Video Wall Controller

User Manual

Manual Version: V1.03

Disclaimer and Safety Warnings

Copyright Statement

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 Introduction 1
2 Login 1
3 System 2
3.1 Basic Info 2
3.2 Time 2
3.3 Serial 4
3.3.1 Serial Port Parameters 4
3.3.2 Screen Control Protocol 5
3.4 Play 7
3.4.1 Play 7
3.4.2 Advanced 7
3.5 Window 7
3.6 Running Mode 8
3.7 Security 8
3.7.1 Telnet 8
3.7.2 SNMPv3 9
3.7.3 Authentication 9
3.7.4 Secure Password 9
3.7.5 Engineering Lock 10
3.8 Holiday 12
4 Network 14
4.1 TCP/IP 14
5 Maintenance 15
5.1 Device Status 15
5.2 Packet Capture 16
5.3 Retrieve Password 17
5.3.1 Set Email 17
5.3.2 Retrieve Password 17
5.4 Maintenance 19

1 Introduction

This product is a high-performance video image processing workstation that can display multiple dynamic screens on multiple displays to realize the window splicing function. This product, designed specifically for high-quality multi-screen scenarios, features flexible control of different types of screens with varied resolutions.

This manual describes how to manage the device on a Web browser. The figures in this manual are only for illustration purpose. The parameters, options, and values actually displayed on the Web pages of your device may be different from those in this manual.

2 Login

Before you start, check that:

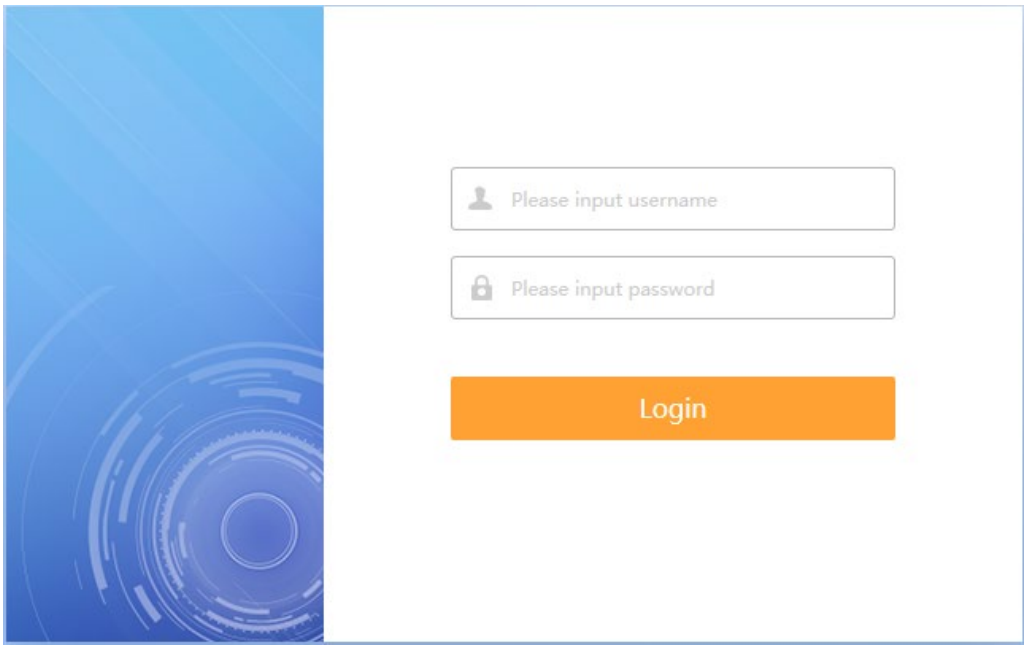
- The device is operating properly.
- The computer is connected to the device.

NOTE!

- The default IP address of your device is 192.168.1.14; the default subnet mask is 255.255.255.0; the default gateway is 192.168.1.1.
- Use **admin** as the username and **123456** as the password for first-time login. Please change the default password under admin to ensure account security.

Follow the steps to log in to the device:

