Apartment Door Station

User Manual

V1.02

Contents

About this Manual

This manual describes the features and operations of apartment door station (hereinafter referred to as “door station”).

Copyright Statement

Disclaimer

Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

This manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty.

The illustrations in this manual are for reference only and may vary depending on the version or model. The screenshots in this manual may have been customized to meet specific requirements and user preferences. As a result, some of the examples and functions featured may differ from those displayed on your monitor.

Safety Symbols

The symbols in the following table may be found in this manual. Carefully follow the instructions indicated by the symbols to avoid hazardous situations and use the product properly.

Symbol	Description
 **NOTE!**	NOTE! Indicates useful or supplemental information about the use of product.
 **CAUTION!**	CAUTION! Indicates a situation which, if not avoided, could result in damage, data loss or malfunction to product.
 **WARNING!**	WARNING! Indicates a hazardous situation which, if not avoided, could result in bodily injury or death.

1 Defaults

The default parameters of the door station are as follows:

• Username: admin	• Password: 123456
• Static IP address: 192.168.1.13	• Subnet mask: 255.255.255.0

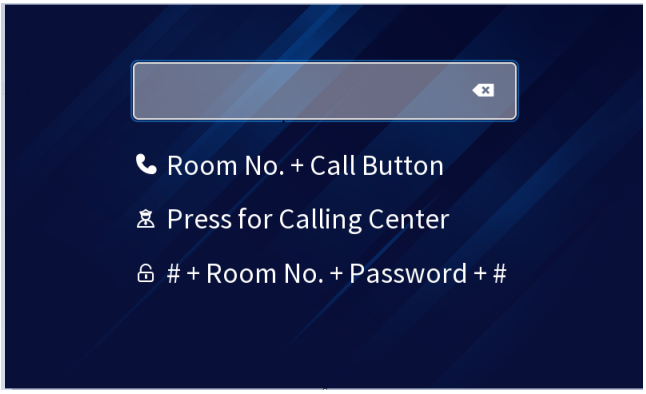
Note: DHCP is enabled by default on the door station. If a DHCP server is deployed in the network, the door station may be assigned an IP address, and you need to use the assigned IP address to log in.

2 Startup

Refer to the device's quick guide to install it properly, and connect it to the power to start up the door station.

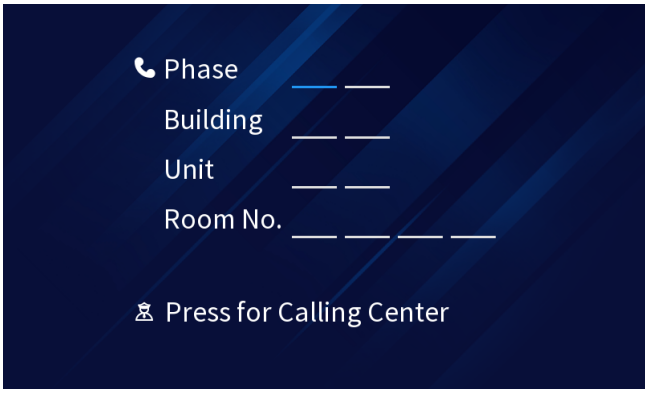
Unit Door Station Mode

The default mode is Unit Door Station (see the screen display below). You can make calls and open the door by password or card.



Zone Station Mode

After switching to Zone Station Mode (see the screen display below), you can make calls only.



3 Call Room

You can call the indoor station in an apartment's room or leave a message to it on the apartment door station's screen.

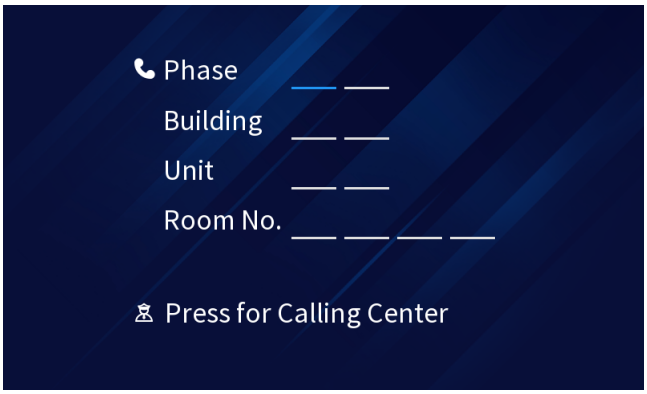
Note: Make sure the apartment door station has been related to the indoor station to be called. You should bind the device on the indoor station's screen. See the *Indoor Station User Manual* for details.

Make a Call

1. Dial the number.
   - Unit door station mode: Enter the room number to be called (for example, if the indoor station to be called is located at room 17, you need to input 17).
   - Zone station mode: The complete location information of the called device must be entered (the range is set here).

     The blue line indicates that the current position is waiting to be entered. If there are not enough digits, pad the first digit(s) with 0.

     For example: If the Room No. is 367, but the screen shows four lines, you need to pad the first digit with a 0, by pressing "0", "3", "6", and "7" in sequence.



2. Press to make a call.
3. You can talk to the indoor station when the call is answered.
4. Press to end the call.

Leave a Message

When **Visitor Message** is enabled, if the indoor door does not answer the call until the calling duration is ended, visitors can leave a message using the door station's microphone after beeps. The message can be ended when the callee presses /the call is ended by the indoor station/the message duration exceeds the upper limit set in the indoor station.

4 Call Management Center

You can call the management center on the door station's screen.

Make sure the door station has been related to the management center to be called.

1. Press to make a call.
2. You can talk to the management center when the call is answered.
3. Press to end the call.

5 Open Door by Password

Open Door by Common Password

Users can open the door by entering the password set in the indoor station during the authentication period.

To use this function, make sure the password authentication in Check Template of the door station is enabled, and the door opening password on the indoor station is configured.

Press #, room number, password, and # in turn, and the door station will automatically send a door opening signal after successful authentication.

Note: If the length of the room number is less than 4 digits, other numbers should be replaced with 0.

For example: If the room number to be opened is 17 and the password is 123456, you need to input #0017123456#.

Open Door by Super Password

The management personnel can open the door by entering the super password (set in Super Password).

Input #, super password, and # in turn, and then the door station will automatically send a door opening signal.

For example: If the super password is 123456, you need to input #123456#.

6 Open Door by Card

Users can open the door by swiping the card during the authentication period.

To use this function, make sure the Card Check Template of the door station is enabled, and the card has been bound to the door station (set in Add/Edit Person Info, up to 4 cards are allowed for each person).

Present the card on the card reading area, the door station will automatically send a door opening signal after successful authentication.

7 Local Settings

The door station's screen supports Network Setting, Super Password, General Setting, and Device Info.

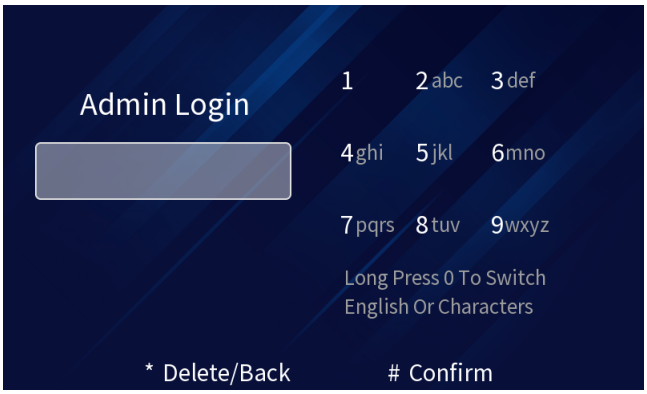
Note:

- Only admin user can log in to the local screen and configure related parameters.
- The door station's buttons allow to enter digits/letters/characters, control the moving direction, edit, save, back, etc. The button functions may vary with device screen. See the button description at the bottom of the screen for details.
- The system will automatically return to the home screen if there is no operation within 60 seconds.

7.1 Login

1. Press and hold * to enter the login screen.

Figure 7-1: Login

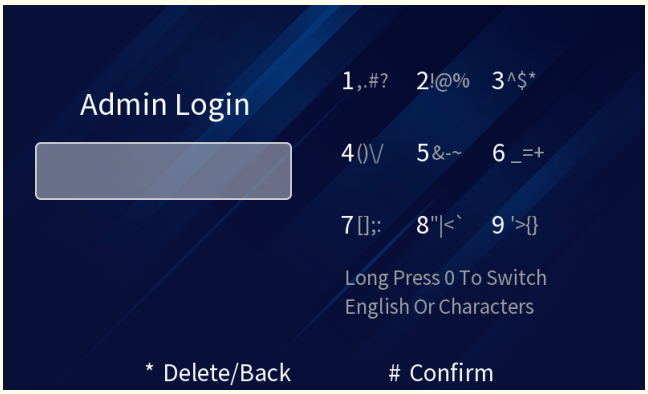


2. Enter the admin password.

Note:

- To enter digits and letters, input in the current screen.
- To enter the special characters, follow the on-screen prompts to long press 0 to switch to the special character screen (digits are also allowed).

  Figure 7-2: Digits and Special Characters



- Enter: The following takes the special character + as an example.

  (1) Press and hold 0 to enter the special character screen.

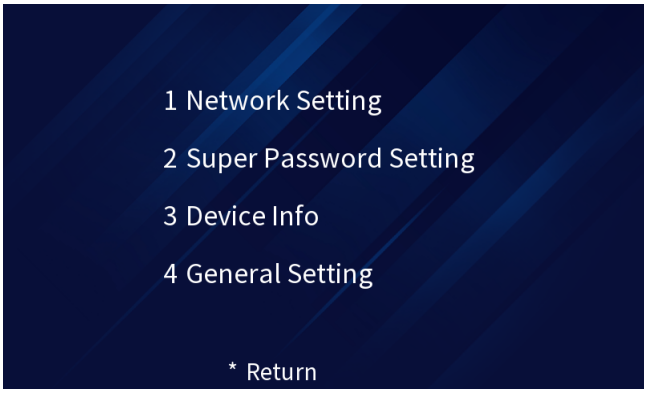
  (2) Find the position of +, which is located at the third position behind 6.

  (3) Press 6 for four times until + is shown in the left text box, and then you can enter the next character.

- Delete password: Press *.
- Return to home screen: Press * until the password is deleted, and press * once again to return to the home screen.

3. Press # to confirm the operation, and the home screen appears.

Figure 7-3: Home Screen



To open a function, press the corresponding digit button. Press * to return to the home screen.

7.2 Network Setting

Configure network parameters for the door station.

See Ethernet for detailed operations on the Web interface.

1. Press and hold * to enter the login screen. Enter the admin password, and press # to confirm.
2. Press 1, and the network settings screen appears.

Figure 7-4: Network Setting

3. Set address information of the door station.
   - Obtain Automatically (DHCP): If a DHCP (Dynamic Host Configuration Protocol) server is configured on the network, it will assign the door station an IP address automatically.

     If **Static Enable** is , it indicates that the DHCP is enabled.
   - Static IP: Set a fixed IP address manually for long term use. Enable static IP, and then set the IP address, subnet mask, and default gateway.

     (1) Press # to enable static IP, and the icon will be .

     (2) Press the buttons (2: Up, 8: Down, 4: Left, 6: Right) to determine the position to be edited. If the content area keeps flashing, it means that the content can be edited.

     (3) Press #, and the content can be edited. Enter the desired content, and press # again to complete the edit.

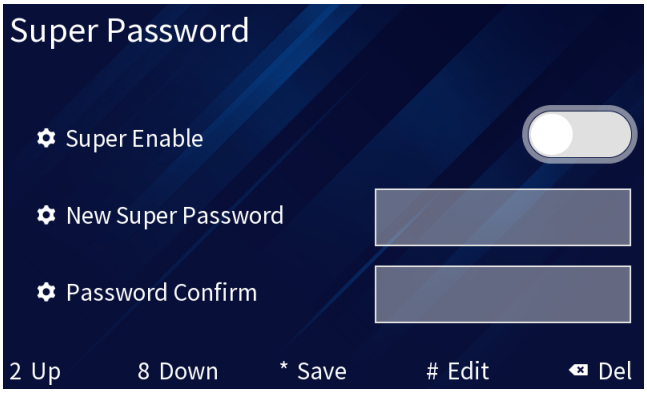
     (4) Move to other areas via the buttons, and complete other IP information configuration.
4. Press * to save the settings, and the system will automatically return to the home screen.

7.3 Super Password

The super password is suitable for management personnel (such as property, etc.), and the door can be opened directly by entering the password (see Open Door by Super Password for details).

1. Press and hold * to enter the login screen. Enter the admin password, and press # to confirm.
2. Press 2, and the **Super Password** screen appears.

Figure 7-5: Super Password



3. Press # to enable super password, and the icon will be .
4. Press 8, press #, enter the new super password (8 digits only), and press # to complete the edit.

5. Press 8, press #, enter the super password to confirm, and press # to complete the edit.
6. Press * to save the settings, and the system will automatically return to the home screen.

7.4 Device Info

Show the basic device information and view the device status in real-time, convenient for quickly access of the real-time information, improving the maintainability.

For details, see Basic Info on the Web interface.

1. Press and hold * to enter the login screen. Enter the admin password, and press # to confirm.
2. Press 3, and the **Device Info** screen appears.

   Switch the screen by pressing the direction buttons (2: page up, 8: page down). Press * to return to the home screen.

Figure 7-6: Device Info-Page 1

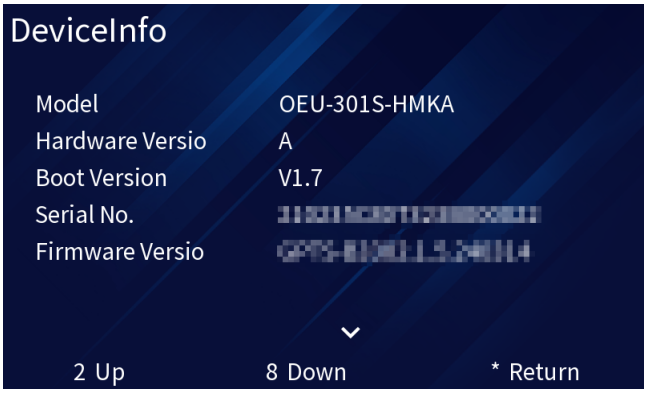
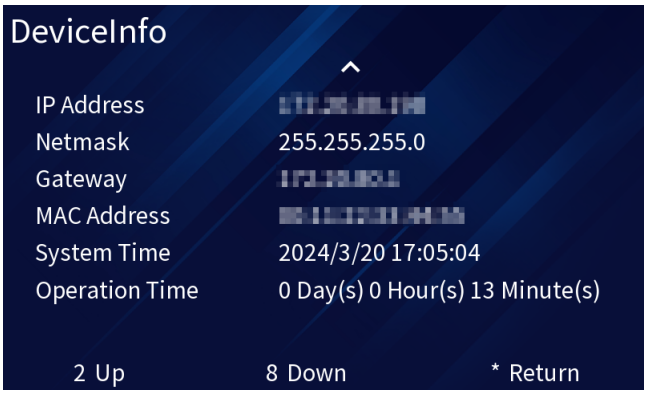


Figure 7-7: Device Info-Page 2



7.5 General Setting

Configure the volume parameters.

See Volume Control for detailed operations on the Web interface.

1. Press and hold * to enter the login screen. Enter the admin password, and press # to confirm.
2. Press 4, and press 1 to enter the **General Setting** screen.

Figure 7-8: General Setting

3. Press # to enable/disable the volume. shows the volume is enabled.
4. When enabled, adjust the volume value by pressing the digit buttons. 4: Reduce the volume, 6: Increase the volume.

   Note: The volume changes 10 for each adjustment.
5. Press * for two times to return to the home screen.

8 Web Operations

This section mainly introduces how to use the door station on the Web interface.

Note: The interface and function operations may vary with software version.

8.1 Login

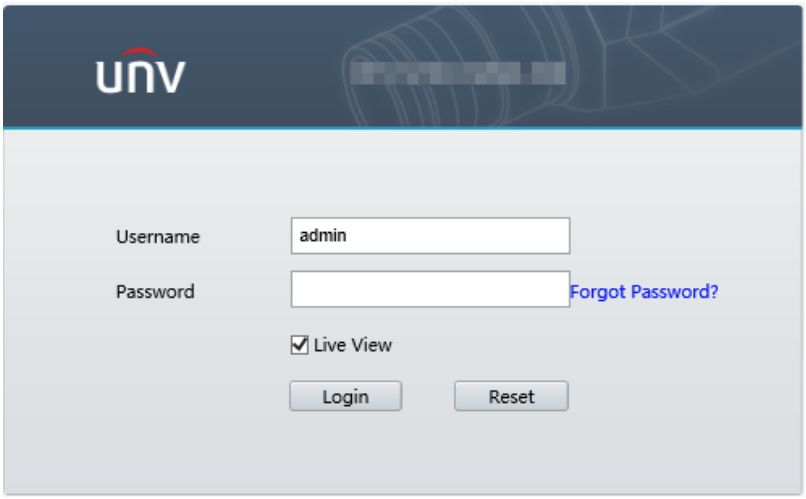
Check Before Login

- The door station runs normally.
- The client computer (hereinafter referred to as "client") is in the same network segment as the door station and is connected to the network.

Log in to Web

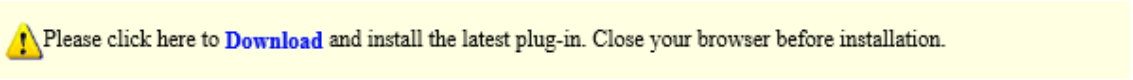
1. Open a browser (IE is recommended), enter the device's IP address (default: **192.168.1.13**) in the address bar, and press **Enter**.

   Figure 8-1: Login



2. At your first login, you need to follow the on-screen instructions to install the latest plug-in; otherwise, the live video is unavailable.

   Figure 8-2: Plug-in Installation Prompt

3. Enter the username and password (**admin**/**123456** by default).
4. Select **Live View**, and the live video will start automatically.
5. Click **Login**, and the **Live View** interface appears.
6. After the first login, the **Change Password** dialog box appears, in which you must set a strong password with 8 to 32 characters, including digits, letters, and special characters. It is recommended to enter your email address so as to receive the security code if you forgot the password (or change the password on the User interface). Then, use the new password to log in again and keep the password safe to ensure that only the authorized user can log in to the device.

Forgot Password

If you forgot your password, click **Forgot Password** and obtain the security code to reset the password.

Note: To use this function, make sure the device has an email address registered, otherwise contact the local technical support to reset the password. The email can be set at the first login, or changed on the User interface.

