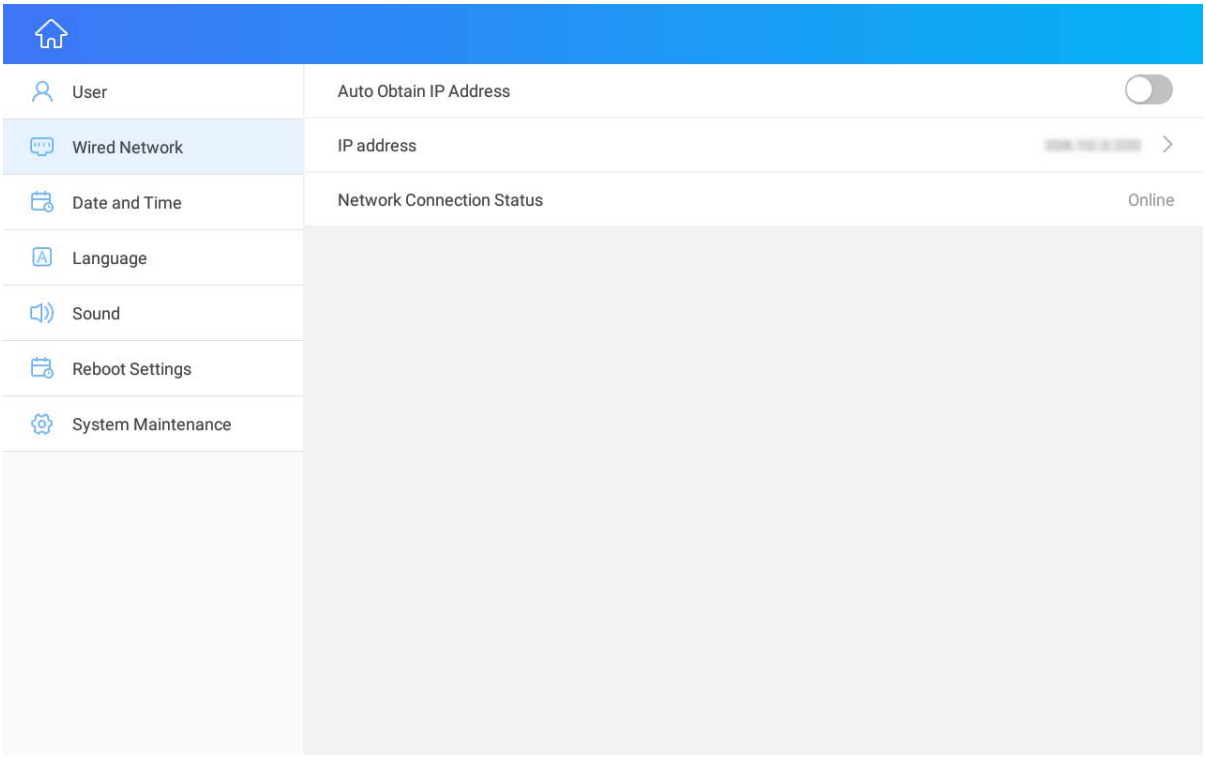
2. Follow the on-screen instructions to set a new login password and then tap .

3. Logout

Tap **Logout** to log out of your account.

3.2 Wired Network

View and configure network parameters. The IP address can be obtained automatically or set manually.



- Auto: Enable **Auto Obtain IP Address** to obtain the IP address automatically.
- Manual: Disable **Auto Obtain IP Address**, tap **IP Address**, set the network parameters as needed, and then tap .

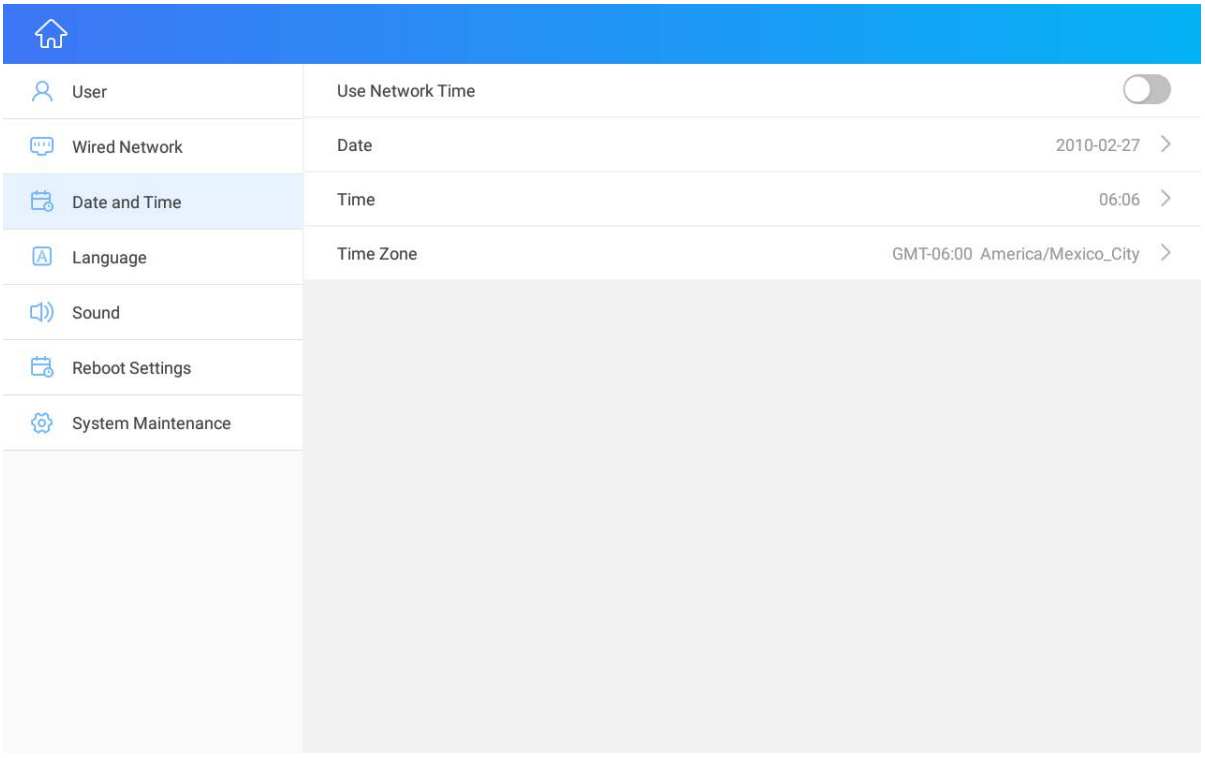


NOTE!

- Before you enable **Auto Obtain IP Address**, make sure a DHCP server is deployed and enabled in the network (DHCP is enabled by default).
- After an IP address is assigned by the DHCP server, you can tap **IP Address** to view network information but cannot edit it.
- Before you set the IP address manually, make sure the IP address to set is not in use to avoid IP conflicts.

3.3 Date & Time

Set the date, time, and time zone. The date and time can be obtained automatically or set manually.



- Auto: Enable **Use Network Time** to obtain the date and time automatically.

NOTE!

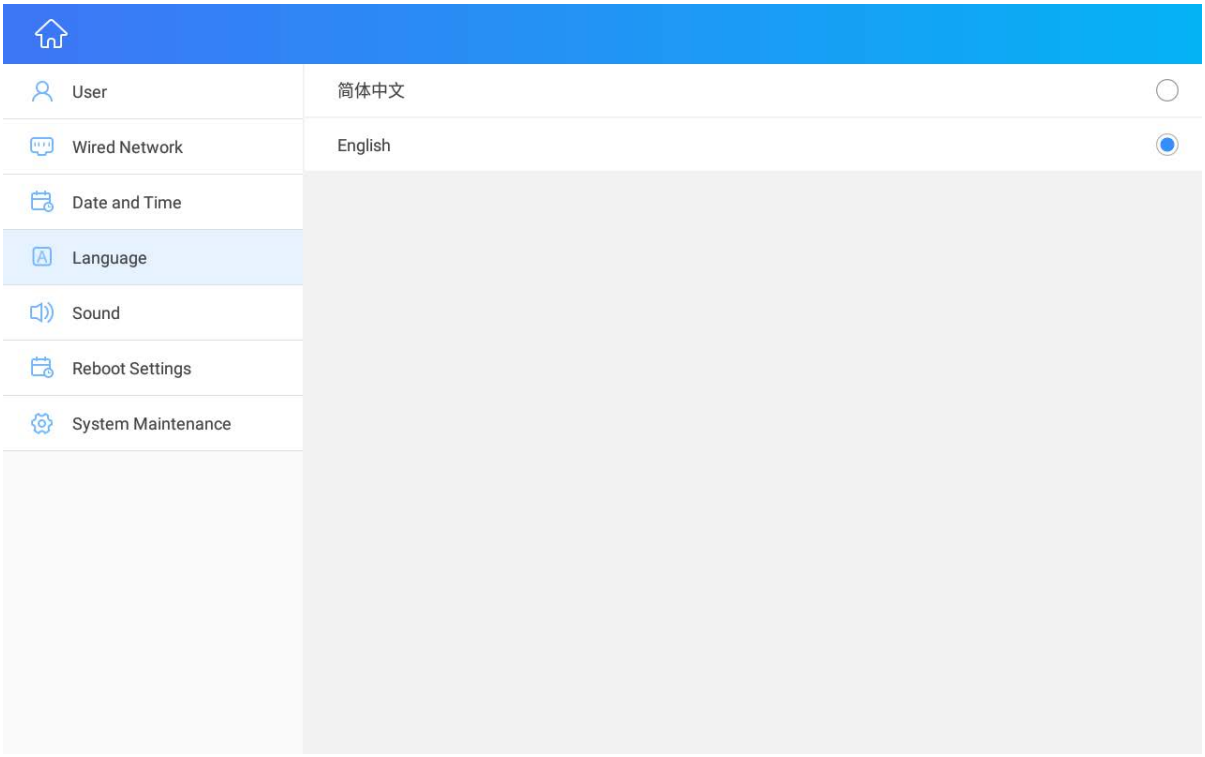
- Before you enable **Use Network Time**, make sure an NTP server is deployed and enabled in the network (NTP is enabled by default).
- The time zone cannot be obtained automatically, and you need to set it manually.

