Face Recognition Time & Attendance

User's Manual

V1.0.1

Foreword

General

This manual introduces the functions and operations of the Face Recognition Time & Attendance (hereinafter referred to as the "Device"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
📖 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	Updated verification mode configuration.	May 2024
V1.0.0	First Release.	January 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or

visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, and comply with the guidelines when using it.

Transportation Requirement

⚠

Transport, use and store the Device under allowed humidity and temperature conditions.

Storage Requirement

⚠

Store the Device under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the Device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Device.
- Do not connect the Device to two or more kinds of power supplies, to avoid damage to the Device.
- Improper use of the battery might result in a fire or explosion.
- Please follow the electrical requirements to power the Device.
  - Following are the requirements for selecting a power adapter.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
  - We recommend using the power adapter provided with the Device.
  - When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the Device label.

⚠

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Install the Device on a stable surface to prevent it from falling.
- Install the Device in a well-ventilated place, and do not block its ventilation.

- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The Device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.

Operation Requirements

⚠

- Check whether the power supply is correct before use.
- Ground the device to protective ground before you power it on.
- Do not unplug the power cord on the side of the Device while the adapter is powered on.
- Operate the Device within the rated range of power input and output.
- Use the Device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Do not disassemble the Device without professional instruction.
- This product is professional equipment.
- The Device is not suitable for use in locations where children are likely to be present.

Table of Contents

1 Overview

The Device can be used to track attendance of people. People can clock in/out through face and password.

It is widely used in parks, communities, business centers and factories, and ideal for places such as office buildings, government buildings, schools and stadiums.

📖

Configurations might differ depending on the models of the product, please refer to the actual product.

2 Local Operations

- Configurations might differ depending on the actual product.
- You might see some UI texts are not displayed because of the limited space. Long press the text for 3 seconds and it will show.

2.1 Common Icons

Table 2-1 Description of icons

Icon	Description
⌂	Main menu icon
✓	Confirm icon
|<	Turn to the first page of the list.
>|	Turn to the last page of the list.
< or ^	Turn to the previous page of the list.
> or ˅	Turn to the next page of the list.
←	Return to the previous menu.
ON ●	Turn on
● OFF	Turn off
🗑	Delete
🔍	Search

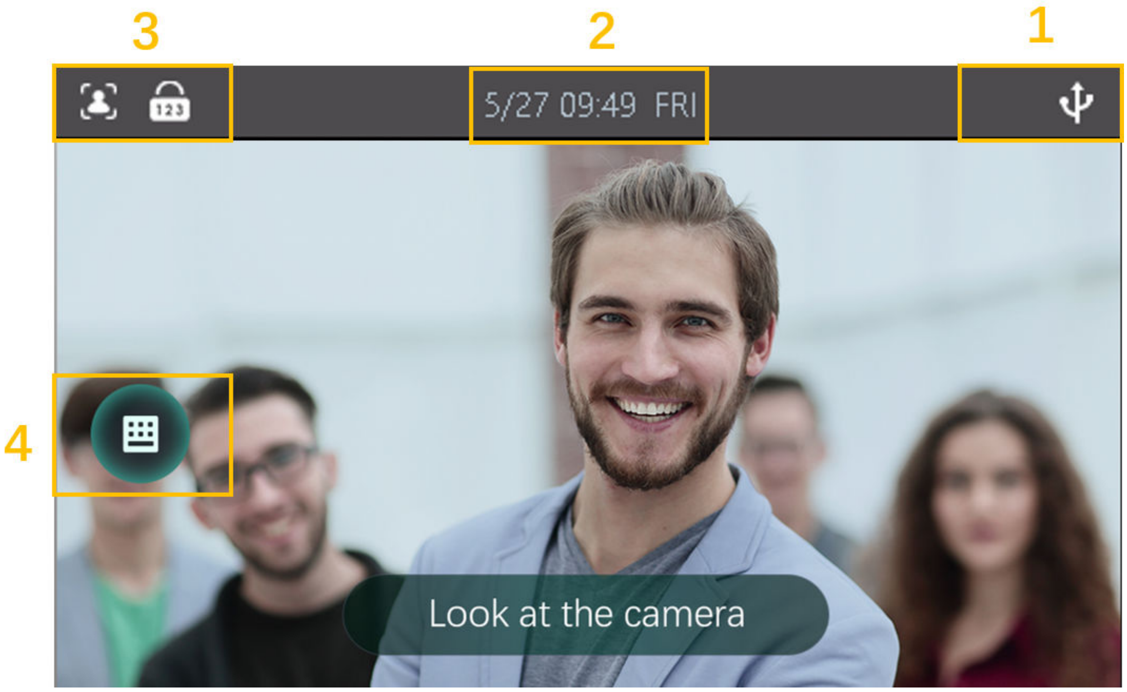
2.2 Standby Screen

Users take attendance through faces or passwords.

📖

- If there is no operation in 30 seconds, the Device will go to the standby mode.
- This manual is for reference only. Slight differences might be found between the standby screen in this manual and the actual device.

Figure 2-1 Standby screen



No.	Name	Description
1	Status display	Displays status of Wi-Fi, network and USB, and more.
2	Date and time	Displays the current date and time.
3	Verification methods	Displays available verification methods.
4	Password	Enter user ID and password to clock in or clock out.

2.3 Initialization

For the first-time use or after restoring factory defaults, you need to select a language on Device, and then set the password and email address for the admin account. You can use the admin account to enter the main menu of the Device and its webpage.

- If you forget the administrator password, send a reset request to your registered e-mail address.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

2.4 Logging In

Log in to the main menu to configure the Device. Only admin account and administrator account can enter the main menu of the Device. For the first-time use, use the admin account to enter the main menu screen and then you can create the other administrator accounts.

Background Information

- admin account: Can log in to the main menu screen of the Device, but does not have door access permissions.

- Administrator account: Can log in to the main menu of the Device and has door access permissions.

Procedure

Step 1 Press and hold the standby screen for 3 seconds.

Step 2 Select a verification method to enter the main menu.

- Face: Enter the main menu by face recognition.
- PWD: Enter the user ID and password of the administrator account.
- admin: Enter the admin password to enter the main menu.

2.5 Person Management

You can add new users, view user/admin list and edit user information.

The pictures in this manual are for reference only, and might differ from the actual product.

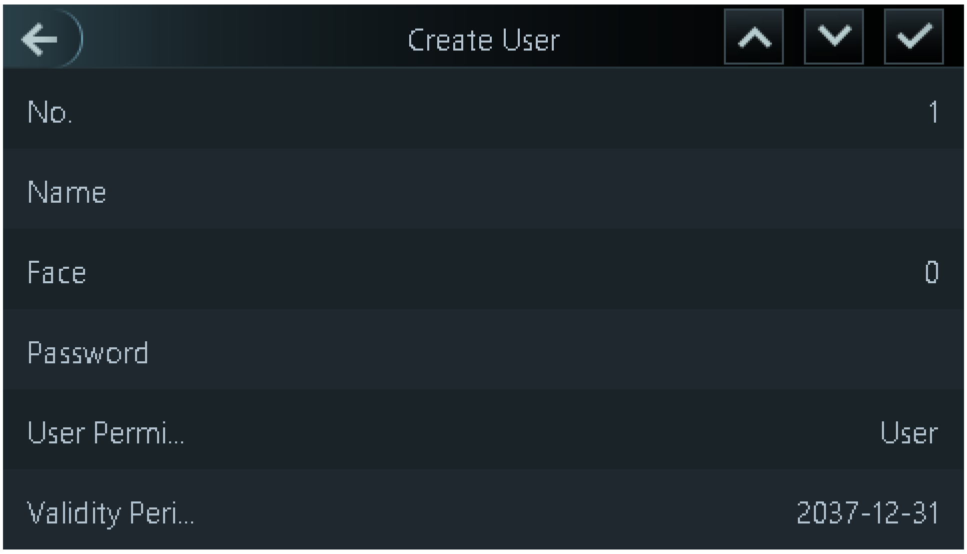
2.5.1 Adding Users

Procedure

Step 1 On the **Main Menu**, select **Person Management** > **Create User**.

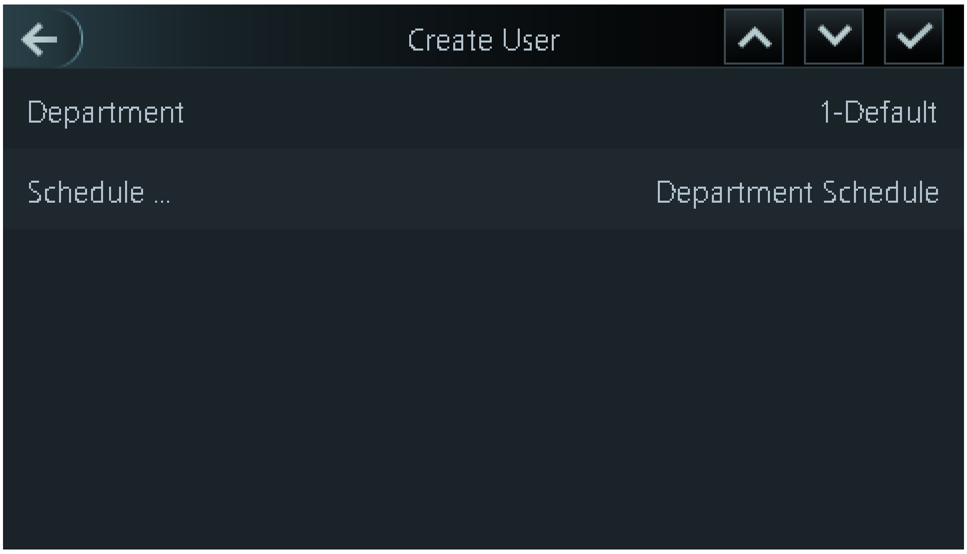
Step 2 Configure the parameters on the interface.

Figure 2-2 Add new user



Create User

No.	1
Name	
Face	0
Password	
User Permi...	User
Validity Peri...	2037-12-31



Create User

Department 1-Default

Schedule ... Department Schedule

Table 2-2 Parameters description

Parameter	Description
No.	The No. is like employee ID, which can be numbers, letters, and their combinations, and the maximum length of the No. is 30 characters.
Name	The name can have up to 32 characters (including numbers, symbols, and letters).
Face	Position your face inside the frame, and a face image will be captured automatically. You can register again if you are not satisfied with the outcome.
Password	Enter the user password. The maximum length of the password is 8 digits.
User Permission	● **User** : Users only have time attendance permissions. ● **Admin** : Administrators can configure the Device besides attendance permissions.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.
Department	Select departments, which is useful when configuring department schedules. For how to create departments, see "2.6.2 Configuring Departments".

Parameter	Description
Schedule Mode	● Department Schedule: Apply department schedules to the user. ● Personal Schedule: Apply personal schedules to the user. For how to configure personal or department schedules, see "2.6.5 Configuring Work Schedules". If you set the schedule mode to department schedule here, the personal schedule you have configured for the user in **Attendance** > **Schedule Config** > **Personal Schedule** become invalid.

Step 3 Tap ☑.

2.5.2 Viewing User Information

Procedure

Step 1 On the **Main Menu**, select **Person Management** > **User List**, or select **User** > **Admin List**.

Step 2 View all added users and admin accounts.

Related Operations

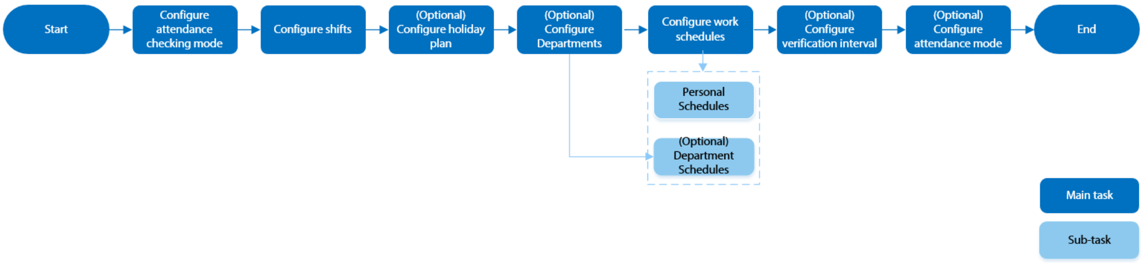
On the **User** screen, you can manage the added users.

- Search for users: Tap 🔍 and then enter the username.
- Edit users: Tap the user to edit user information.
- Delete one by one: Select a user, and then tap 🗑.
- Delete in batches.
  - ◇ On the **User List** screen, tap 🗑 to delete all users.
  - ◇ On the **Admin List** screen, tap 🗑 to delete all admin users.

2.6 Attendance Management

Time attendance supports attendance management both on the Device or and Smart PSS Lite. This section only uses configuring attendance on the Device as an example.

Figure 2-3 Configuration flow chart of time attendance


Start
Configure attendance checking mode
Configure shifts
(Optional) Configure holiday plan
(Optional) Configure Departments
Configure work schedules
(Optional) Configure verification interval
(Optional) Configure attendance mode
End
Personal Schedules
(Optional) Department Schedules
Main task
Sub-task

2.6.1 Configuring Verification Mode

Procedure

Step 1 Select **Attendance** > **Verification Mode**.

Step 2 Select the attendance verification mode.

📖

To cancel your selection, tap the selected method again.

Step 3 Tap **/Or** to configure combinations.

Verify one of the selected verification methods to take attendance.

Step 4 Tap ☑ to save changes.

2.6.2 Configuring Departments

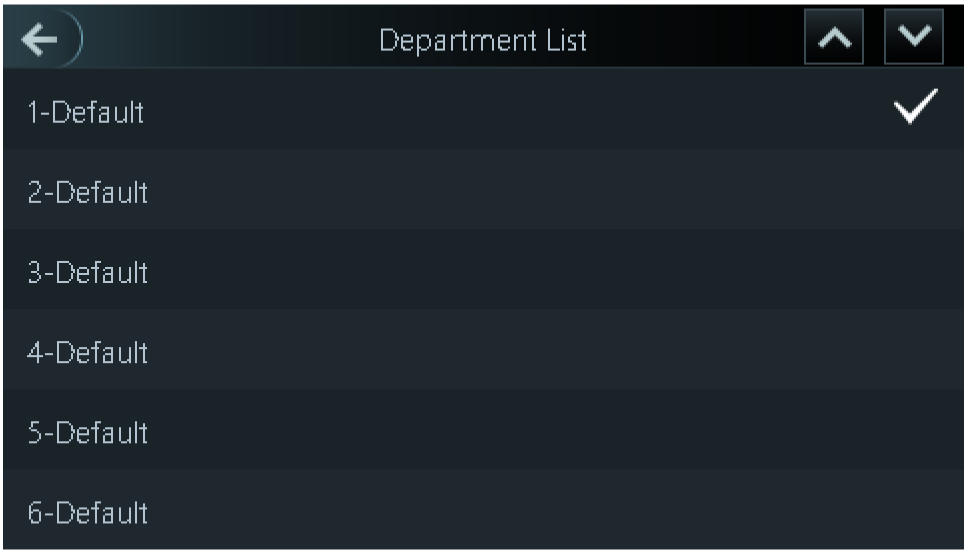
Procedure

Step 1 Select **Attendance** > **Department Settings**.

Step 2 Select a department, and then rename it.

There are 20 default departments. We recommend you rename them.

Figure 2-4 Create departments



1-Default ✓
2-Default
3-Default
4-Default
5-Default
6-Default

Step 3 Tap ☑.

2.6.3 Configuring Shifts

Configure shifts to define time attendance rules. Employees need to come to work at the time scheduled for their shift to start, and leave at the end time, except when they choose to work overtime.

Procedure

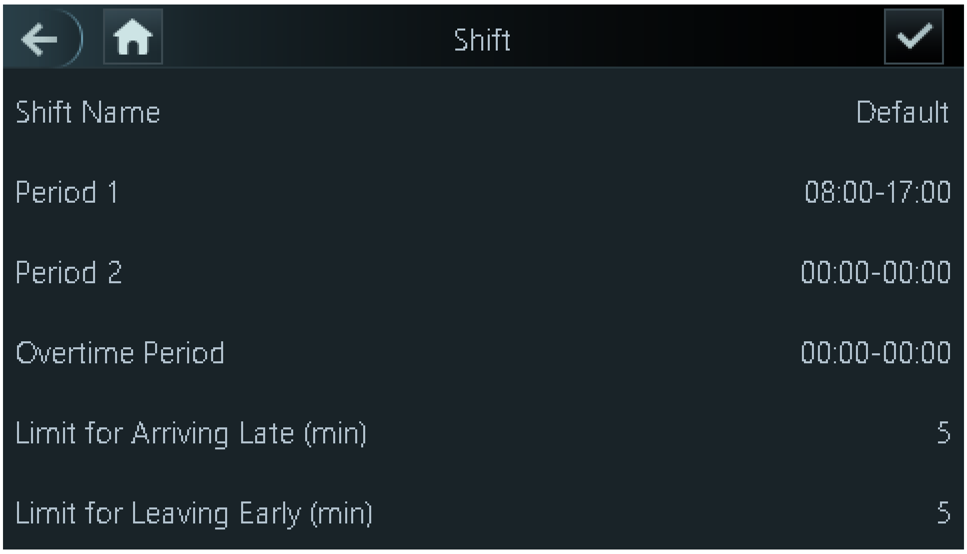
Step 1 Select **Attendance** > **Shift Config**.

Step 2 Tap **Shift**, and then select a shift.

Tap ⌄ to view more shifts. You can configure up to 24 shifts.

Step 3 Configure the parameters of the shift.

Figure 2-5 Create shifts



Shift Name Default

Period 1 08:00-17:00

Period 2 00:00-00:00

Overtime Period 00:00-00:00

Limit for Arriving Late (min) 5

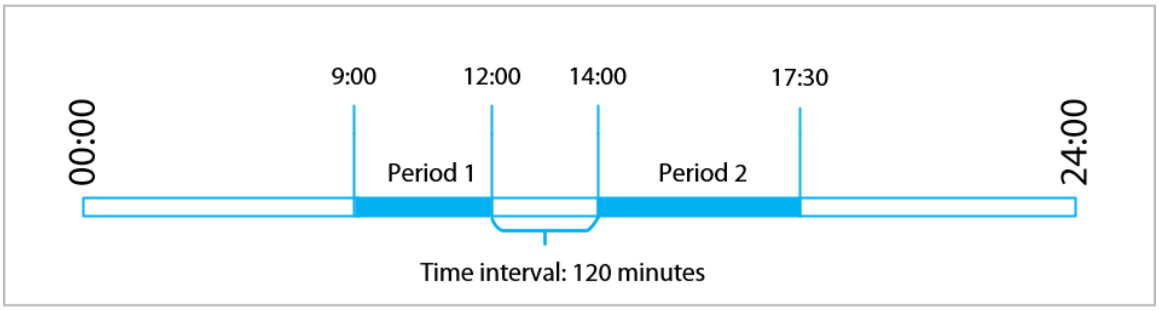
Limit for Leaving Early (min) 5

Table 2-3 Shift parameters description

Parameter	Description
Shift Name	Enter the name of the shift.
Period 1	Specify a time range when people can clock in and clock out for the workday. If you only set one attendance period, employees need to clock in and out by the designated times to avoid an anomaly appearing on their attendance record. For example, if you set 08:00 to 17:00, employees must clock in by 08:00 and clock out from 17:00 onwards. If you set 2 attendance periods, the 2 periods cannot overlap. Employees need to clock in and clock out for both periods.
Period 2	
Overtime Period	Employees who clock in or out during the defined period will be considered as working beyond their normal work hours.
Limit for Arriving Late (min)	A certain amount of time can be granted to employees to allow them to clock in a bit late and clock out a bit early. For example, if the regular time to clock in is 08:00, the tolerance period can be set as 5 minutes for employees who arrive by 08:05 to not be considered as late.
Limit for Leaving Early (min)	

- When the time interval between 2 periods is an even number, you can divide the time interval by 2, and assign the first half of the interval to the first period, which will be the clock out time. The second half of the interval should be assigned to the second period as the clock in time.

Figure 2-6 Time interval (Even number)

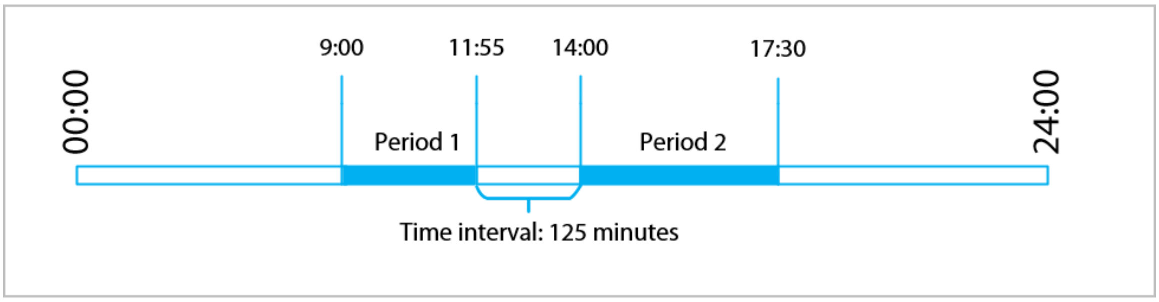


For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.