1. Click **Forgot Password** on the login page, and then the **Retrieve Password** interface appears.

   Figure 8-3: Retrieve Password

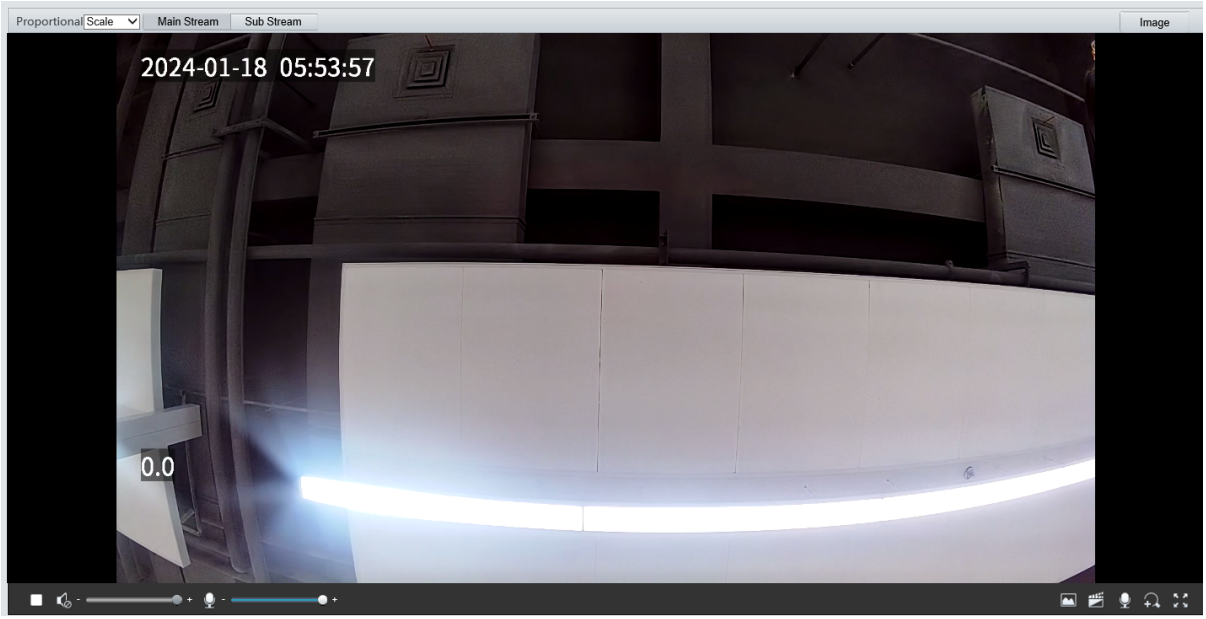
2. Obtain a security code based on the on-screen prompt.
3. Enter the security code, and click **Next** to retrieve the password. Please keep the password safe.

8.2 Live View

Play live video and audio.

After login, the **Live View** interface appears by default (the live video will play automatically when **Live View** on the **Login** page is enabled and the plug-in runs successfully).

Figure 8-4: Live View



Parameter	Description
Proportional Scale	Set the image display ratio in the window. • Scale: Displays 16:9 images. • Stretch: Displays images according to the window size (stretch images to fit the window). • Original: Displays images with original size.
Main Stream Sub Stream	Select a live video stream according to your door station.
Image	Click to enter the Image page.
25 fps 4.30 Mbps H.264 1080 x 1920 0.00%	Show the current frame rate, bit rate, video compression, resolution, and packet loss rate.
	Start/stop live view.
	Turn off/on sound.
	Adjust the output volume for the media player on the PC. Range: [0-255]. Default: 255. The greater the value, the higher the volume.
	Start/stop two-way audio between the client and the door station.
	Adjust the microphone volume on the client during audio communication between the client and the device. Range: [0-255]. Default: 255. The greater the value, the higher the volume.
	Take a snapshot from the displayed live video. **Note:** See Local Settings for the path of the saved snapshots.
	Start/stop local recording. The local recording is saved in .ts format by default. **Note:** See Local Settings for the path of the saved local recordings.
	Enable/disable digital zoom. The detailed operations are as follows. 1. Click to enable digital zoom.

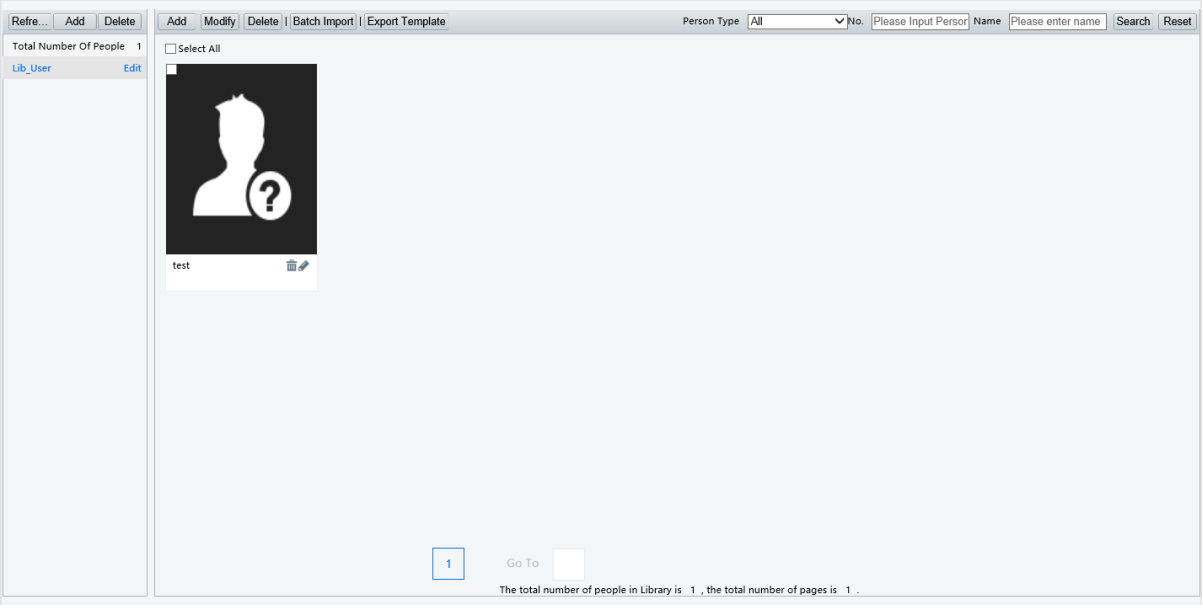
Parameter	Description
	2. Point to any desired position in the live view window, and zoom in on the area with the following two ways. • Method 1: Left click and hold on the live view window, and drag your mouse to specify the area (rectangular area) to be magnified. • Method 2: Slide the mouse wheel up to zoom in on the live view. Drag your mouse to view all the magnified area; right-click to restore to the original ratio. 3. To exit, click  .
	Full screen. • Enter full screen: Double-click the live view window or click to play it in full screen. • Exit full screen: Double-click again or press **Esc** to exit full screen.
	Click to log out from the current user.

8.3 Person Library

Users in the person libraries can pass through the door with the set authentication mode in the set time.

Enter the **Person Library** interface. The left list shows the person libraries, and the top of the list shows the total number of people in libraries.

Figure 8-5: Person Library



Add

- Add Person Library
  1. Click **Add** in the top left corner.

Figure 8-6: Add Person Library - Single-lens Door Station

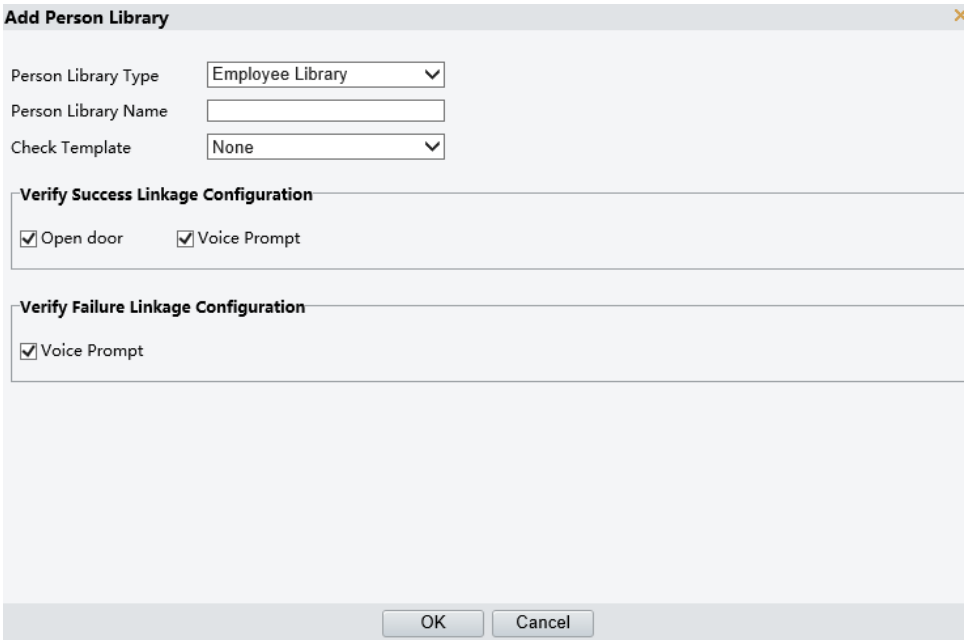
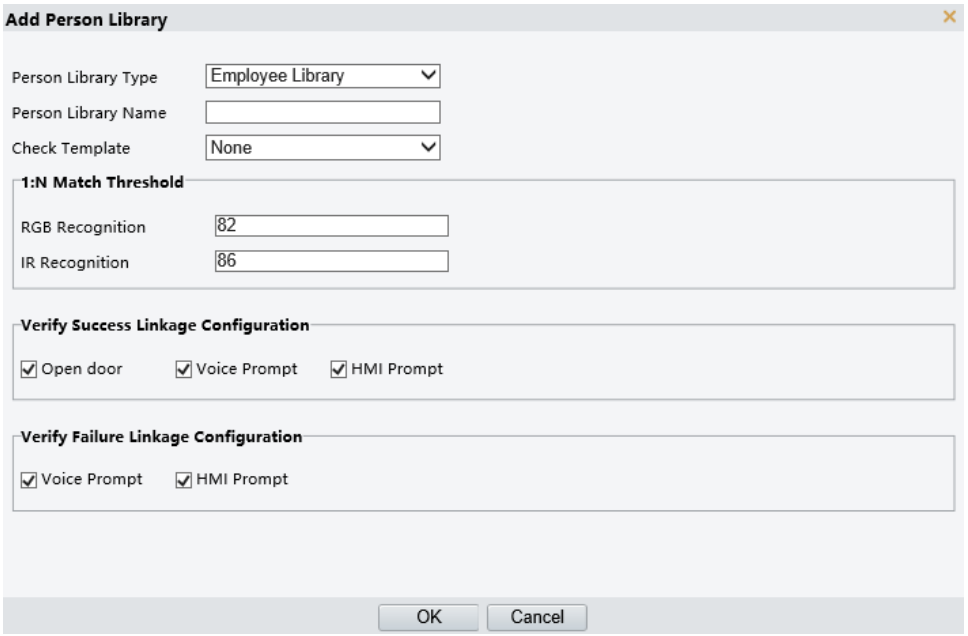


Figure 8-7: Add Person Library - Dual-lens Door Station



2. Choose a person library type.
   - Employee Library: Long-term users, such as residents, security personnel, etc.
   - Visitor Library: Temporary users, for example, visitors.
3. Enter a unique name for the library. 1 to 20 characters are allowed.
4. Choose a check template (configured in Check Template) for authentication.
5. (Only required for dual-lens door stations) Set 1:N similarity threshold. For visible light/infrared recognition, the 1:N matching similarity must be greater than or equal to the set threshold for successful matching.
6. Select the triggered actions after the authentication succeeds. **Open Door** and **Voice Prompt** are enabled by default.
7. Select the triggered actions after the authentication fails. **Voice Prompt** is enabled by default.
8. Click **OK**.

- Add Person Information: You can add persons one by one or import in batches.
  - Add One by One

1. Select the person library to which you want to add the person.
2. Click **Add** on the right.

Figure 8-8: Add Person Info - Single-lens Door Station

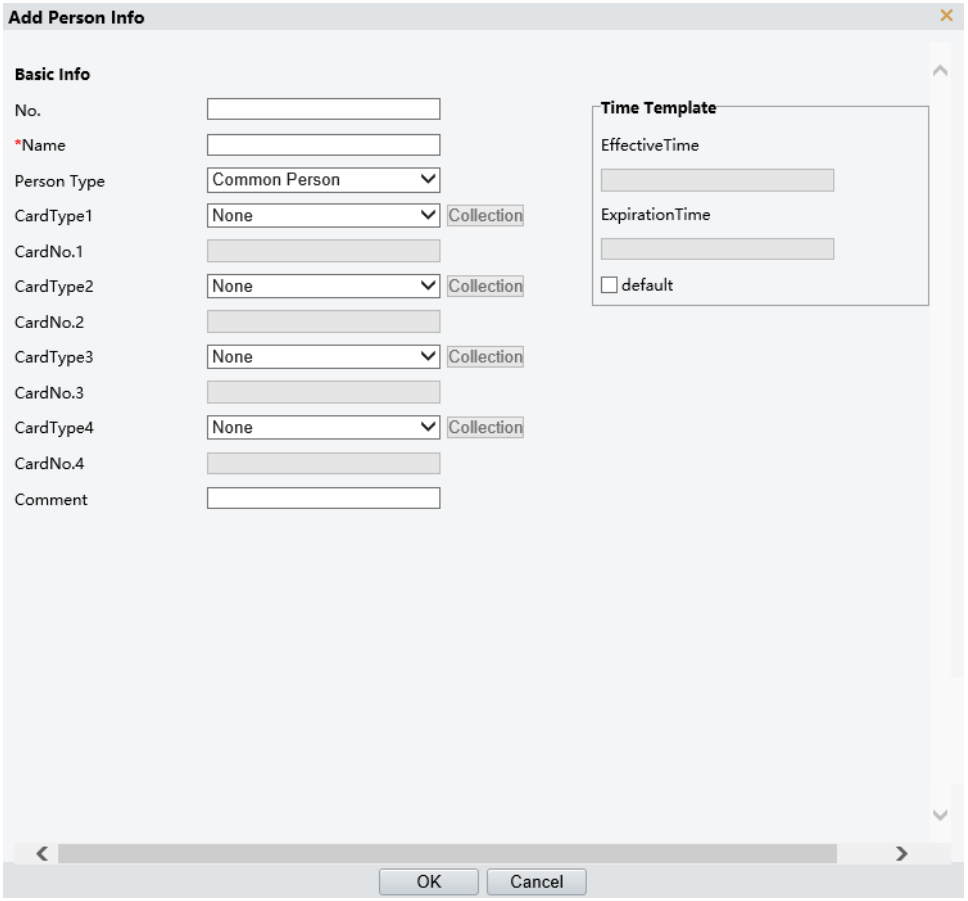
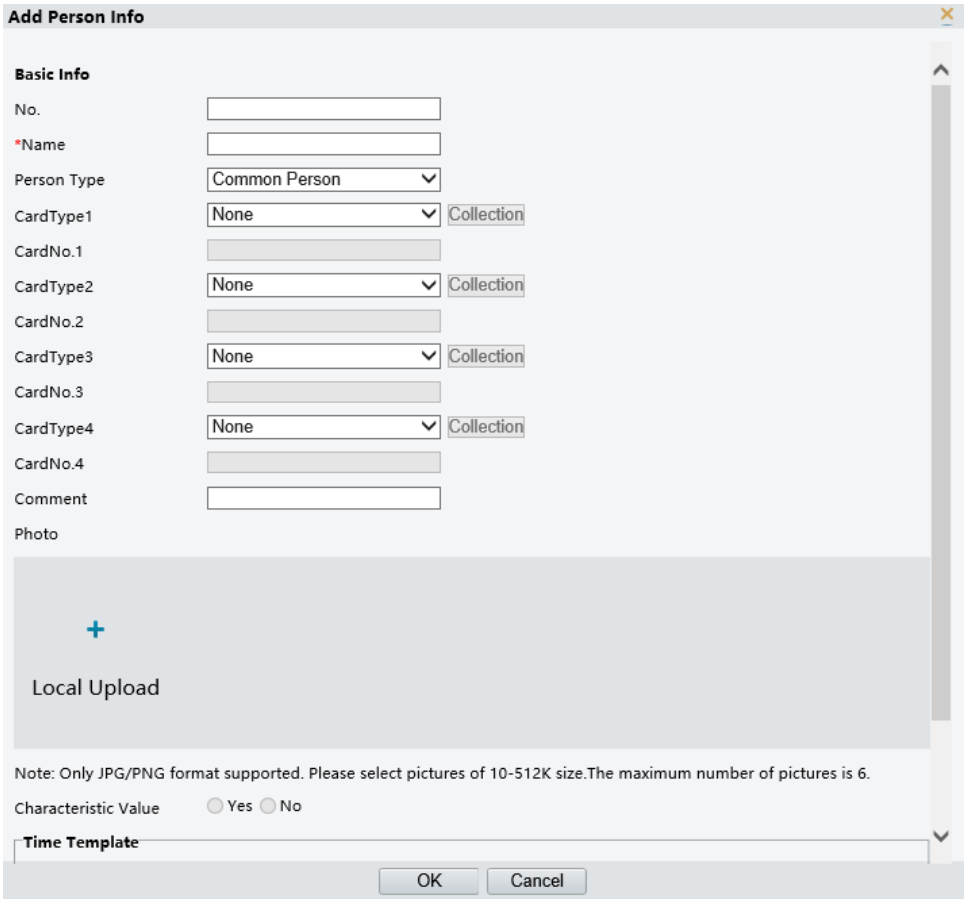


Figure 8-9: Add Person Info - Dual-lens Door Station



3. Enter the person number (0 to 15 characters including letters, digits, underscores, and hyphens), person name (1 to 20 characters), and comment (0 to 20 characters).
4. (Only required for single-lens door stations) Choose the person type, including admin and common person.
5. Set the card information. Up to four cards can be set for each person.

   (1) Set the card type to **IC Card**.

   (2) Enter the card number manually. Or click **Collection** to identify the card number automatically by a card reader connected or swiping card on the door station.
6. (Only required for dual-lens door stations) Upload photos. Up to 6 photos are supported, and each photo must be in JPG/PNG format with a size between 10-512KB.

   Feature value: After completing photo upload and saving, the feature value collection result will be displayed here when reopened. If it shows "None", you need to re-import the photos.
7. Set a specific time period for the person. It is effective permanently by default. At the same time, the time template is grayed out and cannot be set.

   (1) Select the target time template (set in Time Template). Up to 16 templates can be selected. The time template will take effective within the specified time template.

   (2) Set the effective and expiration time. Empty setting indicates the template is effective permanently.

   (3) Click **OK**, and the person can pass through the door with the authentication mode set in the person library during the verification period.

- Add in Batches: Click **Export Template**, enter the person information in the template as required, and then click **Batch Import**.

Edit

- Edit Person Library

  1. Select the person library you want to edit, and click **Edit**.

2. You can edit parameters excluding the person library type.
3. Click **OK** to save the settings.

- Edit Person

1. Click under the person you want to edit.
2. Edit the person information as needed.
3. Click **OK** to save the settings.

Delete

- Delete Person Library: Select the target person library on the left. Click **Delete**, and then click **OK** to delete it.

  Note: Deleting a person library will also delete all related person information. Please handle with caution.

- Delete Person Information: Click the corresponding under the person, or select multiple person information you want to delete and click **Delete**, and then click **OK** in the pop-up window.

8.4 Settings

8.4.1 Common

Configure commonly used functions including basic information, local settings, network, time, etc.