- Manual: Disable **Use Network Time** and then set the date, time, and time zone as needed.



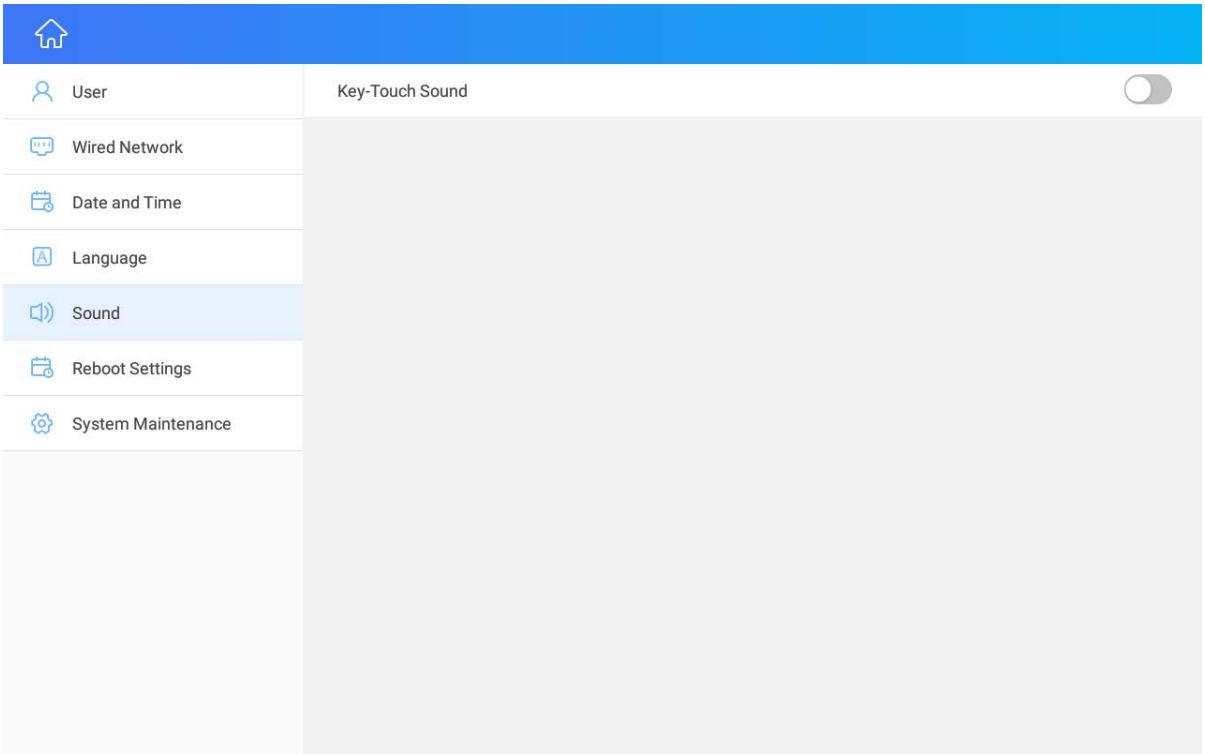
3.4 Language

Set the language displayed on the screen.



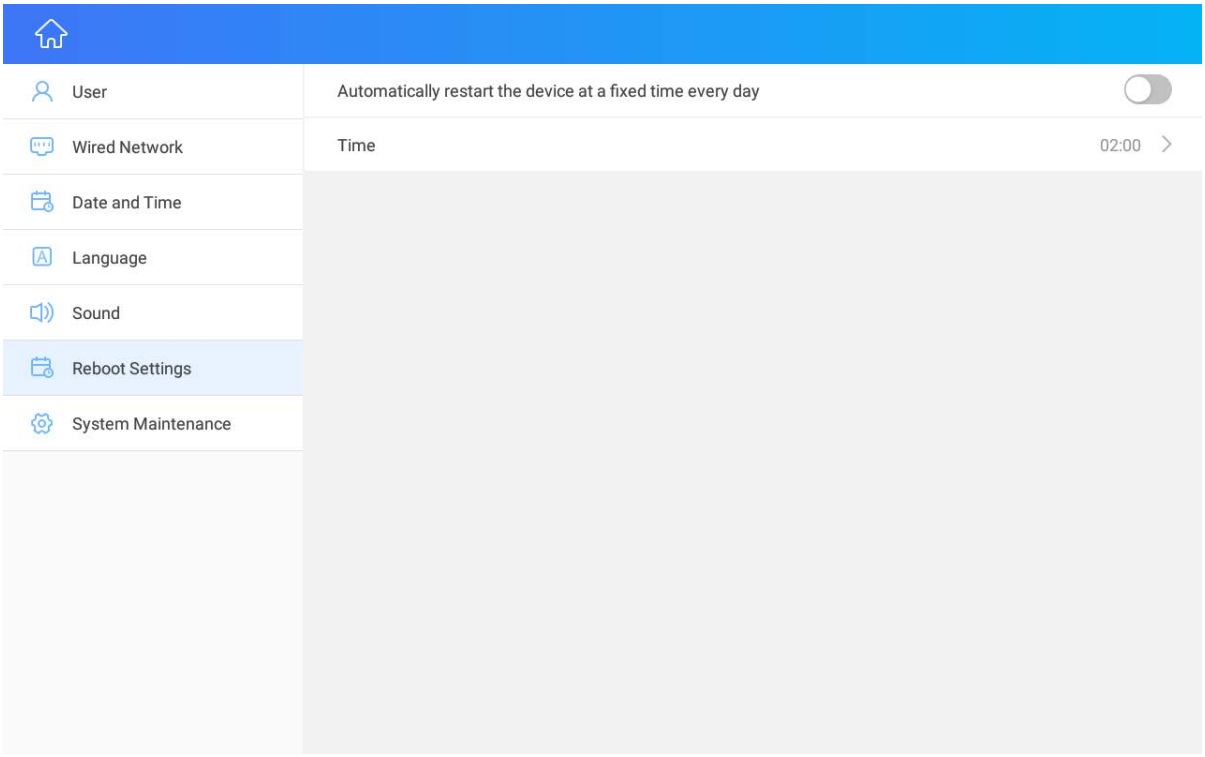
3.5 Sound

Set whether to enable the keyboard sound.

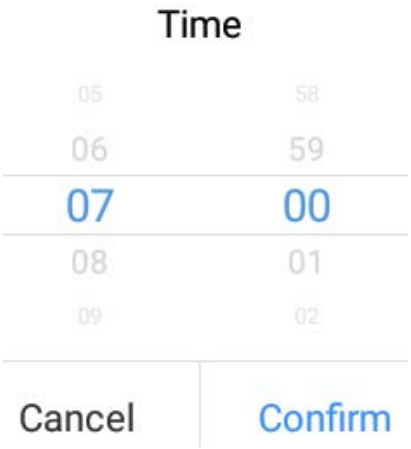


3.6 Restart

Restart the keyboard at a specified time every day.

