

High Definition Video Decoder User Manual

Disclaimer and Safety Warnings


Copyright Statement

©2024 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

 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 Introduction	1
2 Web Login	1
2.1 Web Login	1
2.2 Interface Introduction	3
2.2.1 Login Interface	3
2.2.2 Device Interface	5
3 System	6
3.1 Network	6
3.2 Time	6
3.3 Serial	8
3.4 Service	10
3.5 Security	10
3.5.1 Telnet	10
3.5.2 SNMPv3	11
3.5.3 Secure Password	11
3.5.4 Retrieve Password	12
3.5.5 Engineering Lock	12
4 Running Mode	13
4.1 Running Mode	13
4.1.1 Running Mode	13
4.1.2 Platform	14
5 Personalization	15
5.1 Window	15
5.1.1 Border	15
5.1.2 Main/Sub Stream Policy	15
5.1.3 Double-click Window Maximization	16
5.2 Play	17
6 Maintenance	17
6.1 Device Status	17
6.2 Packet Capture	18
6.3 Decode Info	18
6.4 Maintenance	19

1 Introduction

The high-definition video decoder (hereinafter referred to as "device") is a new generation of integrated software and hardware product designed and developed by our company for large-scale video wall applications. It is a compatible decoding component in the overall solution of the video management system. It supports real-time and high-definition video display, and live sound play, applicable for security, traffic, and other real-time monitoring environments.

This manual mainly introduces Web interface operations to help you understand how to use the device.

**NOTE!**

This manual is available to various device models. The interface and function operations may vary with the device model or function settings.


2 Web Login


Before login, make sure that the device is operating properly and has a network connection to the PC.

2.1 Web Login

1. Open a browser on your PC, enter the device IP address in the address bar (192.168.1.14 by default, can be modified in [Network](#)), press **Enter**, and the **Login** page appears.



 Please enter your username

 Please enter your password

[Forgot PassWord?](#)

Login

Clear

2. Enter the username and password (**admin/123456** by default), and click **Login** to enter the device's Web interface.

ADU8806-E admin Change Password Logout

System ▾

- Network
- Time
- Serial
- Service
- Security
- Running Mode** >
- Personalization** >
- Maintenance** >

Device Status

Basic Info

Model	ADU8806-E
Serial No.	
Firmware Version	
Hardware Versi...	A
Boot Version	UBOOT 003

Running Status

System Time	2024/08/26 15:43:54
Running Time	0 Day(s) 0 Hour(s) 11 Minute(s)
Temperature	32°C
CPU Usage	7%
Memory Usage	30%

Refresh

3. The **Email** window appears at the first login. Select **Email** and enter your email address used to receive a security code in case you need to reset the password, and click **Confirm**.

Email ✕

☒ Email

Confirm

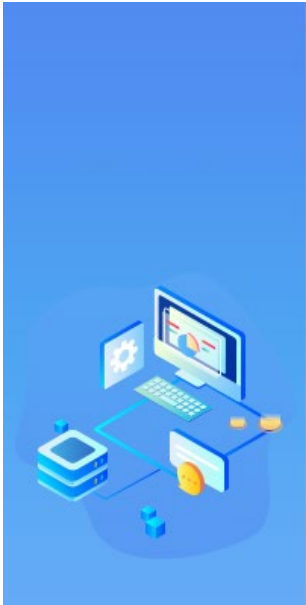
**NOTE!**

To ensure security, please change the default password after your first login and keep the new password secure. See [Change Password](#) for details. If you forgot the password, you can retrieve the password via the following two ways.

- Click **Forgot Password** on the login page, and retrieve the password via the reserved email address. See [Forgot Password](#) for details.
- Press and hold the reset button for over 5 seconds (alarm indicator is flashing) to restore factory settings, and then the device will restart (alarm indicator is off). Then, you can use the default password to log in.

2.2 Interface Introduction

2.2.1 Login Interface



The illustration shows a blue background with a white isometric graphic of a computer system, including a monitor, keyboard, mouse, and server tower, connected by lines.