1. Enter the device's IP address in the address bar and then press **Enter**.

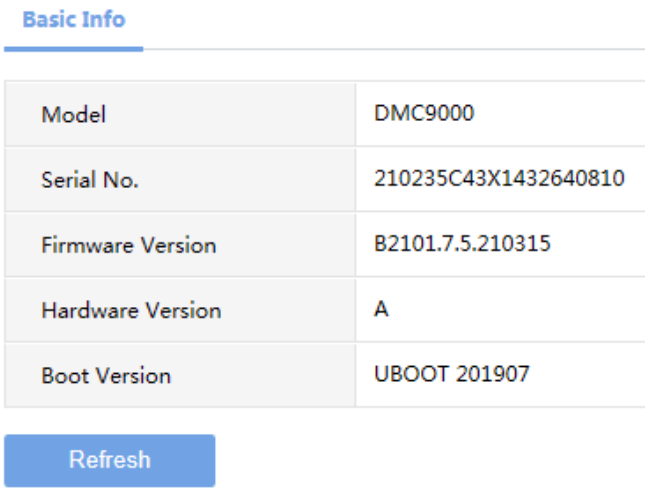


2. Log in with the correct username and password.

3 System

3.1 Basic Info

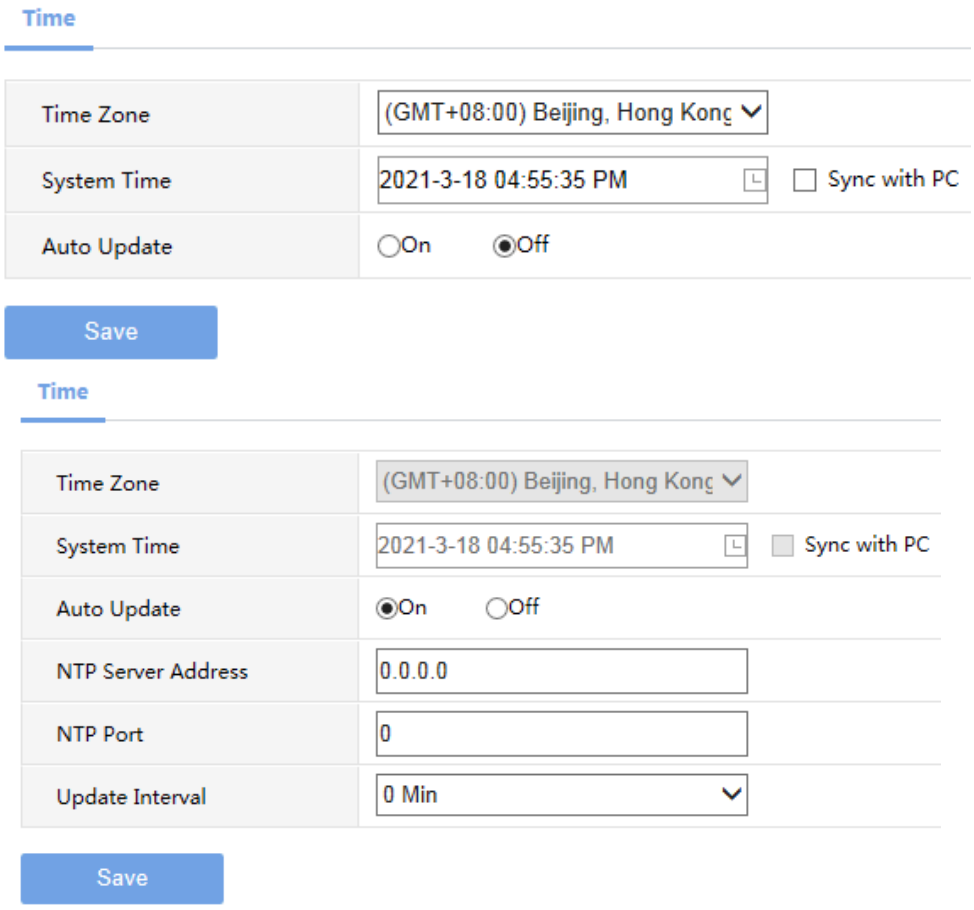
Go to **System** > **Basic Info**. The **Basic Info** page lists the basic information including device type, serial number, software version, hardware version, and boot version.



3.2 Time

Set system time for your device and how to update time.

1. Go to **System** > **Time**.



2. Set the parameters. Some are described in the table below.

Parameter	Description
Time Zone	Choose a time zone for your device.
System Time	Current system time of the device. Click the **Set Time** text box and then set the time manually, or select **Sync with PC** and then the device automatically synchronizes time with your computer.
Auto Update	Enable this function if you have a Network Time Protocol (NTP) server on the network. The device synchronizes time with the NTP server at the set interval when enabled. The NTP server's IP address, port number, and update interval are required.
NTP Server Address	Enter the IP address of the NTP server. **Note:** Set only when automatic update is enabled.
NTP Port	Enter the port number of the NTP server. **Note:** Set only when automatic update is enabled.

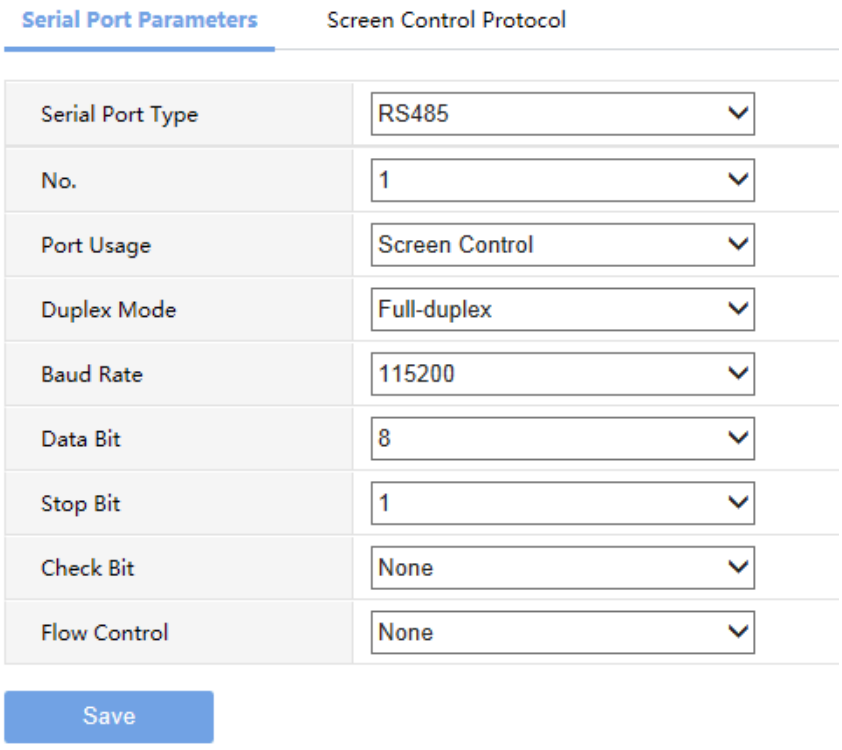
Parameter	Description
Update Interval	The device time is updated every few minutes. **Note:** • The valid range of input time is 1~10080 minutes. • Available when auto update is enabled.

NOTE!
The device synchronizes time with the central server when operating in server mode.

3.3 Serial

3.3.1 Serial Port Parameters

1. Go to **System** > **Serial** > **Serial Port Parameters**.



2. Set the parameters. Some are described in the table below.

Parameter	Description
Serial Port Parameters	Choose the serial port type, including RS232 or RS485.
NO.	Choose the serial port ID. Default: 1.
Port Usage	• Screen Control: If the decoder is connected to the screen through the serial port,

Parameter	Description
	the decoder can control the screen to turn on or turn off. Only parameters of the **Screen Control Protocol** tab are available when this option is selected. ● Center Control: If the decoder is connected to the central control device, the decoder can be controlled on the central control device. Only parameters of the **Serial Port Parameters** tab are available when this option is selected.
Duplex Mode	Full duplex or half duplex. Half duplex allows data to be transmitted only in one direction at a time. Full-duplex allows data to be transmitted simultaneously in both directions. **Note:** The duplex mode is only available to RS485.
Baud Rate	Serial baud rate. **Note:** The baud rate of the serial port must be the same as that of the external device connected to the serial port.
Data Bit	The number of data bits in a data packet.
Stop Bit	Indicates the end of transmission of a group of data.
Check Bit	Used to check whether the received data bits are erroneous.
Flow Control	Used to control data transmission to prevent data loss.