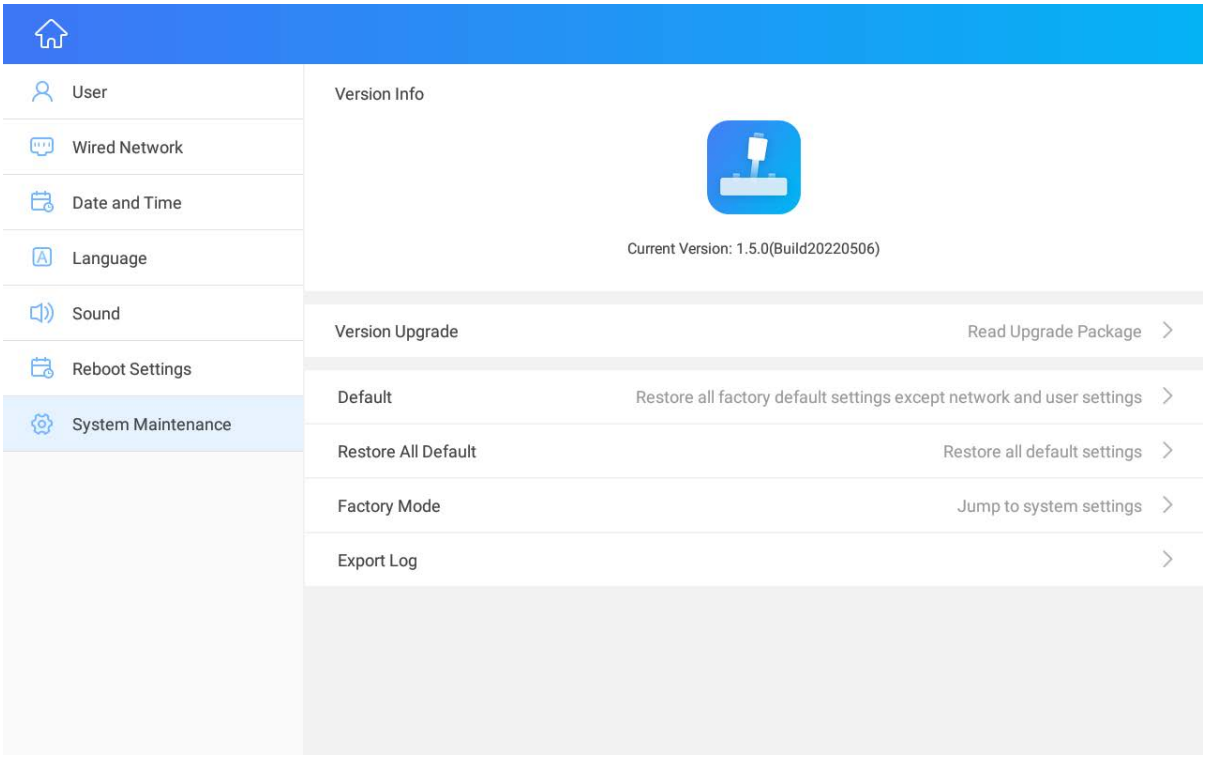


Enable **Automatically restart the device at a fixed time every day**, tap **Time**, set the time to restart, and then tap **Confirm**. The keyboard will automatically restart at the time every day.



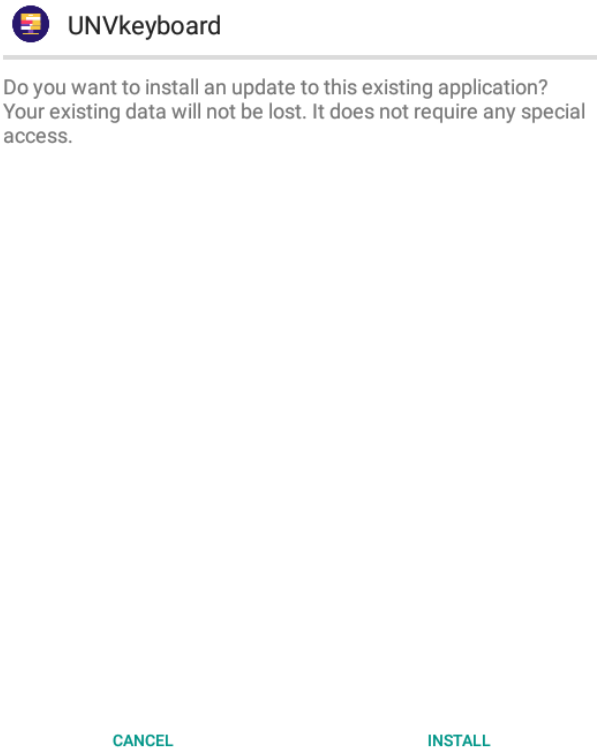
3.7 System Maintenance

View the current version info, upgrade system version, restore factory default settings, and export operation logs.



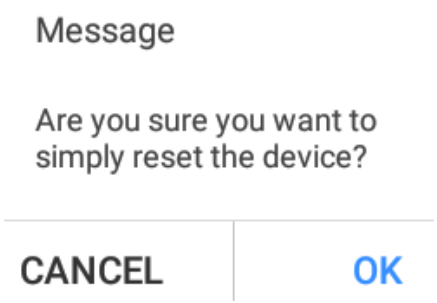
1. System Upgrade

1. Copy the upgrade package to the root directory of a USB flash drive and plug the USB flash drive into the keyboard.
2. Tap **Version Upgrade** to discover the upgrade package and then tap **INSTALL**.



2. Restore Factory Default Settings

Tap **Default** or **Restore All Defaults** and then tap **OK**.



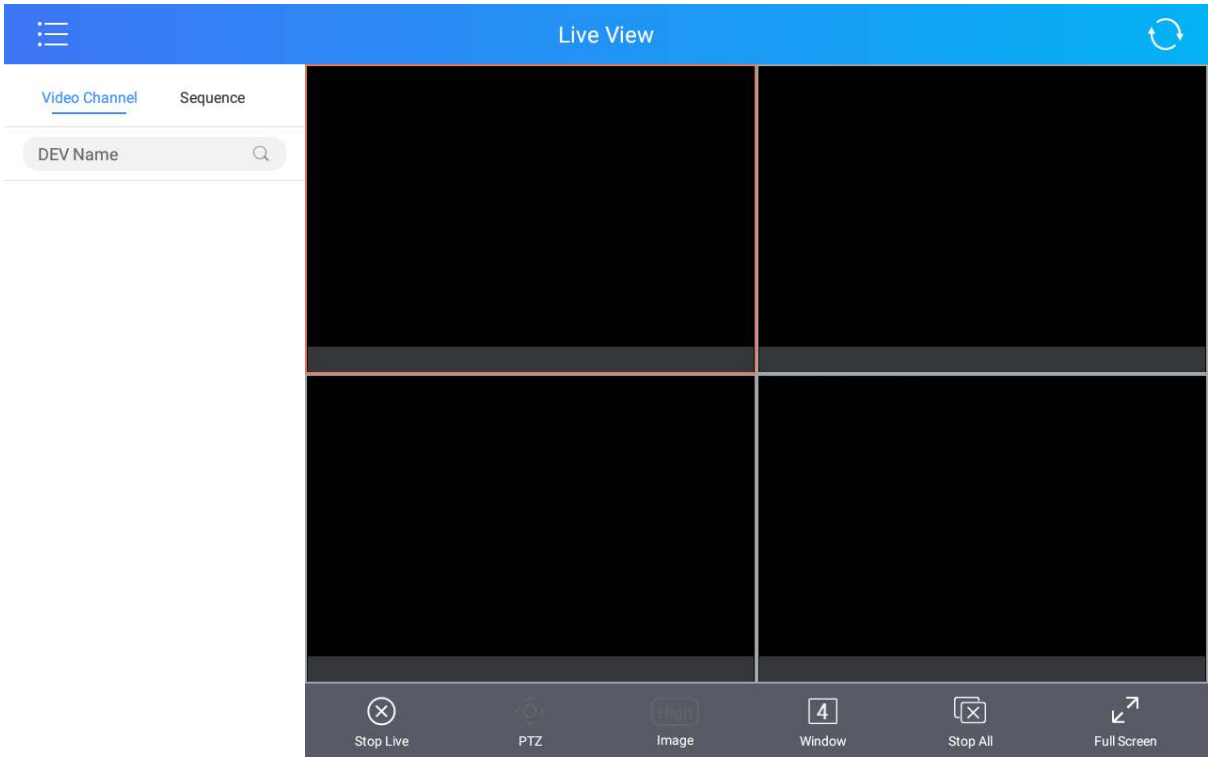
- Default: Keep the current network and user settings and restore other settings to defaults.
- Restore All Defaults: Restore all settings to defaults.

3. Export Operation Logs

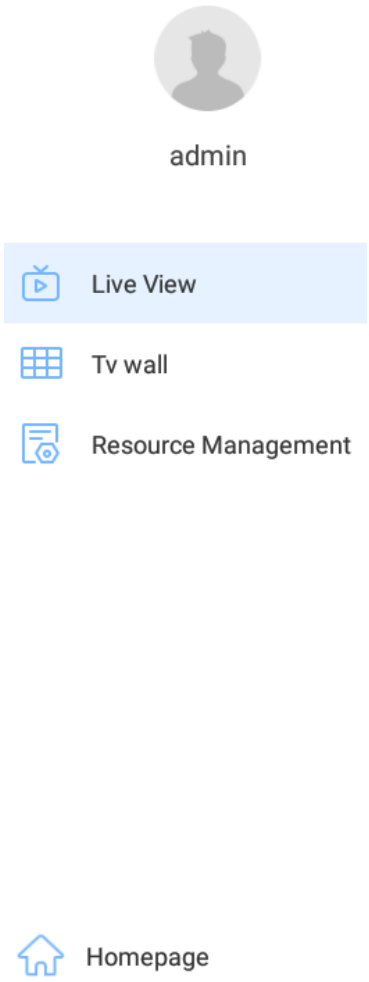
Plug a USB flash drive into the keyboard and tap **Export Log** to export the operation logs to the USB flash drive.

4 Keyboard Operations

Tap **Keyboard Operations** on the home screen to manage encoding/decoding devices and sequence resources and view live videos.