Please enter your username

Please enter your password

[Forgot PassWord?](#)

Login Clear

1. Forgot Password

1. If you forgot the password, click **Forgot Password** on the login page, and the **Retrieve Password** page appears.

Retrieve Password



Please scan the QR code to obtain the security code (for admin only):

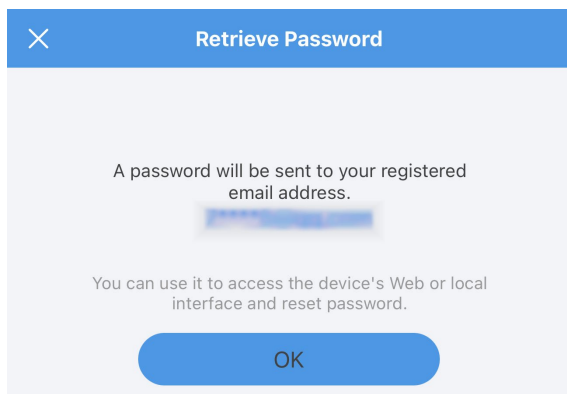
- EZView: Local Config > Forget Device Password

Email:

Security Code

Cancel Next

2. Follow the instructions on the screen to scan the QR code and obtain the security code.
 - With a reserved email address: Scan the QR code with the EZView app, tap **OK** on the **Retrieve Password** page, and the security code will be sent to the reserved address.



- With no reserved email address: Please contact our technical support to obtain the security code.

3. Enter the security code, click **Next**, and the **Change Password** page appears.

A screenshot of the 'Change Password' form. The title bar is blue with the text 'Change Password'. The form has three input fields: 'Security Code', 'New Password', and 'Confirm Password'. Below the fields is a blue button labeled 'Confirm'.

4. Enter the security code again, enter the password, confirm the password, and then click **Confirm**. Then you can log in to the Web interface with the new password.

2.2.2 Device Interface

ADU8806-EadminChange PasswordLogout

System

Network

Time

Serial

Service

Security

Running Mode

Personalization

Maintenance

Device Status

Basic Info

ModelADU8806-E

Serial No.

Firmware Version

Hardware Versi...A

Boot VersionUBOOT 003

Running Status

System Time2024/08/26 15:43:54

Running Time0 Day(s) 0 Hour(s) 11 Minute(s)

Temperature32°C

CPU Usage7%

Memory Usage30%

Refresh

1. Change Password

If you want to change the device password, click **Change Password** in the upper-right corner of the interface, set the new password based on the prompts, and click **Confirm**.

Change Password

Usernameadmin

Old Password

New Password

Confirm Password

Confirm

Cancel

2. Logout

Click **Logout** in the upper-right corner of the interface, and click **Confirm** on the pup-up window.

3 System

3.1 Network

Go to **System > Network**, view and edit the network information to ensure that the device can communicate with other devices properly, and click **Save**.

Network

IPv4 Address

IPv4 Subnet M...

IPv4 Default Ga...

MAC Address

Network Port R... 1000M FULL

Save

Item	Description
IPv4 Address	View or change the IP address. It is used to log in to the device's Web interface. Note: If the current password is a weak one consisting only of digits or letters, you cannot change the IP address across the network segments.
IPv4 Subnet Mask	Set the IPv4 subnet mask, which divides an IP into the network address and host address and determines the host subnet size.
IPv4 Default Gateway	Set the IPv4 default gateway for the host of the local subnet to connect and communicate with the external network.
MAC Address	MAC address, a unique identifier assigned to network interfaces for communications on a physical network.
Network Port Rate	Actual network speed of the device.

3.2 Time

Go to **System > Time**, set the device time, and click **Save**.

**NOTE!**

If the device is a replica device cascaded with the primary device (see [Running Mode](#) for details), its time zone and time will be synced with the primary device and cannot be set separately.

Time

Time Zone

(GMT+08:00) Beijing, Hong Kong ▾

System Time

2024-8-26 03:45:05 PM

Set Time

2024-8-26 03:45:04 PM

⌄


Sync with PC

Auto Update

☐ On

☒ Off

Save

Item	Description
Time Zone	The time zone of the device.
System Time	Real-time time of the device.
Set Time	<ul style="list-style-type: none">Set manually: Click , set the date and time, and click Confirm to save the settings.Auto sync: Click Sync with PC to sync the device time with the PC time.