If a person clocks out multiple times during period 1, the latest time will be valid, and if they clock in multiple times during period 2, the earliest time will be valid.

- When the time interval between 2 periods is an odd number, the smallest portion of the interval will be assigned to the first period, which will be the clock out time. The largest portion of the interval will be assigned to the second period as the clock in time.

Figure 2-7 Time interval (even number)



For example: If the interval is 125 minutes, then the clock-out time for period 1 is from 11:55 to 12:57, and the clock-in time for period 2 is from 12:58 to 14:00. Period 1 has 62 minutes, and period 2 has 63 minutes.

If a person clocks out multiple times during period 1, the latest time will be valid, and if they clock in multiple times during period 2, the earliest time will be valid.

All attendance times are precise down to the second. For example, if the normal clock-in time is set to 8:05 AM, the employee who clocks in at 8:05:59 AM will not be considered as arriving late. But, the employee that arrives at 8:06 AM will be marked as late by 1 minute.

Step 4 Tap ☑.

2.6.4 Configuring Holiday Plans

Configure holiday plans to set periods for attendance to not be tracked.

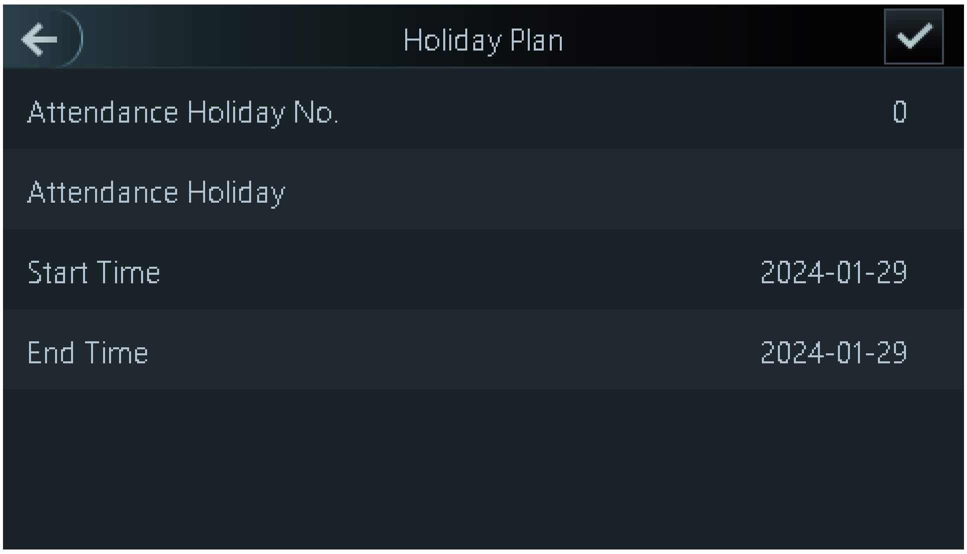
Procedure

Step 1 Select **Attendance** > **Shift Config** > **Holiday**.

Step 2 Click + to add holiday plans.

Step 3 Configure the parameters.

Figure 2-8 Create holiday plans


Holiday Plan

Attendance Holiday No. 0

Attendance Holiday

Start Time 2024-01-29

End Time 2024-01-29

Table 2-4 Parameters description

Parameter	Description
Attendance Holiday No.	The number of the holiday.
Attendance Holiday	The name of the holiday.
Start Time	The start and end time of the holiday.
End Time	

Step 4 Tap ☑.

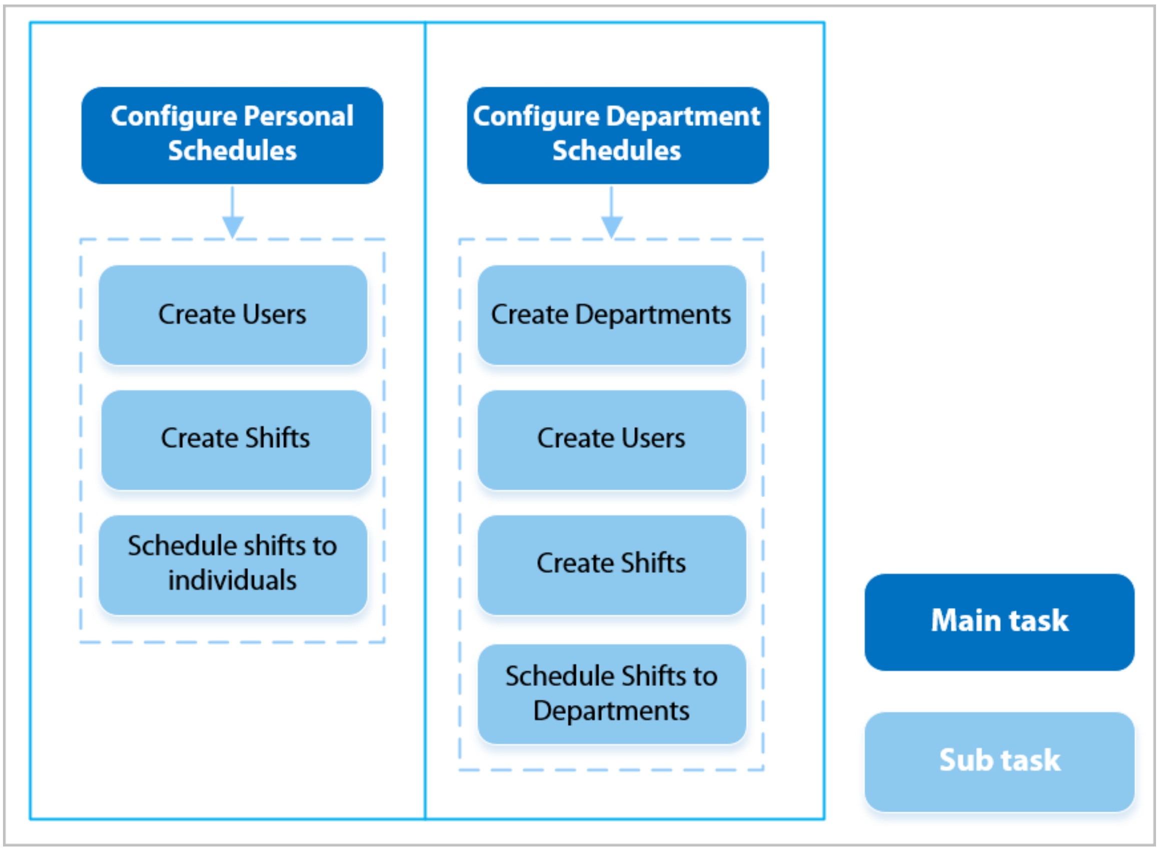
2.6.5 Configuring Work Schedules

A work schedule generally refers to the days per month and the hours per day that an employee is expected to be at their job. You can create different types of work schedules based on different individuals or departments, and then employees must follow the established work schedules.

Background Information

Refer to the flowchart to configure personal schedules or department schedules.

Figure 2-9 Configuring work schedules


Configure Personal Schedules
Create Users
Create Shifts
Schedule shifts to individuals
Configure Department Schedules
Create Departments
Create Users
Create Shifts
Schedule Shifts to Departments
Main task
Sub task

Procedure

Step 1 Select **Attendance** > **Schedule Config**.

Step 2 Set work schedules for individuals.

1. Tap **Personal Schedule**.
2. Enter the user ID, and then tap ☑.
3. On the calendar, select a day, and then select a shift.

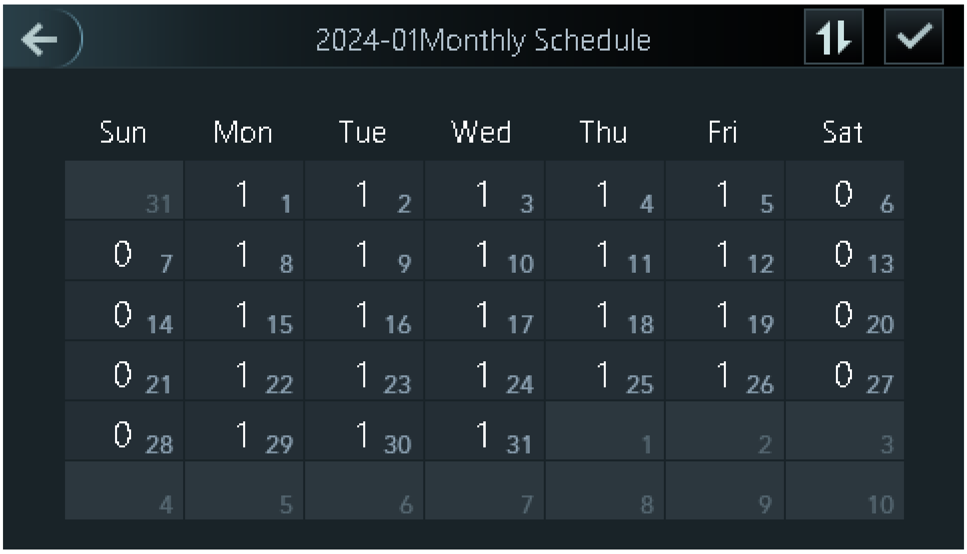
   The shift is scheduled for the day.

   📖

   You can only set work schedules for the current month and the next month.

   - 0 indicates break.
   - 1 to 24 indicates the number of the per-defined shifts. For how to configure shifts, see "2.6.3 Configuring Shifts".
   - 25 indicates business trip.
   - 26 indicates leave of absence.

Figure 2-10 Schedule shifts to individuals



2024-01Monthly Schedule

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1 1	1 2	1 3	1 4	1 5	0 6
0 7	1 8	1 9	1 10	1 11	1 12	0 13
0 14	1 15	1 16	1 17	1 18	1 19	0 20
0 21	1 22	1 23	1 24	1 25	1 26	0 27
0 28	1 29	1 30	1 31	1	2	3
4	5	6	7	8	9	10

4. Tap ✓.

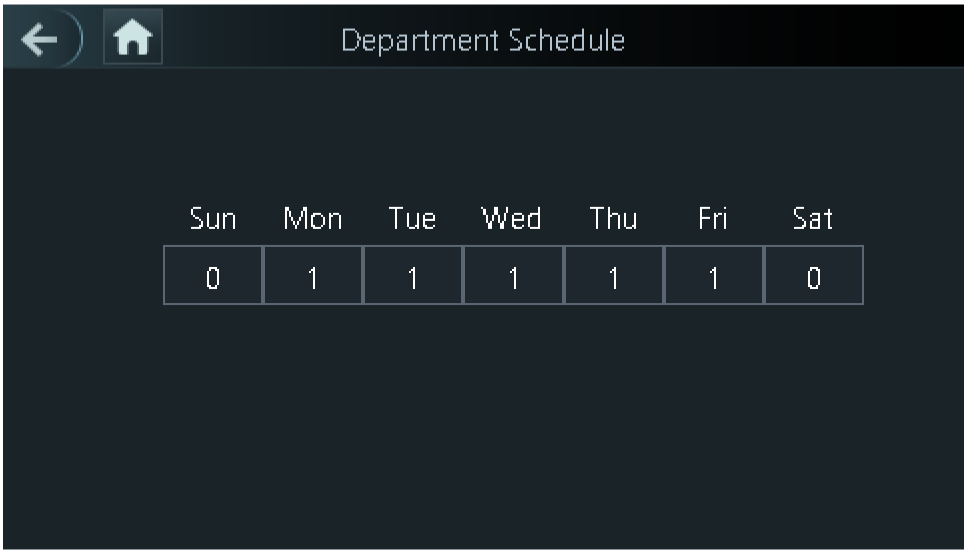
Step 3 Set works schedules for departments.

1. Tap **Department Schedule**.
2. Tap a department, and then select shifts for a week.

   Shifts are scheduled for the week.

- 0 indicates rest.
- 1 to 24 indicates the number of the per-defined shifts. For how to configure shifts, see "2.6.3 Configuring Shifts".
- 25 indicates business trip.
- 26 indicates leave of absence.

Figure 2-11 Schedule shifts to a department



Department Schedule

Sun	Mon	Tue	Wed	Thu	Fri	Sat
0	1	1	1	1	1	0

The defined work schedule is in a week cycle and will be applied to all employees in the department.

Step 4 Tap ✓.

2.6.6 Configuring the Verification Time Interval

When an employee clocks in and out multiple times within a set period, the earliest time will be valid.

Procedure

Step 1 Select **Attendance** > **Verification Interval (sec)**.

Step 2 Enter the time interval, and then tap ✓.

2.6.7 Configuring Attendance Modes

When you clock in or clock out, you can set the attendance modes to define the attendance status.

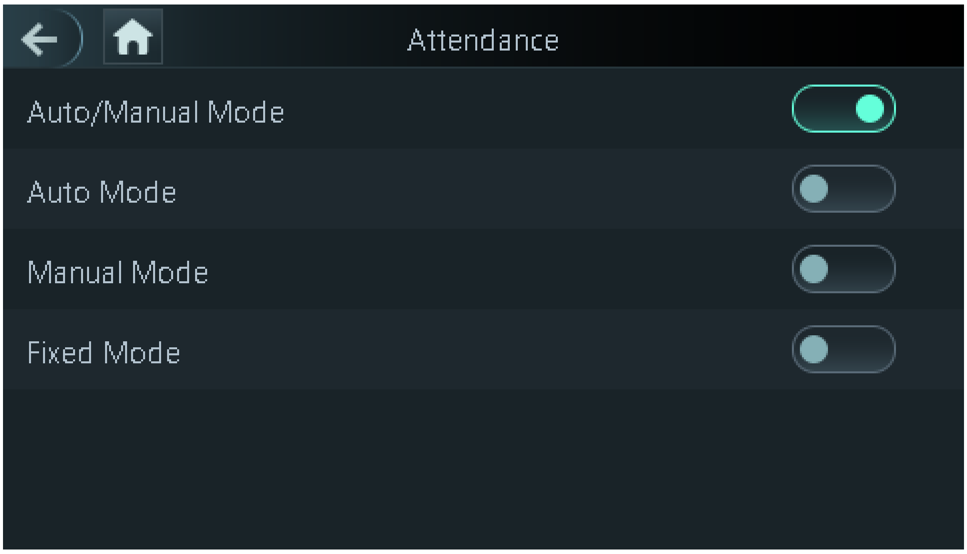
Procedure

Step 1 On the main menu screen, click **Attendance** .

Step 2 Enable **Local or Remote** , and then click ⌄ to page down and tap **Mode Settings**.

The attendance records will also be synchronized to the management platform.

Figure 2-12 Attendance mode



Attendance

Auto/Manual Mode ●

Auto Mode ○

Manual Mode ○

Fixed Mode ○

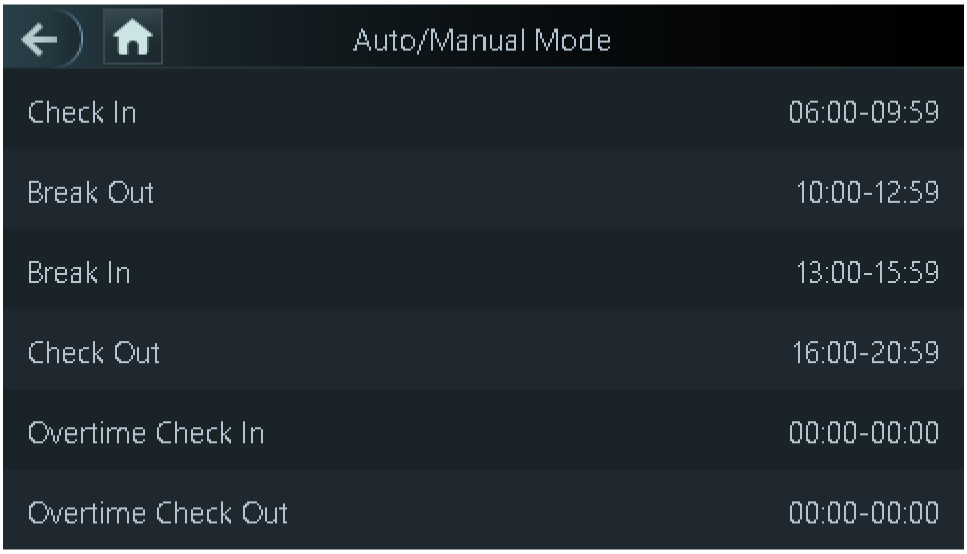
Table 2-5 Attendance mode

Parameter	Description
Auto/Manual Mode	The screen displays the attendance status automatically after you clock in or out, but you can also manually change your attendance status.
Auto Mode	The screen displays your attendance status automatically after you clock in or out.
Manual Mode	Manually select your attendance status when you clock in or out.
Fixed Mode	When you clock in or out, the screen will display the per-defined attendance status all the time.

Step 3 Select an attendance mode.

Step 4 Configure the parameters for the attendance mode.

Figure 2-13 Auto Mode/manual mode



Auto/Manual Mode

Check In 06:00-09:59

Break Out 10:00-12:59

Break In 13:00-15:59

Check Out 16:00-20:59

Overtime Check In 00:00-00:00

Overtime Check Out 00:00-00:00

Table 2-6 Attendance mode parameters

Parameters	Description
Check In	Clock in when your normal workday starts.
Break Out	Clock out when your break starts.
Break In	Clock in when your break ends.
Check Out	Clock out when your normal workday starts.
Overtime Check In	Clock in when your overtime period starts.
Overtime Check Out	Clock out when your overtime period ends.

2.7 Communication Settings

2.7.1 Configuring Auto Registration

Add the device to a management platform, so that you can manage it on the platform.

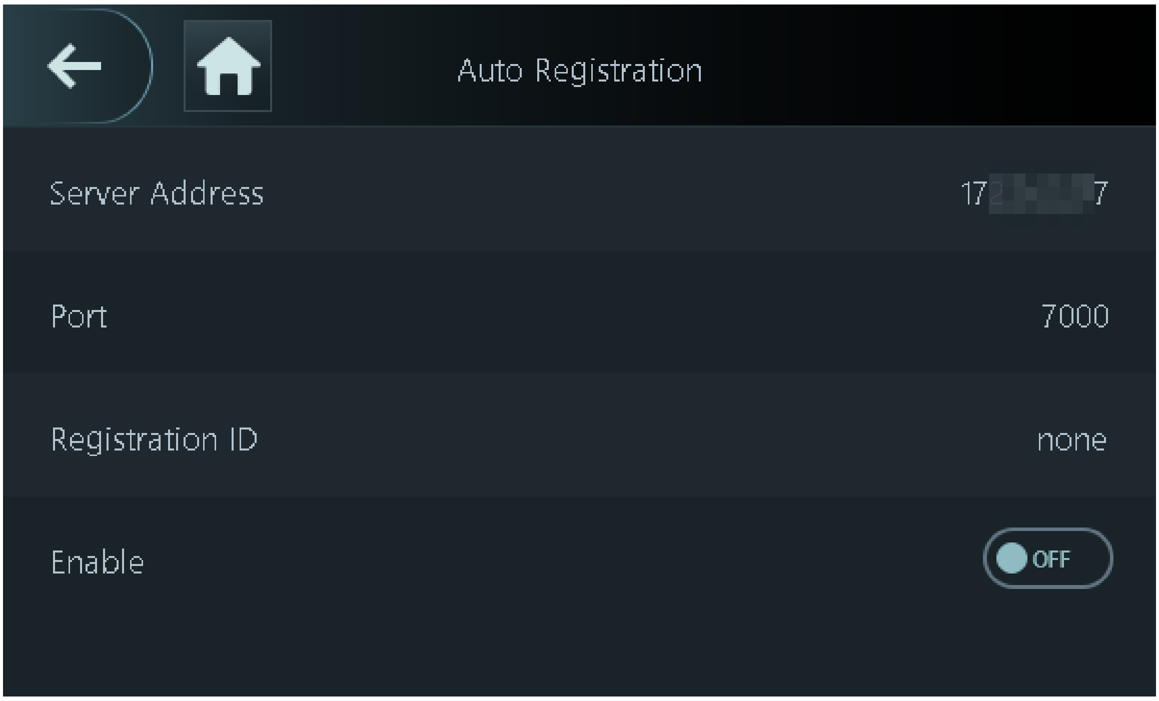
Procedure

Step 1 On the **Main Menu**, select **Communication Settings** > **Network** > **Auto Registration**.