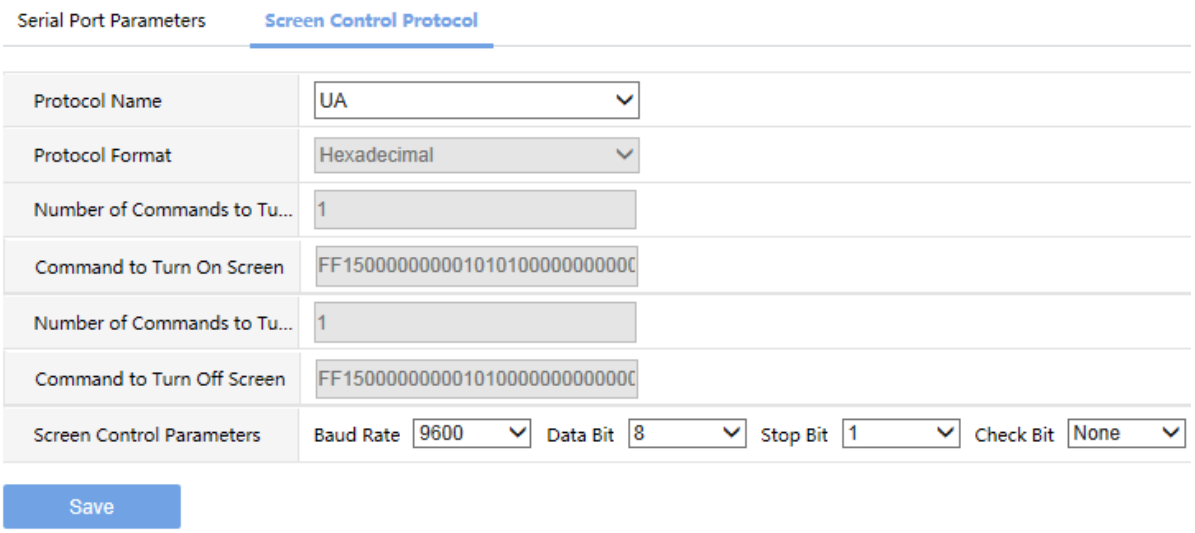
3. Click **Save**.

3.3.2 Screen Control Protocol

Set the screen control protocol based on the actual situation. You can also customize the protocol.

For the custom protocol, the command to turn on/off screen can be configured, and then you can turn on/off the screen with the protocol on the screen-connected client.

1. Go to **System** > **Serial** > **Screen Control Protocol**.



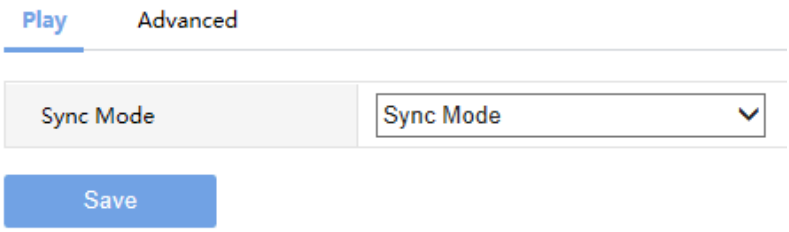
2. Set the parameters. Some are described in the table below.

Parameter	Description
Protocol Name	Choose a screen control protocol, including exiting protocols and custom protocols.
Protocol Format	Use the preset protocol format, or choose a format for custom protocols.
Number of Commands to Turn On Screen	Use the preset number, or customize a number for custom protocols.
Command to Turn On Screen	Use the preset command, or customize the command for custom protocols.
Number of Commands to Turn Off Screen	Use the preset number, or customize a number for custom protocols.
Command to Turn Off Screen	Use the preset command, or customize the command for custom protocols.
Screen Control Parameters	• Baud Rate: Serial baud rate. • Data Bit: The actual number of data bits in a data packet. • Stop Bit: Indicates the end of transmission of a group of data. • Check Bit: Used to check whether the received data bits are erroneous.

3.4 Play

3.4.1 Play

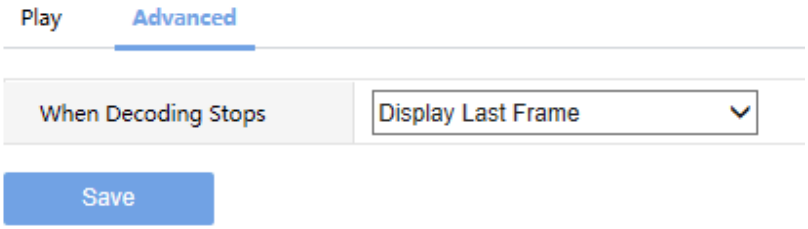
1. Go to **System** > **Play**. Set display mode.