If there is a Network Time Protocol (NTP) server in the system, you can enable **Auto Update** and configure the NTP server to sync the device time with the standard time. At the same time, the parameters in **Time Zone** and **Set Time** are invalid.



NOTE!
Network Time Protocol (NTP) server provides accurate time synchronization service.

Time

Time Zone

(GMT+08:00) Beijing, Hong Kong ▾

System Time

2024-8-26 03:45:34 PM

Set Time

2024-8-26 03:45:04 PM

⌄

Sync with PC

Auto Update

☒ On

☐ Off

NTP Server Ad...

NTP Port

0

Update Interval

5 Mins ▾

Save

Item	Description
NTP Server Address	The IP address of the NTP server.
NTP Port	The port number of the NTP server.
Update Interval	An interval for automatic time synchronization.

3.3 Serial

Connect the device to the LCD screen, LED screen, or central control device via the serial cable, and configure the serial port parameters on the device's Web interface. Then the device can turn on/off the screens on its connected visualization intelligent control platform or VM's Web interface, or be remotely controlled on the central control device.

1. Screen Control

1. Go to **System > Serial > Serial Port Parameters**, set the serial port used to connect the device to the screen, and set the port usage to **Screen Control**.

Serial Port Parameters

Screen On/Off Protocol

Serial Port Type

RS232

▼

No.

1

▼

Port Usage

Flow Control

▼

Save

Item	Description
Serial Port Type	The serial port type used to connect the device to the screen. <ul style="list-style-type: none">● The LCD splicing screens should be connected to the device via the RS232 serial port.● The LED power distribution box connected to the LED screen should be connected to the device via the RS485 serial port.
No.	Check the serial port silk screen on the device to confirm the used serial port.

2. Go to **System > Serial > Screen On/Off Protocol**, choose an existing protocol or customize the protocol, and set the related protocol parameters and screen control parameters, which should be consistent with those of the screen, and then click **Save**.

Serial Port Parameters

Screen On/Off Protocol

Protocol Name

Customize1

▼

Protocol Format

ASCII Character

▼

Number of Co...

1

Command to T...

Number of Co...

1

Command to T...

Screen Control ...

Baud Rate

9600

▼

Data Bit

8

▼

Stop Bit

1

▼

Check Bit

None

▼

Save

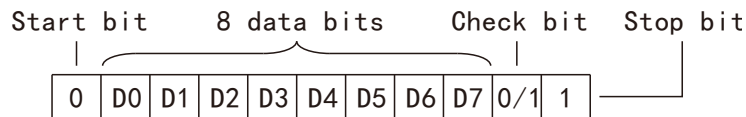
2. Center Control

Go to **System > Serial > Serial Port Parameters**, select the serial port type used to connect the device to the center control device, set the port usage to **Center Control**, set the communication parameters (consistent to the parameters of the central control device), and click **Save**.



NOTE!

The transmitted data should conform to the data format including start bit, data bit, check bit, and stop bit.



Serial Port Parameters	Screen On/Off Protocol
Serial Port Type	RS485
No.	1
Port Usage	Center Control
Duplex Mode	Full-duplex
Baud Rate	115200
Data Bit	8
Stop Bit	1
Check Bit	None
Flow Control	None
<div>Save</div>	

Item	Description
Serial Port Type	The serial port type used by the device to connect to the central control device.
No.	Check the serial port silk screen on the device to confirm the used serial port.
Duplex Mode	<ul style="list-style-type: none"> Full-duplex: Allows data to be transmitted simultaneously in both directions. Half-duplex: Allows data to be transmitted only in one direction at a time. Note: The duplex mode is only available when the serial port type is set to RS485.
Baud Rate	Data transmission speed. The greater the value, the faster the transmission speed.
Data Bit	The actual number of data bits in a group of data packets.
Stop Bit	Indicates the end of transmission of a group of data.
Check Bit	Check if the transmitted data are erroneous. <ul style="list-style-type: none"> Even: Check if the number of "1" bits in the data is even. Odd: Check if the number of "1" bits in the data is odd.