⚠

To avoid exposing the system to security risks and data loss, control the management platform permissions.

Figure 2-14 Auto registration



Auto Registration

Server Address 17[redacted]7

Port 7000

Registration ID none

Enable OFF

Step 2 Turn on the automatic registration function and set the parameters.

Table 2-7 Auto registration

Parameter	Description
Server Address	The IP address of the management platform.
Port	The port No. of the management platform.
Registration ID	Enter the device ID (user defined). When you add the Device to the management platform, the registration ID you enter on the management platform must conform to the defined registration ID on the Device.

2.7.2 Configuring Wi-Fi

You can connect the Device to the network through the Wi-Fi network.

Procedure

Step 1 On the **Main Menu**, select **Communication Settings** > **Network** > **Wi-Fi**.

Step 2 Turn on Wi-Fi.

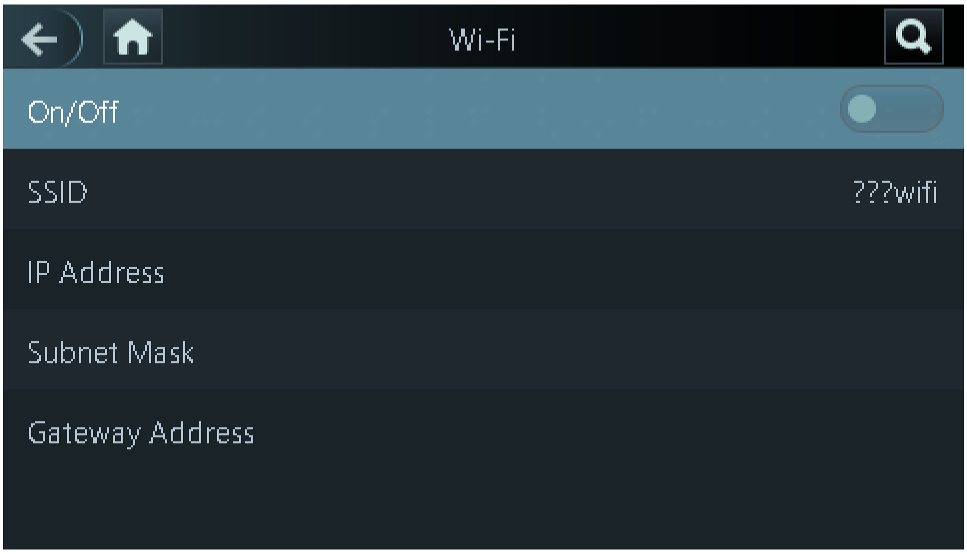
- Wi-Fi AP and Wi-Fi function cannot be enabled at the same time.
- After Wi-Fi is enabled, wait about 1 minutes to connect Wi-Fi.

Step 3 Tap 🔍 to search available wireless networks.

Step 4 Select a wireless network and enter the password.

If the system does not find a Wi-Fi network, tap **SSID** to enter the name of the Wi-Fi.

Figure 2-15 Connect to Wi-Fi



Wi-Fi

On/Off

SSID ???wifi

IP Address

Subnet Mask

Gateway Address

2.7.3 Configuring Wi-Fi AP

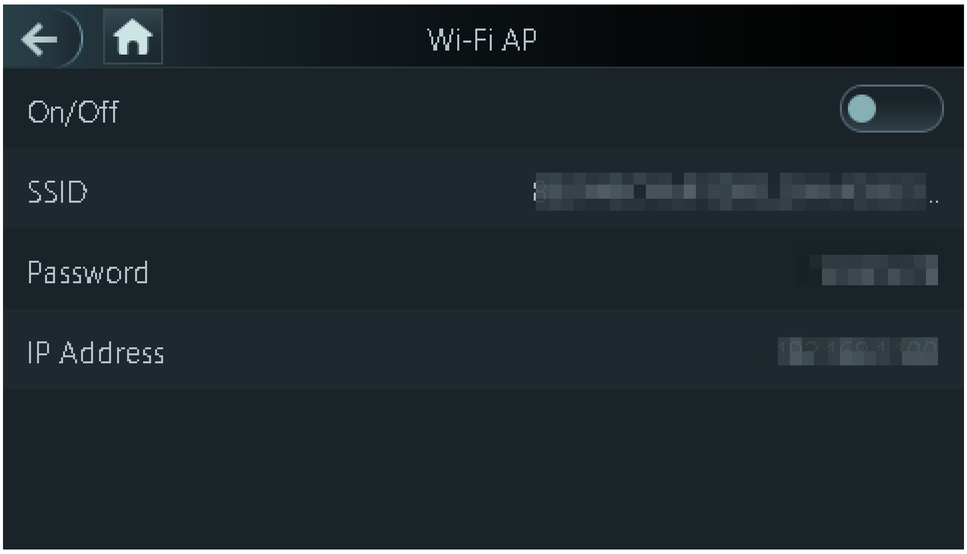
Procedure

Step 1 On the **Main Menu**, select **Communication Settings** > **Network** > **Wi-Fi AP**.

Step 2 Turn on Wi-Fi AP.

Wi-Fi AP and Wi-Fi function cannot be enabled at the same time.

Figure 2-16 Connect to Wi-Fi AP



Wi-Fi AP

On/Off

SSID [redacted]

Password [redacted]

IP Address [redacted]

Results

Use your computer to connect to Wi-Fi AP of the Device to access its webpage.

2.8 System Settings

2.8.1 Configuring Time

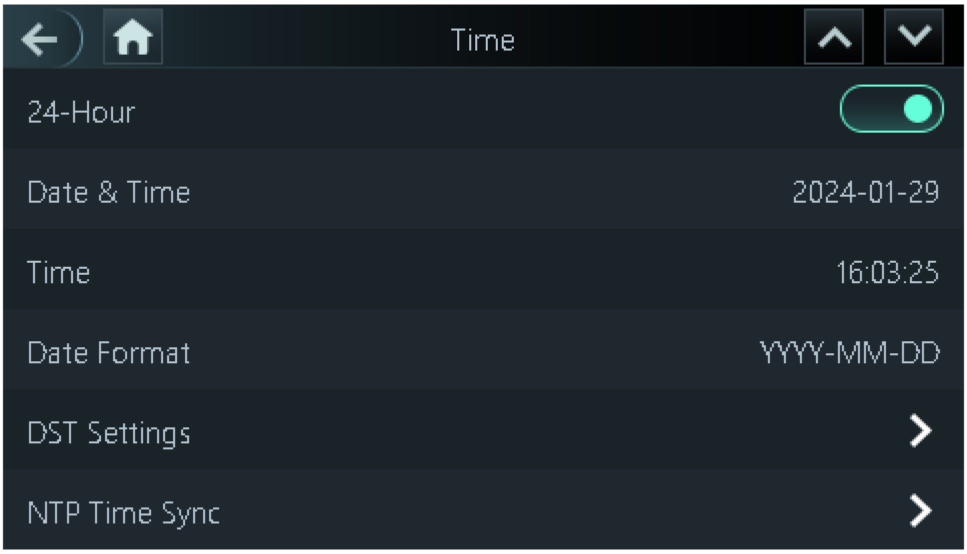
Configure system time, such as date, time, and NTP.

Procedure

Step 1 On the **Main Menu**, select **System Settings** > **Time**.

Step 2 Configure system time.

Figure 2-17 Time



Time

24-Hour

Date & Time 2024-01-29

Time 16:03:25

Date Format YYYY-MM-DD

DST Settings

NTP Time Sync

Table 2-8 Description of time parameters

Parameter	Description
24-hour System	The time is displayed in 24-hour format.
Date & Time	Set up the date.
Time	Set up the time.
Date Format	Select a date format.
DST Setting	1. Tap **DST Setting** and enable it. 2. Select **Date** or **Week** from the **DST** Type list. 3. Enter the start time and end time. 4. Tap ☑.

Parameter	Description
NTP Time Sync	A network time protocol (NTP) server is a machine dedicated as the time sync server for all client computers. If your computer is set to sync with a time server on the network, your clock will show the same time as the server. When the administrator changes the time (for daylight savings), all client machines on the network will also be updated. 1. Tap **NTP Check**, and then enable it. 2. Configure the parameters. ● **Server Address** : Enter the IP address of the NTP server, and the Device will automatically sync time with the NTP server. ● **Port** : Enter the port of the NTP server. ● **Interval** : Enter the time synchronization interval.
Time Zone	Select the time zone.

2.8.2 Configuring Face Parameters

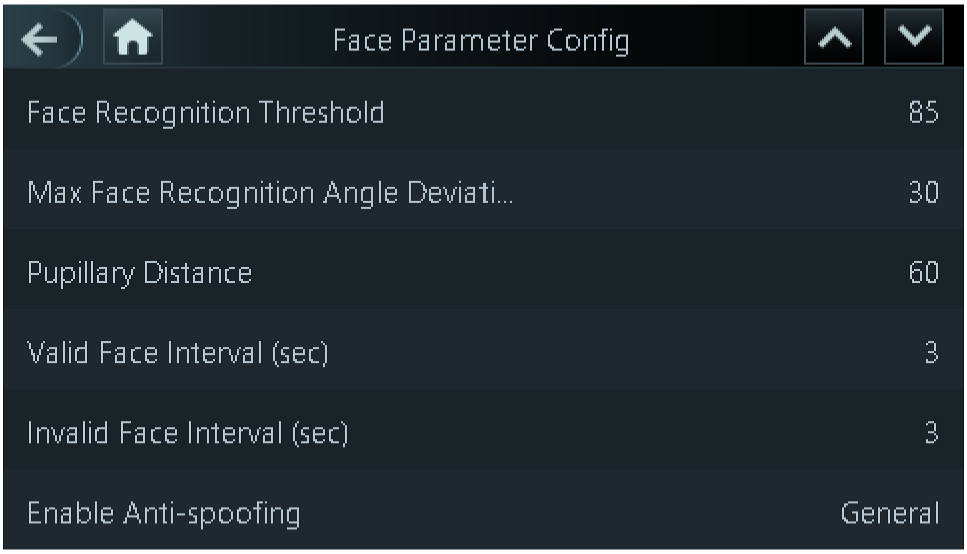
Face parameters might differ depending on the models of the Device.

Procedure

Step 1 On the main menu, select **System Settings** > **Face Parameter Config**.

Step 2 Configure the face parameters, and then tap ☑.

Figure 2-18 Face parameter



Face Parameter Config

Face Recognition Threshold 85

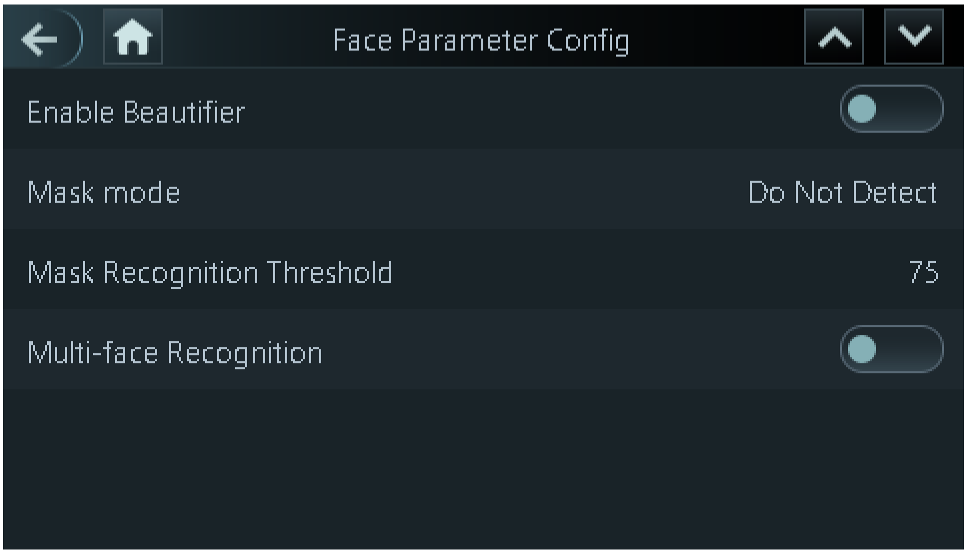
Max Face Recognition Angle Deviati... 30

Pupillary Distance 60

Valid Face Interval (sec) 3

Invalid Face Interval (sec) 3

Enable Anti-spoofing General



Enable Beautifier

Mask mode: Do Not Detect

Mask Recognition Threshold: 75

Multi-face Recognition

Table 2-9 Description of face parameters

Name	Description
Face Recognition Threshold	Adjust the accuracy level of face recognition. Higher threshold means higher accuracy and lower false recognition rate. 📖 When the threshold is too low such as 0, the false recognition rate will be extremely high. Please be advised.
Max Face Recognition Angle Deviation	Set the largest angle that a face can be posed in for face detection. The larger the value, the larger the range for the face angle. If the angle a face is positioned in is not within the defined range, it might not be detected properly.
Pupillary Distance	A certain number of pixels are required between the eyes for recognition to be successful. The default number is 45 pixels. This number changes based on the size of the face and the distance between the face and the lens. If an adult is 1.5 meters away from the lens, the pupillary distance is usually 50 - 70 px.
Valid Face Interval (sec)	When the same face remains in front of the lens after the first successful recognition, the Device will perform recognition again for the face after a defined interval.
Invalid Face Interval (sec)	When the same face remains in front of the lens after the first failed recognition, the Device will perform recognition again for the face after a defined interval.
Enable Anti-spoofing	This prevents people from being able to use photos, videos, mask and other substitutes to gain unauthorized access.
Enable Beautifier	Beautify captured face images.

Name	Description
Mask mode	● **Do Not Detect** : Mask is not detected during face recognition. ● **Mask Reminder** : Mask is detected during face recognition. If the person is not wearing a mask, the system will remind them to wear a mask, but they will still be allowed access. ● **No Authorization without Wearing Face Mask** : Mask is detected during face recognition. If a person is not wearing a mask, the system will remind them to wear masks, and access will be denied.
Mask Recognition Threshold	The higher the threshold, the more accurate face recognition will be when a person is wearing a mask, and there will be a lower false recognition rate.
Multi-face Recognition	Detects up to 4 face images at a time. The number of face images which are supported might differ depending on the model of the product.

2.8.3 Setting the Volume

You can adjust the volume of the speaker and microphone.

Procedure

Step 1 On the **Main Menu**, select **System Settings** > **Volume Settings**.

Step 2 Tap + or − to adjust the volume.

2.8.4 Configuring the Language

Change the language on the Device. On the **Main Menu**, select **System Settings** > **Language**, select the language for the Device.

2.8.5 Screen Settings

Configure when the display should turn off and the logout time.

Procedure

Step 1 On the **Main Menu**, select **System** > **Screen Settings**.

Step 2 Tap **Logout Time** or **Screen Off Settings**, and then tap + or − to adjust the time.

- Logout Time: The system goes back to the standby screen after a defined time of inactivity.
- Screen Off Settings: The system goes back to the standby screen and then the screen turns off after a defined time of inactivity.

For example, if the logout time is set to 15 seconds, and the screen off time is set to 30 seconds, the system goes back to the standby screen after 15 seconds, and then the screen will turn off after another 15 seconds.

The logout time must be less than the screen off time.

2.8.6 Restoring Factory Defaults

Procedure

Step 1 On the **Main Menu**, select **System Settings** > **Factory Defaults**.

Step 2 Restore factory defaults if necessary. Restore the factory default settings if necessary.

- **Factory Defaults** : Resets all configurations and data except for IP settings.
- **Restore to Default Settings (except for user information and logs)** : Resets all the configurations except for user information and logs.

2.8.7 Restarting the Device

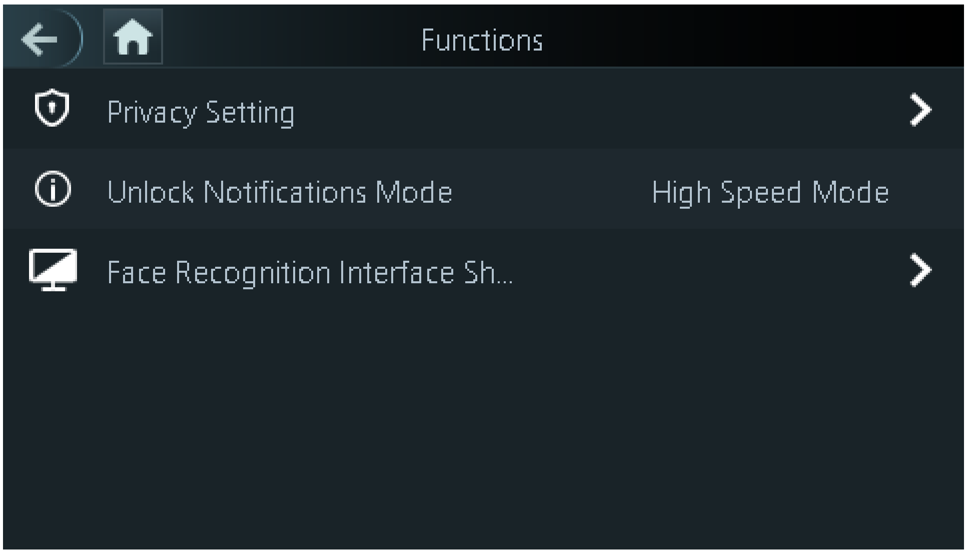
On the **Main Menu**, select **System Settings** > **Restart**, and the Device will be restarted.

2.9 Functions Settings

On the **Main Menu** screen, select **Functions**.

The functions might differ depending on the model of the product.

Figure 2-19 Functions



Functions

Privacy Setting

Unlock Notifications Mode High Speed Mode

Face Recognition Interface Sh...

Table 2-10 Function description

Parameter	Description
Private Setting	● Password Reset: The password can be reset when you turn on this function. ● Enable HTTPS: Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication over a computer network. When HTTPS is enabled, HTTPS will be used to access CGI commands; otherwise HTTP will be used. When HTTPS is enabled, the Device will automatically restart. ● Enable CGI: Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs similar to how console applications run on a server that dynamically generates webpage. The CGI is enabled by default. ● Enable SSH: Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. The data transmitted will be encrypted after this function is enabled. ● Capture: Face images will be captured automatically when people clock in or clock out. ● Clear All Snapshots: Delete all automatically captured photos.
Unlock Notification Mode	Displays the notification on the screen when a person is verifying their identity on the Device. ● High Speed Mode: The system prompts **Successfully verified** or **Not authorized** on the screen. ● Simple Mode: Displays user ID, name and verification time after access is granted, and displays **Not authorized** and the authorization time after access is denied. ● Standard: Displays the user's registered face image, user ID, name and verification time after access is granted, and displays **Not authorized** and the verification time after access is denied. ● Contrast Mode: Displays the captured face image and a registered face image of a user, user ID, name and authorization time after access is granted, and displays **Not authorized** after access is denied.
Face Recognition Interface Shortcut	Select identity verification methods on the standby screen. ● Password: The password icon is displayed on the standby screen. ● Doorbell: The doorbell icon is displayed on the standby screen. ◇ Local Device Ringer: Tap the ring bell icon on the standby screen, Device will ring. ◇ Ringtone Config: Select a ringtone ◇ Ringtone Time (sec): Set ring time (1-30 seconds). The default value is 3.

2.10 USB Management

You can use a USB to update the Device, and export or import user information or attendance records through USB.

- Make sure that a USB is inserted to the Device before you export data or update the system. To avoid failure, do not pull out the USB or perform any operation of the Device during the process.
- You can use a USB to export the information from a Device to another Device. Face images are not allowed to be imported through USB.
- Importing/exporting attendance records is only available on select models.

2.10.1 Exporting to USB

You can export data from the Device to a USB. The exported data is encrypted and cannot be edited.

Procedure

Step 1 On the **Main Menu**, select **USB Management** > **USB Export**.

Step 2 Select the data type you want to export, and then tap **OK**.

- When the data is exported in Excel, it can be edited.
- The USB disk supports the format in FAT32, and the storage capacity is 4 GB–128 GB.

Personnel information, facial features are encrypted when exporting.

2.10.2 Importing from USB

You can import data from USB to the Device.

Procedure

Step 1 On the **Main Menu**, select **USB Management** > **USB Import**.

Step 2 Select the data type that you want to export, and then tap **OK**.

2.10.3 Updating the System

Update the system of the Device through USB.

Procedure

Step 1 Rename the update file to "update.bin", put it in the root directory of the USB, and then insert the USB to the Device.

Step 2 On the **Main Menu**, select **USB Management** > **USB Update**.

Step 3 Tap **OK**.

The Device will restart when the updating completes.

Do not power off the Device during the update.

2.11 Attendance Records

On the main menu, select **Record Management** > **Search for Attendance Records**. The attendance records are displayed. You can search for record by user ID.