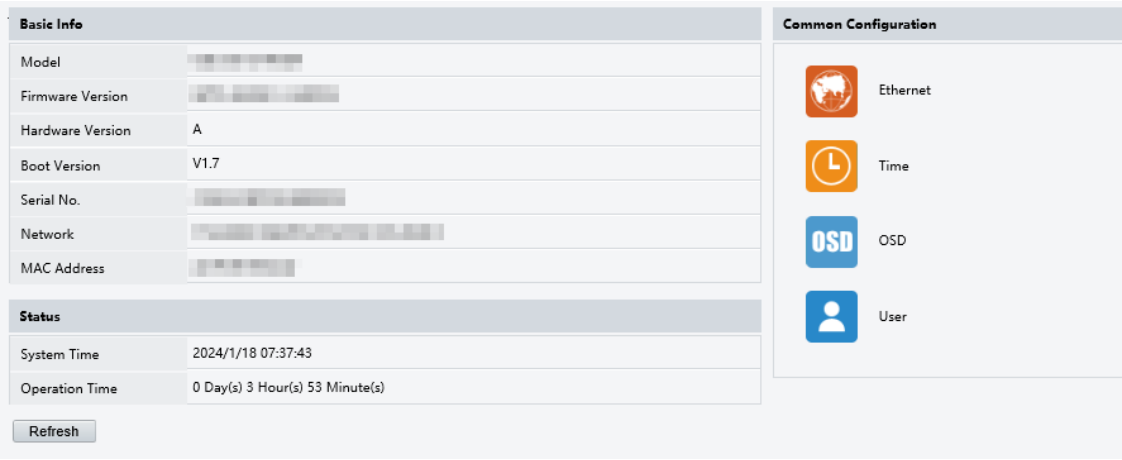
8.4.1.1 Basic Info

View the basic information and real-time operation status of the device and quickly access certain common functions.

You may also view the basic device information on the device's local screen. See Device Info for details.

Go to **Setup** > **Common** > **Basic Info**.

Figure 8-10: Basic Info



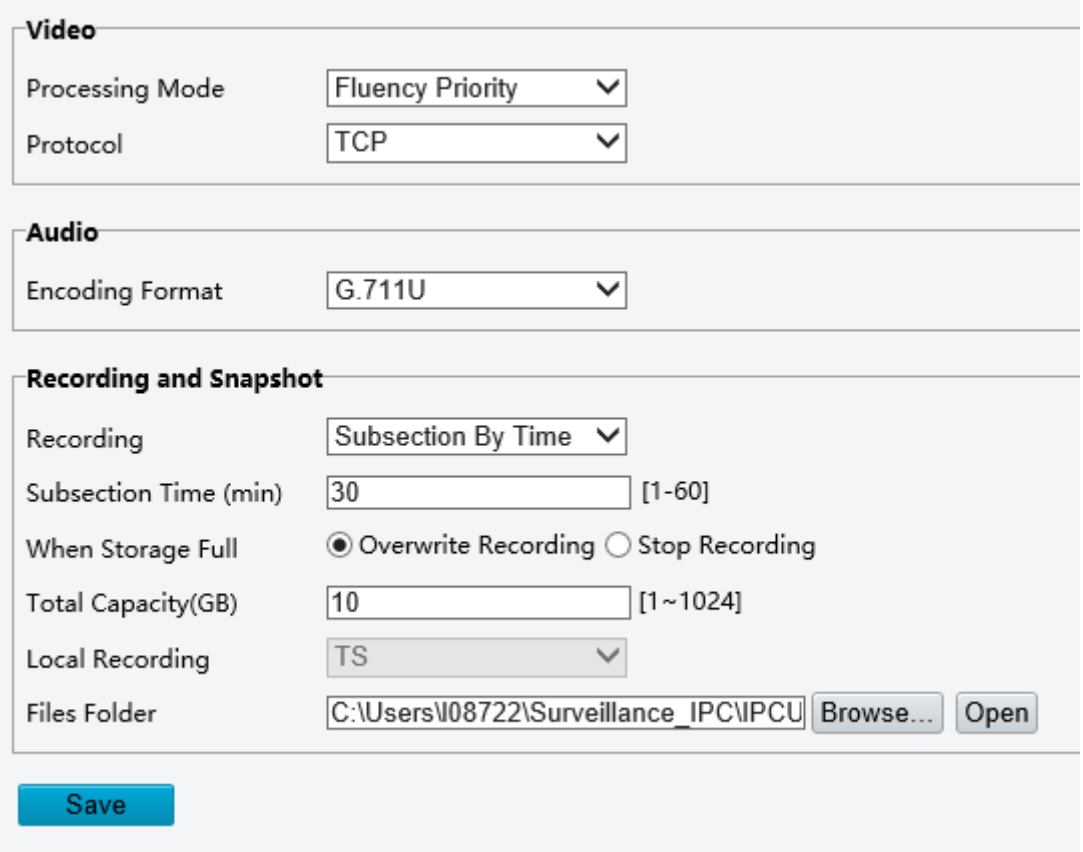
- Basic Info: View the device model, firmware version, hardware version, etc.
- Status: View the system time and device operation time. You can click **Refresh** to update the operation status.
- Common Configuration: Click the icon or text to quickly access the four common functions, including Ethernet, Time, OSD, and User.

8.4.1.2 Local Settings

Set local parameters for the PC, including video, recording and snapshot.

1. Go to **Setup** > **Common** > **Local Settings**.

Figure 8-11: Local Settings



2. Set the local parameters as needed.

Parameter		Description
Video	Processing Mode	Set the video playing mode according to the network status. • Real-Time Priority: Recommended for video playing under good network conditions. • Fluency Priority (default): Recommended for video playing with network delay. • Ultra-low Latency: Recommended for video playing under poor network conditions.
	Protocol	Set the protocol used to transmit media streams. • UDP: Supports one-to-one, one-to-many, many-to-many, and many-to-one communication methods; data can be sent without establishing a logical connection; data security and integrity cannot be guaranteed. • TCP (default): Supports one-to-one communication only; data can only be sent after a logical connection has been established between the receiver and the sender; data transmission is secure and reliable.
Audio	Encoding Format	Audio encoding format. G.711U (default): Mainstream audio encoding format, delivers clear and natural sound.
Recording and Snapshot	Recording	• Subsection By Time (default): Save recording files of the set subsection time. • Subsection By Size: Save recording files of the set subsection size.
	Subsection Time	Length of each recording file, available when **Recording** is set to **Subsection By Time**.

Parameter		Description
	(min)	Range: [1-60]. Default: 30.
	Subsection Size (MB)	Size of each recording file, available when **Recording** is set to **Subsection By Size**. Range: [10-1024]. Default: 100.
	When Storage Full	The storage policy of the new recording when the local recording capacity reaches the upper limit. • Overwrite Recording (default): When the local recording capacity is full, the oldest recordings are overwritten automatically. • Stop Recording: When the local recording capacity is full, recording stops automatically.
	Total Capacity (GB)	Allocate storage capacity for local recordings and snapshots on the PC. Range: [1-1024]. Default: 10.
	Files Folder	Set the location where snapshots and recordings are saved. By default, the snapshots are saved in .jpg or .bmp format. The recordings are saved in .ts format. • Browse: Click to set the file the storage location. • Open: Click to open the selected folder. **Note:** The maximum length of the directory is 260 bytes. If the limit is exceeded, recording or snapshot during live view will fail and a message will appear.

3. Click **Save**.

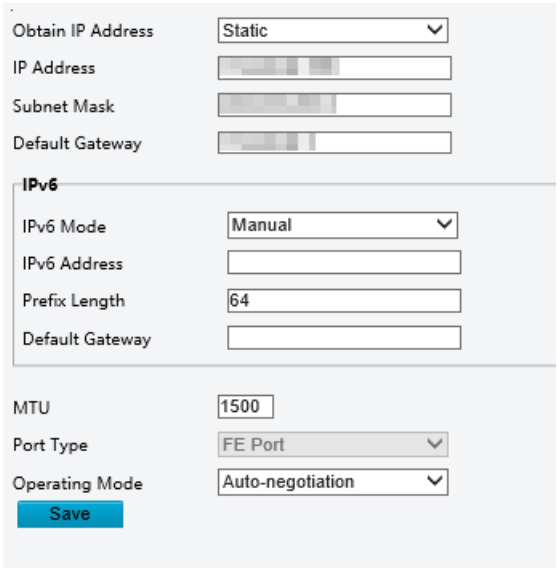
8.4.1.3 Ethernet

Configure network communication parameters for the device so it can communicate with other devices.

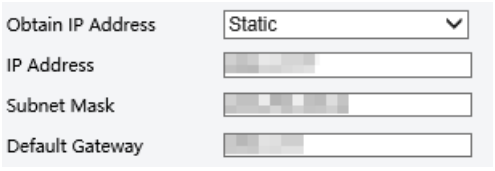
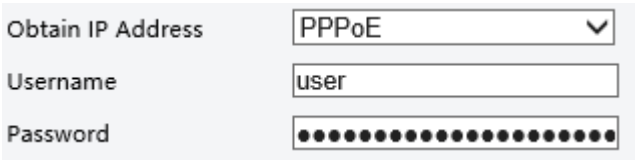
See Network Setting for network settings on the local screen.

1. Go to **Setup** > **Common** > **Ethernet**.

Figure 8-12: Network



2. Edit network parameters.

Parameter		Description
Network Info	Obtain IP Address	Three methods are available: • Static: Configure a static public network IP address for the device manually. Set **Obtain IP Address** to **Static**, and enter the IP address, subnet mask, and default gateway.  • IP Address: The long-term fixed WAN IP of the device. It must be unique in the network. • Subnet Mask/Default Gateway: The subset mask and default gateway of the device. • PPPoE: Configure PPPoE (Point to Point Protocol over Ethernet) to assign the device a dynamic IP address to establish network connection. Set **Obtain IP Address** switch to **PPPoE**, and configure the following parameters.  Username/Password: Enter the username and password provided by your ISP (Internet Service Provider). • DHCP: If a DHCP (Dynamic Host Configuration Protocol) server is deployed in the network, the device can automatically obtain an IP address from the DHCP server.
IPv6	IPv6 Mode	IPv6 has a lot more IP addresses than IPv4, and is faster and safer than IPv4 in terms of data transfer. Default: **Manual**.
	IPv6 Address	The device's IPv6 address. It must be unique.
	Prefix Length	The number of "1" after you convert the subnet mask to binary. (For example: 255.255.255.0 is converted to binary 111111111.11111111.111111111.00000000, the number of 1 is 24, so the subnet prefix length is 24).
	Default Gateway	The device's default gateway.
Other Parameters	MTU	Maximum transmission unit, the maximum packet size supported by the device in bytes. **Note:** It is available when **Obtain Address** is set to **Static** or **DHCP**. Range: [576-1500], integer only. Default: 1500. The greater the value, the higher the communication efficiency, the higher the transmission delay.
	Operating Mode	• Rate + Half Duplex: At the set rate, the port can only receive or send data at a given time, and there is a physical transmission distance limitation. • Rate + Full Duplex: At the set rate, the port can receive and send data at a given time, eliminating the physical transmission distance limitation of half duplex.

Parameter		Description
		• (Rate +) Auto-negotiation: The port automatically negotiates with the port of the peer end about the (speed and) operating mode, allowing both to run in the most efficient mode.

3. Click **Save**.

8.4.1.4 Time

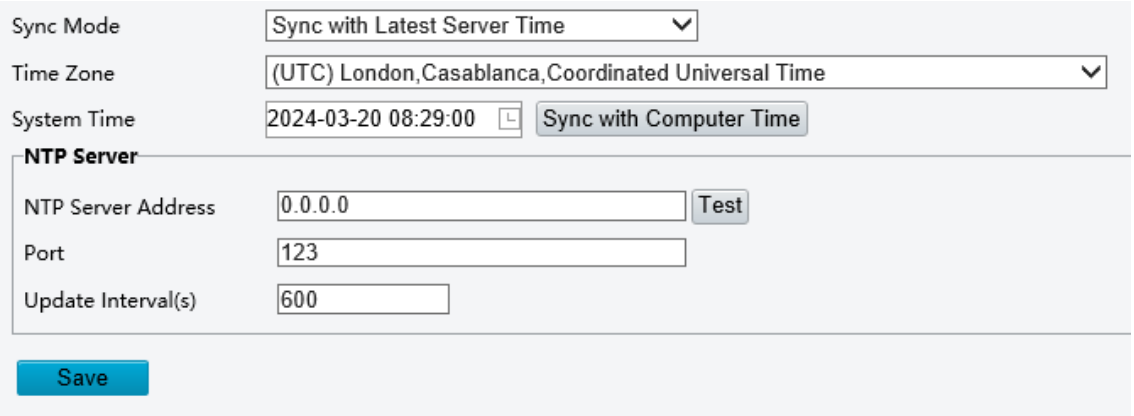
Set the device time and DST.

8.4.1.4.1 Time

Set the door station time.

1. Go to **Setup** > **Common** > **Time** > **Time**.

Figure 8-13: Time



2. You can set the device time manually or sync it with a server.

- Set manually: Set the system time as needed.

  Note: Make sure **Sync Mode** is set to **Sync with System Configuration**; otherwise, the device time will still sync with other sources after you set it manually.

- Sync time automatically:

Parameter	Description
Sync with System Configuration	The door station uses the time provided by its built-in time module.
Sync with NTP Server	NTP Server: A server used to sync time with the distributed server and client via NTP protocol. To sync the server time, you need to configure the NTP server address, port, and update interval. • NTP Server Address: Enter the NTP server address and click **Test** to check the network communication. A message will appear if the NTP is verified successfully. • Port: Range: [1-65535], default: 123. • Update Interval (s): Range: [30-3600], integer only, default: 600.

Parameter	Description
Sync with Management Server(ONVIF)	The device regularly syncs time with the management server connected via Onvif.
Sync with Latest Server Time	Default. The device regularly syncs time with all the connected servers.
Sync with Intelligent Server(LAPI)	The device regularly syncs time with the intelligent server connected via LAPI.
Sync with Computer Time	Sync time with the computer where the door station logs in.

3. Click **Save**.

8.4.1.4.2 DST

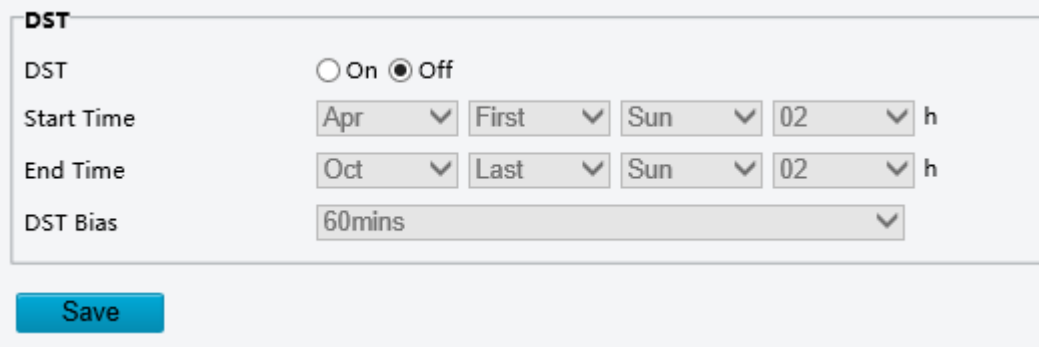
DST (Daylight Saving Time) is a local time system designed to make full use of daytime to save energy, which sets clocks forward by one hour in summer months.

By default, this function is disabled.

Note: DST rules vary in different countries.

1. Go to **Setup** > **Common** > **Time** > **DST**.

Figure 8-14: DST



2. Select **On** to enable DST.
3. Set the start time, end time, and DST bias.
4. Click **Save**.

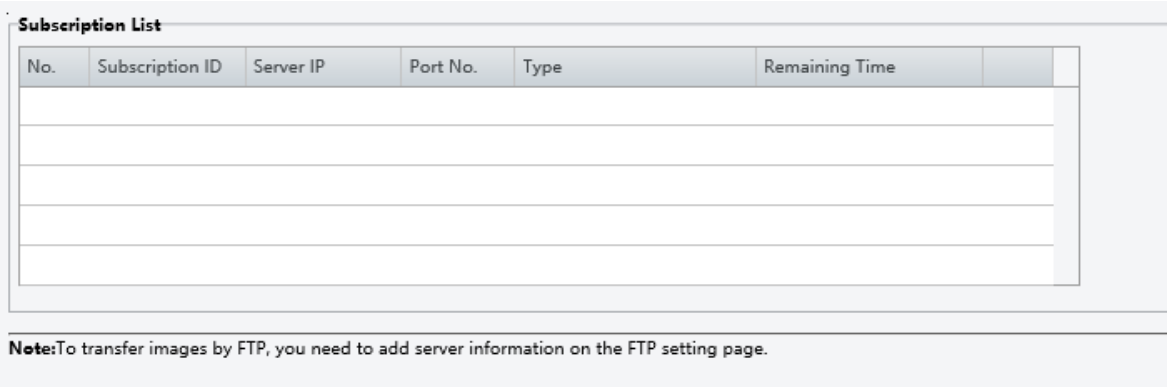
8.4.1.5 Server

8.4.1.5.1 Intelligent Server

The intelligent servers that have been connected to the door station will be displayed in the subscription list.

Go to **Setup** > **Common** > **Server** > **Intelligent Server**.

Figure 8-15: Intelligent Server



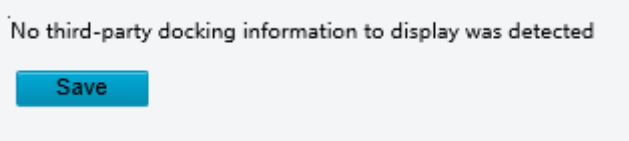
8.4.1.5.2 Third-Party Server

Third-party server refers to the connection configuration automatically detected by the built-in connection program, such as the third-party server IP, key, domain name, etc.

Go to **Setup** > **Common** > **Server** > **Third-Party Server**.

If no third-party server is detected, the page will show as follows.

Figure 8-16: Third-Party Server



8.4.1.6 OSD

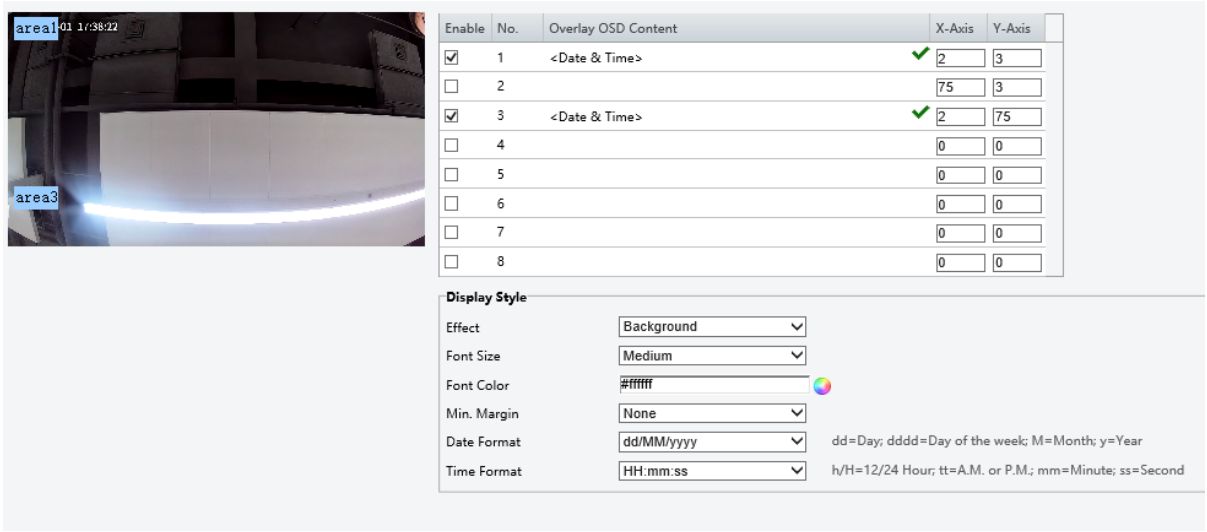
On Screen Display (OSD) are characters overlaid on Live View, including date, time, etc.