Item	Description
Flow Control	Used to control data transmission to prevent data loss. When the data buffer at the receiving end is full, a no longer receiving signal is sent and the sender stops sending until it receives a signal to resume sending. <ul style="list-style-type: none"> ● Software: Send control signal via the software. ● Hardware: Send control signal via the hardware cable. The actual cable is required for connection.

3.4 Service

Go to **System > Service > Media Stream**, set the media stream parameters so as to play the video based on the setting on the screen, and click **Save**.



NOTE!

This function is unavailable when the device is connected to other platforms (see [Platform](#) for details.) To configure the screen display on the **Service** page, clear all video wall configurations and delete the device from other platforms.

Media Stream

Channel:

Split Type: [Copy To](#)

Standard: [Copy To](#)

Layout:

Stream Address... ☐ Unicast ☐ UDP ☐ Client ☐ Nat SessionId

Note: 1.Unicast address format (RTSP): rtsp://204.12.5.78:554/media/video1
2.Multicast address format (RTSP): rtsp://204.12.5.78:554/media/video1/multicast
3.Source IP 0.0.0.0 indicates that the device does not filter IP address when collecting video streams.

Save

Item	Description
Channel	Choose an output channel.
Split Type	The number of windows. The layout displays the corresponding number of splicing screens.
Standard	The image resolution and refresh rate.
Layout	Click the split window box(es), or enable Stream Address of the window(s) you want to set, and set the detailed parameters.
Stream Address	Set the window display, including stream receiving mode, source IP, etc.

3.5 Security

3.5.1 Telnet

Go to **System > Security > Telnet**. Enable or disable **Telnet** as needed, and then click **Save**. When enabled, Telnet establishes a remote connection with the device, allowing you to access the device remotely, which helps with troubleshooting and device upgrades.

**NOTE!**

- Telnet is a network protocol commonly used for remote login service on the Internet, which allows you to remotely access the device on the computer.
- Telnet's username/password is root/123456.

Telnet SNMPv3 Secure Password Retrieve Password Engineering Lock

Telnet ☒ On ☐ Off

Save

3.5.2 SNMPv3

Go to **System > Security > SNMPv3**. The parameters have been set and you can use the default values. When the device is connected to the VM, the VM can manage the device through this protocol.

**NOTE!**

- This function is unavailable when the device connects to the platform via the ONVIF protocol.
- The Simple Network Management Protocol (SNMP) is mainly used to manage network devices. It provides a standardized management interface to manage network devices of different types and brands uniformly. SNMPv3 is the third generation version with greater security.
- Authentication: Add identity authentication to the transmitted information to confirm the identity of the sender. MD5 and SHA are two digest algorithms used to generate the message digest, that is, check value. SHA provides longer length and higher security than MD5, but has lower execution speed than MD5.
- Encryption: Encrypt the transmitted information to prevent it from being tampered during transmission. AES and DES are two encryption algorithms. AES password provides longer length, higher security, and faster execution speed than DES.

Telnet **SNMPv3** Secure Password Retrieve Password Engineering Lock

Username admin

Authentication MD5

Authentication

Confirm Passw...

Encryption DES

Encryption Pass...

Confirm Passw...

Save

3.5.3 Secure Password

Go to **System > Security > Secure Password**, set the password mode, and click **Save**.

If the current password is a weak one consisting only of digits or letters, you can set the password mode to **Enhanced Password**, and change the password to a strong one as prompted.

Telnet SNMPv3 **Secure Password** Retrieve Password Engineering Lock

Password Mode ☒ Friendly Password ☐ Enhanced Password

Friendly Password: You must log in with a strong password except in the same network segment or three private network segments (10.X.X.X/8, 172.16.X.X/12, 192.168.X.X/16).

Enhanced Password: You must log in with a strong password.

Save

3.5.4 Retrieve Password

Go to **System > Security > Retrieve Password**, and enter the email address, which can be used to receive the security code when you retrieve the password. See [Forgot Password](#) for details.

Telnet SNMPv3 Secure Password **Retrieve Password** Engineering Lock

Username admin

Phone Number

Save

3.5.5 Engineering Lock

Go to **System > Security > Engineering Lock**. Through the engineering lock, you can set a usage period for the device. Within this period, the device can be used normally. Once the period expires, the device will stop video output.