2.12 System Information

You can view data capacity and device version.

2.12.1 Viewing Data Capacity

On the **Main Menu**, select **System Info** > **Data Capacity**, you can view storage capacity of each data type.

2.12.2 Viewing Device Version

On the **Main Menu**, select **System Info** > **Device Version**, you can view the device version, such as serial No., software version and more.

3 Web Operations

On the webpage, you can also configure and update the Device.

Web configurations differ depending on models of the Device.

3.1 Initialization

Initialize the Device when you log in to the webpage for the first time or after the Device is restored to the factory defaults.

Prerequisites

Make sure that the computer used to log in to the webpage is on the same LAN as the Device.

Procedure

Step 1 Open a browser, go to the IP address of the Device.

We recommend you use the latest version of Chrome or Firefox.

Step 2 Select a language on Device.

Step 3 Set the password and email address according to the screen instructions.

- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case, lower case, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.
- Keep the password safe after initialization and change the password regularly to improve security.

3.2 Logging In

Procedure

Step 1 Open a browser, enter the IP address of the Device in the **Address** bar, and press the Enter key.

Step 2 Enter the user name and password.

- The default administrator name is admin, and the password is the one you set up during initialization. We recommend you change the administrator password regularly to increase security.
- If you forget the administrator login password, you can click **Forget password?** to reset password.

Step 3 Click **Login**.

3.3 Resetting the Password

Reset the password through the linked e-mail when you forget the admin password.

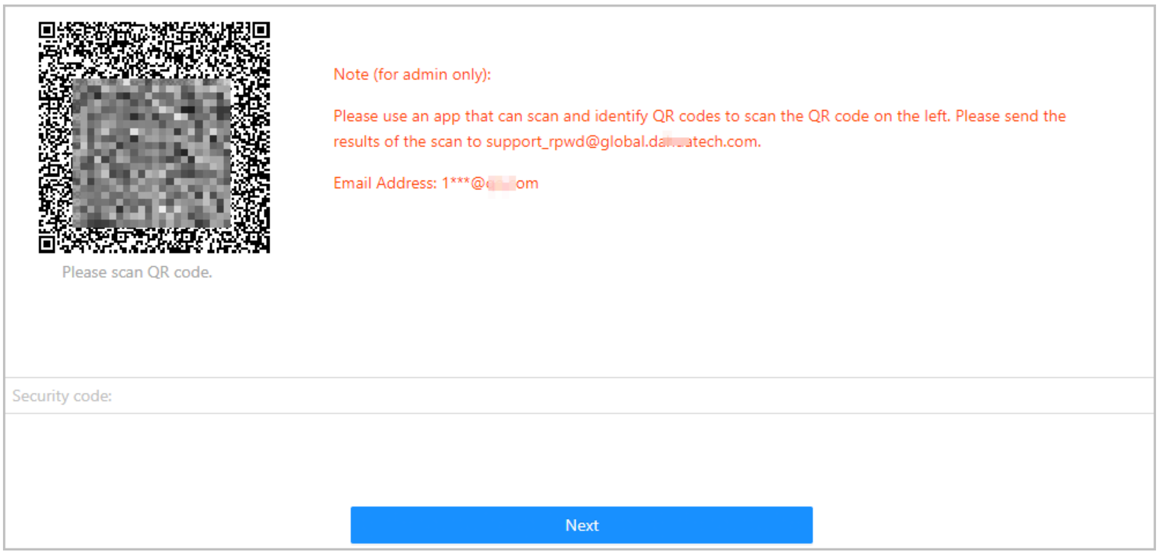
Procedure

Step 1 On the login page, click **Forgot password**.

Step 2 Read the on-screen prompt, and then click **OK**.

Step 3 Scan the QR code, and you will receive a security code.

Figure 3-1 Reset password



Please scan QR code.

Note (for admin only):

Please use an app that can scan and identify QR codes to scan the QR code on the left. Please send the results of the scan to support_rpwd@global.da[redacted]atech.com.

Email Address: 1***@[redacted]om

Security code:

- Up to two security codes will be generated when the same QR code is scanned. If the security code becomes invalid, refresh the QR code and scan again.
- After you scan the QR code, you will receive a security code in your linked e-mail address. Use the security code within 24 hours after you receive it. Otherwise, it will become invalid.
- If the wrong security code is entered 5 times in a row, the administrator account will be frozen for 5 minutes.

Step 4 Enter the security code.

Step 5 Click **Next**.

Step 6 Reset and confirm the password.

The password should consist of 8 to 32 non-blank characters and contain at least two of the following types of characters: upper case, lower case, number, and special character (excluding ' " ; : &).

Step 7 Click **OK**.

3.4 Home Page

The home page is displayed after you successfully log in.

Figure 3-2 Home page

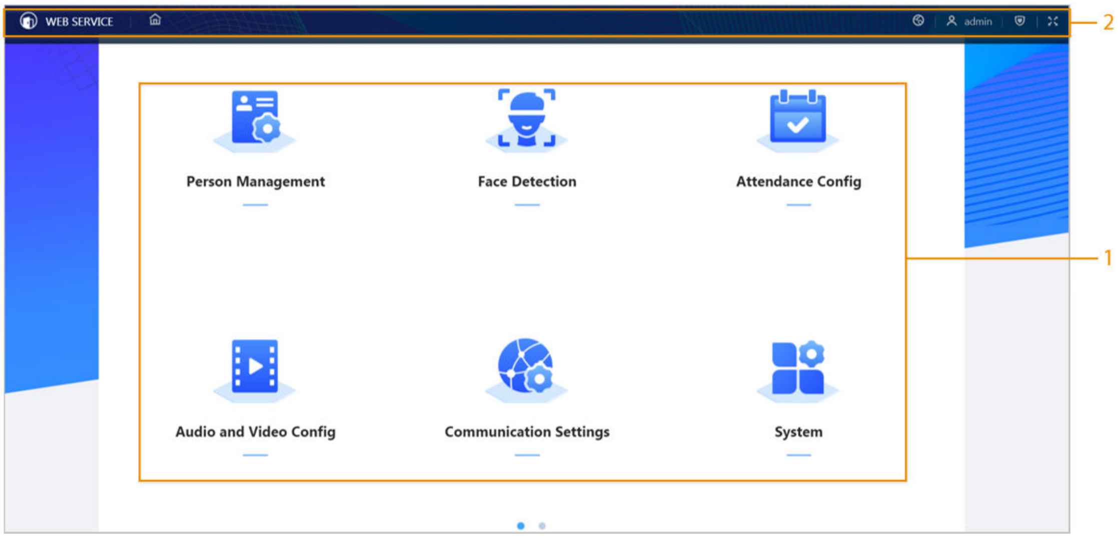


Table 3-1 Home page description

No.	Description
1	Main menu.
2	● ⌂: Enter the home page. ● ⛶: Display in full screen. ● 🛡: Enter the **Security** page. ● admin: Log out or restart the device. ● 🌐: Select a language on the device.

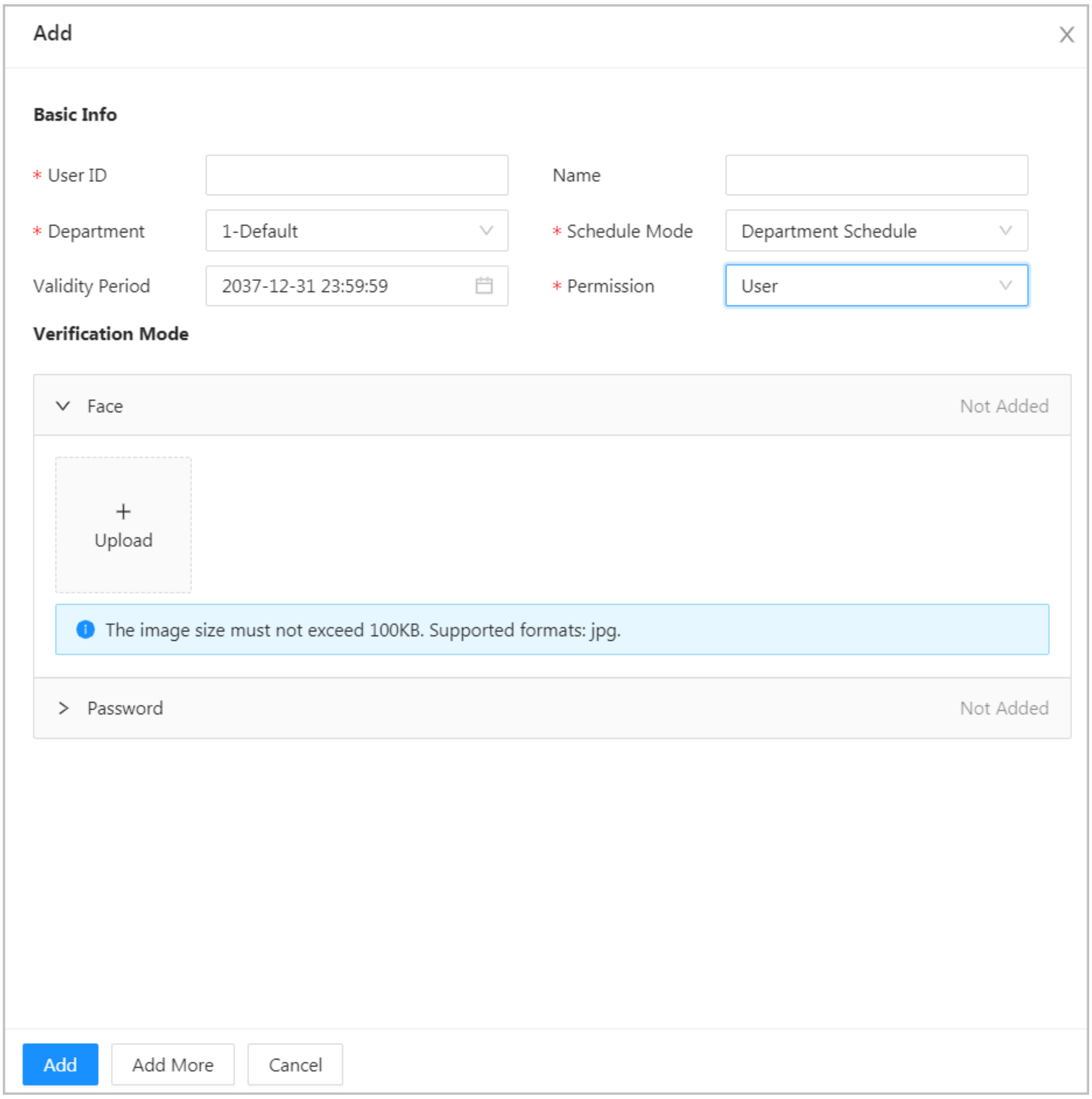
3.5 Person Management

Procedure

Step 1 On the home page, select **Person Management** , and then click **Add**.

Step 2 Configure user information.

Figure 3-3 Add users



Add

Basic Info

* User ID

Name

* Department: 1-Default

* Schedule Mode: Department Schedule

Validity Period: 2037-12-31 23:59:59

* Permission: User

Verification Mode

Face — Not Added

The image size must not exceed 100KB. Supported formats: jpg.

Password — Not Added

Table 3-2 Parameters description

Parameter	Description
User ID	The User ID. is like employee ID, which can be numbers, letters, and their combinations, and the maximum length of the number. is 30 characters.
Name	The name can have up to 32 characters (including numbers, symbols, and letters).

Parameter	Description
Department	Add users to a department. If a department schedule is assigned to the person, they will follow the established department schedule. For how to create department, see "2.6.2 Configuring Departments". ● Department Schedule: Assign department schedule to the user. For details, see "2.6.5 Configuring Work Schedules". ● Personal Schedule: Assign personal schedule to the user. For details, see "2.6.5 Configuring Work Schedules". If you set the schedule mode to department schedule here, the personal schedule you have configured for the user in **Attendance** > **Schedule Config** > **Personal Schedule** is invalid.
Schedule Mode	
Validity Period	Set a date on which the and attendance permissions of the person will be expired.
Permission	● **User** : Users only have time attendance permissions. ● **Admin** : Administrators can configure the Device besides attendance permissions.
Face	Click **Upload** to upload a face image. Each person can only add up to 2 face images. You can view or delete the face image after you upload it. The face image is in jpg format and must be less than 100 KB.
Password	Enter the user password. The maximum length of the password is 8 digits.

Step 3 Click **OK**.

Related Operations

- Import user information: Click **Export Template** , and download the template and enter user information in it. Place face images and the template in the same filepath, and then click **Import User Info** to import the folder.

  Up to 10,000 users can be imported at a time.
- Clear: Clear all users.
- Refresh: Refresh the user list.

3.6 Face Detection

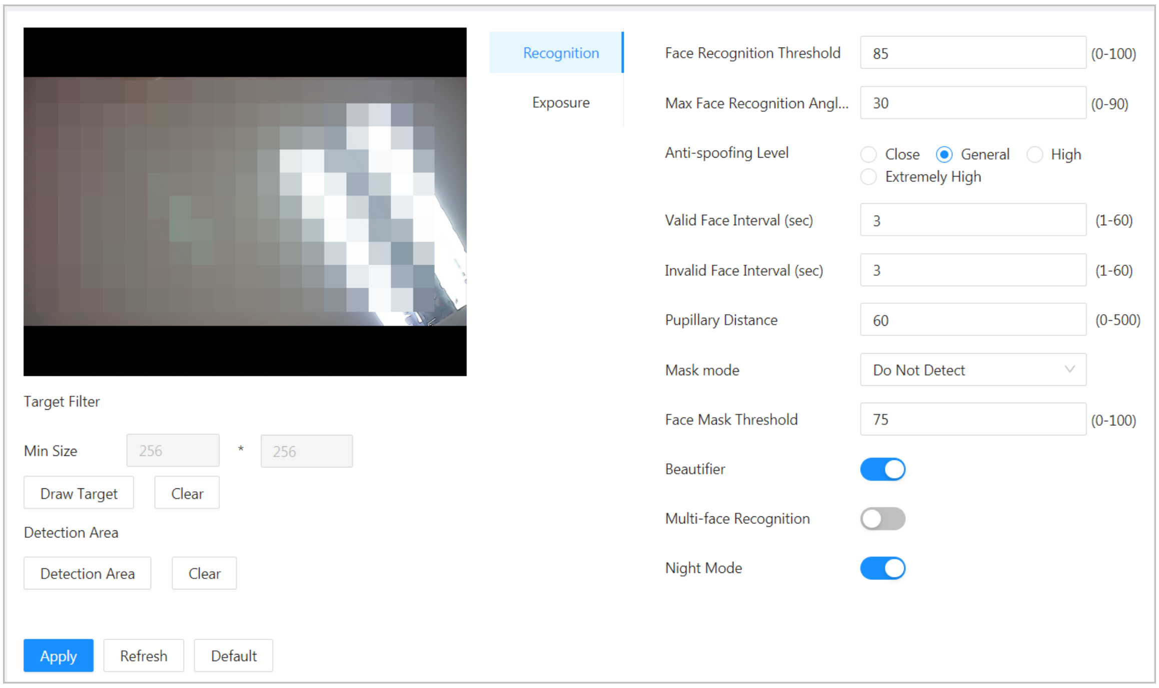
3.6.1 Configuring Face Detection

Configure face detection parameters. Face parameters might differ depending on models of the product.

Procedure

Step 1 Log in to the webpage, select **Face Detection** > **Face Detection**.

Figure 3-4 Face detection parameters



Target Filter

Min Size 256 * 256

Detection Area

Face Recognition Threshold 85 (0-100)

Max Face Recognition Angl... 30 (0-90)

Anti-spoofing Level ○ Close ● General ○ High ○ Extremely High

Valid Face Interval (sec) 3 (1-60)

Invalid Face Interval (sec) 3 (1-60)

Pupillary Distance 60 (0-500)

Mask mode Do Not Detect

Face Mask Threshold 75 (0-100)

Beautifier On

Multi-face Recognition Off

Night Mode On

Step 2 Configure the parameters.

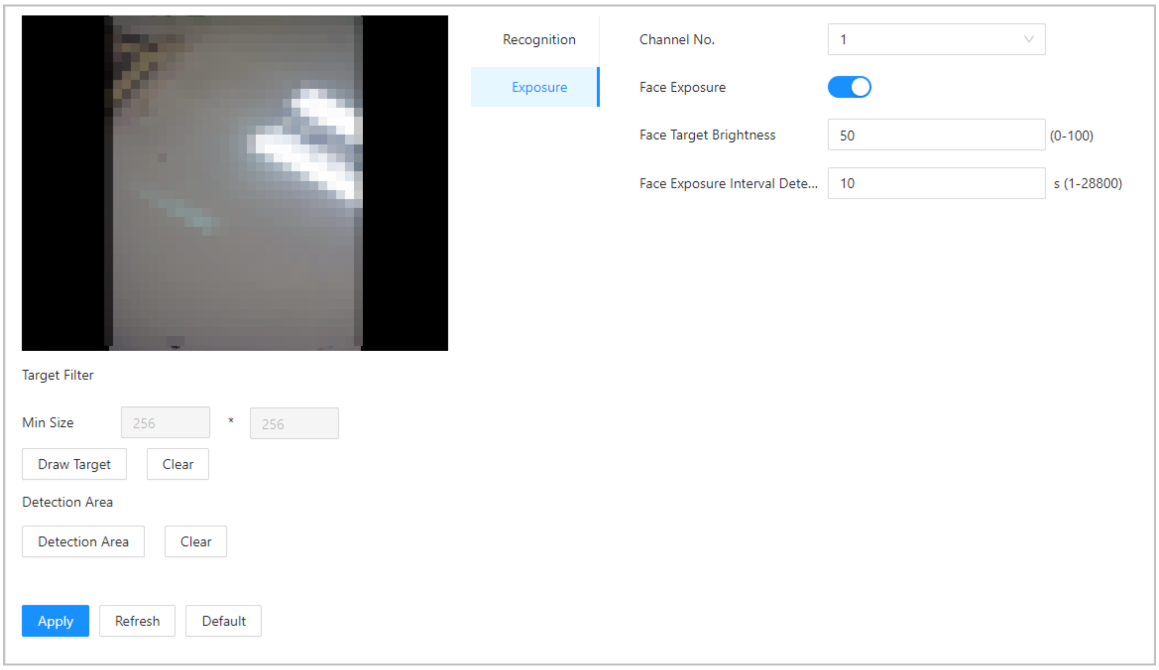
Table 3-3 Description of face parameters

Name	Description
Face Recognition Threshold	Adjust the accuracy level of face recognition. Higher threshold means higher accuracy and lower false recognition rate. When the threshold is too low such as 0, the false recognition rate will be extremely high. Please be advised.
Max Face Recognition Angle Deviation	Set the largest angle that a face can be posed in for face detection. The larger the value, the larger the range for the face angle. If the angle a face is positioned in is not within the defined range, it might not be detected properly.
Anti-spoofing Level	This prevents people from being able to use photos, videos, mask and other substitutes to gain unauthorized access.
Valid Face Interval (sec)	When the same face remains in front of the lens after the first successful recognition, the Device will perform recognition again for the face after a defined interval.

Name	Description
Invalid Face Interval (sec)	When the same face remains in front of the lens after the first failed recognition, the Device will perform recognition again for the face after a defined interval.
Pupillary Distance	A certain number of pixels are required between the eyes for recognition to be successful. The default number is 45 pixels. This number changes based on the size of the face and the distance between the face and the lens. If an adult is 1.5 meters away from the lens, the pupillary distance is usually 50 - 70 px.
Mask Mode	● **Do Not Detect** : Mask is not detected during face recognition. ● **Mask Reminder** : Mask is detected during face recognition. If the person is not wearing a mask, the system will remind them to wear a mask, but they will still be allowed access. ● **No Authorization without Wearing Face Mask** : Mask is detected during face recognition. If a person is not wearing a mask, the system will remind them to wear masks, and access will be denied.
Face Mask Threshold	The higher the threshold, the more accurate face recognition will be when a person is wearing a mask, and there will be a lower false recognition rate.
Beautifier	Beautify captured face images.
Multi-face Recognition	Detects 4 face images at a time. The number of face images which are supported might differ depending on the model of the product.
Night Mode	In dark environment, the standby screen displays white background image to improve the brightness when verifying face.

Step 3 Configure the exposure parameters.

Figure 3-5 Exposure parameters



Channel No. 1

Face Exposure: on

Face Target Brightness 50 (0-100)

Face Exposure Interval Dete... 10 s (1-28800)

Target Filter

Min Size 256 * 256

Detection Area

Table 3-4 Exposure parameters description

Parameter	Description
Channel No.	● Channel 1 is the white light mode. ● Channel 2 is the infrared light mode.
Face Exposure	After the face exposure function is enabled, the face will be exposed at the defined brightness to detect the face image clearly.
Face Target Brightness	
Face Exposure Interval Detection	The face will be exposed only once in a defined interval.