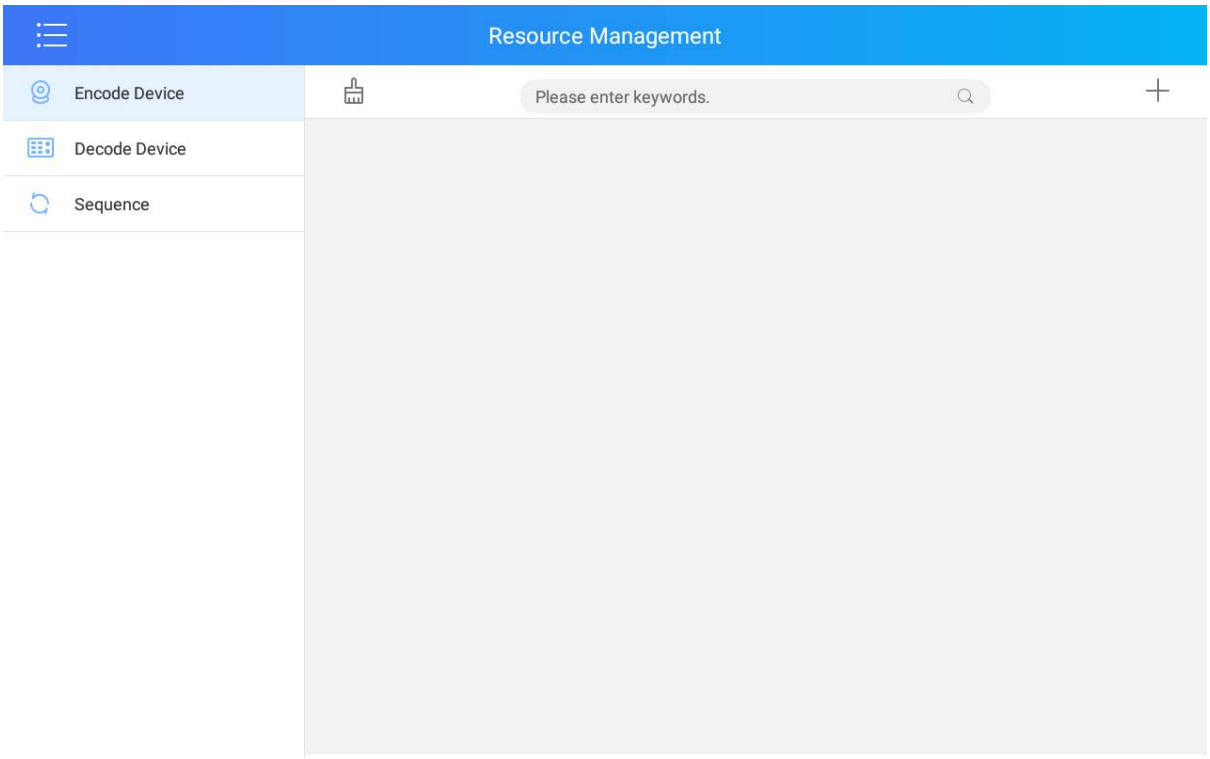


Tap  to open the menu, in which you can switch between live view, video wall (reserved), and resource management. To return to the home screen, tap .



4.1 Resource Management

Tap and select **Resource Management** to manage encoding/decoding devices and sequence resources.

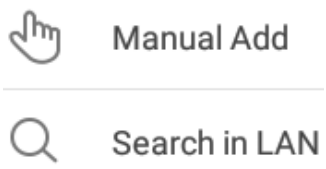


You can search resources by entering keywords of the resource name in the search box, and the search results are listed.

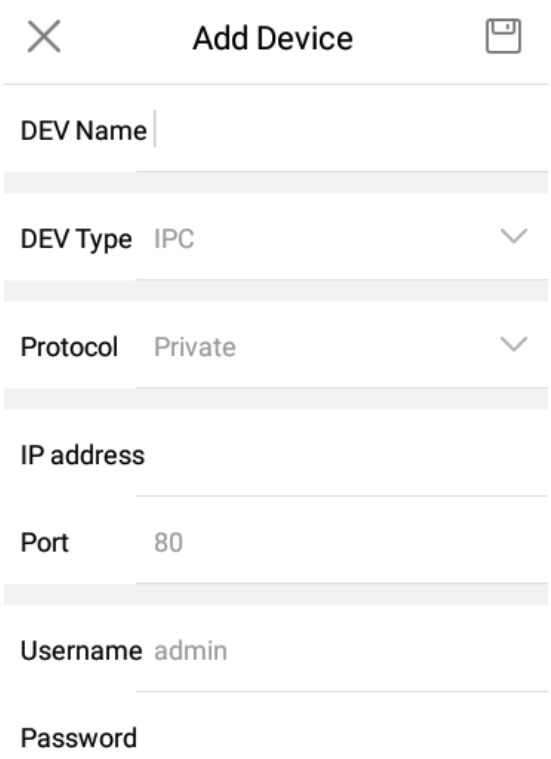
4.1.1 Encoding/Decoding Devices

1. Add Device

Tap +.



- Manual Add: Tap **Manual Add**, enter the device information, and then tap .



NOTE!

The protocol has two options:

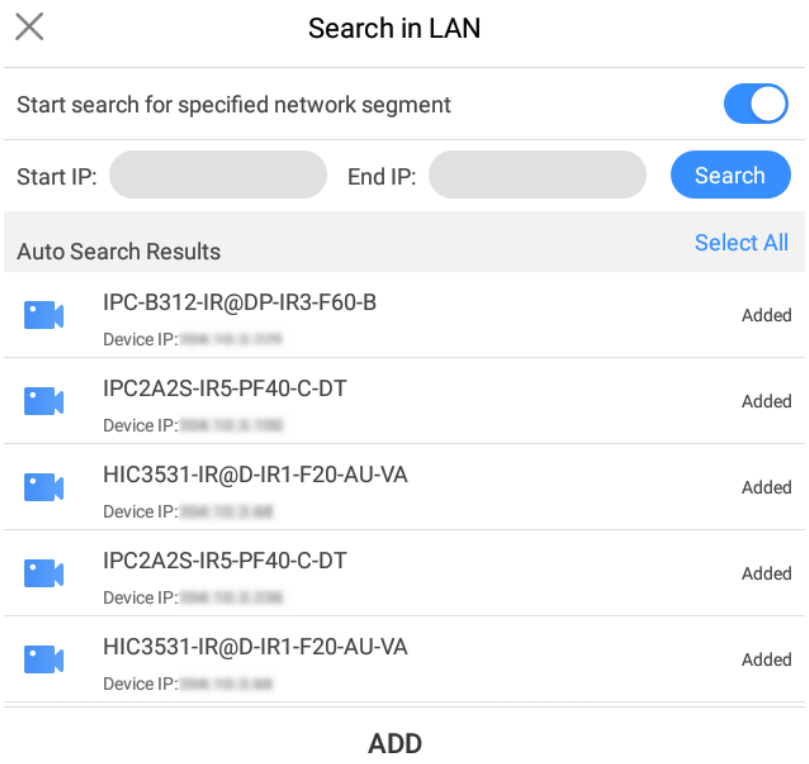
- Private: Used to add Uniview IPCs and NVRs.
- ONVIF: Used to add ONVIF compliant IPCs and NVRs of Uniview and the third party.

- Search in LAN:
  - Auto search (default): Tap **Search in LAN** to discover the online encoding/decoding devices in the same network segment as the keyboard automatically.
  - Search in specified network segment: Enable **Start search for specified network segment**, set the start and end IP addresses, and then tap **Search** to discover the online encoding/decoding devices in the network segment.

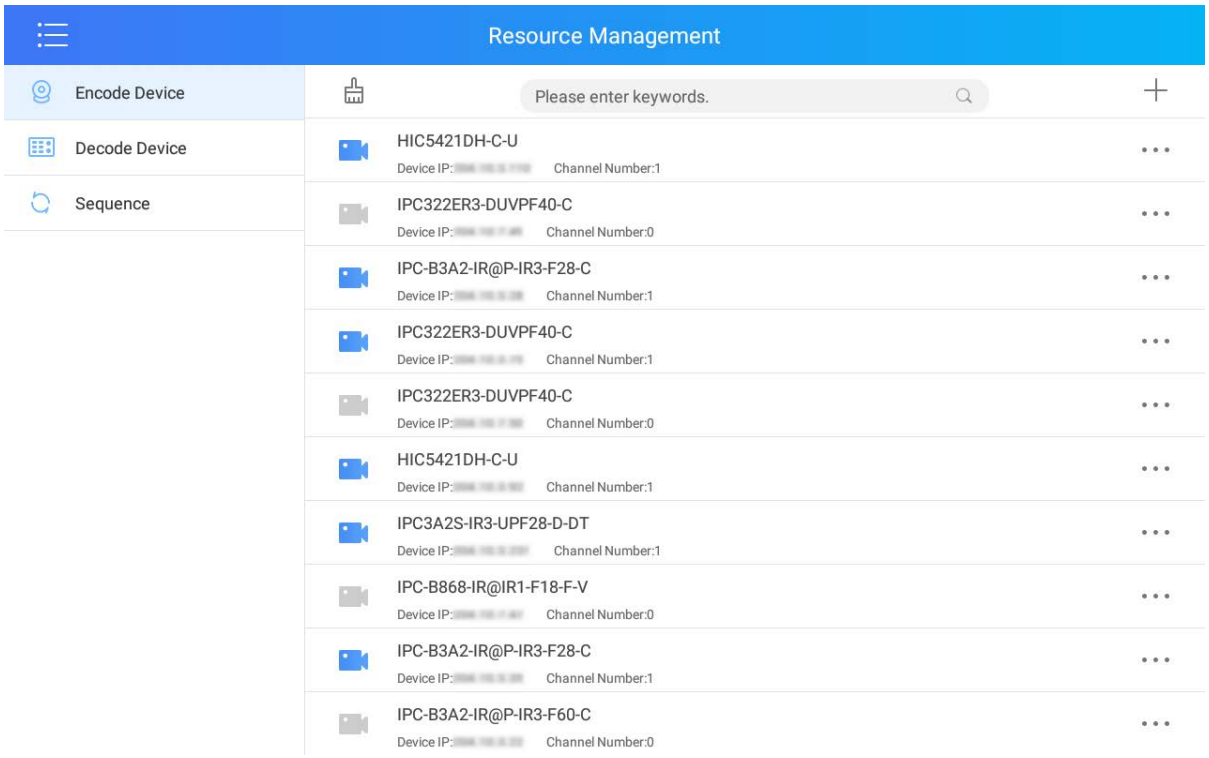
  After search, select the discovered devices to add, and then tap **ADD**.