Telnet SNMPv3 Secure Password Retrieve Password **Engineering Lock**

Engineering Lock ☐ On ☒ Off

Save

1. Lock

1. Select **On**, input the remaining days that the device is usable, input a password, and then click **Save**.

You can click **Change Password** to change the password.

Telnet SNMPv3 Secure Password Retrieve Password **Engineering Lock**

Engineering Lock ☒ On ☐ Off

Remaining Day... 30

Password

Confirm Passw...

Save

2. When the set time expires, the remaining days is 0, and the device stops video output.
You can change the remaining days, input the password, and then click **Save** to resume video output.

Telnet SNMPv3 Secure Password Retrieve Password **Engineering Lock**

Engineering Lock ☒ On ☐ Off

Remaining Day...

Password [Change Password](#)

Save

2. Unlock

Select **Off**, enter the password, and then click **Save** to unlock the device.

Telnet SNMPv3 Secure Password Retrieve Password **Engineering Lock**

Engineering Lock ☐ On ☒ Off

Password [Change Password](#)

Save

4 Running Mode

4.1 Running Mode

4.1.1 Running Mode

Go to **Running Mode > Running Mode > Running Mode**, set the device management mode, and click **Save**. Multiple devices can be cascaded.

Running Mode Platform

Management ... ☒ On ☐ Off

Save

Item	Description
Management Mode	<ul style="list-style-type: none">● On: Set the current device to primary device. The device can log in to the visualization intelligent control platform for device management, control and service operation. You can add and manage replica devices on the device, and cascade the device with replica devices.● Off: Set the current device to replica device. The device cannot log in to the visualization intelligent control platform, and it has lower configuration items on the Web interface, and can be used after being cascaded with the primary device to expand the number of interfaces and device capability.

To change the management mode, please pay attention to the following matters:

- When the primary device A connects to the replica device B, if you want to change the device B to the primary device and disconnect it from the device A, please cancel the cascading

between devices A and B on the visualization intelligent control platform, and then enable the management mode on the Web interface of the device B.

- When the primary device A is cascaded with multiple replica devices, if you want to change the device A to a replica device and cascade it with the other primary device B, you can disable the management mode on the Web interface of the device A, and cascade the device A with device B on the visualization intelligent control platform. At this time, the original services (such as, bound devices, added video walls, etc.) of the device A will be deleted, and the services of the device B will be synced to the device A.
- For the primary device A that has been changed to a replica device and is not cascaded with any primary device, if it is changed back to the primary device, its original services will still be retained.

**NOTE!**

Up to 10 devices can be cascaded (1 primary device + 9 replica devices).

4.1.2 Platform

Go to **Running Mode > Running Mode > Platform**, set the communication protocol and parameters for the device to connect to other platforms, and click **Save**. You can manage and control the device via other platform, for example, configure the video wall display corresponding to the device.

1. ONVIF Protocol

The device can connect to the platforms that comply with the ONVIF protocol. Set the protocol to ONVIF, and the device can be controlled through the visualization intelligent control platform, EZStation software, or VMS software. The device can connect to the third-party platform via SDK.

Running Mode	Platform
Protocol	ONVIF
<input type="button" value="Save"/>	

2. Private Protocol

The device can only connect to the platforms that comply with our private protocol, such as VM.

Running Mode	Platform
Protocol	Private
Device ID	XXXXXXXXXXXXXXXXXXXX
Server Address	192.168.1.100
Server Port	8080
Interface Type	Adaptive
<input type="button" value="Save"/>	

Item	Description
Device ID	It is the same as the device serial number by default.
Server Address	The IP address of the server to be connected.
Server Port	The port number of the server to be connected.
Interface Type	<ul style="list-style-type: none"> ● Adaptive: Adaptive signal. The default interface type is HDMI. ● DVI: Convert the connection signal to DVI. <p>Note: The device supports connecting to VM with the version VM3329 or later. Versions VM3329 to VM3336 do not support HDMI signal, so the interface type should be set to DVI. The VM3337 or later versions support HDMI signal, so the interface type should be set to Adaptive.</p>

5 Personalization

5.1 Window

5.1.1 Border

Go to **Personalization > Window > Border**, set the border style for the image display, and click **Save**.