Step 4 Draw the face detection area.

1. Click **Detection Area**.
2. Right-click to draw the detection area, and then release the left button of the mouse to complete drawing.

The face in the defined area will be detected.

Step 5 Draw the target size.

1. Click **Draw Target**.
2. Draw the face recognition box to define the minimum size of detected face.

   Only when the size of the face is larger than the defined size, the face can be detected by the Device.

Step 6 Draw the detection area.

Step 7 Click **OK**.

3.6.2 Privacy Settings

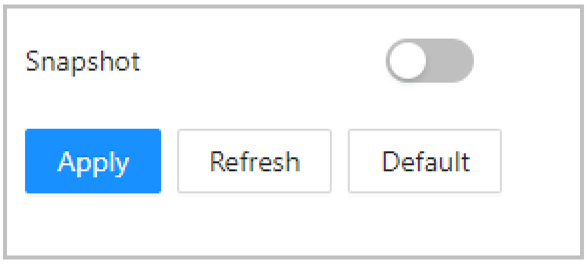
Procedure

Step 1 On the webpage, select **Access Control** > **Privacy Settings**.

Step 2 Enable snapshot function.

Face images will be captured automatically when people clock in or clock out.

Figure 3-6 Enable snapshot



Snapshot ○

Apply | Refresh | Default

Step 3 Click **Apply**.

3.7 Attendance Configuration

This function is only available on select models.

3.7.1 Configuring Departments

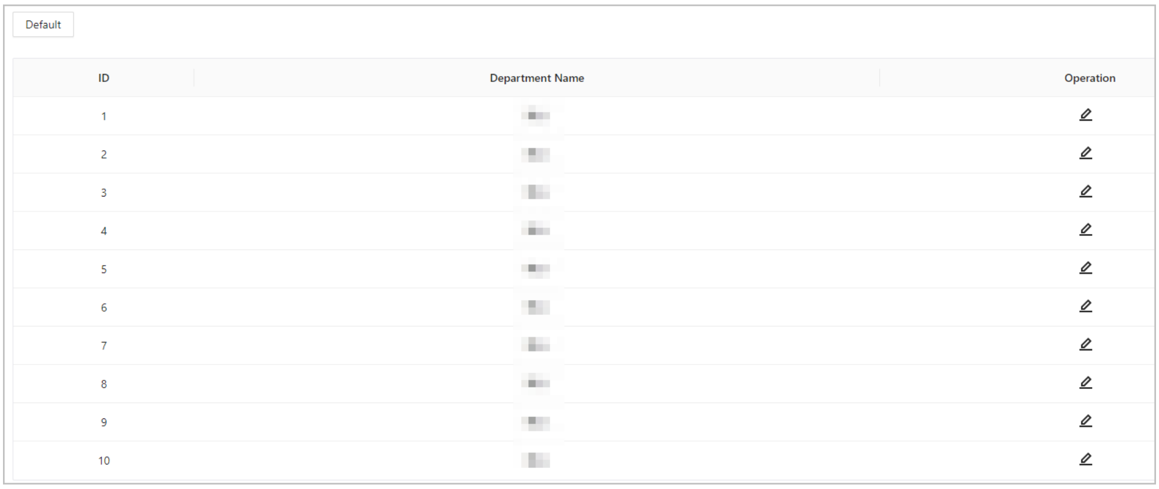
Procedure

Step 1 Select **Attendance Config** > **Department Settings**.

Step 2 Click ✎ to rename the department.

There are 20 default departments. We recommend you rename them.

Figure 3-7 Create departments



Default

ID	Department Name	Operation
1	[redacted]	✎
2	[redacted]	✎
3	[redacted]	✎
4	[redacted]	✎
5	[redacted]	✎
6	[redacted]	✎
7	[redacted]	✎
8	[redacted]	✎
9	[redacted]	✎
10	[redacted]	✎

Related Operations

You can click **Default** to restore departments to default settings.

3.7.2 Configuring Shifts

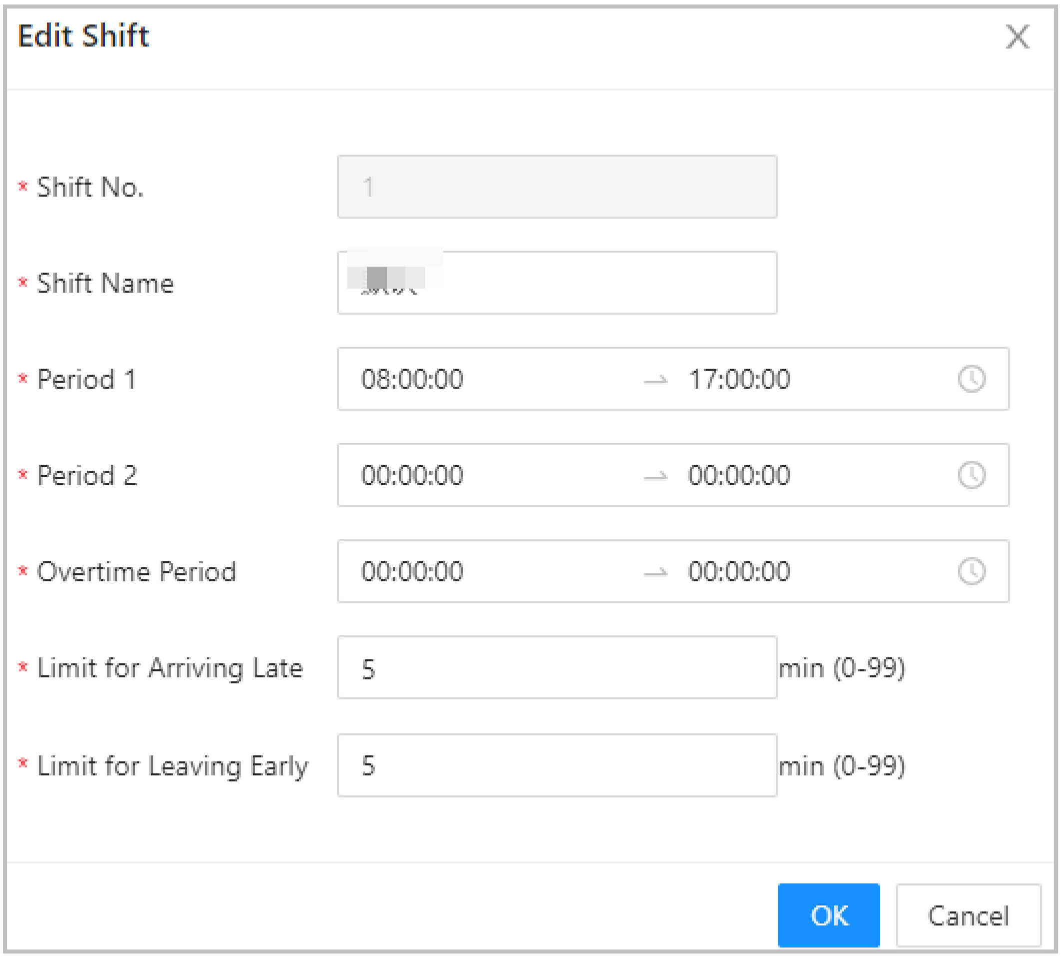
Configure shifts to define time attendance rules. Employees need to work at the time scheduled for their shift to start, and leave at the end time, except when they choose to work overtime.

Procedure

Step 1 Select **Attendance Config** > **Shift Config**.

Step 2 Click ✎ to configure the shift.

Figure 3-8 Create shifts



Edit Shift

- * Shift No.: 1
- * Shift Name: [redacted]
- * Period 1: 08:00:00 → 17:00:00
- * Period 2: 00:00:00 → 00:00:00
- * Overtime Period: 00:00:00 → 00:00:00
- * Limit for Arriving Late: 5 min (0-99)
- * Limit for Leaving Early: 5 min (0-99)

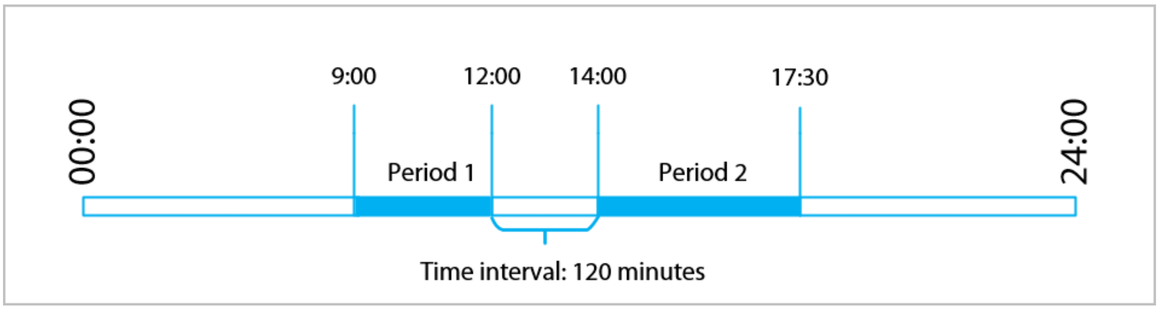
Table 3-5 Shift parameters description

Parameter	Description
Shift Name	Enter the name of the shift.

Parameter	Description
Period 1	Specify a time range when people can clock in and clock out for the workday. If you only set one attendance period, employees need to clock in and out by the designated times to avoid an anomaly appearing on their attendance record. For example, if you set 08:00 to 17:00, employees must clock in by 08:00 and clock out from 17:00 onwards. If you set 2 attendance periods, the 2 periods cannot overlap. Employees need to clock in and clock out for both periods.
Period 2	
Overtime Period	Employees who clock in or out during the defined period will be considered as working beyond their normal work hours.
Limit for Arriving Late (min)	A certain amount of time can be granted to employees to allow them to clock in a bit late and clock out a bit early. For example, if the regular time to clock in is 08:00, the tolerance period can be set as 5 minutes for employees who arrive by 08:05 to not be considered as late.
Limit for Leaving Early (min)	

- When the time interval between 2 periods is an even number, you can divide the time interval by 2, and assign the first half of the interval to the first period, which will be the clock out time. The second half of the interval should be assigned to the second period as the clock in time.

Figure 3-9 Time interval (even number)

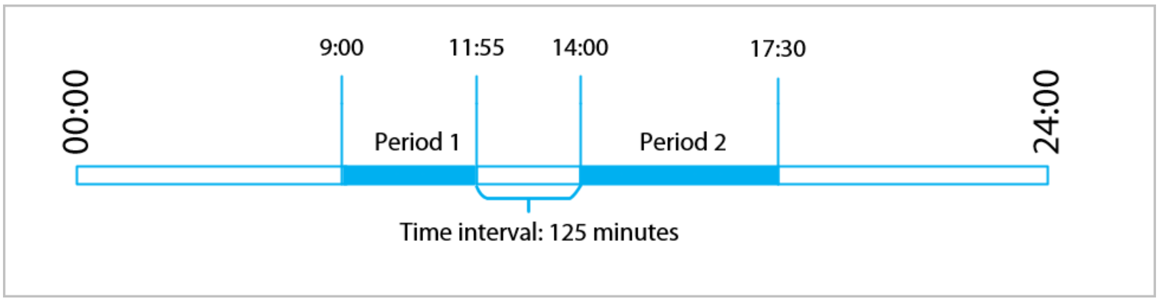


For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.

If a person clocks out multiple times during period 1, the latest time will be valid, and if they clock in multiple times during period 2, the earliest time will be valid.

- When the time interval between 2 periods is an odd number, the smallest portion of the interval will be assigned to the first period, which will be the clock out time. The largest portion of the interval will be assigned to the second period as the clock in time.

Figure 3-10 Time interval (even number)



For example: If the interval is 125 minutes, then the clock-out time for period 1 is from 11:55 to 12:57, and the clock-in time for period 2 is from 12:58 to 14:00. Period 1 has 62 minutes, and period 2 has 63 minutes.

If a person clocks out multiple times during period 1, the latest time will be valid, and if they clock in multiple times during period 2, the earliest time will be valid.

All attendance times are precise down to the second. For example, if the normal clock-in time is set to 8:05 AM, the employee who clocks in at 8:05:59 AM will not be considered as arriving late. But, the employee that arrives at 8:06 AM will be marked as late by 1 minute.

Step 3 Click **OK**.

Related Operations

You can click **Default** to restore shifts to factory defaults.

3.7.3 Configuring Holiday

Configure holiday plans to set periods for attendance to not be tracked.

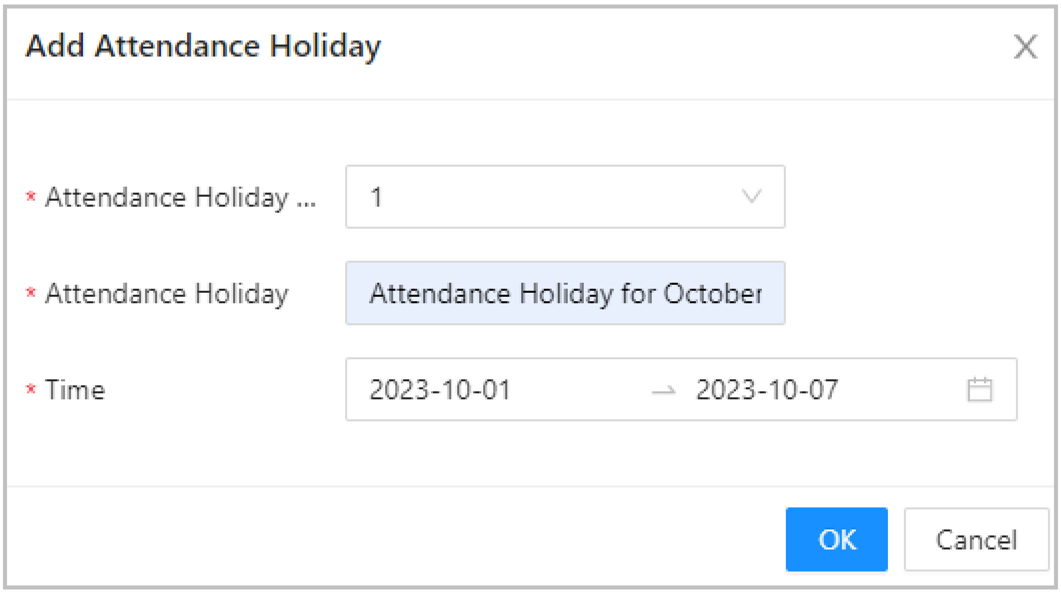
Procedure

Step 1 Select **Attendance Config** > **Shift Config** > **Holiday**.

Step 2 Click **Add** to add holiday plans.

Step 3 Configure the parameters.

Figure 3-11 Create holiday plans



Add Attendance Holiday

* Attendance Holiday ...: 1

* Attendance Holiday: Attendance Holiday for October

* Time: 2023-10-01 → 2023-10-07

Table 3-6 Parameters description

Parameter	Description
Attendance Holiday No.	The number of the holiday.
Attendance Holiday	The name of the holiday.
Start Time	The start and end time of the holiday.
End Time	

Step 4 Click **OK**.

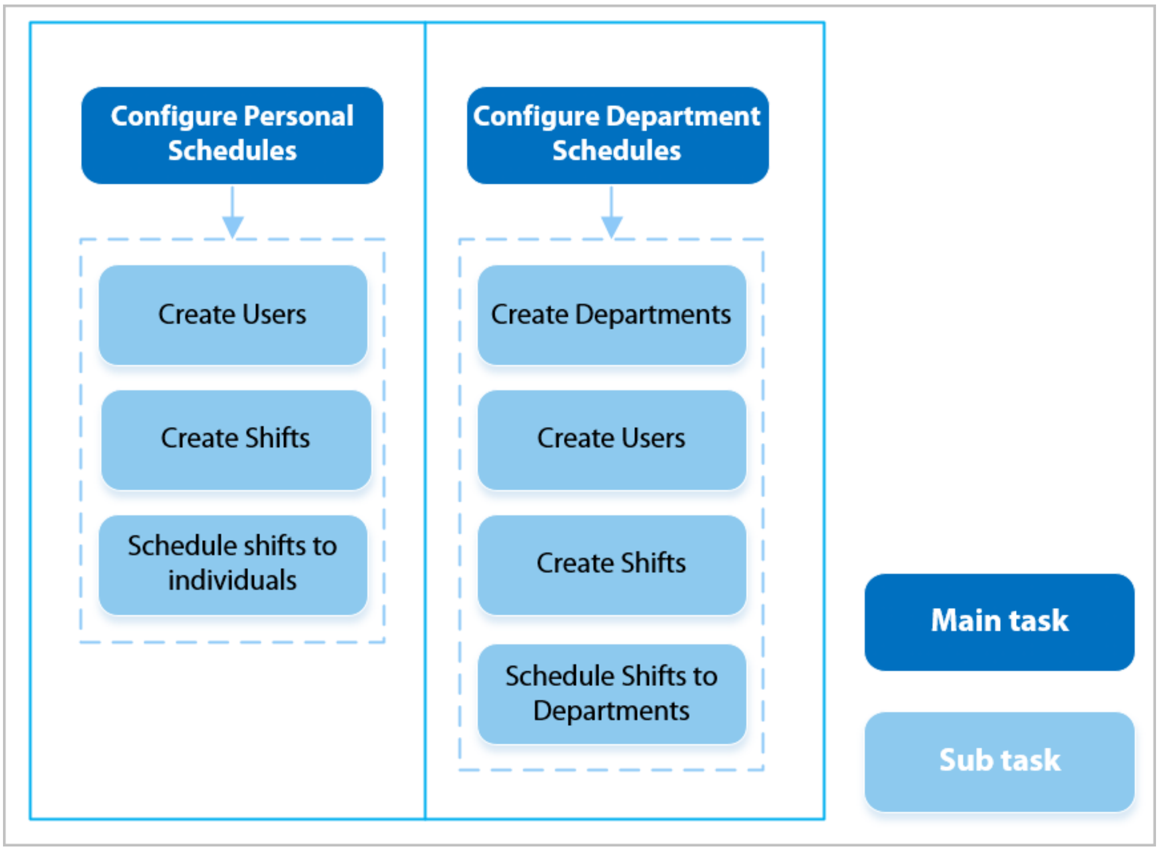
3.7.4 Configuring Work Schedules

A work schedule generally refers to the days per month and the hours per day that an employee is expected to be at their job. You can create different types of work schedules based on different individuals or departments, and then employees must follow the established work schedules.

Background Information

Refer to the flowchart to configure personal schedules or department schedules.

Figure 3-12 Configuring work schedules


Configure Personal Schedules
Create Users
Create Shifts
Schedule shifts to individuals
Configure Department Schedules
Create Departments
Create Users
Create Shifts
Schedule Shifts to Departments
Main task
Sub task

Procedure

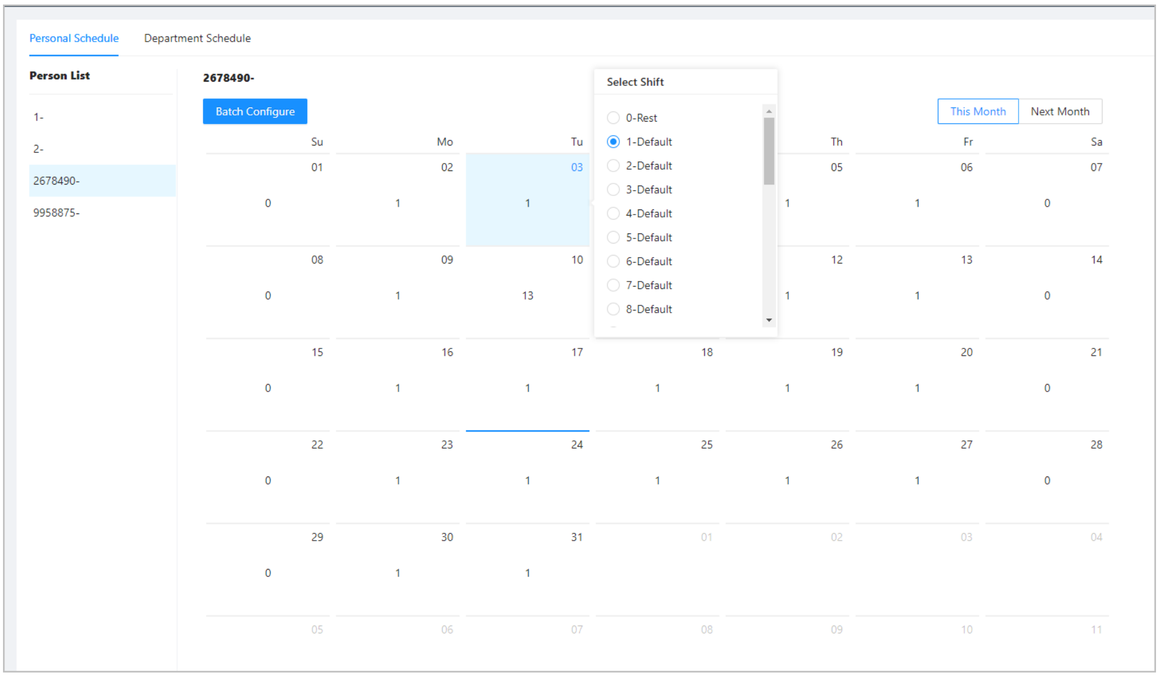
Step 1 Select **Attendance Config** > **Schedule Config**.