2. Click **Save**.

3.4.2 Advanced

1. Go to **System** > **Play** > **Advanced**. Set what to display when decoding stops.



2. Click **Save**.

3.5 Window

1. Go to **System** > **Window**.

2. Set the parameters. Some are described in the table below.

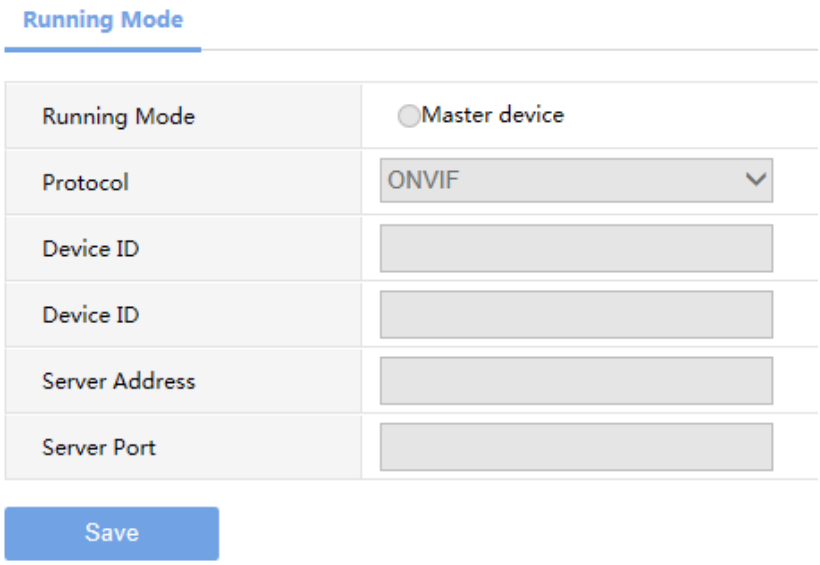
Parameter	Description
Border	Off by default, displays window border after opening.
Border Color	Set border color.

Parameter	Description
Border Width	Set border width.

3. Click **Save**.

3.6 Running Mode

1. Go to **System** > **Running Mode**. Set the running mode and protocol of the device.



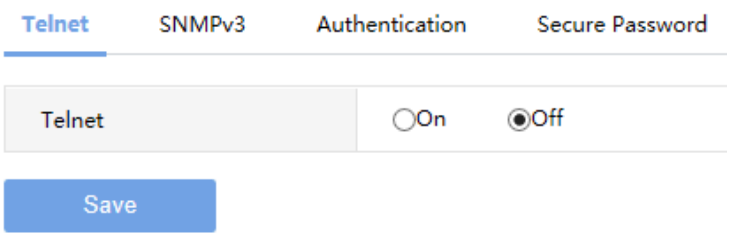
2. Click **Save**.

3.7 Security

3.7.1 Telnet

Enable Telnet if you want to access the device from a computer with Telnet. By default, the admin username cannot be changed.

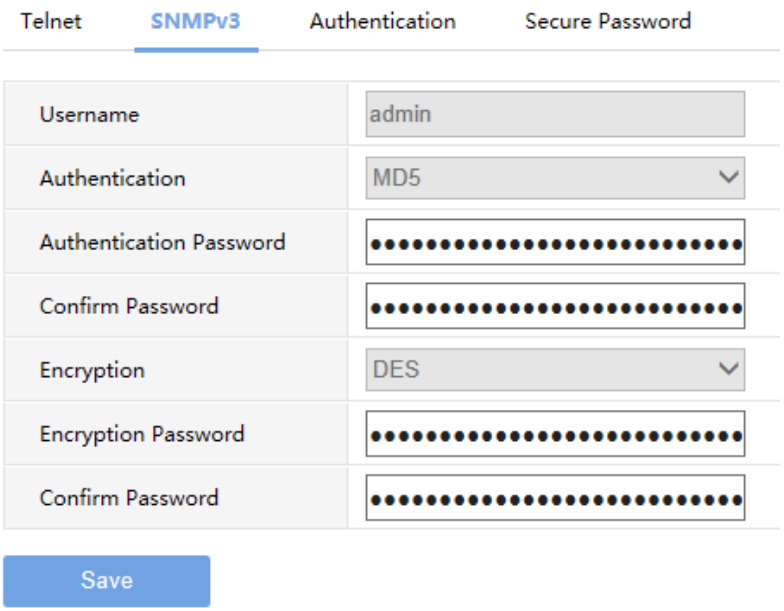
1. Go to **System** > **Security** > **Telnet**.



2. Select the check box to enable **Telnet**, and then click **Save**.

3.7.2 SNMPv3

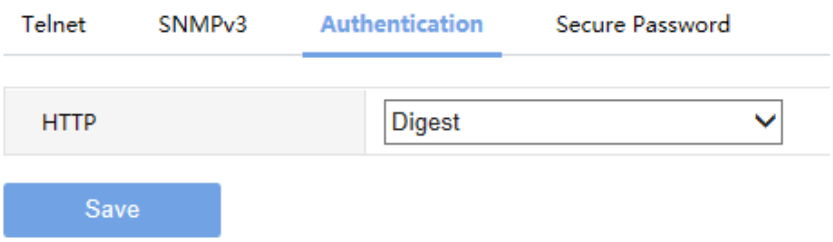
Go to **System** > **Security** > **SNMPv3**. Through SNMP the central server synchronizes audio/video channel configurations and some of the scheduled tasks to the device, and the device reports device alarms to the central server.



3.7.3 Authentication

Select digest or null in the **Authentication** page. Digest access authentication is one of the agreed-upon methods a web server can use to negotiate credentials with server.

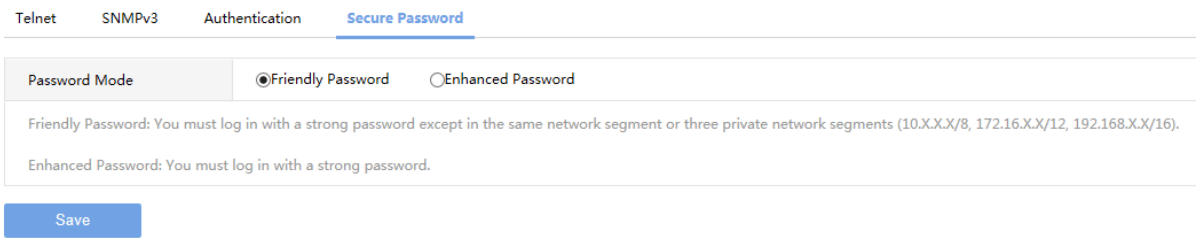
1. Go to **System** > **Security** > **Authentication**.



2. Select **Digest** to enable the digest authentication, and then click **Save**.

3.7.4 Secure Password

1. Go to **System** > **Security** > **Secure Password**.



2. Some parameters are described in the table below.

Parameter	Description
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.