NOTE!

To search again, close the **Search in LAN** window first and then tap **Search in LAN** again.



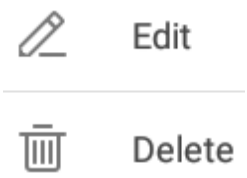
2. Edit Device



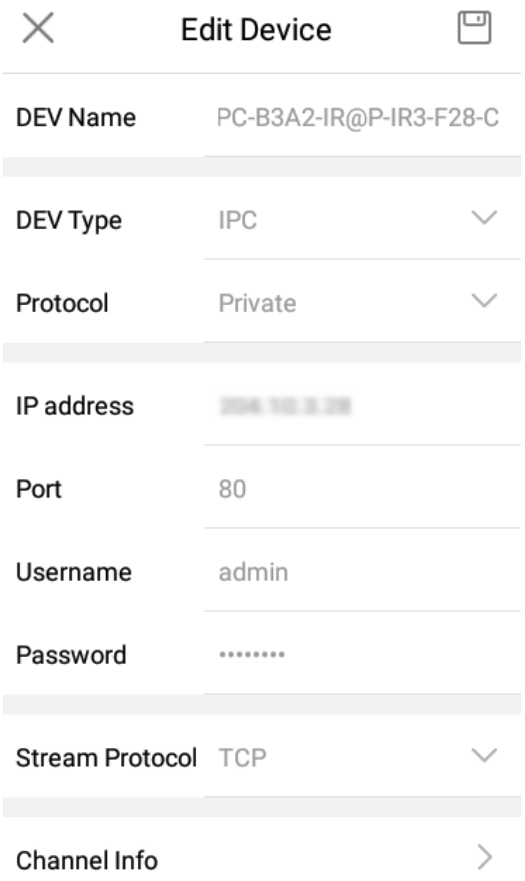
NOTE!

indicates the device is online; indicates the device is offline or unreachable.

1. Select the device to edit and tap • • •.

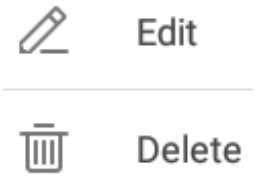


2. Tap **Edit**, edit the device information as needed, and tap .



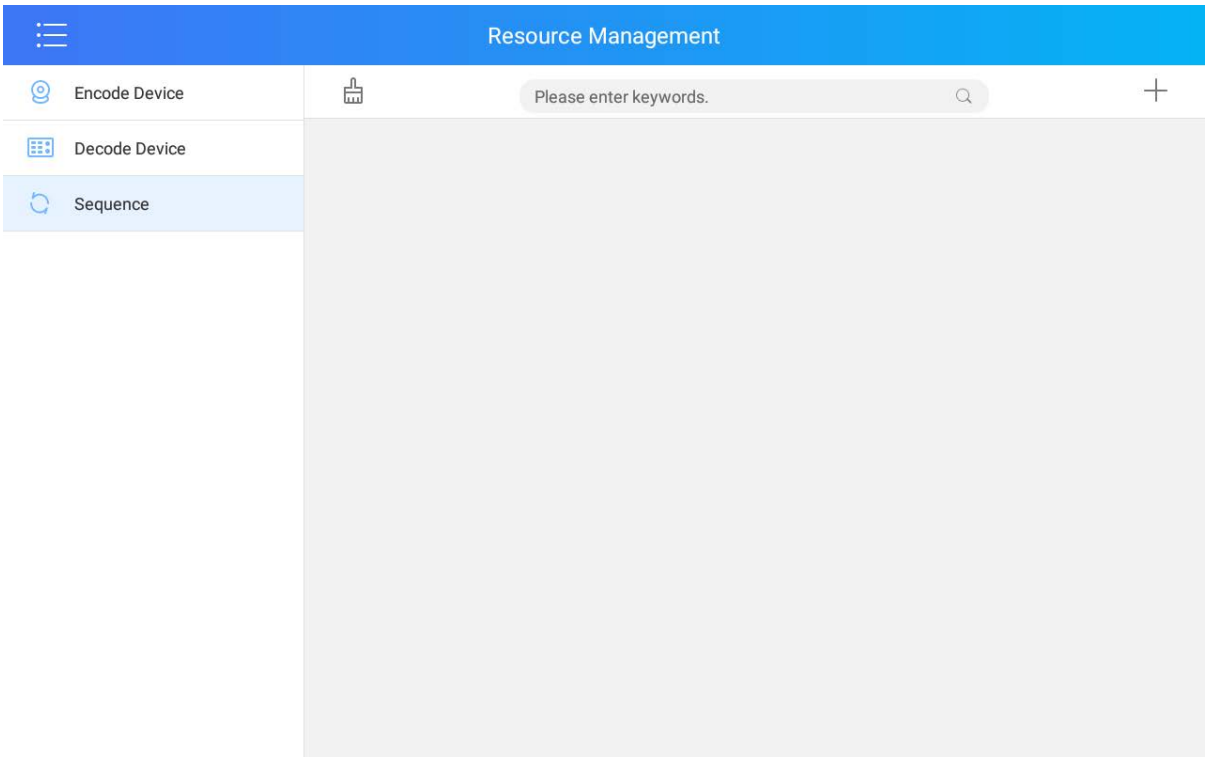
3. Delete Device

- Delete one by one: Select the device to delete, tap • • •, and tap **Delete** to delete the device.



- Delete all: Tap to delete all devices.

4.1.2 Sequence Resources



1. Add Sequence Resource

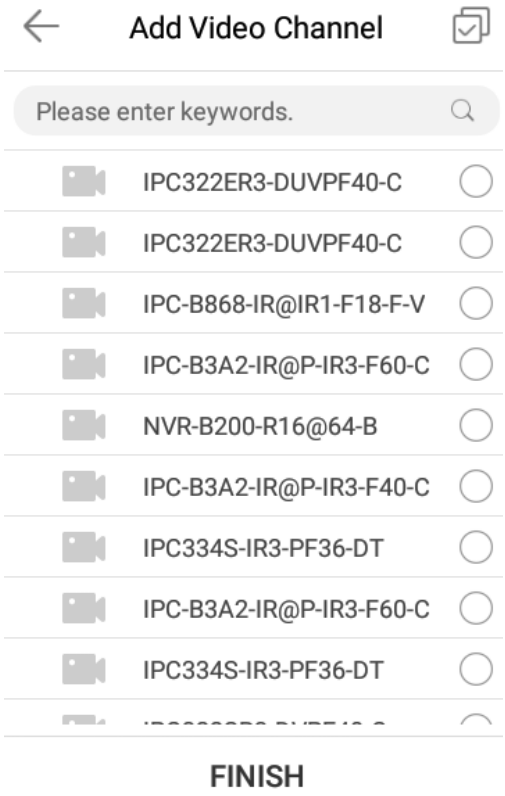
1. Tap + and set the name and sequence time.



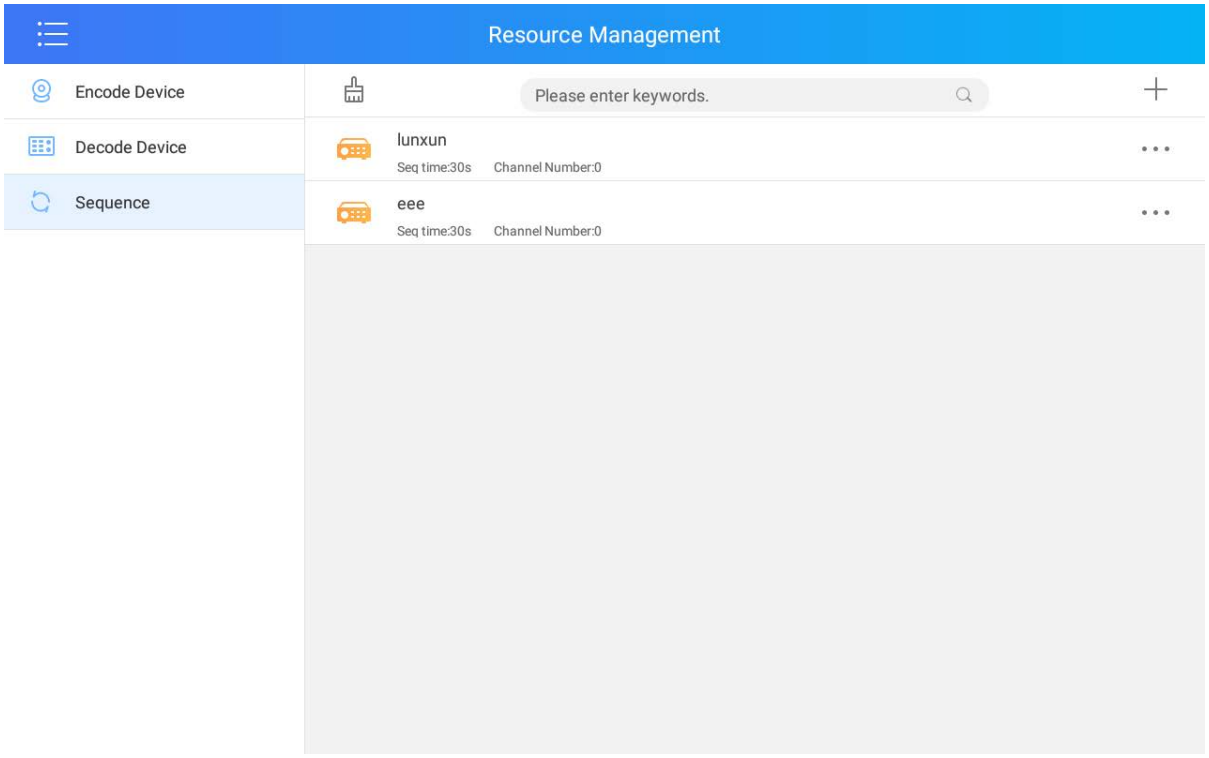


NOTE!
The default and minimum sequence time is 30s.