Step 2 Set work schedules for individuals.

1. Click **Personal Schedule**.
2. Select a person in the person list.
3. On the calendar, select a day, and then select a shift.

   You can also click **Batch Configure** to schedule shifts to multiple days.

Figure 3-13 Personal schedule



Su	Mo	Tu		Th	Fr	Sa
01 0	02 1	03 1		05 1	06 1	07 0
08 0	09 1	10 13		12 1	13 1	14 0
15 0	16 1	17 1	18 1	19 1	20 1	21 0
22 0	23 1	24 1	25 1	26 1	27 1	28 0
29 0	30 1	31 1	01	02	03	04
05	06	07	08	09	10	11

You can only set work schedules for the current month and the next month.

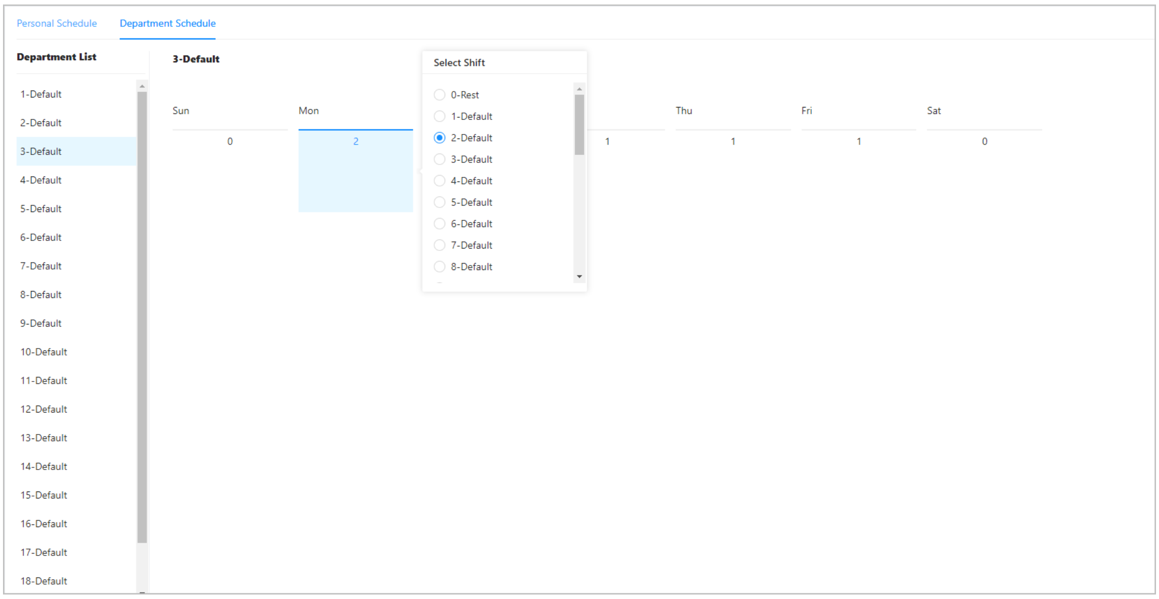
- 0 indicates break.
- 1 to 24 indicates the number of the per-defined shifts. For how to configure shifts, see "2.6.3 Configuring Shifts".
- 25 indicates business trip.
- 26 indicates leave of absence.

Step 3 Set works schedules for departments.

1. Click **Department Schedule**.
2. Select a department in the department list.
3. On the calendar, select a day, and then select a shift.

- 0 indicates rest.
- 1 to 24 indicates the number of the per-defined shifts. For how to configure shifts, see "2.6.3 Configuring Shifts".
- 25 indicates business trip.
- 26 indicates leave of absence.

Figure 3-14 Schedule shifts to a department


Personal Schedule

Department Schedule

Department List

1-Default
2-Default
3-Default
4-Default
5-Default
6-Default
7-Default
8-Default
9-Default
10-Default
11-Default
12-Default
13-Default
14-Default
15-Default
16-Default
17-Default
18-Default

3-Default

Sun 0
Mon 2
1
Thu 1
Fri 1
Sat 0

Select Shift

○ 0-Rest
○ 1-Default
● 2-Default
○ 3-Default
○ 4-Default
○ 5-Default
○ 6-Default
○ 7-Default
○ 8-Default

The defined work schedule is in a week cycle and will be applied to all employees in the department.

3.7.5 Configuring Attendance Modes

Procedure

Step 1 Select **Attendance Config** > **Attendance Config**.

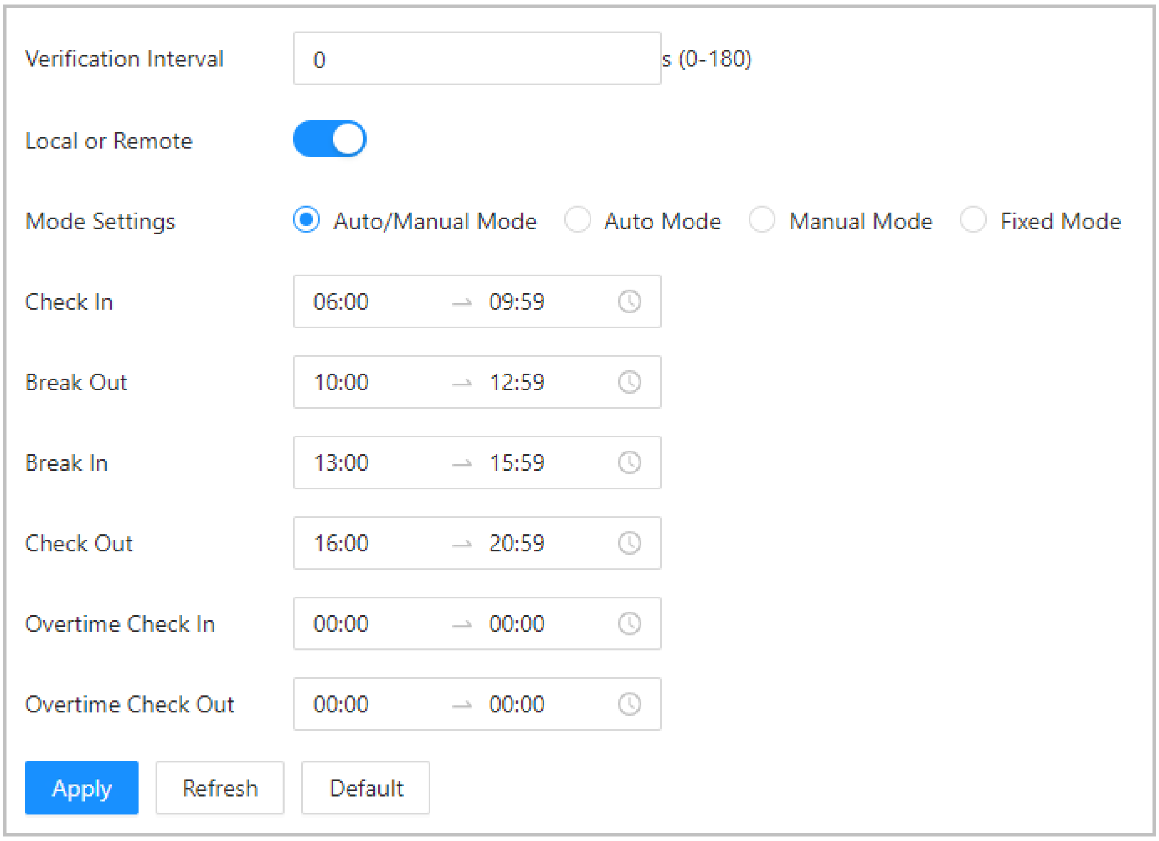
Step 2 Enter the verification interval.

When an employee clocks in and out multiple times within a set interval, the earliest time will be valid.

Step 3 Enable **Local or Remote**, and then set the attendance mode.

Step 4 Configure attendance modes.

Figure 3-15 Attendance modes



Verification Interval: 0 s (0-180)

Local or Remote: on

Mode Settings: ● Auto/Manual Mode ○ Auto Mode ○ Manual Mode ○ Fixed Mode

Check In: 06:00 → 09:59

Break Out: 10:00 → 12:59

Break In: 13:00 → 15:59

Check Out: 16:00 → 20:59

Overtime Check In: 00:00 → 00:00

Overtime Check Out: 00:00 → 00:00

Table 3-7 Attendance mode

Parameter	Description
Auto/Manual Mode	The screen displays the attendance status automatically after you clock in or out, but you can also manually change your attendance status. ● Check In: Clock in when your normal workday starts. ● Break Out: Clock out when your break starts. ● Break In: Clock in when your break ends. ● Check Out: Clock out when your normal workday starts. ● Overtime Check In: Clock in when your overtime period starts. ● Overtime Check Out: Clock out when your overtime period ends.
Auto Mode	The screen displays your attendance status automatically after you clock in or out. ● Check In: Clock in when your normal workday starts. ● Break Out: Clock out when your break starts. ● Break In: Clock in when your break ends. ● Check Out: Clock out when your normal workday starts. ● Overtime Check In: Clock in when your overtime period starts. ● Overtime Check Out: Clock out when your overtime period ends.
Manual Mode	Manually select your attendance status when you clock in or out.
Fixed Mode	When you clock in or out, the screen will display the per-defined attendance status all the time.

Step 5 Click **Apply**.

Related Operations

- Refresh: If you do not want to the save the current changes, click **Refresh** to cancel changes and restore it to previous settings.
- Default: Restore the attendance settings to factory defaults.

3.8 Configuring Audio and Video

3.8.1 Configuring Video

On the home page, select **Audio and Video Config** > **Video**, and then configure the video parameters.

Background Information

- Channel No.: Channel 1 is for configurations of visible light image. Channel 2 is for configurations of infrared light image.
- Default: Restore to defaults settings.
- Capture: Take a snapshot of the current image.

3.8.1.1 Configuring Channel 1

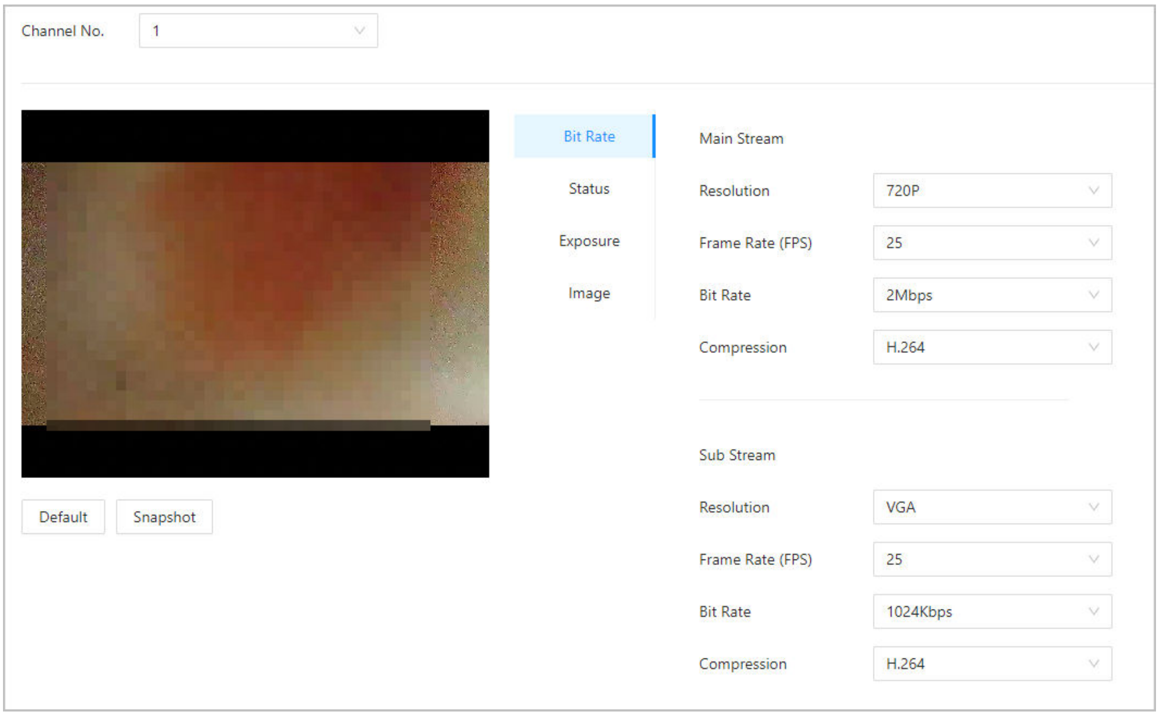
Procedure

Step 1 Select **Audio and Video Config** > **Video**.

Step 2 Select **1** from the **Channel No.** list.

Step 3 Configure the bit rate.

Figure 3-16 Date rate



Channel No. 1

Main Stream

Resolution	720P
Frame Rate (FPS)	25
Bit Rate	2Mbps
Compression	H.264

Sub Stream

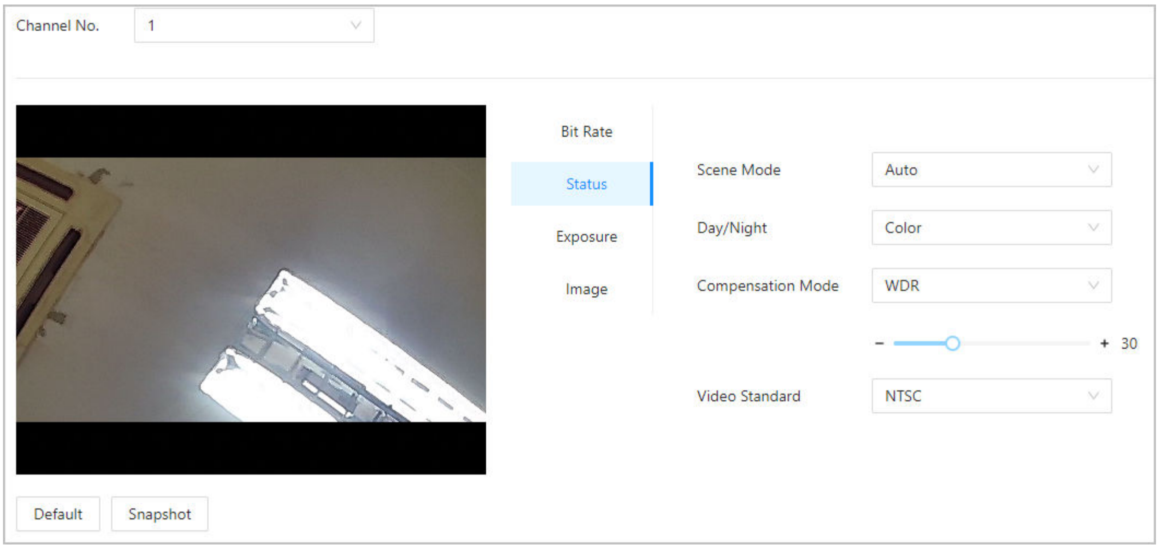
Resolution	VGA
Frame Rate (FPS)	25
Bit Rate	1024Kbps
Compression	H.264

Table 3-8 Bit rate description

Parameter		Description
Main Format	Resolution	📖 When the Device functions as the a VTO and connects the VTH, the acquired stream limit of VTH is 720p.When resolution is changed to 1080p, the call and monitor function might be affected.
	Frame Rate (FPS)	The number of frames (or images) per second.
	Bit Rate	The amount of data transmitted over an internet connection in a given amount of time. Select a proper bandwidth based on your network speed.
	Compression	Video compression standard to deliver good video quality at lower bit rates.
Sub Stream	Resolution	The sub-stream supports D1, VGA and QVGA.
	Frame Rate (FPS)	The number of frames (or images) per second.
	Bit Rate	It indicates the amount of data transmitted over an internet connection in a given amount of time.
	Compression	Video compression standard to deliver good video quality at lower bit rates.

Step 4 Configure the status.

Figure 3-17 Status



Channel No. 1

Scene Mode Auto

Day/Night Color

Compensation Mode WDR

− + 30

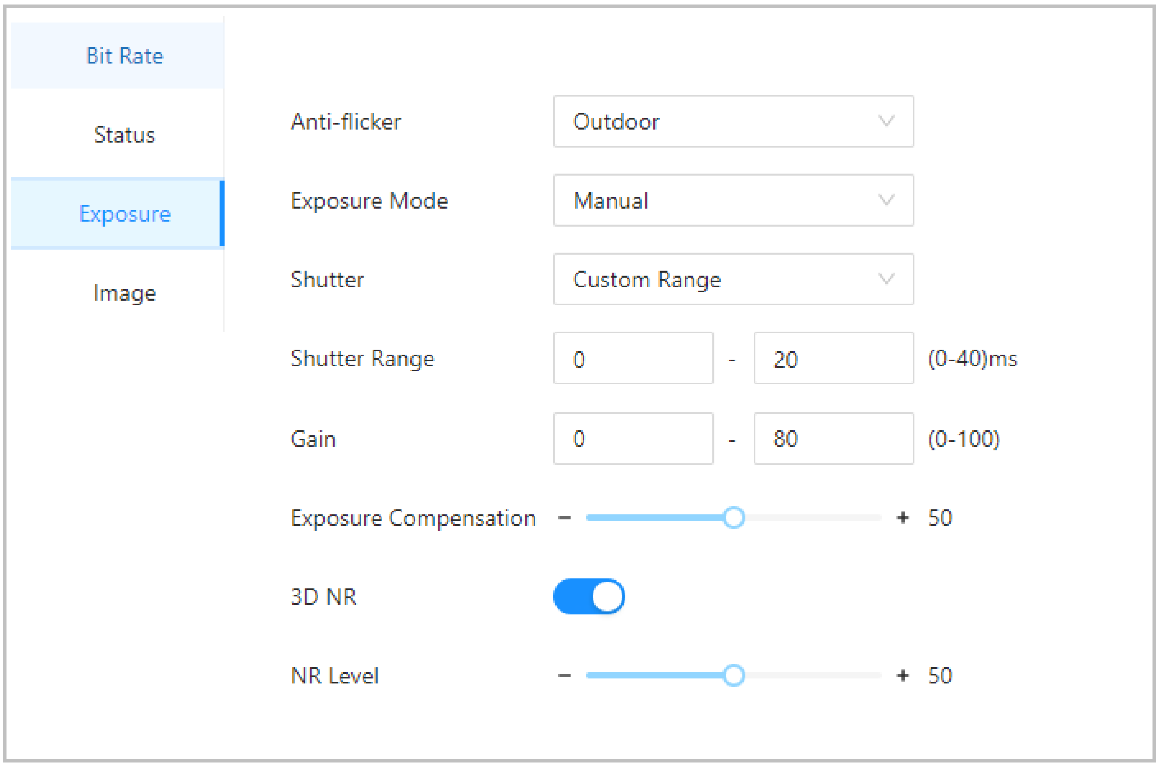
Video Standard NTSC

Table 3-9 Parameters description of status

Parameter	Description
Scene Mode	The image hue is different in different scene mode. ● **Close** : Scene mode function is turned off. ● **Auto** : The system automatically adjusts the scene mode based on the photographic sensitivity. ● **Sunny** : In this mode, image hue will be reduced. ● **Night** : In this mode, image hue will be increased.
Day/Night	Day/Night mode affects light compensation in different situations. ● **Auto** : The system automatically adjusts the day/night mode based on the photographic sensitivity. ● **Colorful** : In this mode, images are colorful. ● **Black and white** : In this mode, images are in black and white.
Compensation Mode	● **Disable** : Compensation is turned off. ● **BLC** : Backlight compensation automatically brings more light to darker areas of an image when bright light shining from behind obscures it. ● **WDR** : The system dims bright areas and compensates for dark areas to create a balance to improve the overall image quality. ● **HLC** : Highlight compensation (HLC) is a technology used in CCTV/IP security cameras to deal with images that are exposed to lights like headlights or spotlights. The image sensor of the camera detects strong lights in the video and reduces exposure in these spots to enhance the overall quality of the image.

Step 5 Configure the exposure parameters.