Note:

- Up to 8 OSDs are allowed.
- OSD operations supported may vary with device model.

1. Go to **Setup** > **Common** > **OSD**.

   Figure 8-17: OSD



2. To enable an OSD, select the check box in the **Enable** column to overlay the corresponding contents on the live video (OSD name format: area + OSD number, for example, area 1).
3. Set the OSD content you want to overlay.
   - Custom: 0 to 40 characters are allowed.
   - Date & Time/Time/Date/Temperature: Overlay the current date & time, time, date, or temperature.
   - Serial Port: The door station will receive and parse the serial port information in correct format and overlay the information. This function is only available to the certain model.
   - Scroll OSD: The OSD text is scrolled from right to left on the live video.

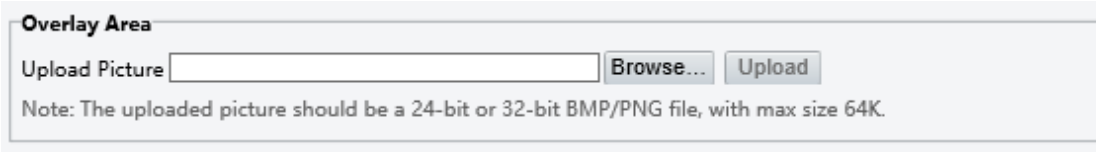
     Enter the text information you want to overlay. Up to 200 characters are allowed, and it will be only displayed in the area with the smallest number.

     Figure 8-18: ScrollOSD

- Picture Overlay: Overlay the imported picture.

  You can set the picture transparency as needed (an integer from 1 to 100 is allowed; the greater the value, the higher the transparency effect). Then, you can upload a picture with 24 or 32 bit depth, **.bmp** or **.png** format, and size of no more than 64K.

  Figure 8-19: Picture Overlay



4. Specify the exact position of the OSD by entering the X and Y coordinates. Take the top left corner of the image as the origin coordinates (0, 0), the horizontal axis is the X-axis, and the vertical axis is the Y-axis.
5. Set the OSD content style as needed.
   - Effect: **Background** by default.
   - Font Size/Font Color: **Medium**, **#ffffffff** by default.
   - Date Format/Time Format: **dd/MM/yyyy**, **HH:mm:ss** by default.
   - Min.Margin: The distance between the OSD area and the coordinate. Default: **None**.

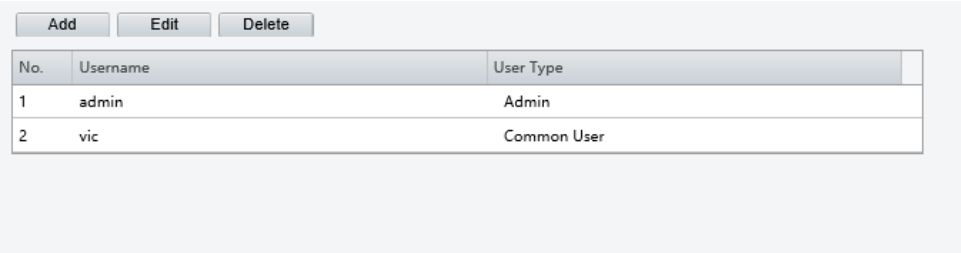
8.4.1.7 User

The system supports two user types: **Admin** and **Common User**.

- Admin: Has all permissions for managing the device and common users. Only 1 admin user is allowed. The username is admin and cannot be changed.
- Common User: Only has live view and playback permissions. Up to 32 common users are allowed.

Go to **Setup** > **Common** > **User**. On this page, you can add, delete, or edit user information.

Figure 8-20: User

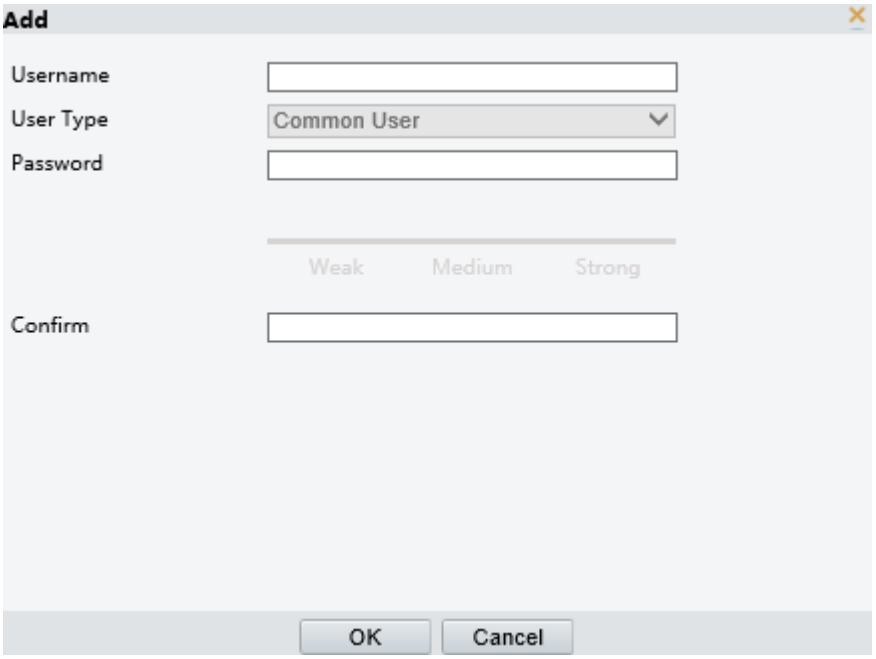


Add User

Note: Only common users can be added.

1. Log in to the Web interface with the admin account.
2. Go to **Setup** > **Common** > **User**.
3. Click **Add**.

Figure 8-21: Add User



4. Enter the username. 1 to 32 characters allowed, including letters(A-Z, a-z), digits(0-9), underscores(_), hyphens(-), dots(.), and plus signs(+).
5. Enter the password. 8 to 32 characters, including digits, letters, and special characters.
6. Click **OK**.

Edit User

1. Log in to the Web interface with the admin account.
2. Go to **Setup** > **Common** > **User**.
3. Select the user you want to edit, and click **Edit**.
4. Enter the admin password, new password and then confirm it by entering again.
5. (Only for admin) Change the registered email address, which is used to reset the password in case you forget it.
6. Click **OK**.

Delete User

Note: The admin user cannot be deleted. The vic user cannot be deleted as it is used for video intercom on the door station with other devices.

1. Log in to the Web interface with the admin account.
2. Go to **Setup** > **Common** > **User**.
3. Select the user you want to delete, and click **Delete**.
4. Click **OK** to confirm the deletion.

8.4.1.8 Ports & Devices

8.4.1.8.1 Wiegand Interface

Wiegand interfaces can be used to connect card readers.

1. Go to **Setup** > **Common** > **Ports & Devices** > **Wiegand Interface**.

Figure 8-22: Wiegand Interface

2. Select the interface type, including Wiegand input (for card reader), and Wiegand output.
3. Select the protocol.
   - Wiegand 26: Reads 3-byte card numbers.
   - Wiegand 34: Reads 4-byte card numbers.
   - None: Disable Wiegand.
4. Select the format. The card number read by our card readers is in ascending order. Two options are available:
   - Ascending Order (default): Used when the sequence of card number read by the external card reader is the same as the sequence of card number read by our card readers.
   - Descending Order: Used when the sequence of card number read by the external card reader is opposite to the sequence of card number read by our card readers.
5. Click **Save**.

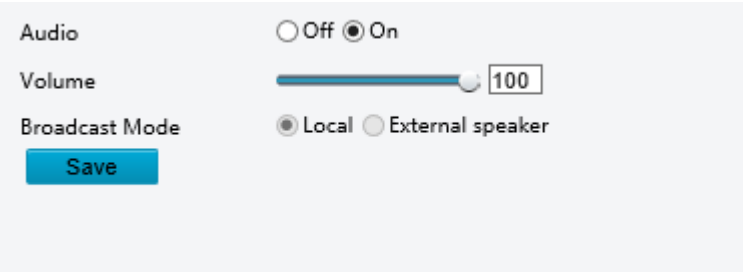
8.4.1.8.2 Volume Control

Configure the volume the door station.

You may also configure the volume on the local interface. See General Setting for details.

1. Go to **Setup** > **Common** > **Ports & Devices** > **Volume Control**.

   Figure 8-23: Volume Control



2. Select whether to turn audio off. When audio is turned on (default), you can adjust the volume.

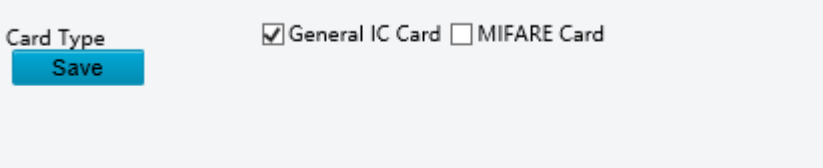
   Range: [0-100], integer only. Default: 100.
3. Select the broadcast mode. By default, the audio is broadcast from the local device. It can be broadcast from the external speaker.
4. Click **Save**.

8.4.1.8.3 Card Reader

The built-in card reader of the device supports card authentication.

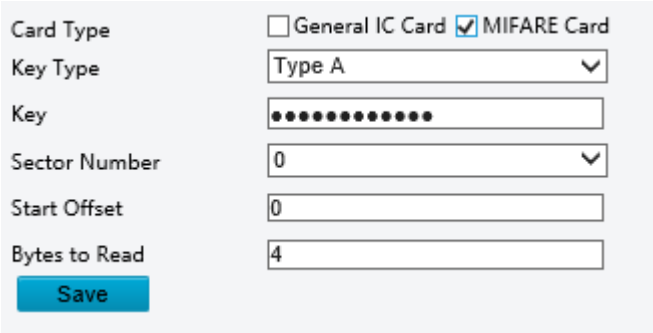
1. Go to **Setup** > **Common** > **Ports & Devices** > **Card Reader**.

Figure 8-24: Card Reader



2. Select a card type. IC card and MIFARE card cannot be used together.
   - General IC Card: The device can read general IC cards.
   - MIFARE Card: Inductive smart IC cards.

     Figure 8-25: MIFARE Card

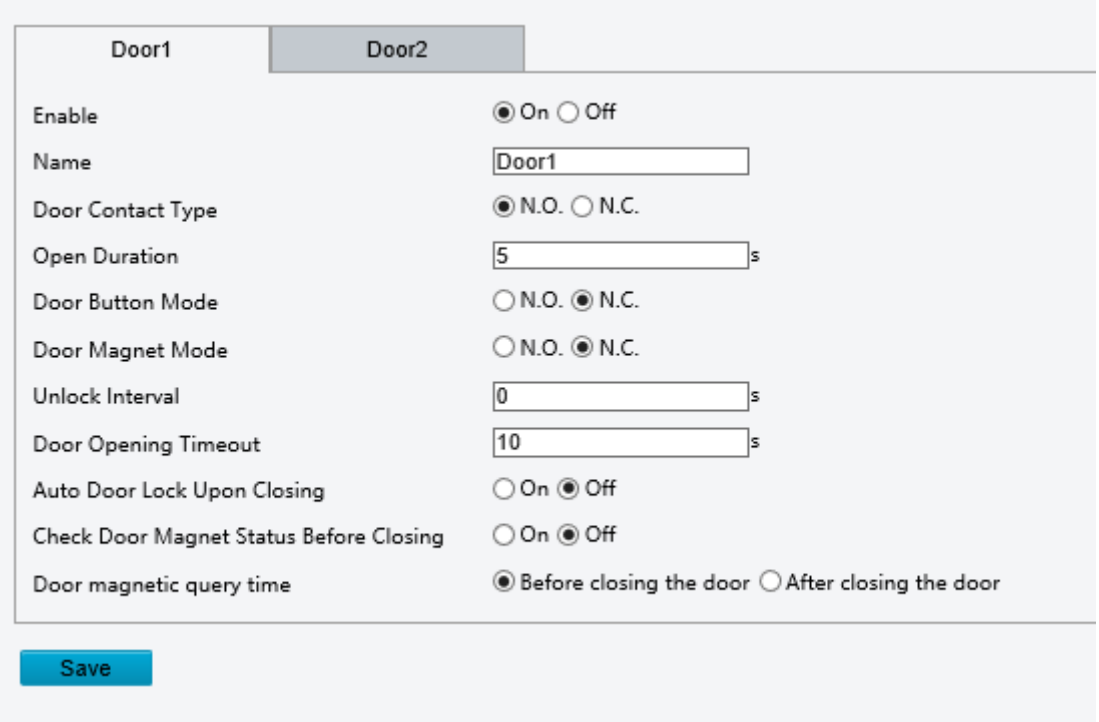
     - Key Type: **Type A** by default.
     - Key: Enter the password of the MIFARE card.
     - Sector Number: The storage space of MIFARE card is divided into 16 sectors from 0-15. Please select the sector number according to the actual situation. Default: 0.
     - Start Offset: Enter the sector offset of the MIFARE card to be read. Range: [0-7], integer only. Default: 0.
     - Bytes to Read: Enter the sector length of the MIFARE card to be read. Range: [1-8], integer only. Default: 4.
3. Click **Save**.

8.4.1.8.4 Door Configuration

Configure the door that is physically connected to the door station.

1. Go to **Setup** > **Common** > **Ports & Devices** > **Door Configuration**.

Figure 8-26: Door Configuration



2. Enable **Door1**.
3. Configure door parameters.
   - Name: **Door 1** by default. It can be named as needed, and must be unique.
   - Door Contact Type: Set it to **N.O.**, otherwise this function cannot be used.
   - Door Button Mode: **N.C.** by default.
   - Door Magnet Mode: **N.C.** by default.
   - Unlock Interval (s): The time interval between two unlocks. After the door lock is opened, it can only be opened again after the set time.

     If it is set to 0, the door lock opens every time it receives an opening signal.

     Range: [0-300], integer only. Default: 0.
   - Door Opening Timeout (s): The door lock automatically locks when the closing time exceeds the set time and the door magnet detects that the door is closed in place.

     Range: [1-300], integer only. Default: 10.

     Note:
     - To use this function, enable **Auto Door Lock Upon Closing** first.
     - Set an appropriate value according to the actual situation, otherwise a short timeout may affect door opening.
   - Auto Door Lock Upon Closing
     - On: The door lock automatically locks when the door closing time exceeds the set **Door Opening Timeout** and the door magnet detects that the door is closed in place.
     - Off: The door lock locks after the set pulse width.
   - Check Door Magnet Status Before Closing: Check if the door has the door magnet.
   - Door Magnetic Query Time: For the door with door magnet, set **Door Magnetic Query Time** to **Before closing the door** or **After closing the door** based on the actual door lock type. If the door magnet is closed, it means that the door is locked.

     Note: To use this function, enable **Check Door Magnet Status Before Closing** first.

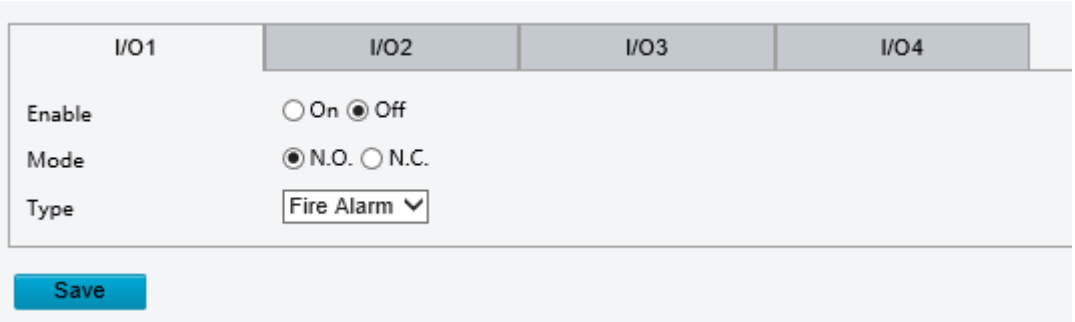
4. To enable the second door, click the **Door2** tab, enable **Door2**, and configure other parameters as the above description.
5. Click **Save**.

8.4.1.8.5 I/O Input

Configure the fire alarm input devices that are physically connected to the door station.

1. Go to **Setup** > **Common** > **Ports & Devices** > **I/O Input**.

   Figure 8-27: I/O Input



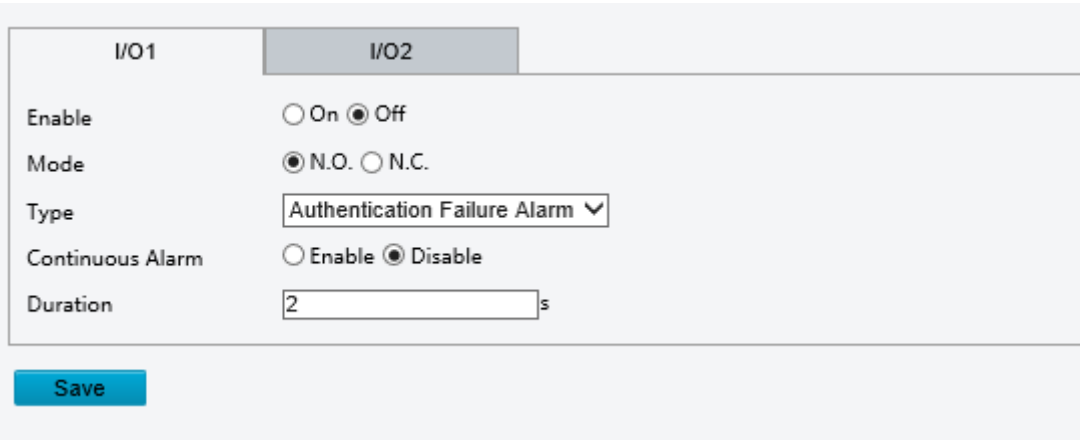
2. Enable **I/O1**.
3. Set the mode to **N.O.**, otherwise the door station cannot receive the input signal. A door station can connect 4 fire alarm input devices at the same time. To set the other three I/O inputs, follow the steps above.
4. Click **Save**.

8.4.1.8.6 I/O Output

Configure the fire alarm output devices that are physically connected to the door station.