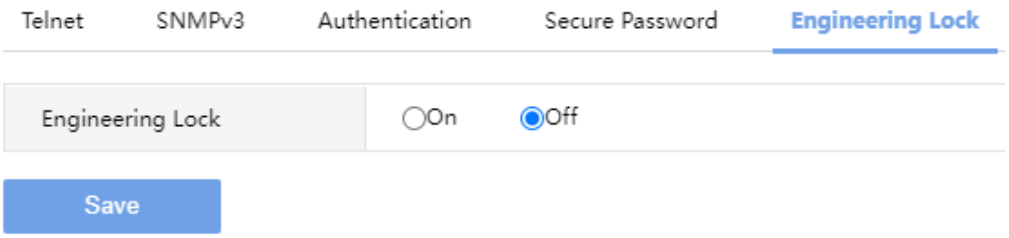
3. Select password mode, and then click **Save**

3.7.5 Engineering Lock

NOTE!

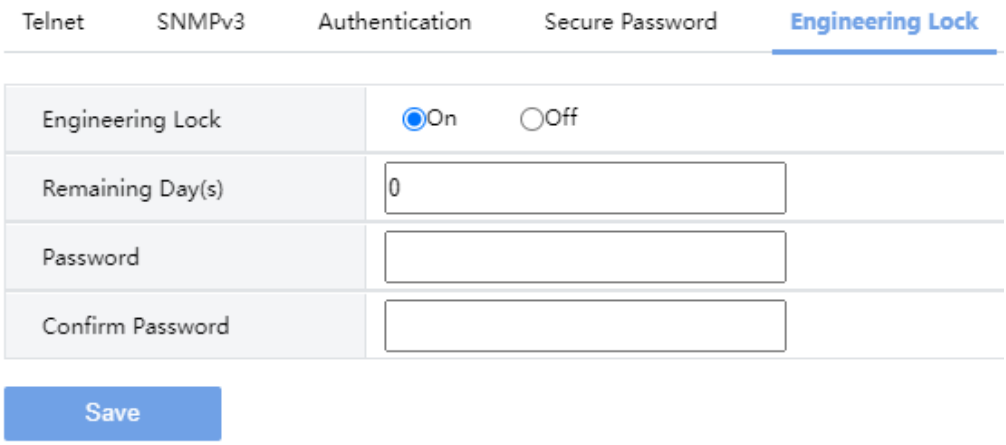
This function is only available to certain devices.

Go to **System** > **Security** > **Engineering Lock**, and you can set the validity period for the device. The device will not display the image when the set validity period has been reached.

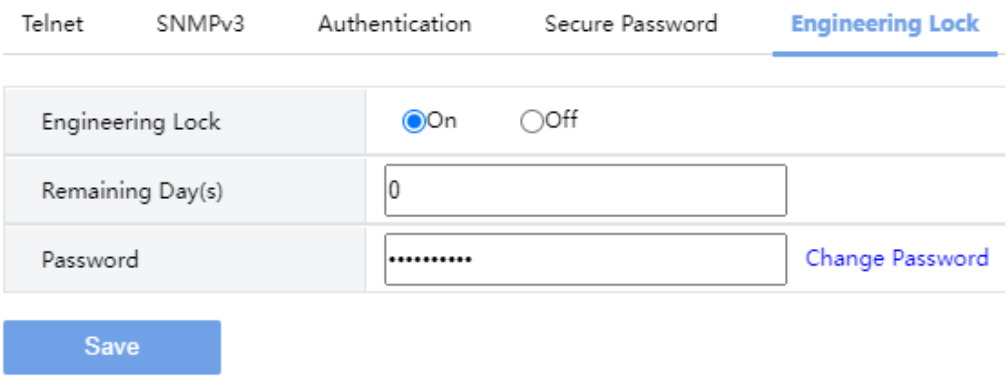


1. Lock

Click **On** to enable engineering lock, set the remaining days and password, and click **Save**.

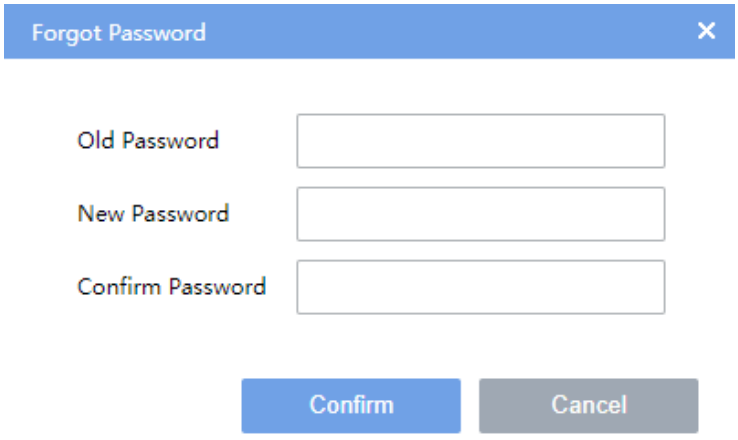


When the remaining day(s) is 0, the device will not display the image. You can change the remaining day(s), enter the password, and click **Save**. Then the image can be displayed normally.



2. Change Lock Password

After the device is locked, click **Forgot Password**, and change the lock password as needed.



3. Unlock

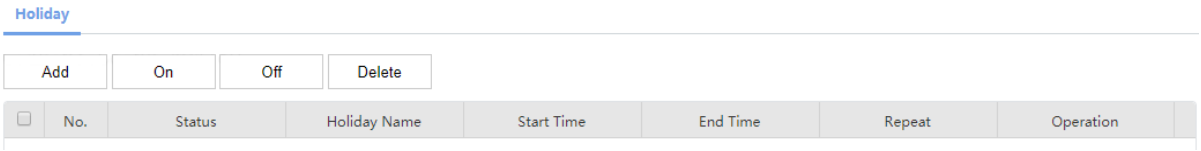
After the device is locked, click **Off** to disable engineering lock, and enter the password to unlock the device for normal image display.

3.8 Holiday

NOTE!