Figure 3-18 Exposure



Anti-flicker: Outdoor

Exposure Mode: Manual

Shutter: Custom Range

Shutter Range: 0 - 20 (0-40)ms

Gain: 0 - 80 (0-100)

Exposure Compensation: 50

3D NR

NR Level: 50

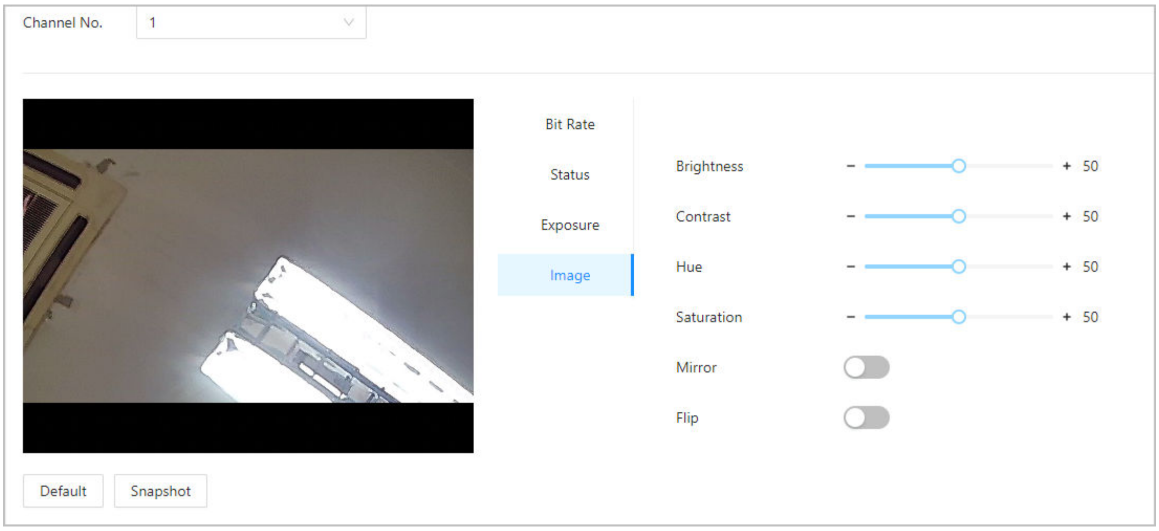
Table 3-10 Exposure parameter description

Parameter	Description
Anti-flicker	Set anti-flicker to reduce flicker and decrease or reduce uneven colors or exposure. ● **50Hz** : When the mains electricity is 50 Hz, the exposure is automatically adjusted based on brightness of the surroundings to prevent the appearance of horizontal lines. ● **60Hz** : When the mains electricity is 60 Hz, the exposure is automatically adjusted based on brightness of the surroundings to reduce the appearance of horizontal lines. ● **Outdoor** : When **Outdoor** is selected, the exposure mode can be switched.

Parameter	Description
Exposure Mode	You can set the exposure to adjust image brightness. ● **Auto** : The Device automatically adjusts the brightness of images based the surroundings. ● **Shutter Priority** : The Device adjust the image brightness according to the set range of the shutter. If the image is not bright enough but the shutter value has reached its upper or lower limit, the Device will automatically adjust the gain value for ideal brightness level. ● **Manual** : You can manually adjust the gain and shutter value to adjust image brightness. ◇ When you select **Outdoor** from the **Anti-flicker** list, you can select **Shutter Priority** as the exposure mode. ◇ Exposure mode might differ depending on models of Device.
Shutter	Shutter is a component that allows light to pass for a determined period. The higher the shutter speed, the shorter the exposure time, and the darker the image. You can select a shutter range or add a custom range.
Gain	When the gain value range is set, video quality will be improved.
Exposure Compensation	The video will be brighter by adjusting exposure compensation value.
3D NR	When 3D Noise Reduction (RD) is turned on, video noise can be reduced to ensure higher definition of videos.
NR Level	You can set its grade when this function is turned on. Higher grade means clearer image.

Step 6 Configure the image.

Figure 3-19 Image



Channel No. 1

Brightness 50

Contrast 50

Hue 50

Saturation 50

Mirror

Flip

Table 3-11 Image description

Parameter	Description
Brightness	The brightness of the image. Higher value means brighter images.

Parameter	Description
Contrast	Contrast is the difference in the luminance or color that makes an object distinguishable. The larger the contrast value is, the greater the color contrast will be.
Hue	Refers to the strength or saturation of a color. It describes the color intensity, or how pure it is.
Saturation	Color saturation indicates the intensity of color in an image. As the saturation increases, the appear stronger, for example being more red or more blue. The saturation value does not change image brightness.
Mirror	When the function is turned on, images will be displayed with the left and right side reversed.
Flip	When this function is turned on, images can be flipped over.

3.8.1.2 Configuring Channel 2

Procedure

Step 1 Select **Audio and Video Config** > **Video**.

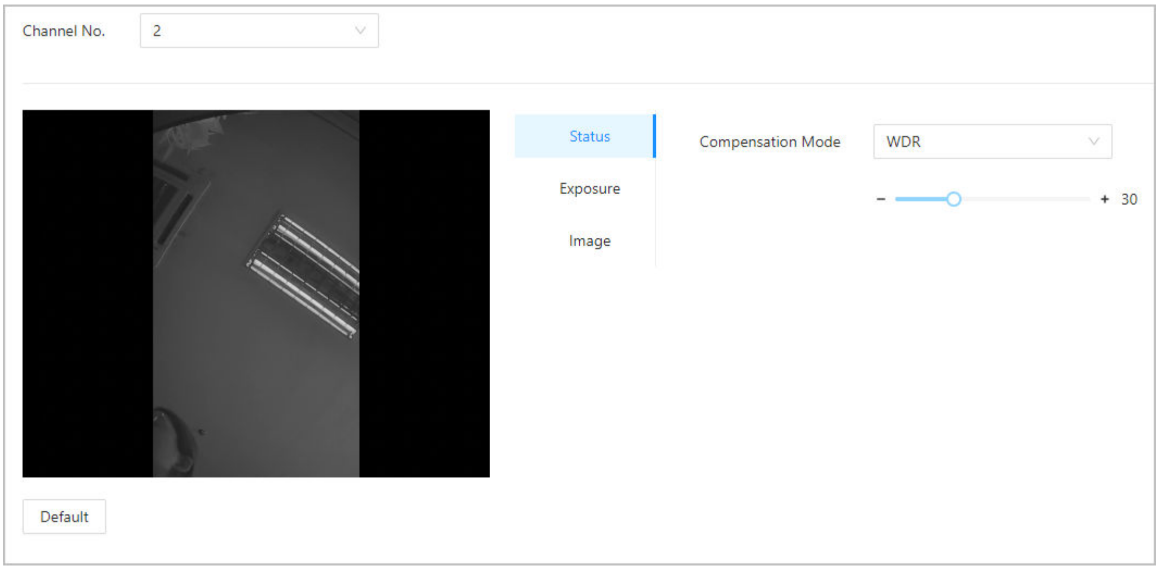
Step 2 Select **2** from the **Channel No.** list.

Step 3 Select 2 from the **Channel No.**.

Step 4 Configure the video status.

We recommend you turn on the WDR function when the face is in back-lighting.

Figure 3-20 Configure status



Channel No. 2

Compensation Mode WDR

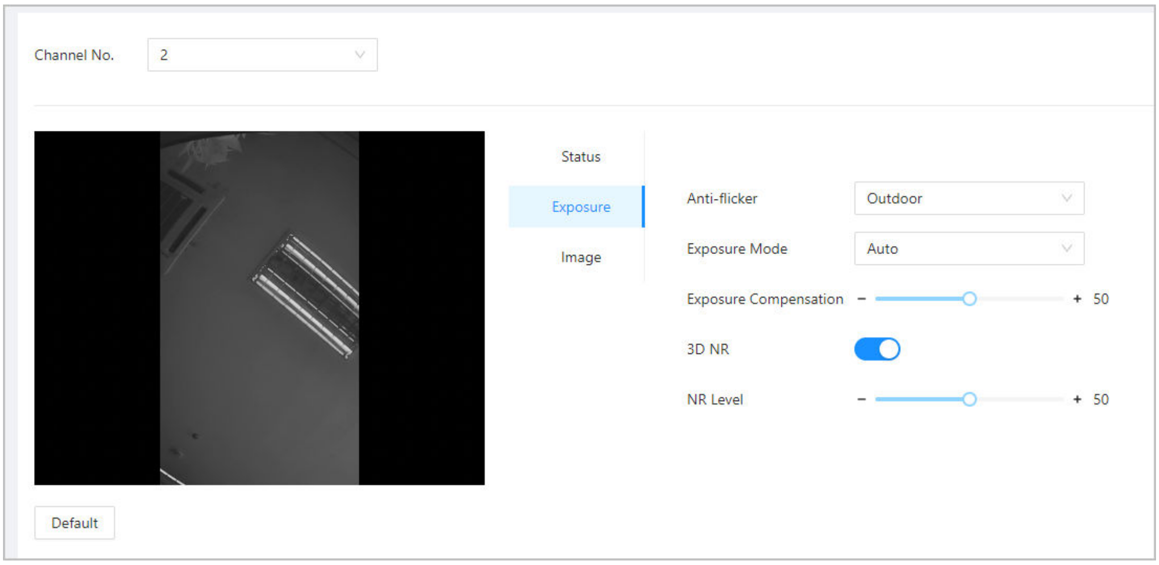
− + 30

Table 3-12 Status description

Parameter	Description
Compensation Mode	● **Disable** : Compensation is turned off. ● **BLC** : Backlight compensation automatically brings more light to darker areas of an image when bright light shining from behind obscures it. ● **WDR** : The system dims bright areas and compensates for dark areas to create a balance to improve the overall image quality. ● **HLC** : Highlight compensation (HLC) is a technology used in CCTV/IP security cameras to deal with images that are exposed to lights like headlights or spotlights. The image sensor of the camera detects strong lights in the video and reduces exposure in these spots to enhance the overall quality of the image.

Step 5 Configure the exposure parameters.

Figure 3-21 Exposure parameter



Channel No. 2

Anti-flicker: Outdoor

Exposure Mode: Auto

Exposure Compensation: 50

3D NR: on

NR Level: 50

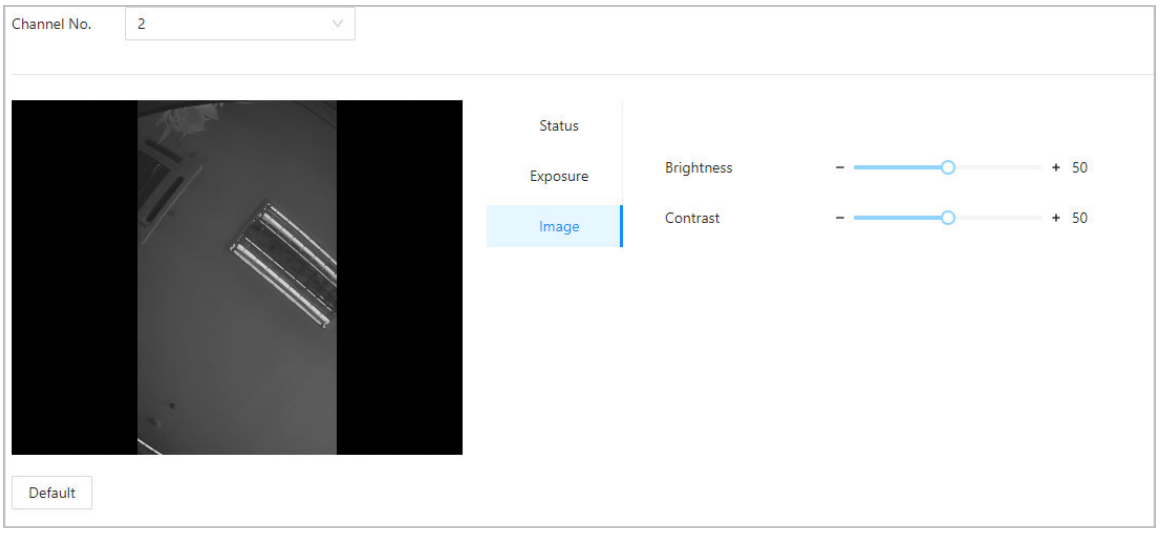
Table 3-13 Exposure parameter description

Parameter	Description
Anti-flicker	Set anti-flicker to reduce flicker and decrease or reduce uneven colors or exposure. ● **50Hz** : When the mains electricity is 50 Hz, the exposure is automatically adjusted based on brightness of the surroundings to prevent the appearance of horizontal lines. ● **60Hz** : When the mains electricity is 60 Hz, the exposure is automatically adjusted based on brightness of the surroundings to reduce the appearance of horizontal lines. ● **Outdoor** : When **Outdoor** is selected, the exposure mode can be switched.

Parameter	Description
Exposure Mode	You can set the exposure to adjust image brightness. ● **Auto** : The Device automatically adjusts the brightness of images based the surroundings. ● **Shutter Priority** : The Device adjust the image brightness according to the set range of the shutter. If the image is not bright enough but the shutter value has reached its upper or lower limit, the Device will automatically adjust the gain value for ideal brightness level. ● **Manual** : You can manually adjust the gain and shutter value to adjust image brightness. ◇ When you select **Outdoor** from the **Anti-flicker** list, you can select **Shutter Priority** as the exposure mode. ◇ Exposure mode might differ depending on models of Device.
Exposure Compensation	The video will be brighter by adjusting exposure compensation value.
3D NR	When 3D Noise Reduction (RD) is turned on, video noise can be reduced to ensure higher definition of videos.
NR Level	You can set its grade when this function is turned on. Higher grade means clearer image.

Step 6 Configure the image parameters.

Figure 3-22 Image parameters



Channel No. 2

Brightness 50

Contrast 50

Table 3-14 Image description

Parameter	Description
Brightness	The brightness of the image. Higher value means brighter images.
Contrast	Contrast is the difference in the luminance or color that makes an object distinguishable. The larger the contrast value is, the greater the color contrast will be.

3.8.2 Configuring Audio Prompts

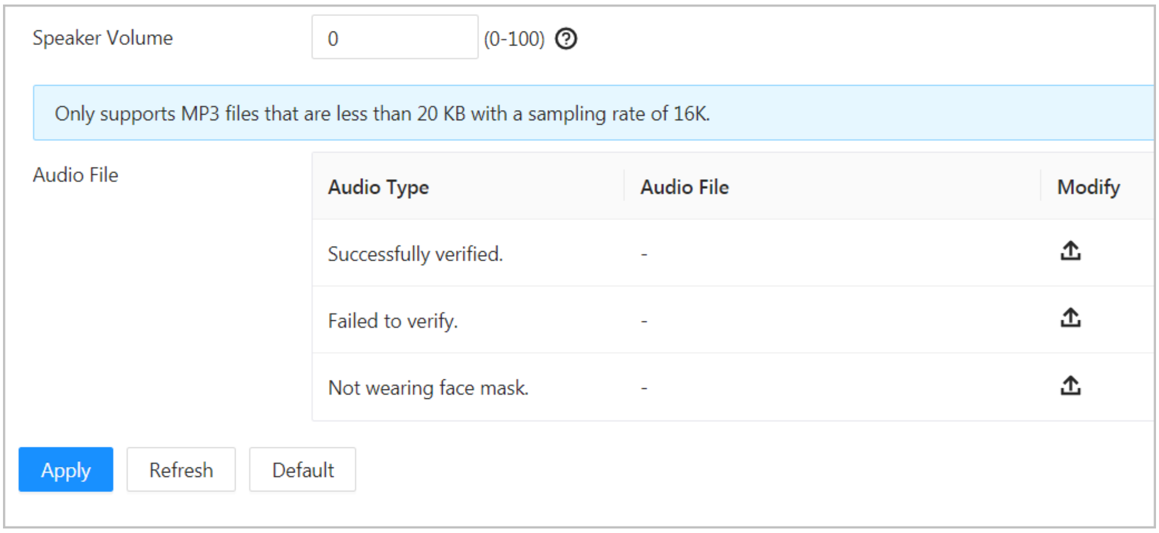
Set audio prompts during identity verification.

Procedure

Step 1 Select **Audio and Video Config** > **Audio**.

Step 2 Configure the audio parameters.

Figure 3-23 Configure audio parameters



Speaker Volume 0 (0-100)

Only supports MP3 files that are less than 20 KB with a sampling rate of 16K.

Audio File

Audio Type	Audio File	Modify
Successfully verified.	-	⬆
Failed to verify.	-	⬆
Not wearing face mask.	-	⬆

Table 3-15 Parameters description

Parameters	Description
Speaker	Set the volume of the speaker.
Audio File	Click Upload audio files to the platform.

Step 3 Click ⬆ to upload audio files to platform for each audio type.

Only supports MP3 files that are less than 20 KB with a sampling rate of 16 K.

Step 4 Click **Apply**.

3.8.3 Configuring Motion Detection

When there are moving objects detected and reaches the set threshold, the screen will be awaken.

Procedure

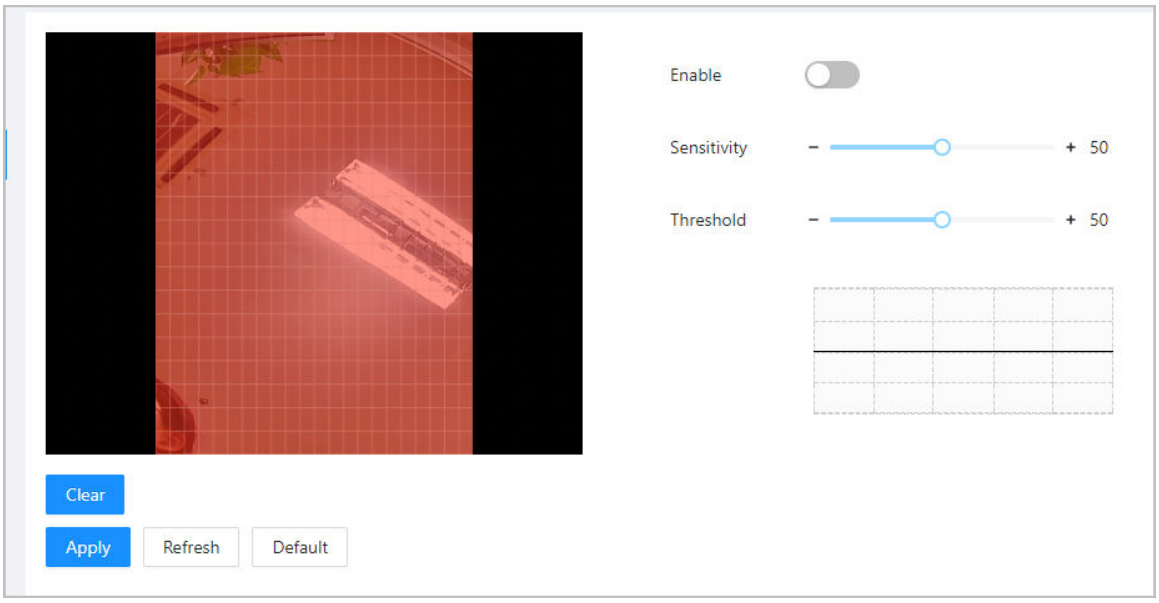
Step 1 Select **Audio and Video Config** > **Motion Detection Settings**.

Step 2 Enable the motion detection function.

Step 3 Press and hold the left mouse button, and then draw a detection area in the red area.

- The motion detection area is displayed in red.
- To remove the existing the motion detection area, click **Clear**.
- The motion detection area you draw will be a non-motion detection area if you draw in the default motion detection area.

Figure 3-24 Motion detection area



Step 4 Configure the parameters.

- Sensitivity: The sensible to the surroundings. Higher sensitivity means easier to trigger alarms.
- Threshold: The percentage of the moving object area in the motion detection area. Higher threshold means easier to trigger alarms.

Step 5 Click **Apply**.

The motion detection is triggered when the red lines are displayed; the green lines are displayed when it is not triggered.

3.9 Communication Settings

3.9.1 Configuring Wi-Fi

Procedure

Step 1 Select **Communication Settings** > **Network Setting** > **Wi-Fi**.

Step 2 Turn on Wi-Fi.

All available Wi-Fi are displayed.

Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

Step 3 Tap +, and then enter the password of the Wi-Fi.