1. Go to **Setup** > **Common** > **Ports & Devices** > **I/O Output**.

   Figure 8-28: I/O Output



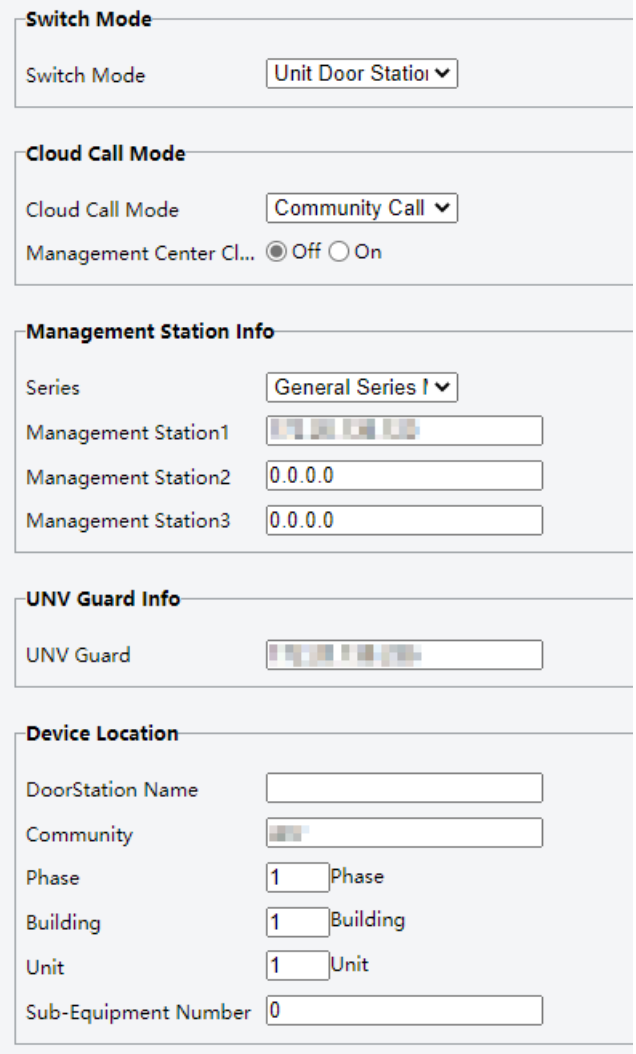
2. Enable **I/O1**.
3. Set the mode to **N.O.**, otherwise the door station cannot output the signal.
4. Enable **Continuous Alarm**.
5. Configure the output duration (s). Range: [0-200], integer only. Default: 2.
6. A door station can connect 2 fire alarm output devices at the same time. To set the other three I/O outputs, follow the steps above.
7. Click **Save**.

8.4.1.9 Intercom Config

Configure call protocol, management station information, and device location.

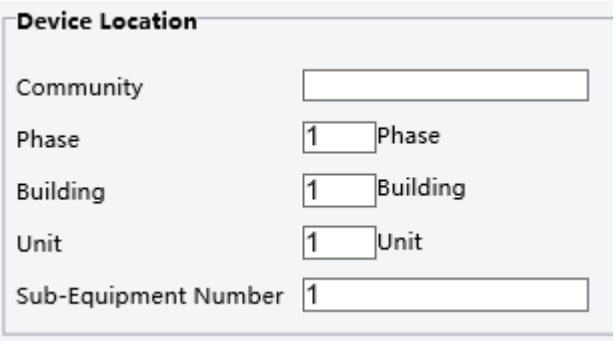
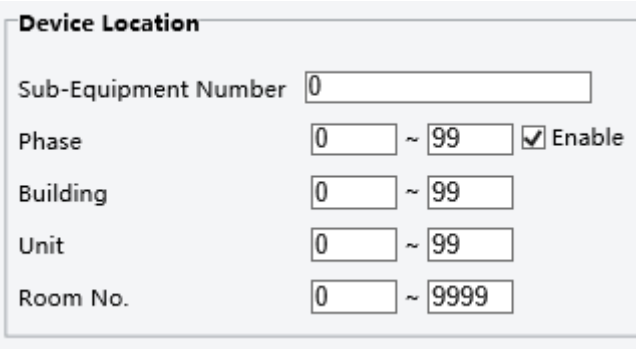
1. Go to **Setup** > **Common** > **Intercom Config**.

Figure 8-29: Intercom Config



2. Set the parameters.

Parameter		Description
Switch Mode		The mode applies when an indoor station is configured, and the device can work with an indoor station to achieve functions such as calling, opening door by password, and video intercom.
Cloud Call Mode	The device generates a call alarm when it detects an anomaly.	
	Community Call	Reports alarms to the bound management stations and community indoor stations.
	Community Cloud Calling	Reports alarms to the bound mobile app.
Main Station	Series	Use the default.
	Main Station 1/2/3	One door station can be bound to a maximum of three main stations. Fill in the main station's IP address here.
UNV Guard Info		If UNV Guard device is a management station, bind the door station on the UNV Guard first, and then the IP address of the UNV Guard will be displayed on the door station screen.
Device Location	Door Station Mode	It should be consistent with the location of the indoor station and management station to be bound.

Parameter		Description
		
	Zone Station Mode	Set the maximum callable range. Select **Enable** to display this item on the device screen; otherwise, it will not be displayed. 

3. Click **Save**. A success message means the settings are saved.

8.4.2 Network Config

8.4.2.1 Network

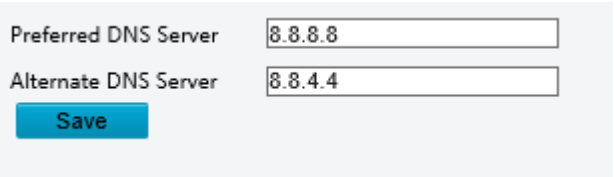
See Ethernet for details.

8.4.2.2 DNS

The DNS server can automatically translate the domain name address into IP address so as to access the door station.

1. Go to **Setup** > **Network** > **DNS**.
2. The default DNS server addresses are shown below.

Figure 8-30: DNS



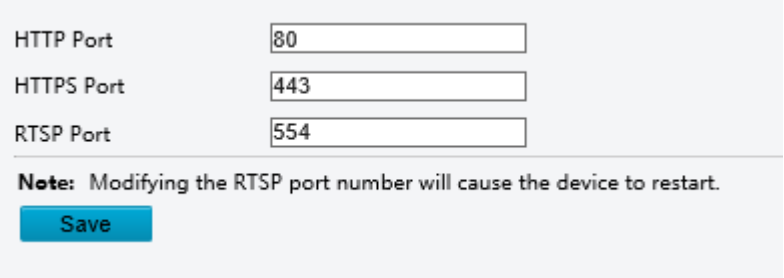
3. Click **Save**.

8.4.2.3 Port

8.4.2.3.1 Port

1. Go to **Setup** > **Network** > **Port** > **Port**.

Figure 8-31: Port



2. You can use the defaults or customize them in case of port conflicts.

Note: If the HTTP port number you entered has been used, a message "Port conflicts. Please try again." will appear. 23, 81, 82, 85, 3260, and 49152 have been assigned for other purposes and cannot be used. In addition to the above port numbers, the system can also dynamically detect other port numbers that are already in use.

- HTTP/HTTPS Port: If you change the HTTP/HTTPS port number, then you need to add the new port number after the IP address when logging in. For example, if the HTTP port number is set to 88, you need to use http://192.168.1.13:88 to log in to the device.
- RTSP Port: Real-Time Streaming Protocol port, enter an available port number.

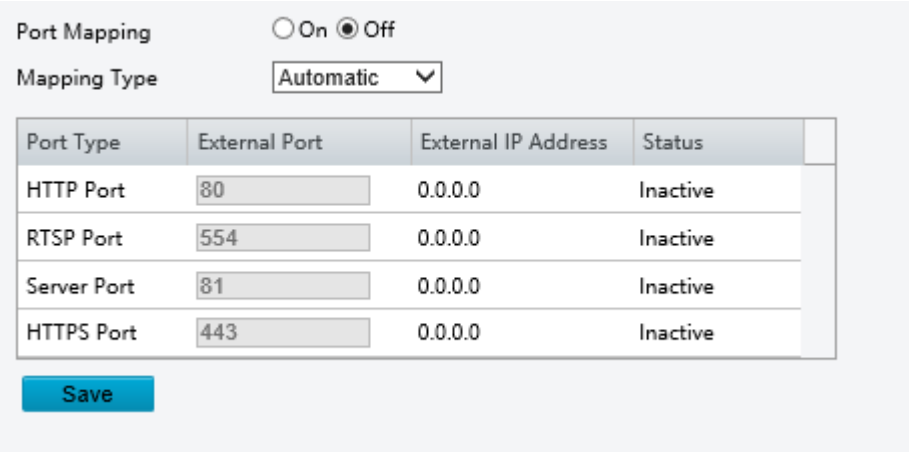
3. Click **Save**.

8.4.2.3.2 Port Mapping

Configure port mapping so computers on the WAN can access the device on the LAN.

1. Go to **Setup** > **Network** > **Port** > **Port Mapping**.

Figure 8-32: Port Mapping



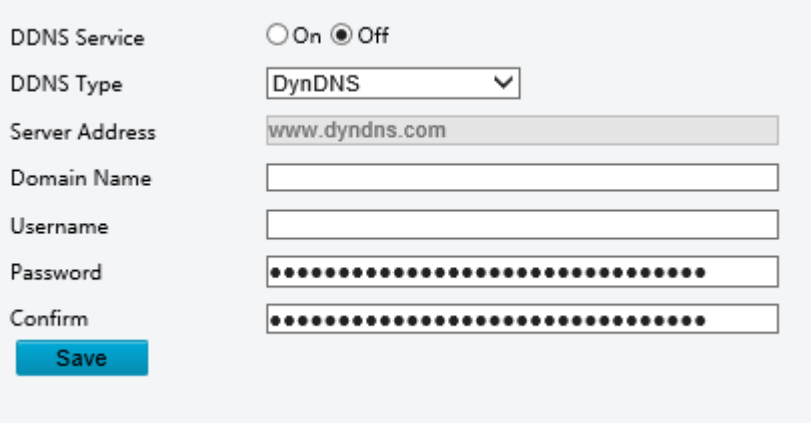
2. Enable **Port Mapping**.
3. Set the mapping type.
   - Automatic: The external port numbers and external IP address are assigned automatically.
   - Manual: The external port numbers need to be set manually.
4. Click **Save**.

8.4.2.4 DDNS

DDNS (Dynamic Domain Name Server) can map the dynamic IP address of the device to a fixed domain name, which is designed to help other devices on the public network access the network with the fixed domain name. With DDNS, users can access the private network device for remote control with the public IP address.

1. Go to **Setup** > **Network** > **DDNS**.
2. Enable **DDNS Service**.

Figure 8-33: DDNS



3. Select the DDNS type.
   - DynDNS/No-IP: Enter the domain name, username, and password, and confirm the password.
     - Domain name: Domain name assigned by your DDNS service provider, for example, www.dyndns.com.
     - Username and password: The corresponding username/password for your DDNS account.
   - EZDDNS: Enter a domain name for your device (4 to 63 characters are allowed, including letters, digits, underscores, and hyphens).

     Click **Test** to check if the domain name is available.
4. Click **Save**.

8.4.2.5 EZCloud

You can add the device to the cloud app/website to remotely access the door station and view the live video.

To use the function, add the door station to EZCloud with or without a cloud account.

Go to **Setup** > **Network** > **EZCloud**. EZCloud is enabled by default.

Figure 8-34: EZCloud

Add Device on EZCloud Website

1. Enable **EZCloud**.
2. Enter **ezcloud.uniview.com** in the address bar of a web browser, and then the login page of the EZCloud website appears.
3. Click **Sign Up**, follow the on-screen instructions to create an account, and the log in to the EZCloud.
4. Go to **Device Management** > **My Cloud Devices**, and click **Add**.

Parameter	Description
Device Name	Enter the door station name.

Parameter	Description
Register Code	Enter the register code.
Organization	Select an organization for your device. By default, the root organization is selected. You may add or delete organizations in **Organization Management** > **My Cloud Organizations**.

5. Click **OK**.
6. Click **Save**.
7. Check device status.
   - EZCloud website: Go to **Device Management** > **My Cloud Devices** to check whether the device is online.
   - Device's Web interface: Go to **Setup** > **Network** > **EZCloud** to check whether the device is online.

Device Status

When the device is online, clicking **Logout** can delete the device from cloud.

Add Device on UniEase/UNV Guard

- You can download the UniEase app to your phone on the app store. Follow the on-screen instructions to create an account and log in to the app. Add the door station to the app, and then the functions are available including viewing live video, visual intercom, remote door opening, receiving alarm message, adding personnel, syncing card number, etc.
- Visit the Uniview official website to download the UNV Guard software to your PC. Follow the on-screen instructions to create an account and log in to the software, and the functions are available including adding personnel, adding and binding devices, assigning permissions, etc.

See the corresponding user manual for details.

Add Device on EZTools Software

Visit the Uniview official website to download the EZTools software to your PC.

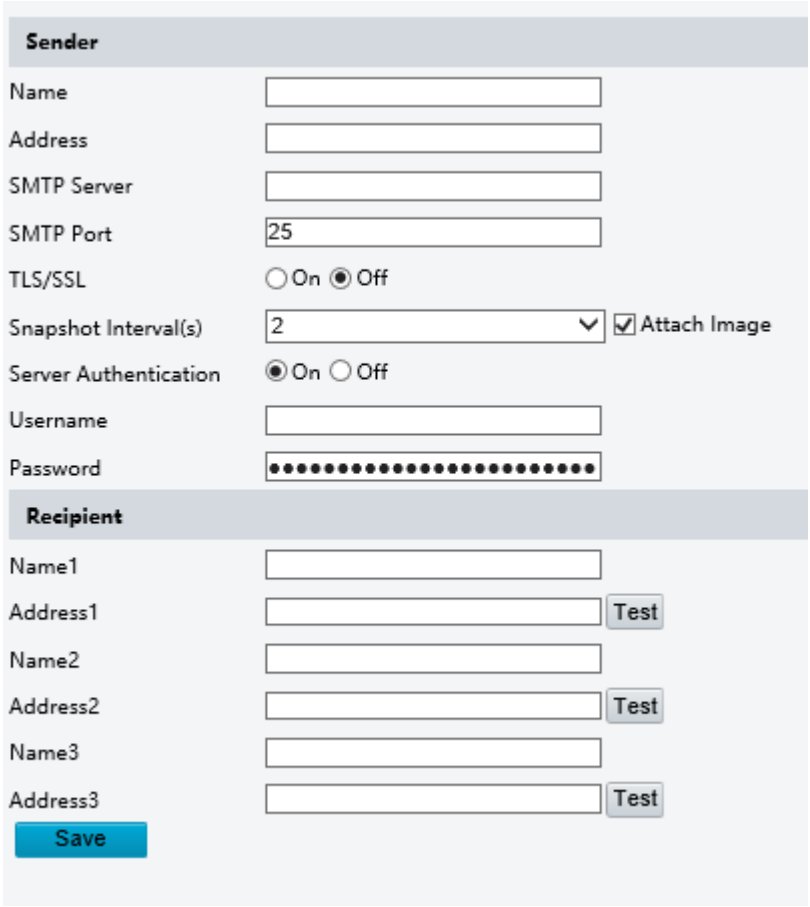
On the software, you can add the door station, edit the device password, view network information, log in to the door station’s Web interface, etc. See the corresponding user manual for details,

8.4.2.6 E-mail

Configure E-mail so the specified email address can receive the alarm messages from the door station.

1. Go to **Setup** > **Network** > **E-mail**.

Figure 8-35: E-mail



2. Set the sender and recipient information.

Parameter		Description
Sender	Sender Name	Enter the sender name, which is generally the name of the door station.
	Sender Address	Enter the IP address of the door station.
	SMTP Server/SMTP Port	Enter the IP address and port number of the SMTP server of the sender's e-mail. Taking Gmail and QQ mailbox as examples, the SMTP server address can be obtained from the help center. The default SMTP port number is 25.
	TLS/SSL	Enable **TLS/SSL**, and then emails will be encrypted by TLS or SSL to ensure data security and integrity. **Note:** If SMTP supports TLS/SSL, it tries SSL first to establish a secure connection for email sending.
	Snapshot Interval(s)	Choose a snapshot interval: 2s, 3s, 4s, or 5s. **Note:** The interval for taking snapshots attached to alarm e-mails is subject to the settings on the **E-mail** page.
	Attach Image	When enabled, the door station will automatically send an alarm e-mail with 3 attached snapshots taken at set intervals in the event of an alarm.
	Server Authentication	Enable **Server Authentication** to secure e-mail transmission security and verify the reliability of the accessed website.
	Username/Password	Enter the username and password of SMTP server. **Note:** The email only shows the sender name not the username.

Parameter		Description
Recipient	Recipient Name/ Address	(1) Enter the e-mail name and address to receive e-mails. (2) After recipient configuration, you can click **Test** to test the email sending function.

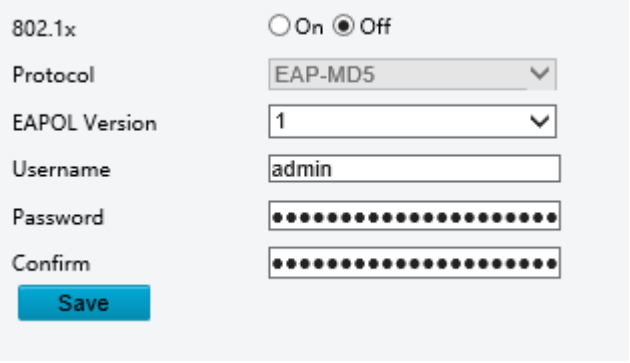
3. Click **Save**.

8.4.2.7 802.1x

The 802.1x protocol is an access control protocol for a device to access the network. In situations with high security requirements, 802.1x authentication is necessary when the device is connected to the network. Only successfully authenticated devices are allowed to access the LAN, so as to ensure network security and realize normal communication.

1. Go to **Setup** > **Network** > **802.1x**.

Figure 8-36: 802.1x



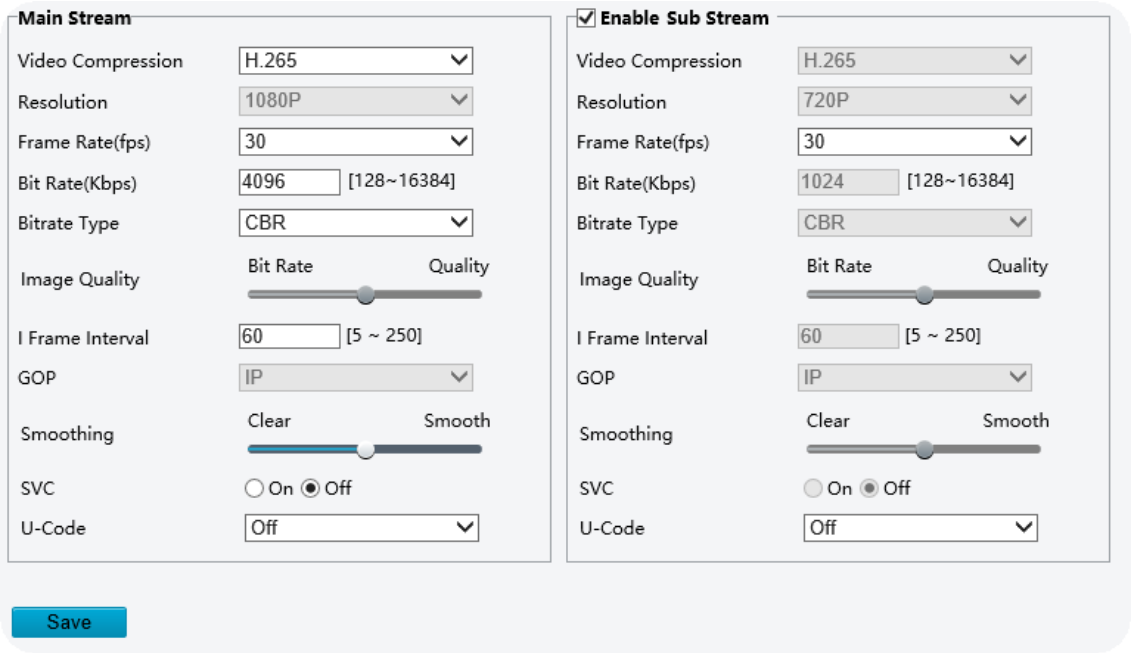
2. Enable **802.1x**.
3. Select the EAPOL version (Extensible Authentication Protocol over LAN) as needed.
4. Enter the username and password, and enter the password again to confirm.
5. Click **Save**.