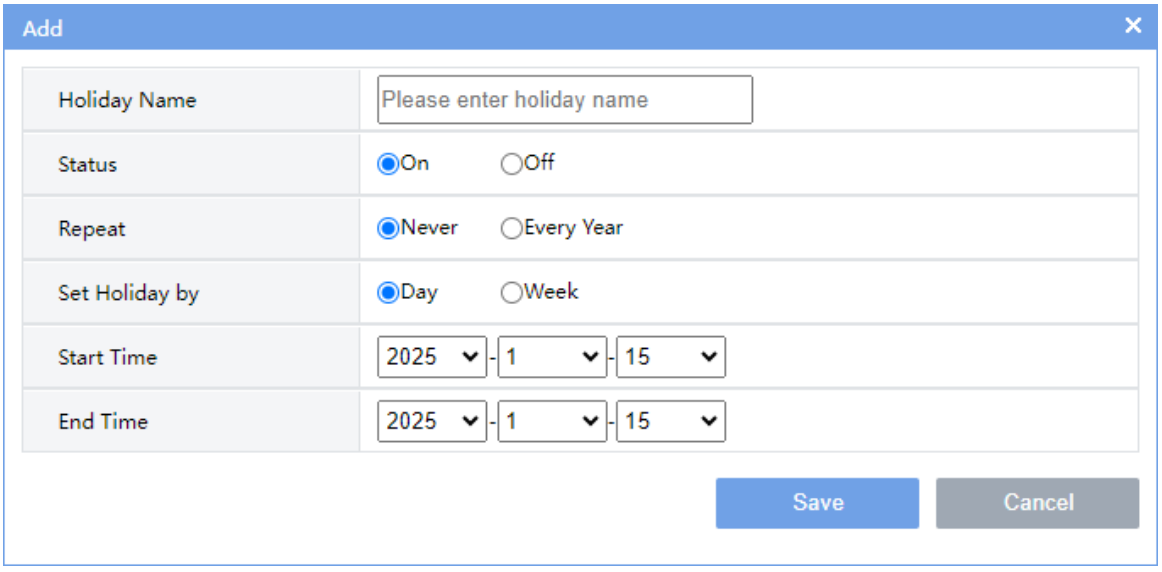
This function is only available to certain devices.

Go to **System** > **Holiday** to set the holiday, and the screen can turn on/off automatically based on the set holidays on the visualization intelligent control platform.



1. Add Holiday

1. Click **Add**.



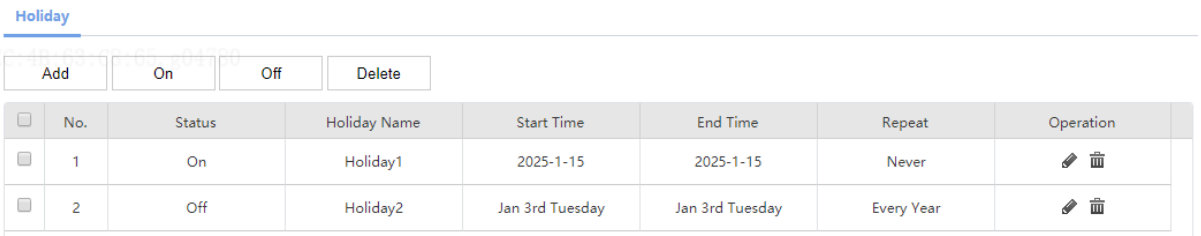
2. Configure holiday parameters.

Item	Description
Holiday Name	Set the holiday name. **Note:** The name must be unique.
Status	Choose the holiday status. ● On: The holiday is effective. ● Off: The holiday is not effective.
Holiday Time	Choose the repeat mode, and then set the start time and end time. ● Never: The holiday is effective once in the specified year. ➢ Day: Set the holiday in year/month/day format, for example, 2025/1/1. ➢ Week: Set the holiday in year/month/week/day of week format, for example, 2025/January/1st/Monday. ● Every Year: The holiday is effective every year. ➢ Day: Set the holiday in month/day format, for example, 1/1. ➢ Week: Set the holiday in month/week/day of week format, for example, January/1st/Monday.

3. Click **Save**.

2. Manage Holiday

View and manage the added holidays.



Item	Description
Edit	Click  to edit the current holiday, and then click **Save**.
Enable/Disable	Select the holiday(s) or select the **All** checkbox, and click **On/Off** to enable/disable the holiday(s).
Delete	You can delete the holiday(s) one by one or in batches. ● Delete one by one: Click  to delete a holiday. ● Delete in batches: Select the holiday(s) you want to delete or select the **All** checkbox, and then click **Delete**.

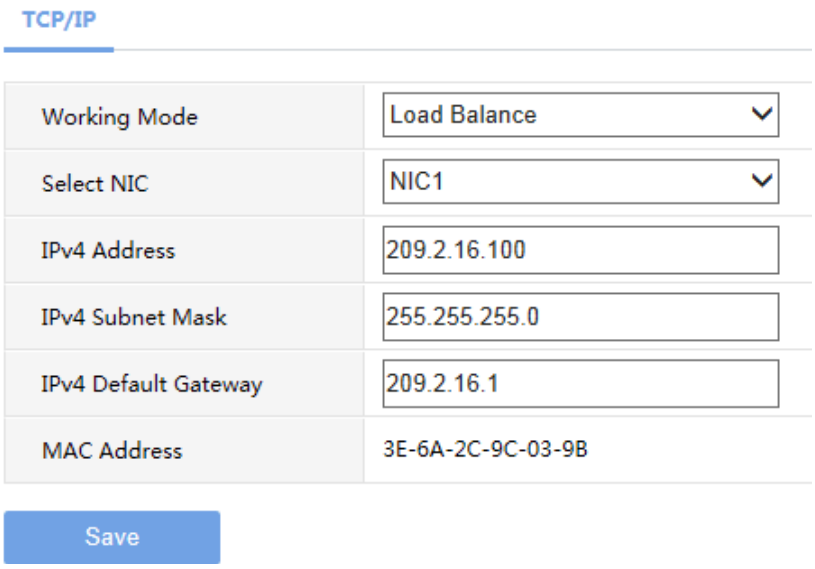
4 Network

Set network settings include TCP/IP and Telnet so that the device can communicate with other devices on the network.