2. Tap **ADD VIDEO CHANNEL**, select the channels to add, and tap **FINISH**.



3. Tap to save the sequence resource.



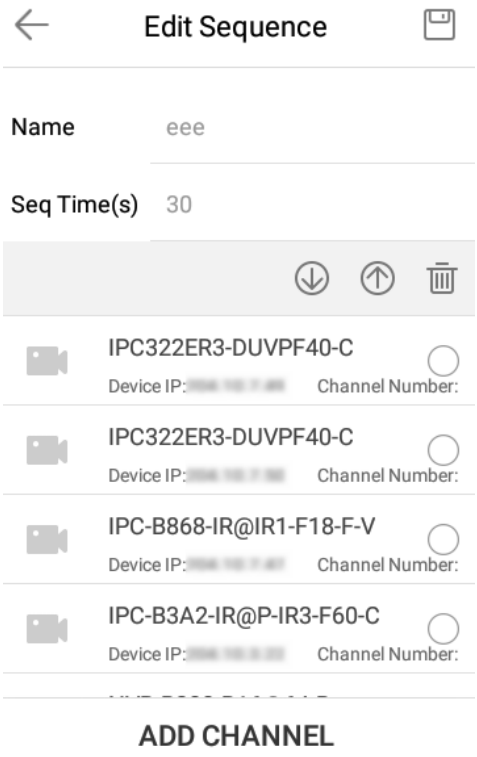
2. Edit Sequence Resource

1. Select the sequence resource to edit and tap • • •.



2. Tap **Edit**, edit the sequence information, and tap .

- Change sequence order: Select the video channel to change order, and tap or .
- Add video channel: Tap **ADD CHANNEL**.
- Delete video channel: Select the channels to delete and tap .



3. Delete Sequence Resource

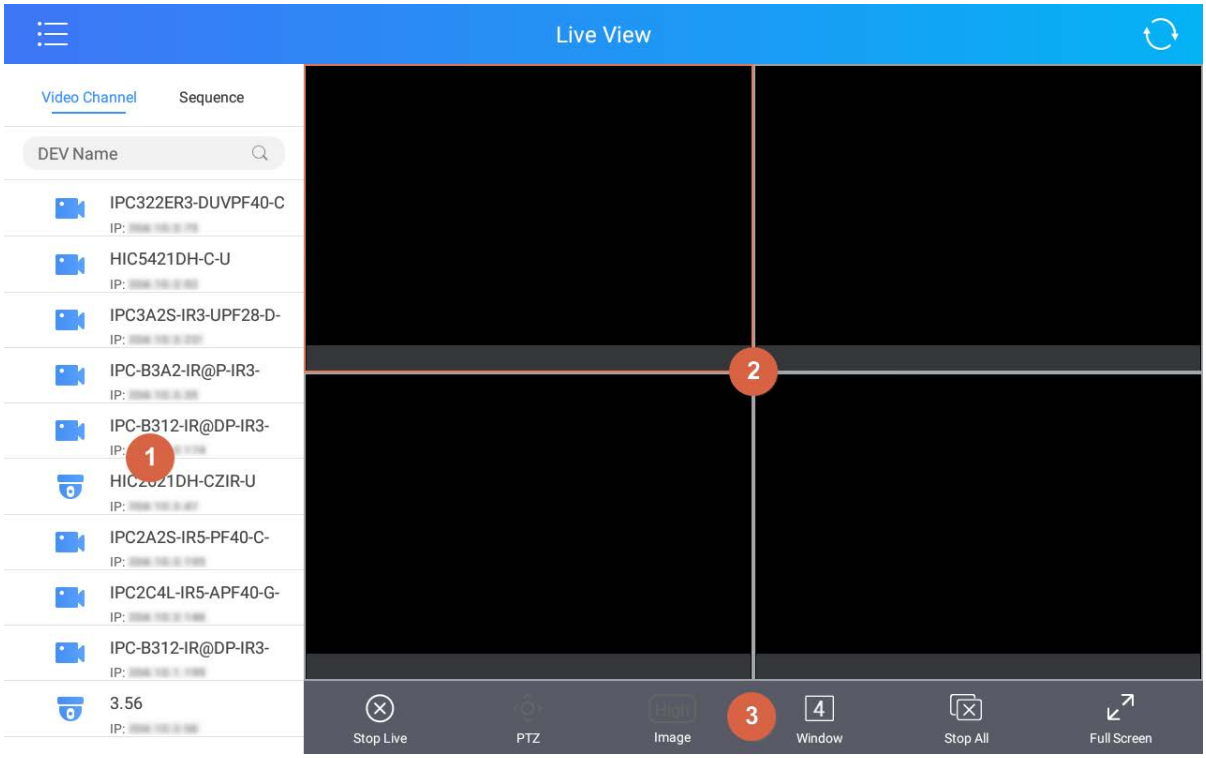
- Delete one by one: Select the sequence resource to delete, tap • • •, and tap **Delete**.



- Delete all: Tap to delete all sequence resources.

4.2 Live View

Tap and select **Live View** to view the live video of added resources.

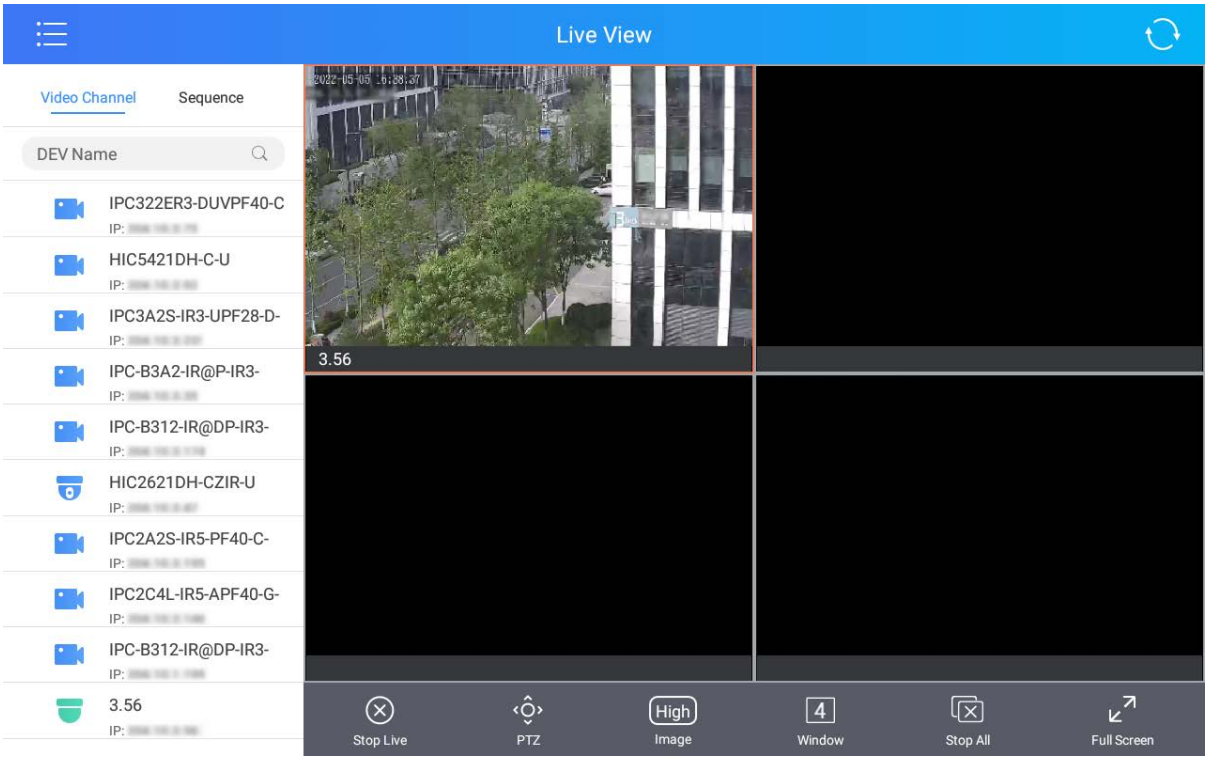


No.	Description
1	Resource list, displays added video channels and sequence resources. Tap to refresh the list.
2	Video output window, displays live video.
3	• Stop Live: Stop live view in the selected window. • PTZ: PTZ control. • Image: Set the video clarity, including High, Medium, and Low. • Window: Set the number of windows. • Stop All: Stop live view in all windows. • Full Screen: View live video in full screen.