8.4.3 Video & Audio

8.4.3.1 Video

1. Go to **Setup** > **Video & Audio** > **Video**.

Figure 8-37: Video



2. Set the main stream parameters.

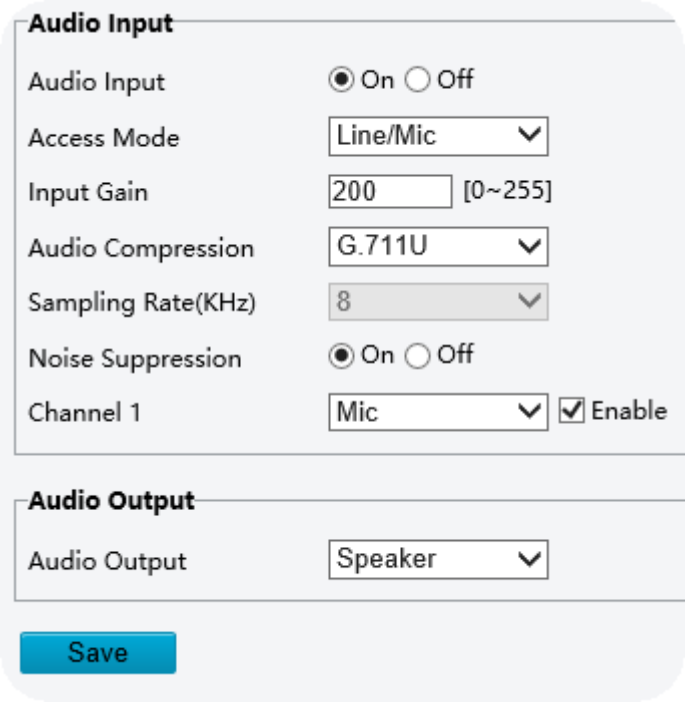
Parameter	Description
Video Compression	When H.265 or H.264 is selected, image quality is not available.
Frame Rate(fps)	The number of frames per second. Choose a frame rate from the drop-down list. **Note:** To ensure image quality, the frame rate shall not be greater than the reciprocal of the shutter speed.
Bitrate Type	• CBR: The device keeps a specific bit rate by varying the quality of video streams. • VBR: The device keeps the quality of video streams as constant as possible by varying the bit rate.
Image Quality	Adjust the image quality by dragging the slider. It is configurable when **Bitrate Type** is set to **VBR**. The closer the slider is to **Quality**, the higher the bit rate, and the higher the image quality. The closer the slider is to **Bit Rate**, the lower the bit rate, and the image quality will be affected.
I Frame Interval	The number of frames between two adjacent I frames. A shorter interval presents better image quality but consumes more bandwidth and storage. It is recommended to use the default value.
Smoothing	Set the smoothness of the video stream. Drag the slider to choose whether smoothness or clarity takes precedence. **Note:** Smoothing is recommended for fluent video in a poor network environment.
SVC	SVC (Scalable Video Coding) enables a video stream to be broken into multiple layers of resolution, quality and frame rate, reducing bandwidth consumption without compromising the image quality.
U-Code	• Basic Mode: The bit rate is reduced by about 25%. • Advanced Mode: The bit rate is reduced by about 50%.

3. The sub stream is enabled by default. To disable it, unselect the **Enable Sub Stream** check box.
4. Click **Save**.

8.4.3.2 Audio

1. Go to **Setup** > **Video & Audio** > **Audio**.

   Figure 8-38: Audio



2. Set the audio parameters.

Parameter	Description
Audio Input	Click **On** to enable audio input. **Note:** If the audio is not required, click **Off** to improve device performance.
Noise Suppression	It can reduce noises to improve audio output quality. This function is enabled by default.
Channel 1	**Mic** by default. Select the **Enable** checkbox to enable audio input for the channel 1.

3. Click **Save**.

8.4.4 Image

8.4.4.1 Image

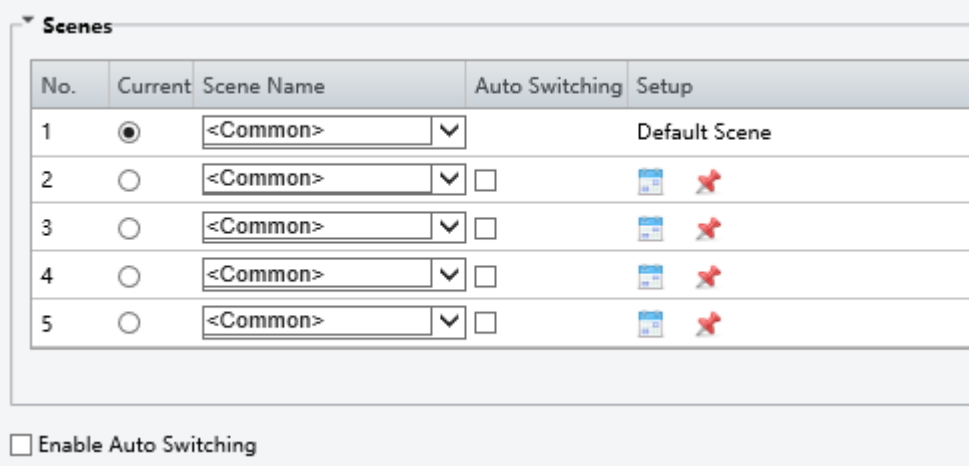
The function supported may vary with device model.

8.4.4.1.1 Scenes

Set image parameters to achieve the desired image effects for different scenes.

1. Go to **Setup** > **Image** > **Image**, and click **Scenes**.

Figure 8-39: Scenes



2. Select a scene and set the parameters. Some parameters are described in the table below.

Parameter	Description
Current	Select the scene you want to use. **Note:** • After a scene mode is selected, image parameters are automatically switched. • If auto switching is enabled, the device switches scenes automatically based on the set schedule.
Scene Name	Select the scene mode. The device provides several predefined scene modes for different scenarios. After a scene mode is selected, image parameters are automatically switched (you can also adjust the parameters as needed). • Common: Recommended for outdoor scenes. • Indoor: Recommended for indoor scenes. • QR code: Suitable for QR code scanning. • WDR: Recommended for scenes with high-contrast lighting, such as window, corridor, front door or other scenes that are bright outside but dim inside. • Custom: Set a scene as needed.
Auto Switching	Select whether to add the scene to the auto-switching list (including the default scene). When enabled, if the time is within the set schedule, the device will automatically switch to the scene. **Note:** • Set the auto-switching schedule. The device will switch scenes automatically according to the set time periods. See the specific operations in the below. • Select **Enable Auto Switching**, and the configured parameters will take effect.
Configuration	• Click to set the time period for automatic scene switching. The time periods in the same scene cannot overlap. If both the start time and end time are 0, the settings do not take effect. • Click to set the current scene as the default scene.
Enable Auto Switching	• When enabled, if the current time is within a specified time period, the device automatically switches to the corresponding scene of the specified period; if the current time is not within any of the specified periods, the device uses the default scene.

Parameter	Description
	Note: • If multiple non-default scenes meet the switching condition at the same time, the device will switch to the scene with the smallest number (starting from 1 to 5). • All the scene parameters cannot be configured. • When disabled, the device uses the currently selected scene.

8.4.4.1.2 Image Enhancement

1. Go to **Setup** > **Image** > **Image**, and then click **Image Enhancement**.

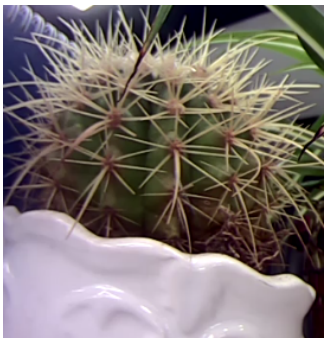
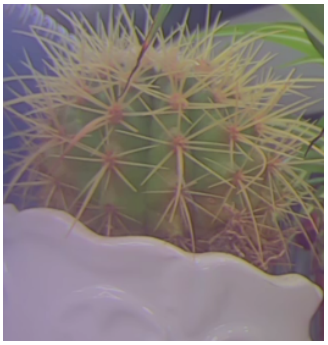
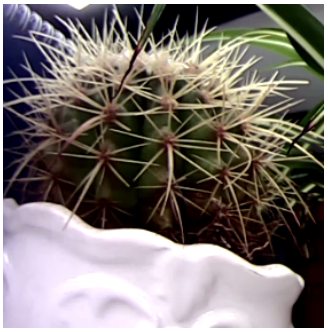
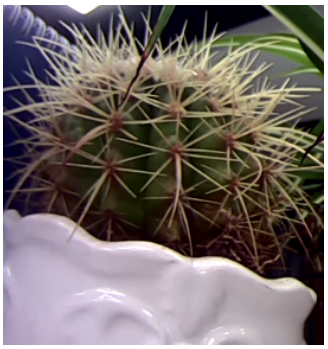
Figure 8-40: Image Enhancement

2. Set the image enhancement parameters.

Note:

- The valid range is 0 to 225. The default is 128.
- To restore the default settings, click **Default**.

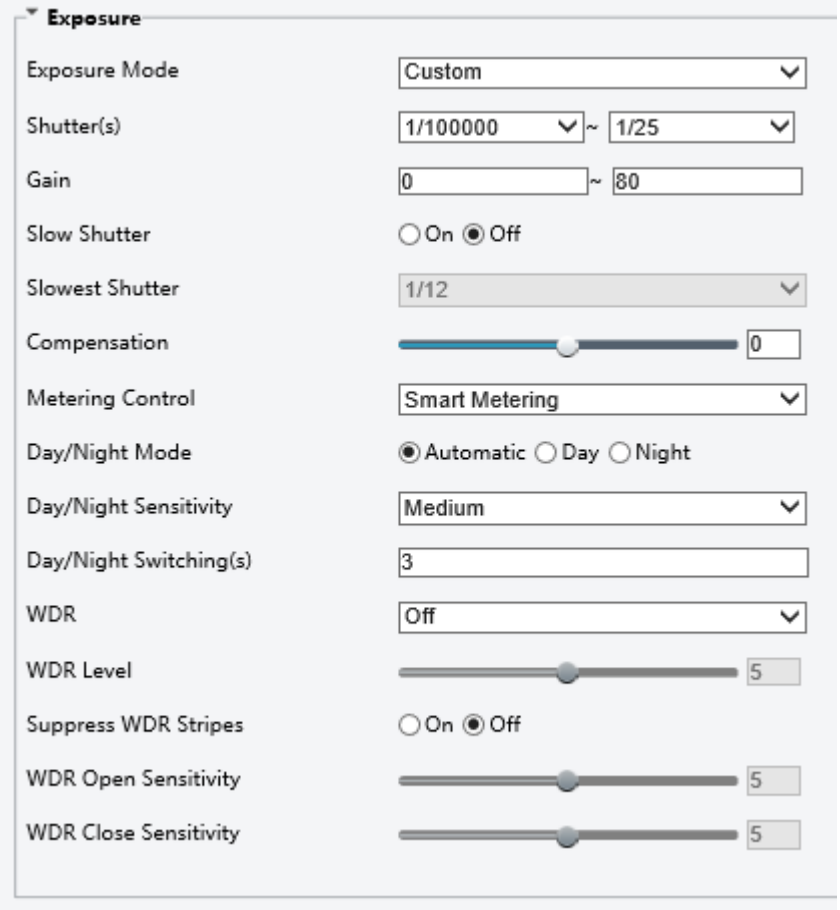
Parameter	Description
Brightness	The overall lightness or darkness of the image.  Low brightness  High brightness
Saturation	The intensity or vividness of colors in the image.

Parameter	Description
	 Low saturation  High saturation
Contrast	The black-to-white ratio in the image, that is, the gradient of color from black to white.
	 Low contrast  High contrast
Sharpness	The definition of edges in the image.
	 Low sharpness  High sharpness
2D Noise Reduction	Reduce noise by individually analyzing each frame, which may cause image blur.
3D Noise Reduction	Reduce noise by analyzing the difference between successive frames, which may cause image smearing or ghosting.

8.4.4.1.3 Exposure

1. Go to **Setup** > **Image** > **Image**, and then click **Exposure**.

Figure 8-41: Exposure



2. Set the exposure parameters.

Note: To restore the default settings, click **Default**.

Parameter	Description
Exposure Mode	Select the exposure mode from the drop-down list to achieve the desired exposure effect. • Automatic: The door station automatically adjusts the exposure parameters based on the environment. • Custom: User can set exposure parameters as needed. • Indoor 50Hz/60Hz: Reduce stripes by limiting shutter frequency. **Note:** • Stripe effect: The high-contrast condition in an image caused by uneven light energy received by the sensor. • Using this mode in brighter environments aids in adjusting the stripe effect in the image with linear stripe suppression. • Manual: Fine-tune image quality by setting shutter and gain manually.
Shutter(s)	Shutter is used to control the light that comes into the door station's lens. A fast shutter speed is ideal for scenes in quick motion. A slow shutter speed is ideal for scenes that change slowly. The default range is 1/100000 to 1/25.

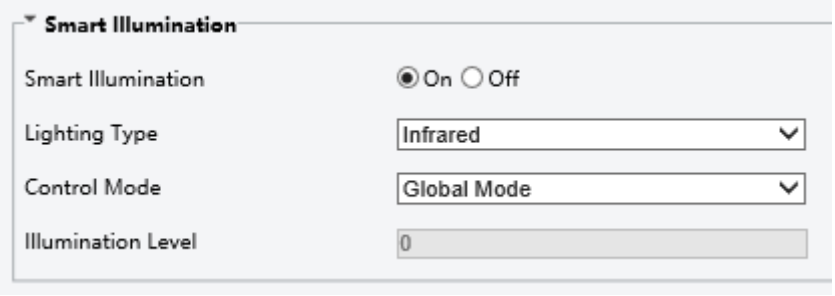
Parameter	Description
	Note: • This parameter is configurable when **Exposure Mode** is set to **Manual**. The minimum and maximum time can be configurable when **Exposure Mode** is set to **Custom**. • If **Slow Shutter** is disabled, the reciprocal of the shutter speed must be greater than the frame rate.
Gain	Control image signals so that the device can output standard video signals in different light conditions. The valid range is 0 to 100. The default is 0 to 80. **Note:** This parameter is configurable when **Exposure Mode** is set to **Manual** or **Custom**. The minimum and maximum gain value can be configurable when **Exposure Mode** is set to **Custom**.
Slow Shutter	When enabled, the device can improve image brightness in low light conditions.
Slowest Shutter	Set the slowest shutter speed for exposure. Default: 1/12.
Compensation	Adjust the compensation value as required to achieve the desired image effect. The valid range is -100 to 100. The default is 0. **Note:** This parameter is configurable when **Exposure Mode** is not set to **Manual**.
Metering Control	Set how the door station measures the intensity of light. • Center-Weighted Average Metering: Measure light mainly in the central part of the image. • Evaluative Metering: The device measures light mainly in the central part of the image. • Smart Metering: The device obtains an accurate exposure by weighting according to the exposure and importance of each area on the whole image. **Note:** This parameter is configurable when **Exposure Mode** is not set to **Manual**.
Day/Night Mode	• Automatic: The device automatically switches between day mode and night mode according to the ambient lighting condition to output optimum images. • Day: The device outputs high-quality images in daylight conditions. • Night: The device outputs high-quality images in low-light conditions.
Day/Night Sensitivity	Light threshold for switching between day mode and night mode when **Day/Night Mode** is **Automatic**. A higher sensitivity value means that the device is more sensitive to the change of light and is therefore more easily to switch between day mode and night mode.
Day/Night Switching(s)	When **Day/Night Mode** is **Automatic**, set the length of time before the device switches between day mode and night mode after the switching conditions are met.
WDR	Suitable for high-contract scenes. WDR can balance the brightness in the bright area and dark area, and provide clear image with more details. • On/Off: User needs to identify WDR scenes, and manually enable or disable WDR as needed.

Parameter	Description
	• Automatic: The door station can automatically identify typical WDR scenes, and then enable or disable WDR. **Note:** This parameter is configurable when **Exposure Mode** is set to **Automatic**, **Custom**, **Indoor 50Hz**, or **Indoor 60Hz**.
WDR Level	When WDR is enabled, you can adjust the WDR level to improve image quality. The valid range is 1 to 9. The default is 5. **Note:** In the case of low contrast, it is recommended to disable WDR or use level 1 to 6. Level 7 or higher is recommended if there is a high contrast between the bright and dark areas in the scene.
Suppress WDR Stripes	When enabled, the door station automatically adjusts the slow shutter frequency according to the light frequency to minimize stripes in the image.
WDR Sensitivity	When **WDR** is set to **Automatic**, adjust the parameter to change the WDR switching sensitivity. The valid range is 1 to 9. The default is 5.

8.4.4.1.4 Smart Illumination

Go to **Setup** > **Image** > **Image**, and then click **Smart Illumination**.

Figure 8-42: Smart Illumination



Note: To restore the default settings, click **Default**.

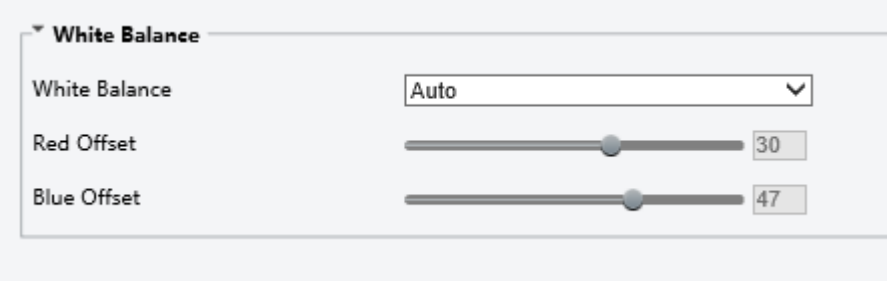
- Lighting Type: Uses the infrared light illumination.
- Control Mode: Uses the global mode. The device automatically adjusts illumination and exposure to achieve the balanced image effect.

8.4.4.1.5 White Balance

Adjust red gain and blue gain of the entire image under different color temperatures so as to output images that best suit human eyes.

1. Go to **Setup** > **Image** > **Image**, and then click **White Balance**.

   Figure 8-43: White Balance

2. Set the white balance parameters.

   Note: To restore the default settings, click **Default**.

Parameter	Description
White Balance	• Auto/Auto 2: Automatically adjust the red and blue gains according to the lighting conditions. If there are still color casts in **Auto** mode, try **Auto 2** mode. • Outdoor: Recommended for outdoor scenes where the color temperature varies widely. • Fine Tune: Allows user to manually adjust red and blue offsets. • Fine Tune (Base on night mode): Allows user to red and blue offsets manually to adapt to poor lighting conditions. • Sodium Lamp: Automatically adjust the red and blue gains for optimal color reproduction in sodium light sources. • Locked: Keep the current color temperature.
Red Offset	When **White Balance** is set to **Fine Tune**, adjust the red offset manually by dragging the slider or enter the number.
Blue Offset	When **White Balance** is set to **Fine Tune**, adjust the blue offset manually by dragging the slider or enter the number.

8.4.4.2 OSD

See OSD for details.