4.1 TCP/IP

Assign a static IP address manually, or obtain one using the DHCP server.

1. Go to **Network** > **TCP/IP**.



2. Set the parameters. Some are described in the table below.

Parameter	Description
Working Mode	Load Balance.
Select NIC	Select the network interface.
IPv4 Address	Set the IP Address.
IPv4 Subnet Mask	Set the subnet mask.
IPv4 Default Gateway	Set the gateway.
MAC Address	Display the mac address.

3. Click **Save**.

5 Maintenance

5.1 Device Status

Go to **Maintenance** > **Device Status** to view information of the device.

Device Status

Basic Info

Model	DMC9000		
Serial No.	210235C43X1432640810	Firmware Version	[redacted]
Hardware Version	A	Boot Version	UBOOT 7.00

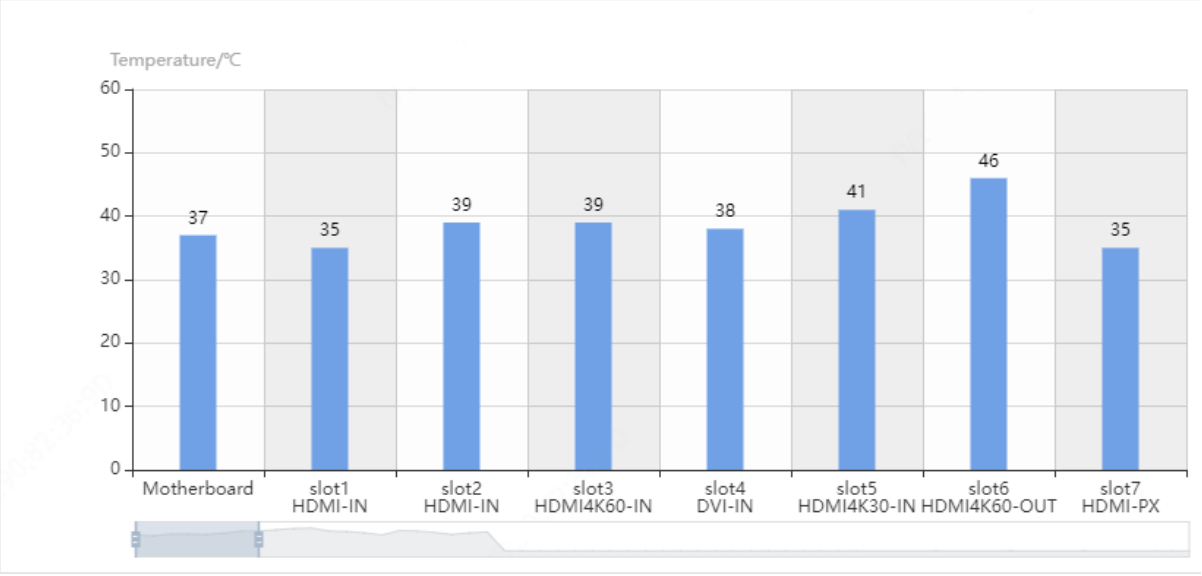
Running Status

Running Mode	Master device		
Access Mode	Multi-screen Controller	Protocol	ONVIF
System Time	2024/10/13 16:57:33		
Running Time	0 Day(s) 23 Hour(s) 55 Minute(s)	Temperature	30℃
CPU Usage	5%	Memory Usage	22%

Fan Status

Fan 1 Status	Online	Fan 1 Speed	4950
Fan 2 Status	Online	Fan 2 Speed	4920
⋮		⋮	
Fan 23 Status	Offline	Fan 23 Speed	0
Fan 24 Status	Offline	Fan 24 Speed	0

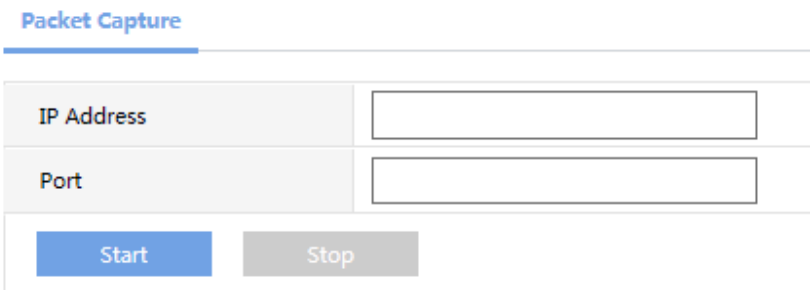
Slot Temperature



Refresh

5.2 Packet Capture

1. Go to **Maintenance** > **Packet Capture**.



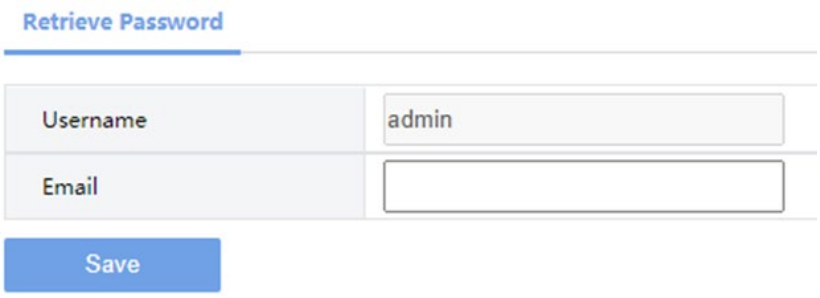
2. Set the parameters according to the following table, and then click **Start**.

Parameter	Description
IP Address	Set the IP address of the device to capture packets.
Port	Set the port number of the device to capture packets.