NOTE!
The PTZ function is only available for PTZ cameras.

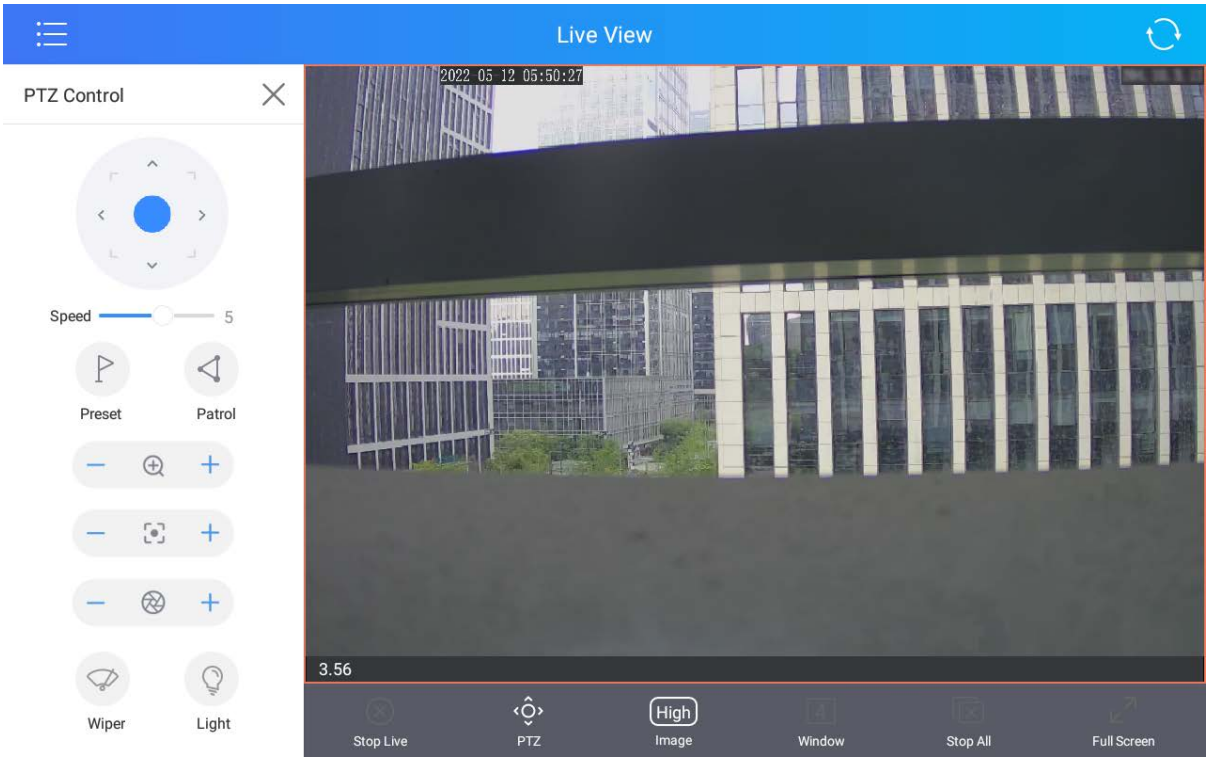
1. Live View

Select a video output window and double-tap a video channel or sequence resource in the resource list to start live view.



2. PTZ Control

1. Select a live view window and tap **PTZ** to open the PTZ control panel.



2. Adjust PTZ position and view live video of the corresponding PTZ position.
   - PTZ control on screen

–  : Control the rotation direction of the PTZ camera.

– 

: Control the rotation speed of the PTZ camera.

–  : Zoom +/-, zoom in/out on images.

–  : Focus +/-, focus far/near for sharp images at a distance/at close range.

–  : Iris +/-, increase/reduce the amount of light that enters the camera for brighter/darker images.

➢ PTZ control by keyboard

– Move the joystick to control the PTZ camera to rotate in all directions.

– Rotate the knob on the joystick to zoom.

– Rotate the outer wheel of the dial to adjust the focus.

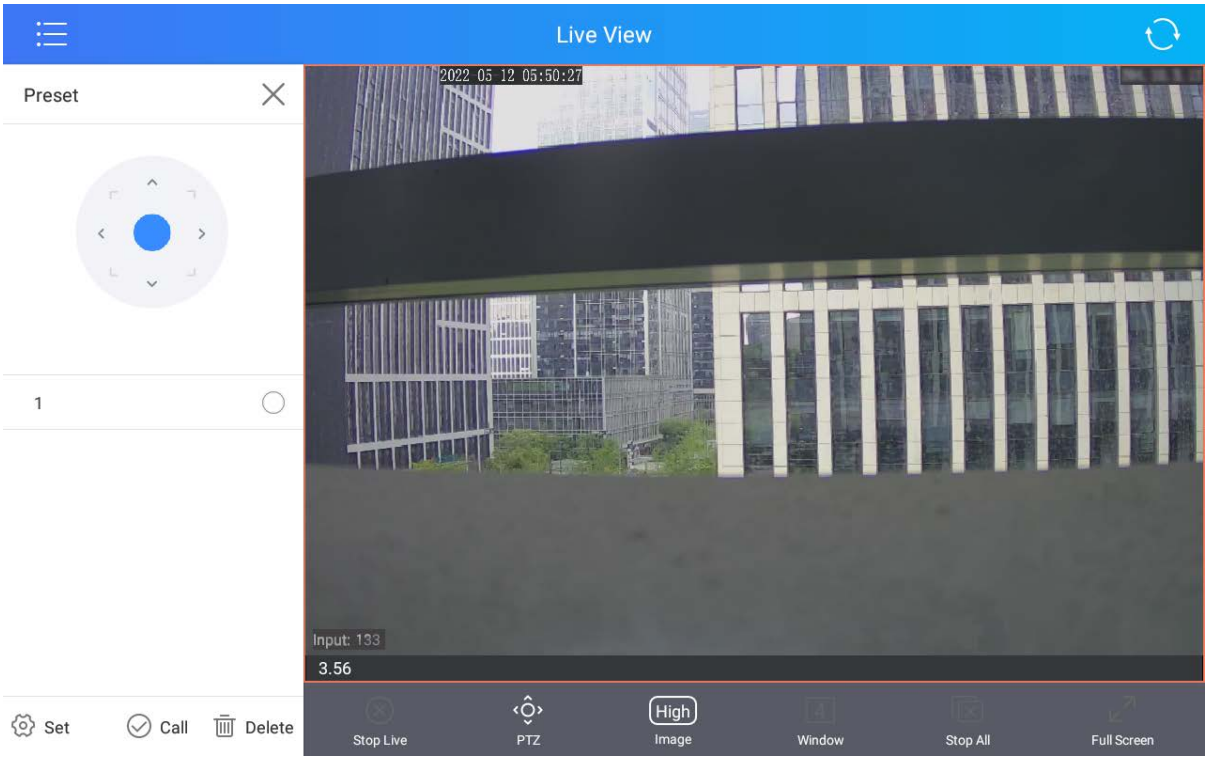
– Rotate the inner wheel of the dial to adjust the iris.

3. To enable wiper or light, tap **Wiper** or **Light**.

NOTE!
The wiper and light functions are only available for cameras with wipers and illuminators.

3. Set a Preset

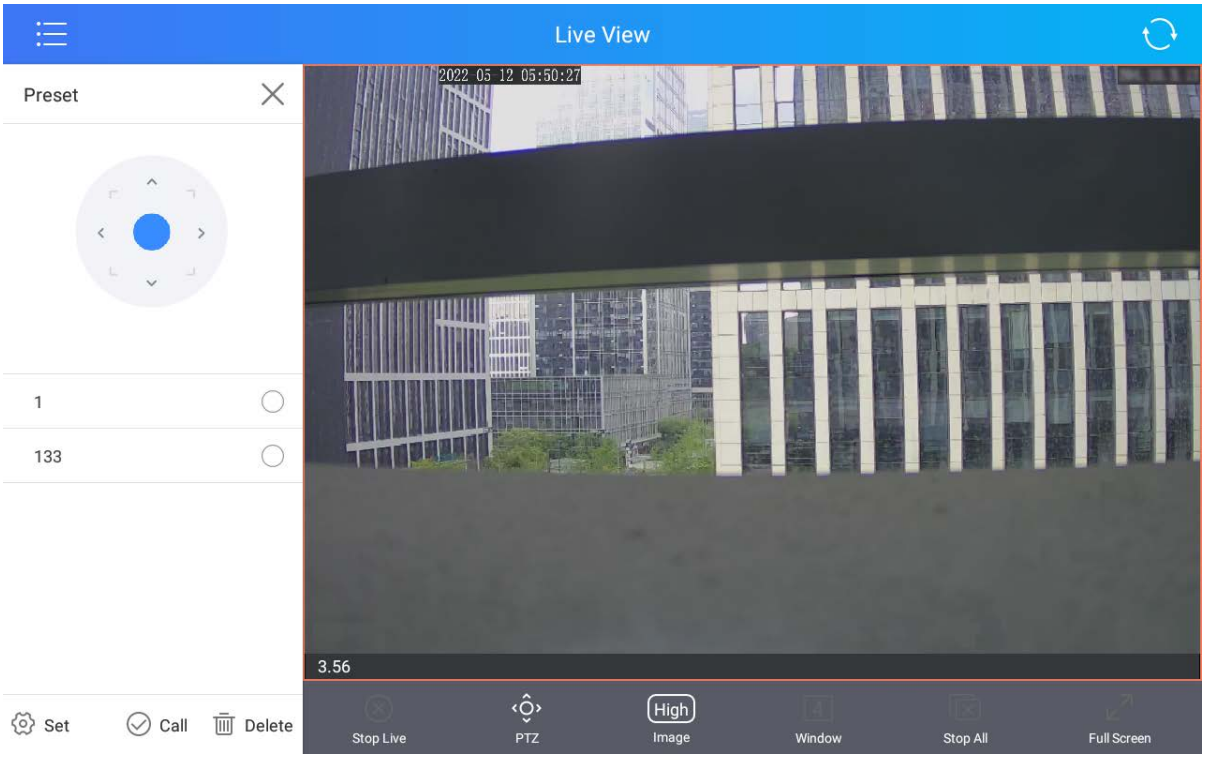
1. Select a live view window and tap **PTZ** to open the PTZ panel.
2. In the PTZ control panel, tap **Preset**.
3. Rotate the PTZ camera to the desired position, tap in the live view window, and name the position using number keys. The preset name input box appears in the lower left corner of the window.