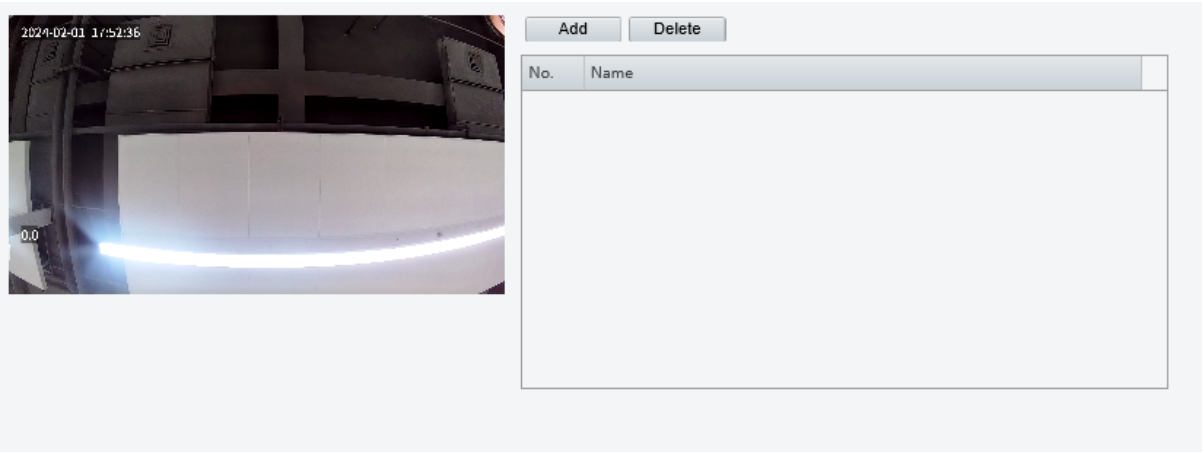
8.4.4.3 Privacy Mask

Cover certain areas on the image for privacy.

Note: Up to 8 privacy areas are allowed, and their names are respectively Mask 1, Mask 2, Mask 3, Mask 4, Mask 5, Mask 6, Mask 7, and Mask 8.

Go to **Setup** > **Image** > **Privacy Mask**.

Figure 8-44: Privacy Mask



Add

1. Click **Add**, and then a rectangle mask appears on the left image.
2. Set the privacy area.
   (1) Double-click the image on the left to play it in full screen.
   (2) Select a privacy mask, and set the size of the mask as the following two ways.
   - Drag the rectangle to the desired position, point to a handle of the mask and drag to resize it.
   - Long press the left mouse button and drag it to draw a privacy mask.

   (3) Double-click the image again or press **Esc** to exit full screen.
3. (Optional) To add multiple privacy areas, please follow the steps above.

Delete

To delete a privacy mask, select the mask from the right list, and then click **Delete**.

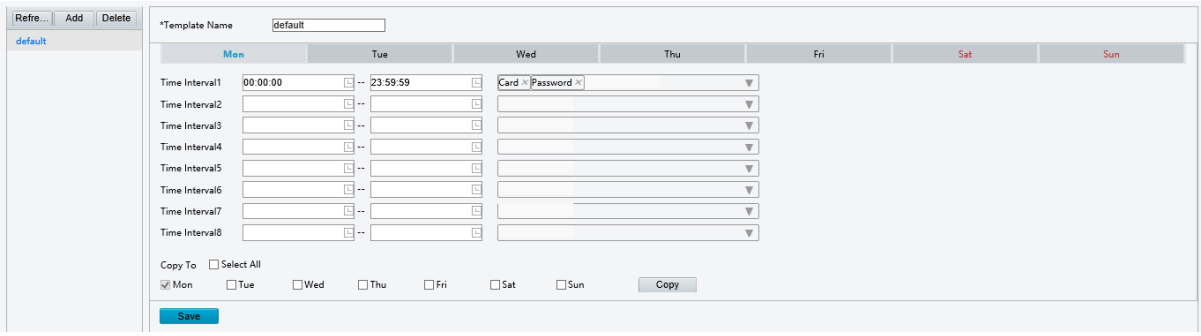
8.4.5 Smart

8.4.5.1 Check Template

Set authentication modes for different time periods in a week for different scenarios.

Go to **Setup** > **Intelligent** > **Check Template**.

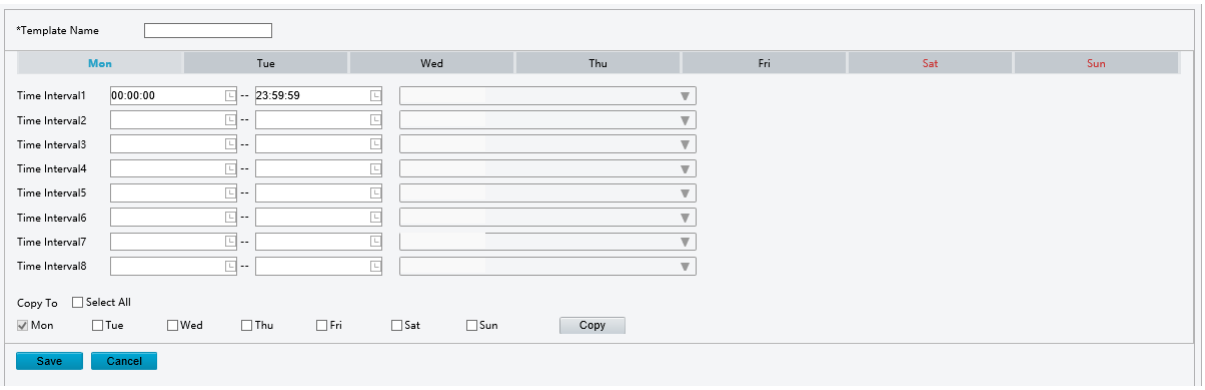
Figure 8-45: Check Template



Add

1. Click **Add**, and an empty template appears on the right.

   Figure 8-46: Empty Check Template



2. Enter the template name with 1 to 20 characters, including lowercase and uppercase letters, digits, underscores, and hyphens.
3. Set the time interval. Up to 8 periods are allowed, and periods cannot overlap.
4. Repeat the above steps and complete the settings for other six days. To apply the current settings to other days, select the check box(es) for the days and then click **Copy**.
5. Click **Save**.

Edit

1. Select the template to be edited on the left, and then edit the settings. See Add for details.
2. Click **Save**.

Delete

Note: The default template cannot be deleted.

1. Select the template to be deleted on the left.
2. Click **Delete**, and then click **OK** to delete it.

Search

Support searching the set check template information.

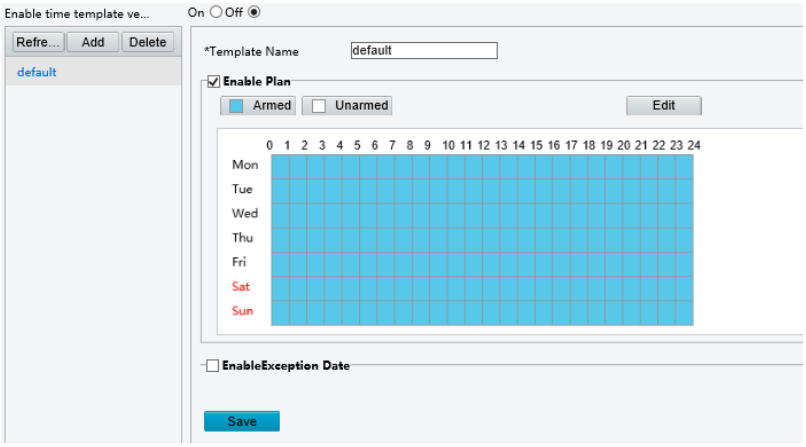
Select the target template on the left (click **Refresh** to show the latest template status), and the detailed template information is displayed on the right.

8.4.5.2 Time Template

Set time periods for an arming schedule in a week.

Go to **Setup** > **Intelligent** > **Time Template**.

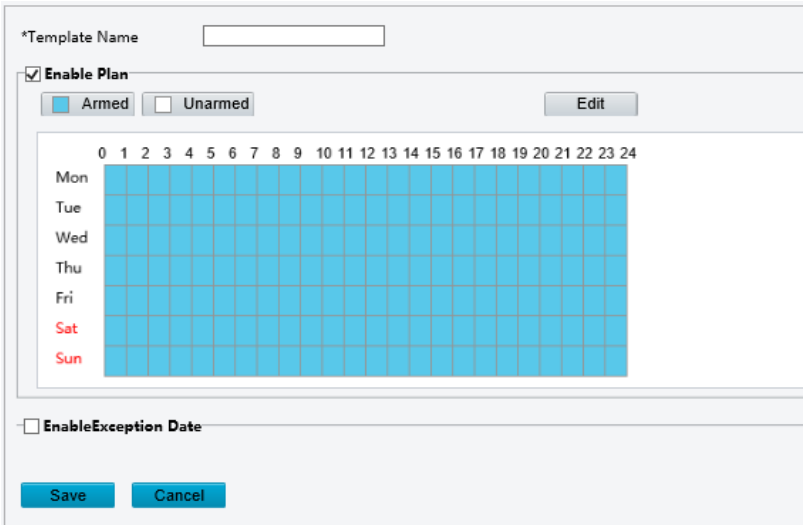
Figure 8-47: Time Template



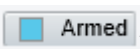
Add

1. Click **Add**, and an empty template appears on the right.

   Figure 8-48: Empty Time Template



2. Enter the template name with 1 to 20 characters, including lowercase and uppercase letters, digits, underscores, and hyphens.
3. Set the arming schedule. The default arming schedule is 24/7. The following two ways are available.
   - Use the blue and white grids

     Click 

, and select blue grids to add time periods.

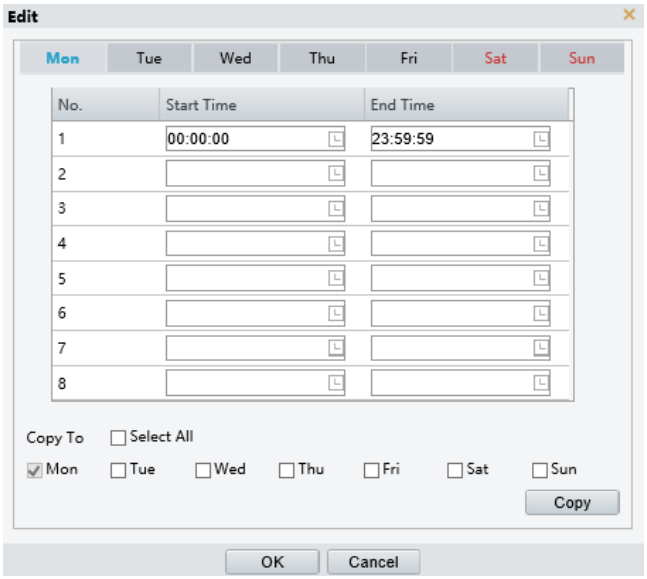
     Click 

, and select white grids to delete time periods.

   - Use the **Edit** button

     (1) Click **Edit**. The **Edit** page appears.

Figure 8-49: Edit



(2) Set the time periods for the current day. Up to 8 time periods are allowed and periods cannot overlap.

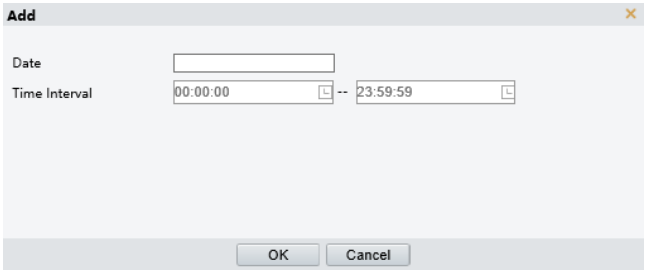
(3) Repeat the above steps and complete the settings for other six days. To apply the current settings to other days, select the check box(es) for the days and then click **Copy**.

(4) Click **OK** to save the arming schedule.

4. (Optional) To set exception dates, select the **Enable Exception Date** check box, and set disarming periods.

(1) Click **Add**.

Figure 8-50: Add



(2) Set the exception date and time period, and then click **OK**.

(3) Repeat the above steps and add other exception dates. Up to 16 exception dates are allowed.

5. Click **Save**.

Edit

1. Select the template to be edited on the left, and then edit the settings. See Add for details.
2. Click **Save**.

Delete

Note: The default template cannot be deleted.

1. Select the template to be deleted on the left.
2. Click **Delete**, and then click **OK** to delete it.

Search

You can search the configured time information.

Select the target template on the left (click **Refresh** to show the latest template status), and the detailed template information is displayed on the right.

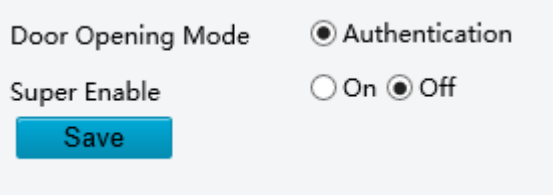
8.4.5.3 Advanced Settings

The door station supports the super password. The administrator can open doors by inputting the super password.

The super password can also be configured on the door station screen. See Open Door by Super Password.

1. Go to **Setup** > **Intelligent** > **Advanced Setting**.

   Figure 8-51: Advanced Settings

2. Select **On** to enable super password .
3. Set a super password and enter it again for confirmation.
4. Click **Save**.

8.4.6 Events

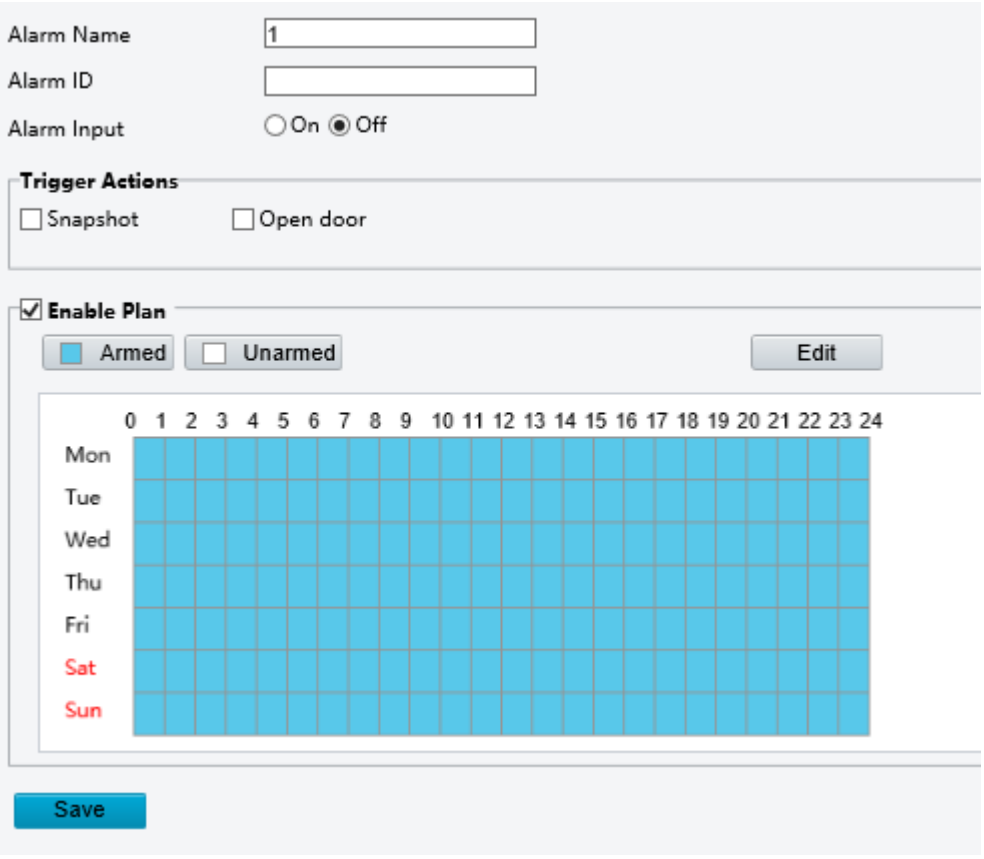
Report the alarm information to Intelligent Server. When an event occurs, the device can report the alarm to the connected intelligent server, and trigger other devices to perform one or several types of action(s) to alert users.

8.4.6.1 Fire Alarm

A fire alarm occurs when the connected external device detects fire.

1. Go to **Setup** > **Events** > **Fire Alarm**.

   Figure 8-52: Fire Alarm

2. Edit the fire alarm parameters.

Parameter		Description
Alarm Info	Alarm Name	Set the fire alarm name. 1 to 20 characters are allowed.
	Alarm ID	Set the alarm ID as needed. It must be unique on the intelligent server. 0 to 20 common characters (input using the keyboard) are allowed.
	Alarm Input	• **On**: The door station can receive fire alarms. • **Off**: The door station cannot receive fire alarms.
Trigger Actions		When a fire alarm occurs, the door station can trigger snapshot, and door opening. Choose actions as needed.
Enable Plan		Only during the set by the arming periods can the alarm be reported. **Note:** When the **Enable Plan** check box is not selected, the device cannot receive alarms. The default arming schedule is 24/7. To change the schedule, refer to Add Time Template. Up to 4 periods are allowed.

3. Click **Save**.

8.4.6.2 Tamper Alarm

If the device is disassembled, the tamper button will be triggered and the device will report a tamper alarm.

1. Go to **Setup** > **Events** > **Tamper Alarm**.

Figure 8-53: Tamper Alarm

2. Edit the tamper alarm parameters.

Parameter		Description
Alarm Info	Alarm Name	Set the tamper alarm name. 1 to 20 characters are allowed.
	Alarm ID	Set the alarm ID as needed. It must be unique on the intelligent server. 0 to 20 common characters (input using the keyboard) are allowed.
	Alarm Type	Choose **N.O.** or **N.C.**. The default is **N.O.**.
	Alarm Input	• **On**: The door station can receive tamper alarms. • **Off**: The door station cannot receive tamper alarms.
Trigger Actions		When a tamper alarm occurs, the door station can trigger snapshot. Choose the action as needed.
Enable Plan		Only during the set by the arming periods can the alarm be reported. **Note:** When the **Enable Plan** check box is not selected, the device cannot receive alarms. The default arming schedule is 24/7. To change the schedule, refer to Add Time Template. Up to 4 periods are allowed.

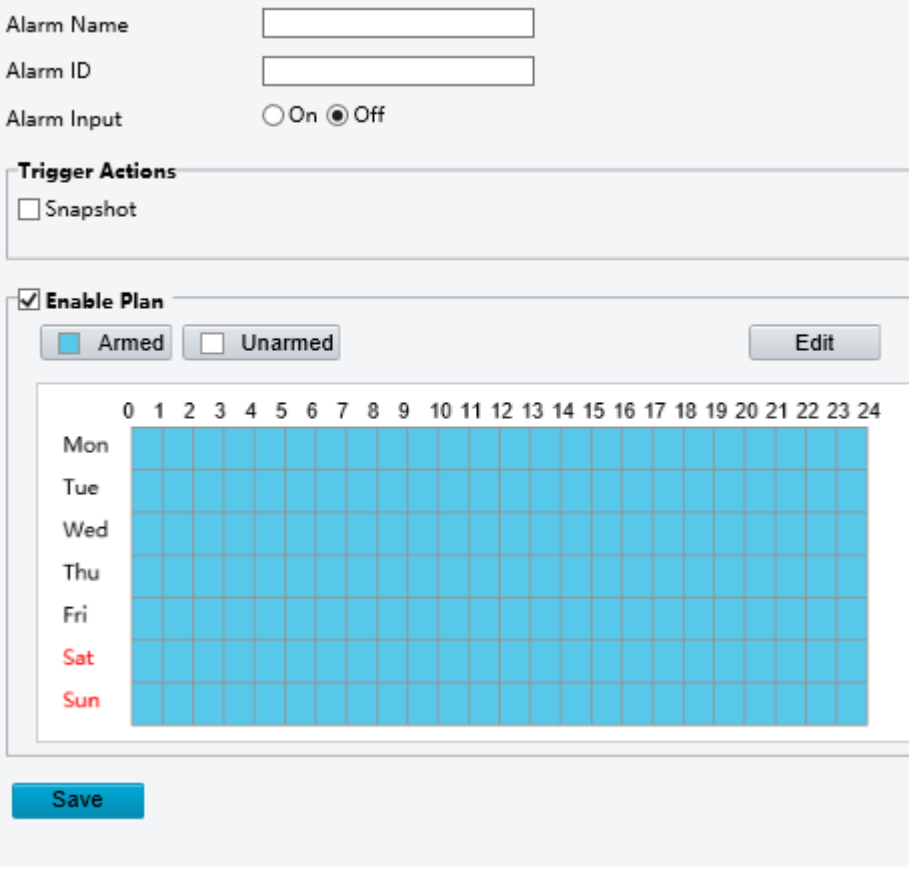
3. Click **Save**.