5.3 Retrieve Password

5.3.1 Set Email

1. Go to **Maintenance** > **Retrieve Password**. A page as shown below appears.



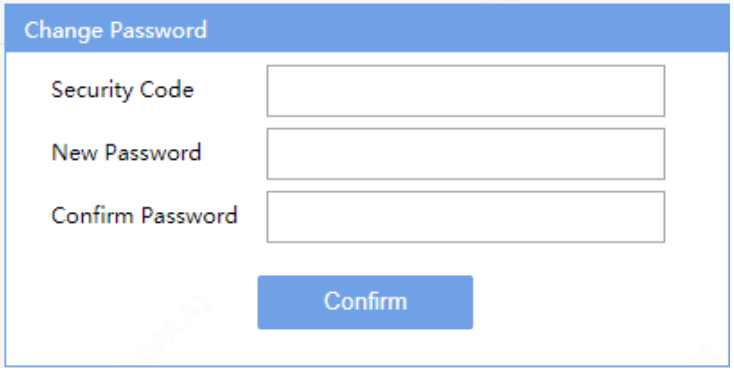
2. Enter your email correctly, and click **Save**.

5.3.2 Retrieve Password

1. Retrieve With an Email Address

1. Click **Forgot Password** on the login page. A page as shown below appears.

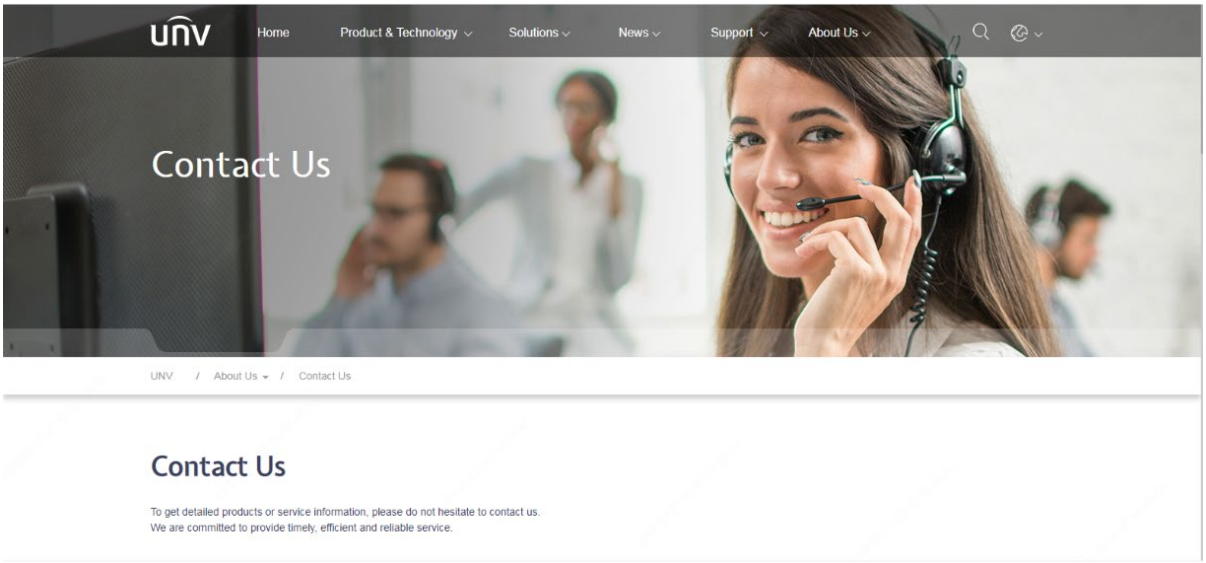
2. Follow the on-screen instructions and use the app to scan the QR code on the left to get the security code. Enter the security code and click **Next**.
3. Enter the security code, new password, and confirm the new password. Then click **Confirm** to change the password.



2. Retrieve Without An Email Address

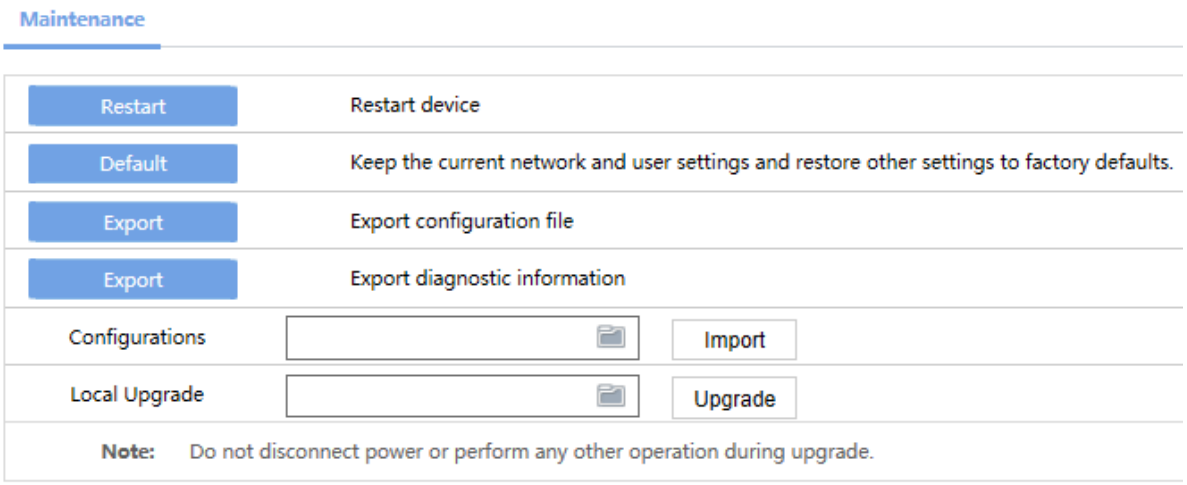
1. Click **Forgot Password** on the login page. A page as shown below appears.

2. Click **Please contact us to retrieve the password.** to enter the **Contact Us** page.



5.4 Maintenance

Go to **Maintenance** > **Maintenance,** and perform maintenance operations as needed. You can restart the device, restore some factory default settings, import and export configuration files, export diagnostic information, and upgrade the device.


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
Configurations
Import
Local Upgrade
Upgrade
Note:
Do not disconnect power or perform any other operation during upgrade.