4. Tap **Set** or press the **SHOT** key on the keyboard to set the position as a preset.

4. Call a Preset

1. Select a live view window and tap **PTZ** to open the PTZ control panel.
2. In the PTZ control panel, tap **Preset**.



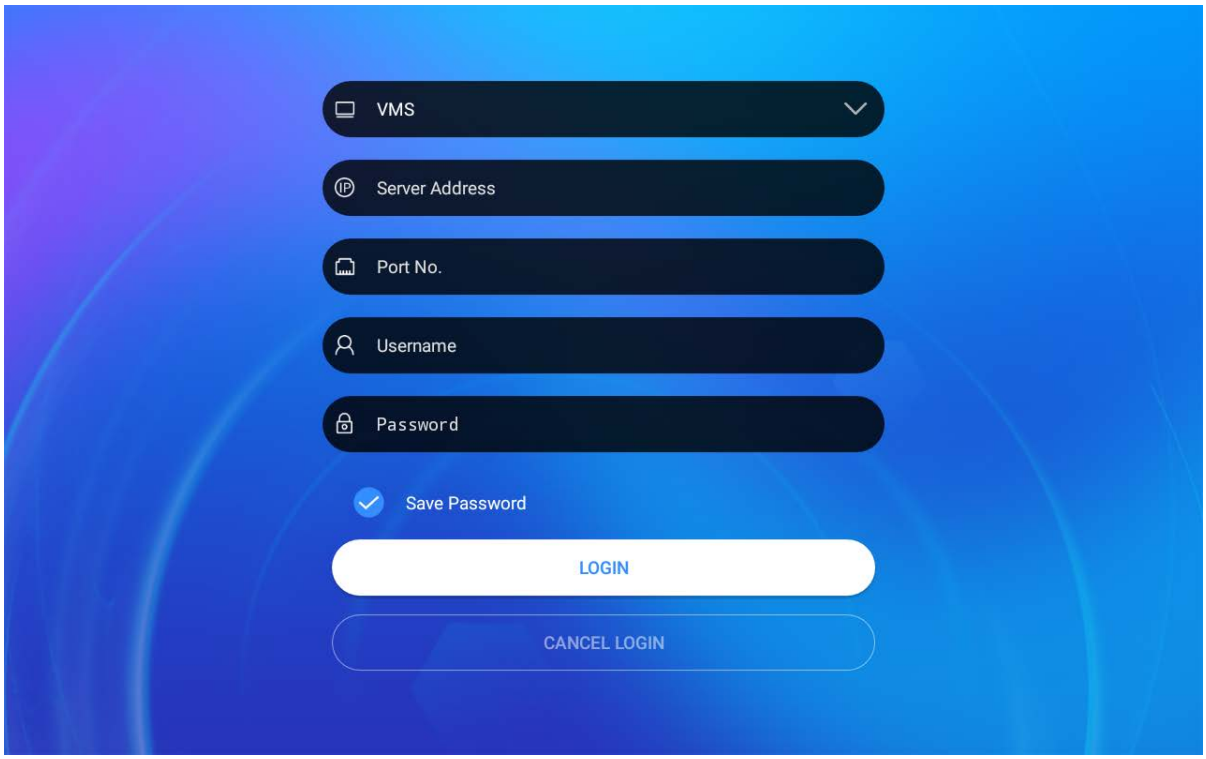
3. Select a preset and tap **Call** or press the **PRESET** key on the keyboard to call the preset.

5 Platform Operations

You can connect the keyboard to platforms to play live video on video wall.

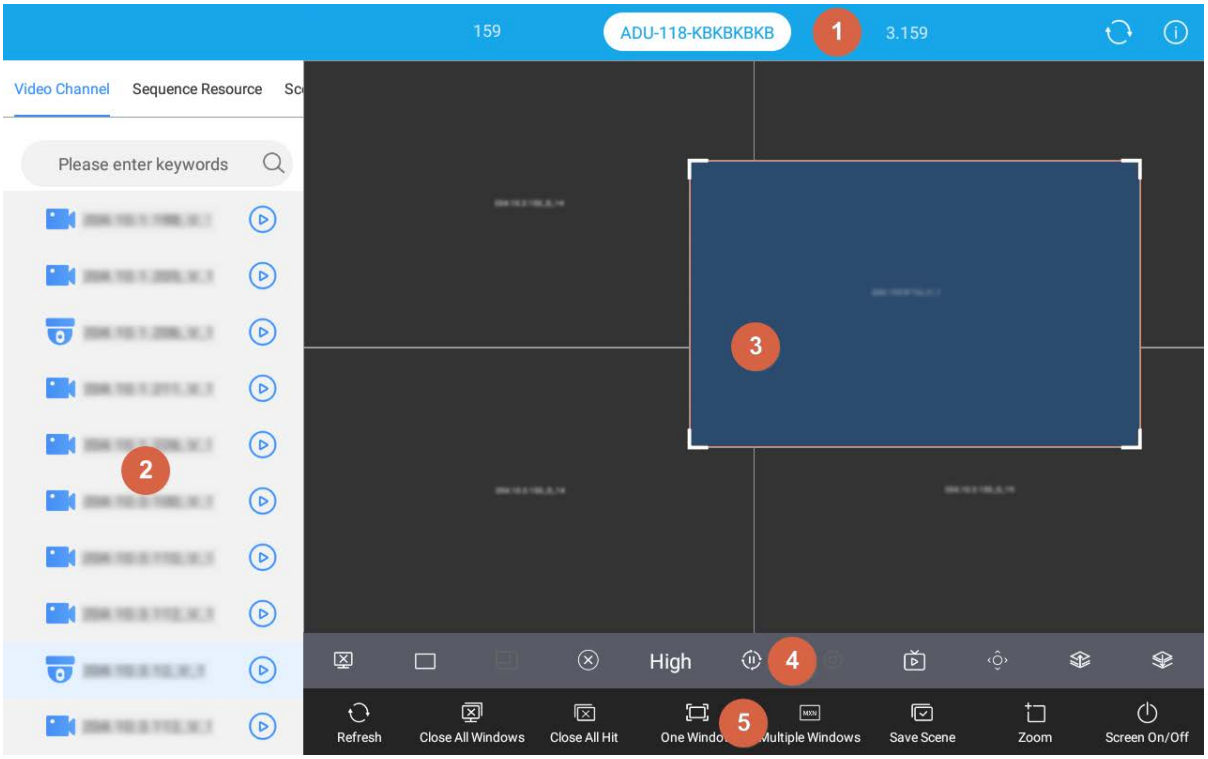
5.1 Platform Login

1. Tap **Platform Operations** on the home screen.



2. Enter the platform information and tap **LOGIN**. To return to the home screen, tap **CANCEL LOGIN**.

5.2 Platform Operations



No.	Description
1	Video wall list. Tap  to refresh the list.
2	Resource list, including video channels, sequence resources, and scenes. Pull down to refresh the list.
3	Video output window.
4	Window toolbar. ● : Close the selected window. ● : Set the number of split windows in the selected window. ● : Splice multiple windows into one. ● : Stop live view in the selected window. ● : Video clarity, including High, Medium, and Low. ● : Start/stop live view or sequence. ● : Stop sequence in the selected window. ● : Start live view in the selected window. ● : PTZ control. ● : Display the selected window on top when multiple windows overlap. ● : Display the selected window at bottom when multiple windows overlap.

No.	Description
5	Video wall toolbar. ● Refresh: Refresh images in all windows. ● Close All Windows: Close all windows. ● Close All Services: Stop services (e.g. live view and sequence) in all windows without closing the windows. ● One Window: Open a window on the video wall. ● Multiple Windows: Open multiple windows on the video wall. You can select an existing template or customize. ● Save Scene: Save the current window layout and services as a scene for quick recall. ● Zoom: Pinch with two fingers to zoom in or out on images. ● Screen On/Off: Turn on/off the display.

1. Live View on Video Wall

Select an online resource in the resource list and tap  to start preview.

Select an online resource in the resource list and drag it to a window to start live view on the video wall.

2. Platform Logout

Tap  to view the system information of the platform. To log out, tap **LOGOUT**.