Border
Main/Sub Stream Policy
Double-click Window Maximization


Border

☒ On
 ☐ Off

Win ID

☒ On
 ☐ Off

Border Color




Border Width

5.1.2 Main/Sub Stream Policy

Go to **Personalization > Window > Main/Sub Stream Policy**, set the image number threshold on the output channel, and click **Save**. When the image number on the output channel is less than or equal to the threshold, the images are output from the main stream, otherwise, the images are output from the sub stream.

Border
Main/Sub Stream Policy
Double-click Window Maximization

Number of Windows of Single-VO



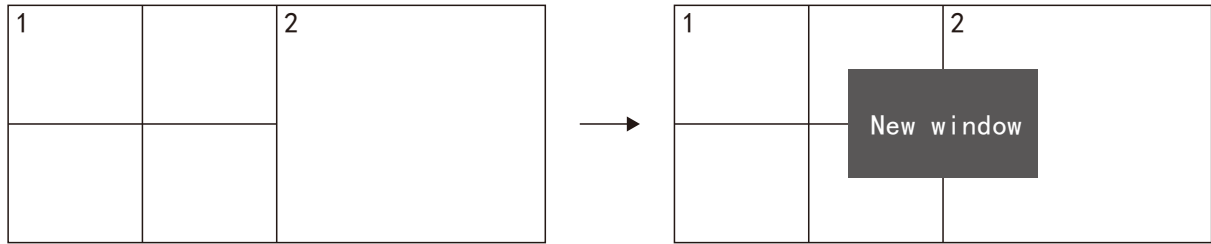
or less, main stream by default

Note: Each image corresponds to one window or split screen.

**NOTE!**

- The main/sub stream policy is only available when the device connects to the visualization intelligent control platform. You can set the media stream type on the visualization intelligent control platform (main stream, sub stream, and third stream, with a decrease in image quality in that order), and the stream threshold will not be affected.
- When a window covers multiple channels, the number of output channels covered by this window is increased by 1. When a new window covers multiple channels, the stream type will be determined based on the maximum image number of the channels.

For example, the threshold is set to 3, and the new window covers channel 1 (4 images) and channel 2 (1 image), and the maximum image number is 5, which exceeds the threshold 3, so the new window will play the sub stream.



5.1.3 Double-click Window Maximization

Go to **Personalization > Window > Double-click Window Maximization**, set the window maximization mode, and click **Save**. On the visualization intelligent control platform, you can double-click the window to magnify the image.

**NOTE!**

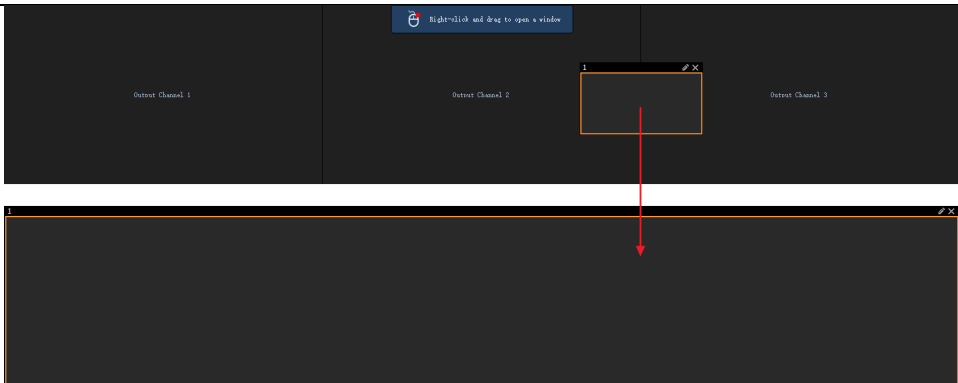
This function is available when the device connects to the visualization intelligent control platform.