8.4.6.3 Door Magnet Alarm

When a door magnet is connected to the device, it can receive door magnet alarms.

1. Go to **Setup** > **Events** > **Door Magnet Alarm**.

Figure 8-54: Door Magnet Alarm



2. Edit the door magnet alarm parameters.

Parameter		Description
Alarm Info	Alarm Name	Set the door magnet alarm name. 1 to 20 characters are allowed.
	Alarm ID	Set the alarm ID as needed. It must be unique on the intelligent server. 0 to 20 common characters (input using the keyboard) are allowed.
	Alarm Type	Choose **N.O.** or **N.C**. according to the external alarm input device. **Note:** If the external alarm input device is normally open, choose **N.O.**, and then the door station can receive alarms from the external device.
	Alarm Input	• **On**: The door station can receive door magnet alarms. • **Off**: The door station cannot receive door magnet alarms.
Trigger Actions		When a tamper alarm occurs, the door station can trigger snapshot. Choose the action as needed.
Enable Plan		Only during the set by the arming periods can the alarm be reported. **Note:** When the **Enable Plan** check box is not selected, the device cannot receive alarms. The default arming schedule is 24/7. To change the schedule, refer to Add Time Template. Up to 4 periods are allowed.

3. Click **Save**.

8.4.7 Security

8.4.7.1 User

See User for details.

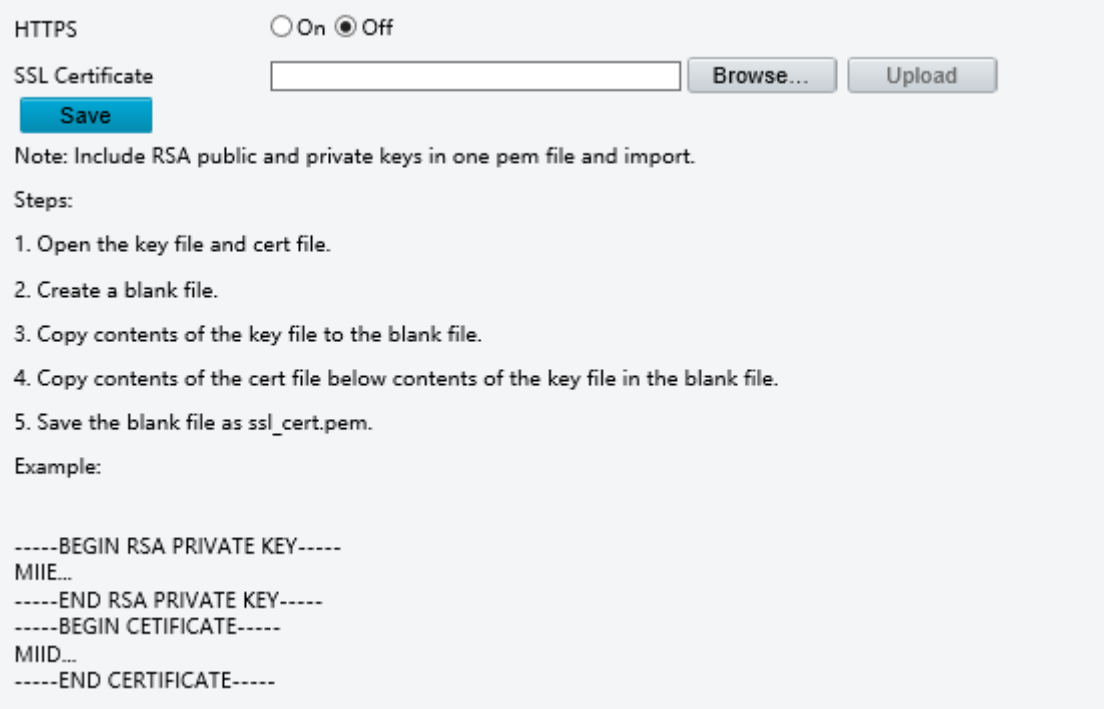
8.4.7.2 Network Security

8.4.7.2.1 HTTPS

HTTPS is a secure version of the HTTP protocol that uses SSL protocol to authenticate both a client and a server, and encrypt data during transmission to prevent data from being stolen or altered, enhancing data security. By default, this function is disabled. To enable it, follow the steps below.

1. Go to **Setup** > **Security** > **Network Security** > **HTTPS**.

Figure 8-55: HTTPS



2. Click **On** to enable **HTTPS**.
3. Click **Browse**, locate the SSL certificate, and click **Upload**.

Note:

- An SSL certificate is issued by the Certificate Authority after verifying that the server is reliable and compliant with the SSL protocol.

  It is used to activate SSL protocol (an Internet protocol used for authentication and encryption), transmit encrypted data between client and server so that it cannot be leaked and tampered with, and confirm the reliability of the server.

  An SSL certificate includes a public key (for encryption) and private key (for decryption).
- Put the RSA public key and private key in one pem file, and then import. Follow the on-screen instructions for specific operations.

4. Click **Save**.

8.4.7.2.2 Authentication

Authentication refers to the procedure of identifying clients. Only after successful authentication can the data be transmitted based on the protocol, improving the security of data transmission.

- RTSP Authentication: Transmits audio and video data in real time through the RTSP protocol. It establishes a two-way connection between the server and the client, and controls either a single or several streams of continuous media such as audio and video for a long time.
- HTTP authentication: Transfers data as a file via the HTTP protocol. It establishes a one-way connection between the client and the server, and the connection will end after the server responds to the request from the client. The connection will be re-built to transfer data if there is a new request.

1. Go to **Setup** > **Security** > **Network Security** > **Authentication**.

Figure 8-56: Authentication

2. Choose an authentication mode.

Parameter	Description
RTSP Authentication	Choose an authentication mode, including **None**, **Basic**, and **Digest** (default). • None: Transmits data without authentication. • Basic: Authentication information is transferred in plaintext without encryption, which imposes serious security risks. • Digest: Authentication information is encrypted to provide higher security.
HTTP Authentication	Choose an authentication mode, including **None**, and **Digest** (default). • None: Transmits data without authentication. • Digest: Authentication information is encrypted to provide higher security.

3. Click **Save**.

8.4.7.2.3 ARP Protection

ARP attack mainly exists in local area network, which forges IP address and physical address (MAC address) to achieve ARP spoofing, causing communication failures among devices within the local area network.

Configure ARP protection, and the device will verify the physical address (MAC address) of the access source, so as to avoid ARP spoofing attacks.

By default, this function is disabled. To enable it, follow the steps below.

1. Go to **Setup** > **Security** > **Network Security** > **ARP Protection**.

Figure 8-57: ARP Protection

2. Click **On** to enable **ARP Protection**.
3. Enter the gateway's physical address (legal MAC address).
4. Click **Save**.

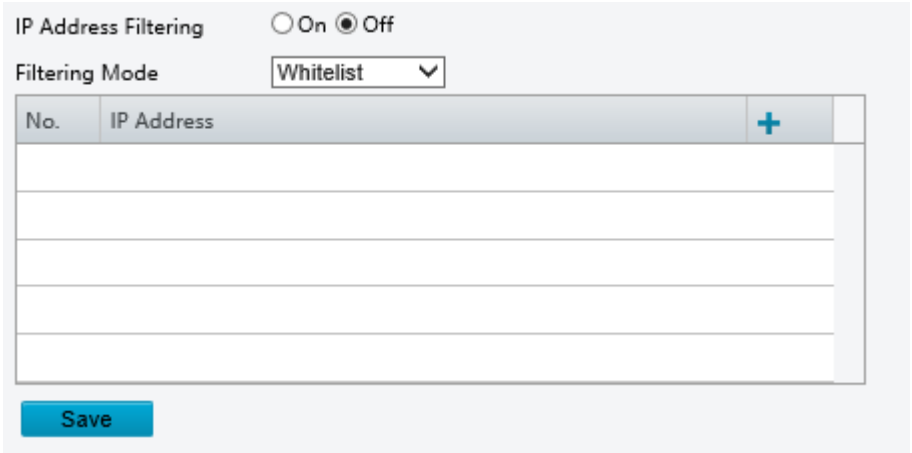
8.4.7.2.4 IP Address Filtering

Use IP address filtering to allow or forbid access from specified IP addresses.

By default, this function is disabled. To enable it, follow the steps below.

1. Go to **Setup** > **Security** > **Network Security** > **IP Address Filtering**.

Figure 8-58: IP Address Filtering



2. Click **On** to enable **IP Address Filtering**.

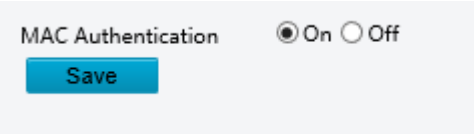
3. Select the filtering mode from the drop-down list. If **Whitelist** is selected, only the added IP addresses are allowed to access the device. If **Deny Access** is selected, only the added IP addresses cannot access the device.
4. Click **+**, and enter IP address(es).
   - Up to 32 IP addresses can be added. Duplicate addresses are not allowed.
   - The first byte of the IP must be 1-233, and the fourth byte cannot be 0. Invalid IP addresses such as 0.0.0.0, 127.0.0.1, 255.255.255.255, and 224.0.0.1 are not allowed.
5. Click **Save**.

8.4.7.2.5 Access Policy

When enabled, access is allowed only if the Mac address is authenticated successfully, which has higher security; When disabled, access is allowed for any Mac address, which poses security risks. This function is enabled by default.

1. Go to **Setup** > **Security** > **Network Security** > **Access Policy**.

   Figure 8-59: Access Policy

2. Click **Off** to disable MAC authentication as needed.
3. Click **Save**.

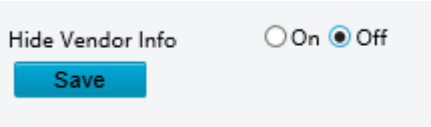
8.4.7.3 Registration Info

The vendor information is provided on the management platform.

The vendor information is provided by default. To hide the information, do as follows:

1. Go to **Setup** > **Security** > **Registration Info**.

   Figure 8-60: Registration Info

2. Click **On** to hide the vendor information.
3. Click **Save**.

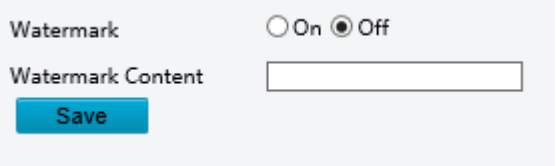
8.4.7.4 Watermark

Use the watermark function to encrypt custom information into video contents to prevent video tampering. By default, this function is disabled.

You can view the watermark effect of the video player on the EZPlayer website.

1. Go to **Setup** > **Security** > **Watermark**.

   Figure 8-61: Watermark

2. Click **On** to enable the watermark.
3. Set the watermark content (0 to 16 characters including lowercase and uppercase letters, and digits).
4. Click **Save**.

8.4.8 System

8.4.8.1 Time

See Time for details.

8.4.8.2 Server

See Server for details.

8.4.8.3 Ports & Devices

See Ports & Devices for details.

8.4.8.4 Maintenance

Supports maintenance and network diagnosis.

8.4.8.4.1 Maintenance

Note:

- The device will restart if you perform operations such as software upgrade, device restart, restoring default configurations, and importing configurations.
- Restarting the door station with cause service interruptions.

Go to **Setup** > **System** > **Maintenance** > **Maintenance**.

Software Upgrade

Figure 8-62: Software Upgrade

Local upgrade and cloud upgrade are available.

Note:

- Make sure the upgrade file matches the door station model; otherwise unexpected problems may occur.
- The version file is a .zip file that includes all the upgrade files.
- Power must be connected throughout the upgrade.

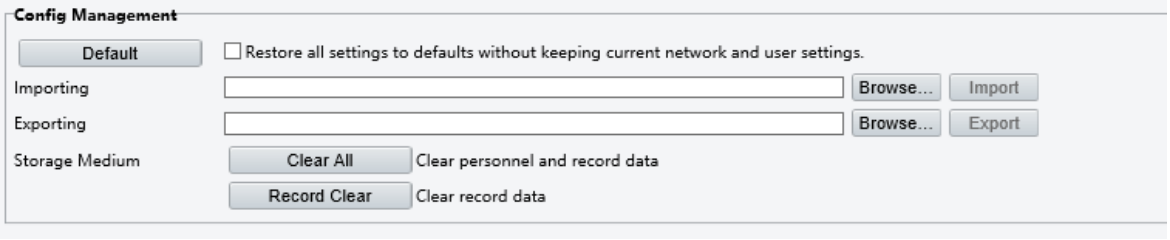
- Local Upgrade
  1. Click **Browse**, and then select the correct upgrade file.

     If applicable, select **Upgrade Boot Program**, and the boot program will also be upgraded.
  2. Click **Upgrade** to start. The door station will restart automatically after the upgrade is completed, and then the **Login** page is displayed.
- Cloud upgrade: Click **Detect** to check for new versions. You can perform a cloud upgrade if a new version is available on the cloud server.

Config Management

You can export the current configurations of the door station and save them to the local device or an external storage device. You can also restore configurations by re-importing an exported configuration file.

Figure 8-63: Config Management



- Default: Clicking **Default** will restore settings to defaults except the administrator login password, network settings, and system time, and then the door station will automatically restart.

  To restore all settings to factory defaults, select **Restore all settings to defaults without keeping current network and user settings**.

- Import configurations

  Note: Make sure the configuration file to be imported matches the door station model. otherwise unexpected results may occur.

  1. Click **Browse** next to the **Import** button.
  2. Select the configuration file you want to import, and click **Import**.
  3. Click **OK**. The door station will restart after you import the configuration file.

- Export configurations

  1. Click **Browse** next to the **Export** button.
  2. Choose the destination folder, and then click **Export**. If a prompt of successful download appears, it indicates the export is successful.

- Storage Medium
  - Clear All: Clear people library data and authentication records.
  - Record Clear: Only clear authentication records.

People Library Management

You can export library data from a door station and then import it to another door station of the same type.

Note: Do not modify the exported data, otherwise failure may occur when you import the data to a door station.

Figure 8-64: People Library Management

- Import People Library

  Note: After the data is imported, the door station will clear the existing library data and will restart.

  1. Click **Browse** next to the **Import People Library** box.
  2. Select the configuration data, and then click **Import**.
  3. Click **OK** to import system configuration.

- Export People Library

  Note: The historical people library data will be cleared after export.

  1. Click **Browse** next to the **Export People Library** box.
  2. Select the storage path on the local device.
  3. (Optional) To export check template data, select **Export template data synchronously**.
  4. Click **Export**.

Diagnosis Info

Diagnosis information includes logs and system configurations, and you can export them to the PC.

Figure 8-65: Diagnosis Info

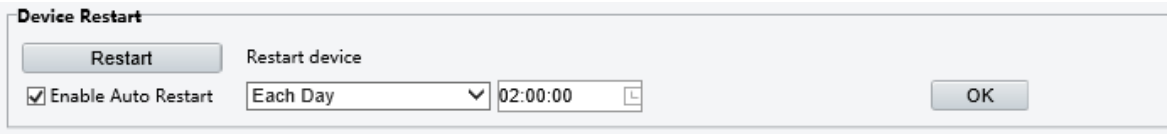
1. Click **Browse** and choose the destination folder.
2. (Optional) **Collect Image Debugging Info** is enabled by default. The snapshots and debugging information will be exported for problem analysis.
3. Click **Export** to export diagnosis information to the selected folder. If a prompt of successful download appears, it indicates the export is successful.

Device Restart

You can choose to restart the device manually or automatically.

Note: Restarting the door station will interrupt the ongoing services.

Figure 8-66: Device Restart



- Restart manually: Click **Restart**, and then confirm to restart the door station.
- Restart automatically:
  1. Select **Enable Auto Restart** and set the restart time.
  2. Click **OK**, and then the door station will automatically restart at the set time.

8.4.8.4.2 Network Diagnosis

Go to **Setup** > **System** > **Maintenance** > **Network Diagnosis**.

Network Diagnosis

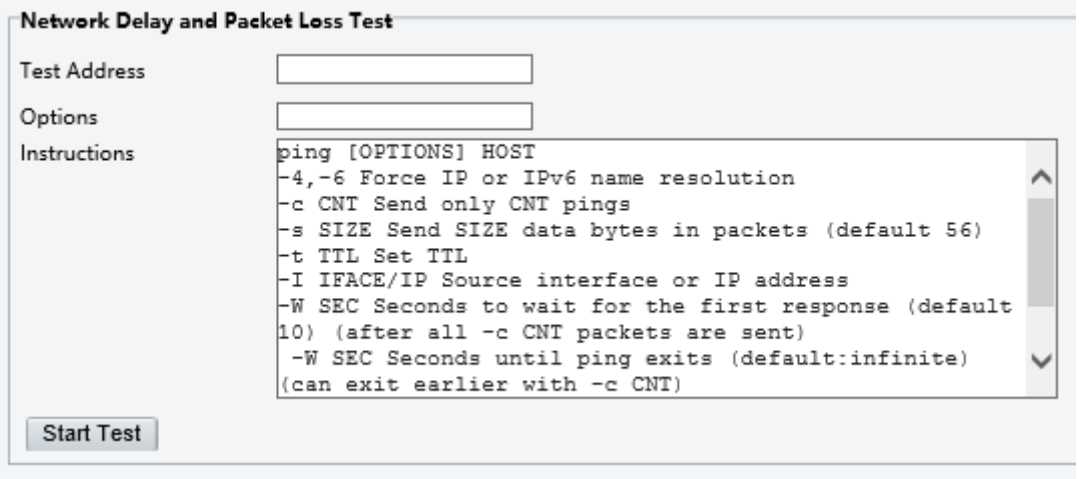
Figure 8-67: Network Diagnosis

1. Select an NIC.
2. Choose an IP and port filter mode.
   - All: Capture packets of all the ports and IPs.
   - Specify: Capture packets of the specified port and IP.
   - Filter: Capture packets except that of the specified port and IP.
3. (Optional) Set the custom rules according to description.
4. Click **Start Capture** to capture packets.
5. Click **Stop Capture**, and the captured data are saved to the custom directory.

Network Delay and Packet Loss Test

The system can send test packets multiple times, and check if the operation is normal and network is smooth based on average delay and packet loss, which can help users to find the cause of network failures. The average delay refers to the average length of time from test packets are sent till responses are received. The packet loss rate refers to the ratio of lost packets to the sent packets.

Figure 8-68: Network Delay and Packet Loss Test



1. Enter the test address.
2. Enter the options based on instructions.
3. Click **Start Test**. The results will appear after the test is completed.