Border Main/Sub Stream Policy Double-click Window Maximization

Double-click W... Normal Mode ▼

Save

Item	Description
Normal Mode	<p>The window will be magnified to fill the currently occupied output channel(s).</p>
Video Wall Mode	<p>The window will be magnified to fill all output channels on the video wall.</p>

Item	Description
	 <p>The screenshot shows a video decoder interface with three output channels labeled 'Output Channel 1', 'Output Channel 2', and 'Output Channel 3'. A small window titled '1' is positioned over 'Output Channel 2'. A red arrow points from this window to a larger window below it, which also has a title bar with '1' and window control buttons.</p>

5.2 Play

Go to **Personalization > Play**, set the image display mode, and click **Save**.

Play

Processing Mode: Real Time Priority ▼

When Decodin...: Display Last Frame ▼

When Video Lo...: Display Last Frame ▼

Save

Item	Description
Processing Mode	<ul style="list-style-type: none"> Real Time Priority: Display real-time video, no delay or low delay (requires high network condition). Fluency Priority: Display smooth video, but with a certain delay (requires low network condition).
When Decoding Stops	<ul style="list-style-type: none"> Display Last Frame: Display the last frame before stopping decoding. Display Black Screen: Display black screen.
When Video Lost	<ul style="list-style-type: none"> Display Last Frame: Display the last frame of the video before it is lost. Display Video Loss Message: Display the message of video loss.

6 Maintenance

6.1 Device Status

Go to **Maintenance > Device Status**, and you can view the basic information and operation status of the device and click **Refresh** to update the latest information.

Device Status

Basic Info

Model	ADU8806-E
Serial No.	27002700 0000000000000000
Firmware Version	811001.2.15.00000001
Hardware Versi...	A
Boot Version	UBOOT 003

Running Status

System Time	2024/08/26 15:43:54
Running Time	0 Day(s) 0 Hour(s) 11 Minute(s)
Temperature	32°C
CPU Usage	7%
Memory Usage	30%

[Refresh](#)

6.2 Packet Capture

Go to **Maintenance > Packet Capture**, and capture data packets of the interaction between the device and other devices so as to troubleshoot the problem.

Packet Capture

IP Address	<input type="text"/>
Port	<input type="text"/>
Start	Stop

1. Enter the IP address and port number of other device.



NOTE!

When the IP address is empty, the system captures all packets..

2. Click **Start** to start capturing packets, click **Stop** to stop capturing packets, and the system will capture data from the start time to end time.

6.3 Decode Info

Go to **Maintenance > Decode Info**, and you can view the device decoding information to check if the current stream is normal and if there is packet loss.

Click the refresh icon in the **Operation** column to refresh a decoding information. Click **Refresh** to refresh all decoding information.

Decode Info

Refresh

No.	Wall Nar	Win ID	Split Sc	Win C	Source	Src Po	Destinatio	Dst Port	Protocol	Resolution	Frame R	Video	Audio	Format	Realtime F	Total Pack	Total Pack	Opera
1	Wall 1	1	1	1		0		0		0*0	0				0	0	0	



6.4 Maintenance

Go to **Maintenance > Maintenance**, and you can perform system maintenance and upgrade.

Maintenance

Restart	Restart device
Default	Keep the current network and user settings and restore other settings to factory defaults.
Export	Export configuration file
Export	Export diagnostic information
Auto Restart	Never <input type="button" value="v"/> 00:00 <input type="button" value="v"/> <input type="button" value="OK"/>
Configurations	<input type="button" value="Folder icon"/> <input type="button" value="Import"/>
Local Upgrade	<input type="button" value="Folder icon"/> <input type="button" value="Upgrade"/>

Note: Do not disconnect power or perform any other operation during upgrade.

Item	Description
Restart	Restart the device.
Default	Restore all settings to defaults except current network and user settings, and then restart the device.
Export Configuration	Export configuration information. Allows to view and save configuration information.
Export Diagnosis Information	Export diagnosis information. Allows to view and save diagnosis information.
Auto Restart	Set the time and repetition period for auto restart, click OK , and the device will automatically restart at the set time.
Import Configuration	Click  , select the local configuration file, and click Import to import configuration and restart the device.
Local Upgrade	Click  , select the local upgrade file, and click Upgrade to upgrade the system and restart the device. Note: The system can only be upgraded to a newer version, not an older one.



CAUTION!

Do not disconnect the device from power or perform other operations during system maintenance and upgrade.