3.9.2 Configuring Port

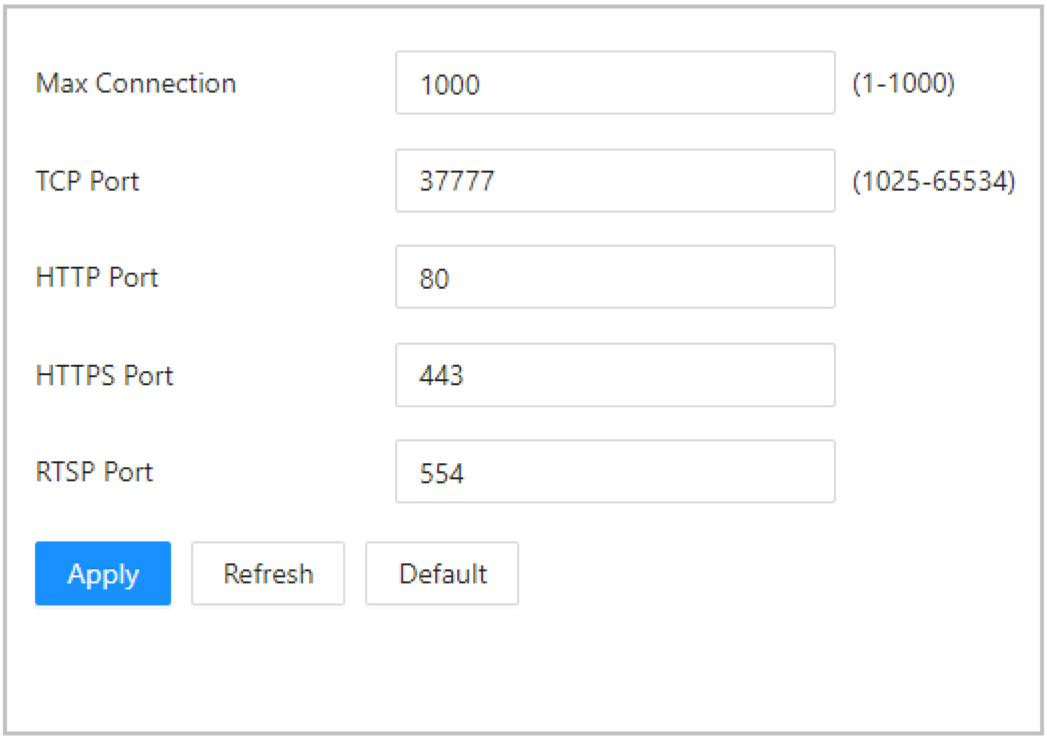
You can limit access to the Device at the same time through webpage, desktop client and mobile client.

Procedure

Step 1 Select **Communication Settings** > **Network Setting** > **Port**.

Step 2 Configure the ports.

Figure 3-25 Configure ports



Max Connection 1000 (1-1000)

TCP Port 37777 (1025-65534)

HTTP Port 80

HTTPS Port 443

RTSP Port 554

Except for **Max Connection** and **RTSP Port**, you need to restart the Device to make the configurations effective after you change other parameters.

Table 3-16 Description of ports

Parameter	Description
Max Connection	You can set the maximum number of clients (such as webpage, desktop client and mobile client) that can access the Device at the same time.
TCP Port	Default value is 37777.
HTTP Port	Default value is 80. If you have changed the port number, add the port number after the IP address when access the webpage.
HTTPS Port	Default value is 443.
RTSP Port	Default value is 554.

Step 3 Click **Apply**.

3.9.3 Configuring Basic Service

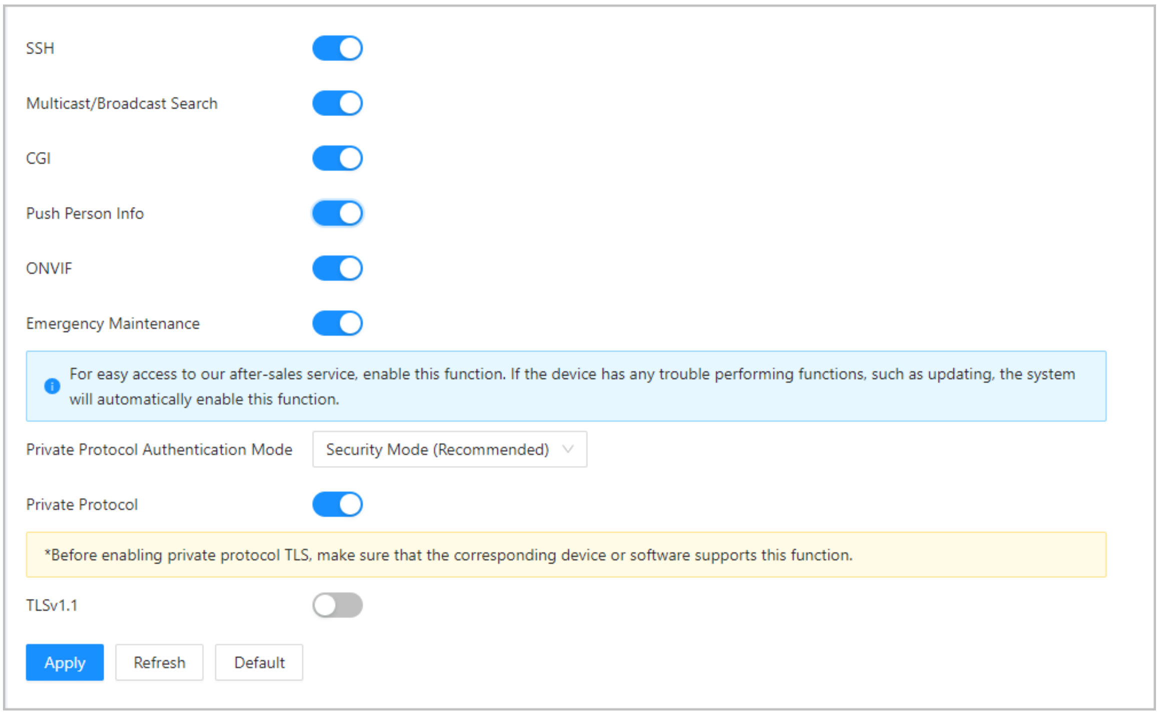
When you want to connect the Device to a third-party platform, turn on the CGI and ONVIF functions.

Procedure

Step 1 Select **Network Settings** > **Basic Services**.

Step 2 Configure the basic service.

Figure 3-26 Basic service



SSH: on

Multicast/Broadcast Search: on

CGI: on

Push Person Info: on

ONVIF: on

Emergency Maintenance: on

For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function.

Private Protocol Authentication Mode: Security Mode (Recommended)

Private Protocol: on

*Before enabling private protocol TLS, make sure that the corresponding device or software supports this function.

TLSv1.1: off

Table 3-17 Basic service parameter description

Parameter	Description
SSH	SSH, or Secure Shell Protocol, is a remote administration protocol that allows users to access, control, and modify their remote servers over the Internet.
Mutlicast/Broadcast Search	Search for devices through multicast or broadcast protocol.
CGI	The Common Gateway Interface (CGI) is an intersection between web servers through which the standardized data exchange between external applications and servers is possible.
Push Person Info	When the user information is updated or new users are added, the Device will automatically push user information to the management platform.
ONVIF	ONVIF stands for Open Network Video Interface Forum. Its aim is to provide a standard for the interface between different IP-based security devices. These standardized ONVIF specifications are like a common language that all devices can use to communicate.

Parameter	Description
Emergency Maintenance	It is turned on by default.
Private Protocol Authentication Mode	Set the authentication mode, including safe mode and compatibility mode. It is recommended to choose **Security Mode**. ● Security Mode (recommended): Does not support accessing the device through Digest, DES, and plaintext authentication methods, improving device security. ● Compatible Mode: Supports accessing the device through Digest, DES, and plaintext authentication methods, with reduced security.
Private Protocol	The platform adds devices through TLSv1.1 protocol. 📖 Security risks might present when TLSv1.1 is enabled. Please be advised.

Step 3 Click**Apply**.

3.9.4 Configuring Cloud Service

The cloud service provides a NAT penetration service. Users can manage multiple devices through DMSS. You do not have to apply for dynamic domain name, configure port mapping or deploy server.

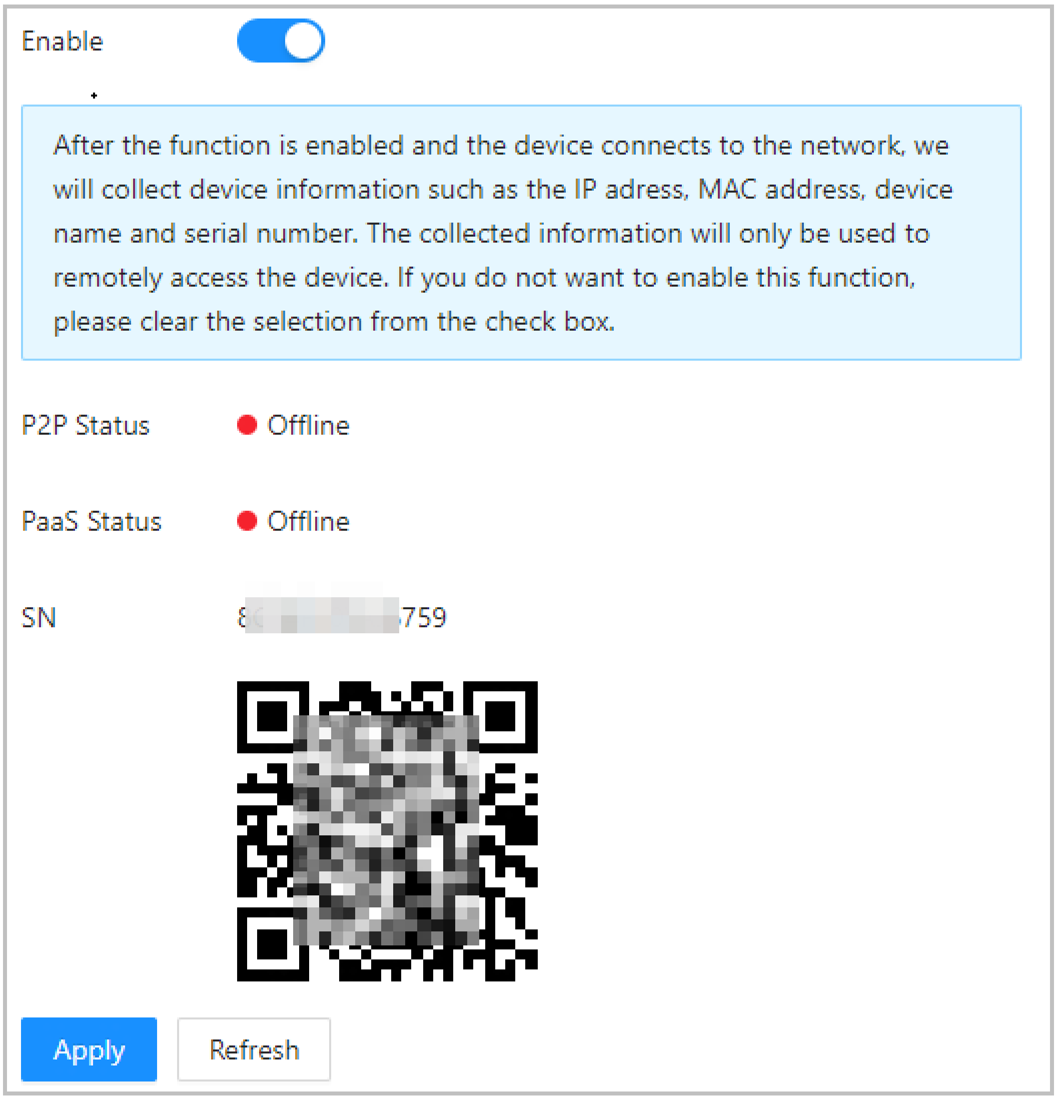
Procedure

Step 1 On the home page, select **Communication Settings** > **Network Setting** > **Cloud Service**.

Step 2 Turn on the cloud service function.

The cloud service goes online if the P2P and PaaS are online.

Figure 3-27 Cloud service



Enable ●

After the function is enabled and the device connects to the network, we will collect device information such as the IP adress, MAC address, device name and serial number. The collected information will only be used to remotely access the device. If you do not want to enable this function, please clear the selection from the check box.

P2P Status ● Offline

PaaS Status ● Offline

SN 8[redacted]759

Step 3 Click **Apply**.

Step 4 Scan the QR code with DMSS to add the device.

3.9.5 Configuring Auto Registration

The auto registration enables the devices to be added to the management platform without manual input of device information such as IP address and port.

Background Information

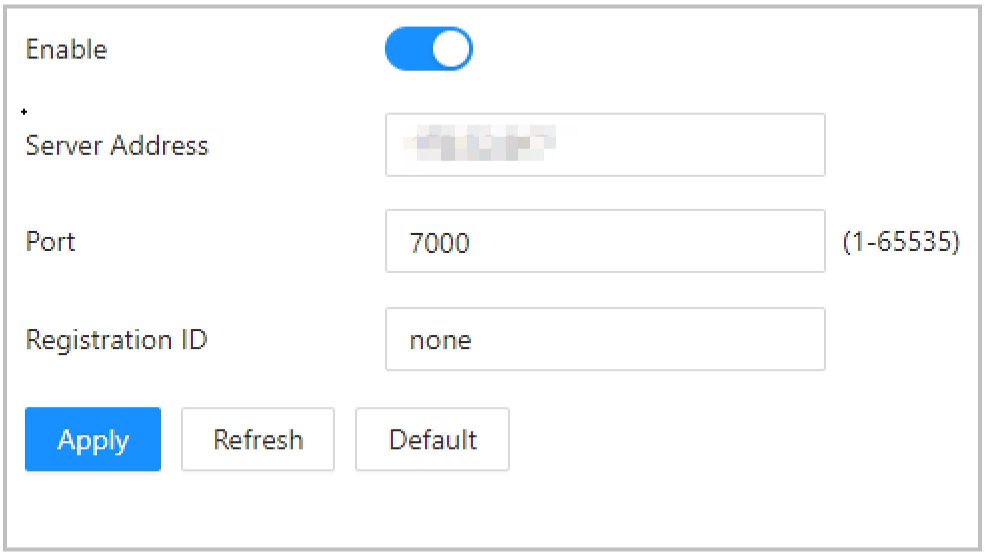
The auto registration only supports SDK.

Procedure

Step 1 On the home page, select **Communication Settings** > **Network Setting** > **Auto Registration**.

Step 2 Enable the auto registration function and configure the parameters.

Figure 3-28 Auto Registration



Enable: ●

Server Address: [redacted]

Port: 7000 (1-65535)

Registration ID: none

Table 3-18 Automatic registration description

Parameter	Description
Server Address	The IP address or the domain name of the server.
Port	The port of the server that is used for automatic registration.
Registration ID	The registration ID (user defined) of the device. Adding the device to the management by entering the registration ID on the platform.

Step 3 Click **Apply**.

3.9.6 Configuring CGI Actively Registers

Connect to a third-party platform through CGI protocol.

Background Information

Only supports IPv4.

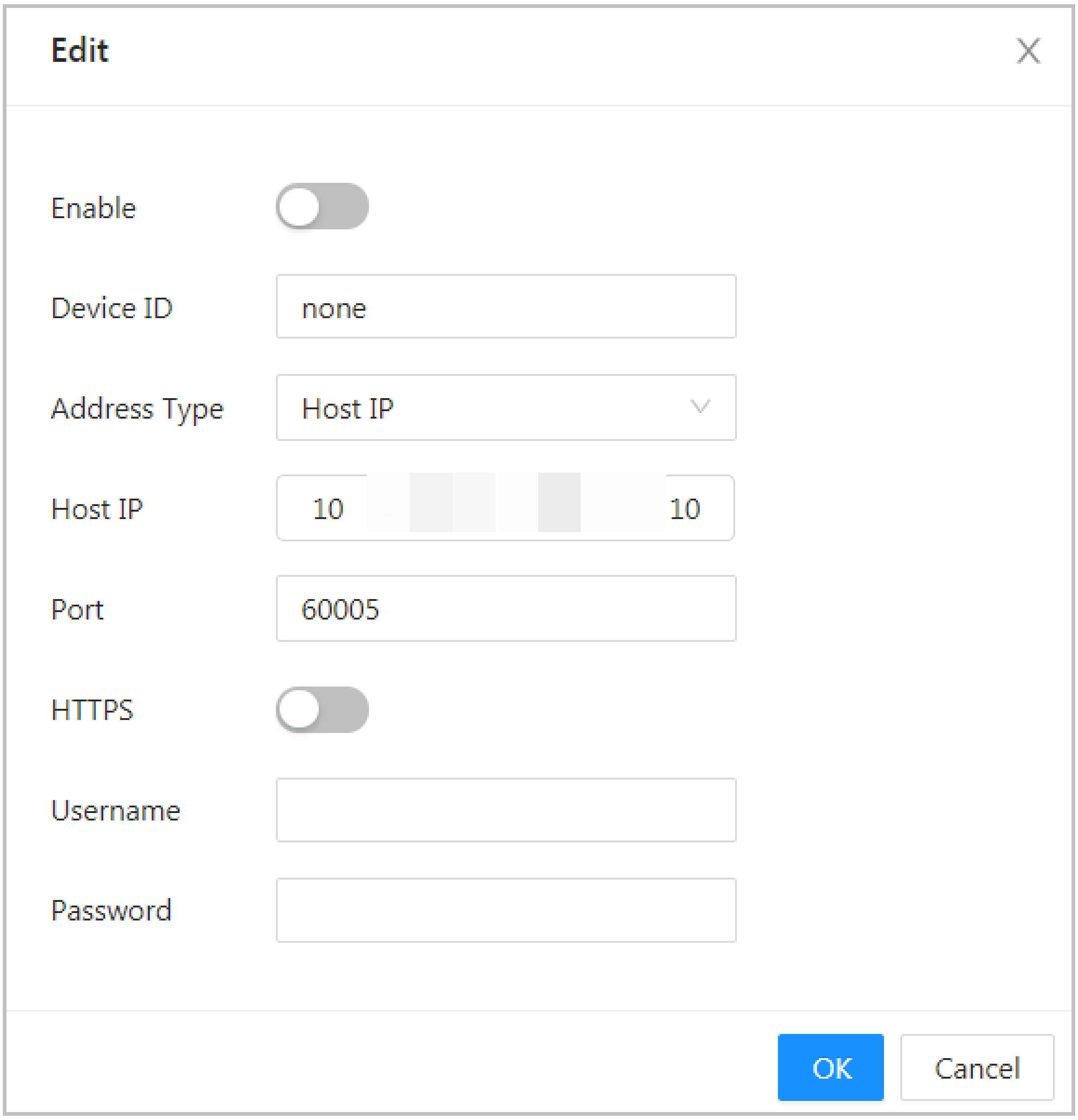
Procedure

Step 1 On the home page, select **Communication Settings** > **Network Settings** > **CGI actively registers**.

Step 2 Enable this function, and then configure the parameters.

Step 3 Click **Add**, and then configure parameters.

Figure 3-29 CGI active registration


Edit

Enable ○

Device ID: none

Address Type: Host IP

Host IP: 10 [redacted] 10

Port: 60005

HTTPS ○

Username:

Password:

Table 3-19 Automatic registration description

Parameter	Description
Device ID	Supports up to 32 bytes, including Chinese, numbers, letters, and special characters.
Address Type	Supports 2 methods to register. ● Host IP: Enter the IP address of the third-party platform. ● Domain Name: Enter the domain name of the third-party platform.
Host IP	
Domain Name	
HTTPS	Access the third-party platform through HTTPS. HTTPS secures communication over a computer network.

Step 4 Click **Apply**.

3.9.7 Configuring Auto Upload

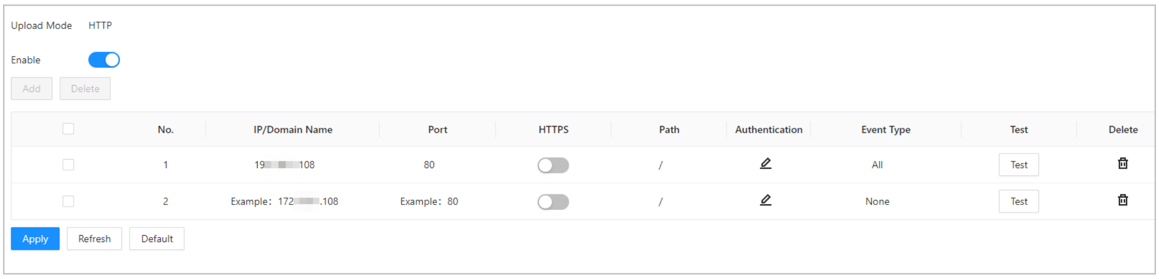
Send user information and attendance records through to the management platform

Procedure

Step 1 On the home page, select **Communication Settings** > **Network Settings** > **Auto Upload**.

Step 2 Enable HTTP upload mode.

Step 3 Click **Add**, and then configure parameters.



Upload Mode HTTP

Enable ●

□	No.	IP/Domain Name	Port	HTTPS	Path	Authentication	Event Type	Test	Delete
□	1	19[redacted]108	80	○	/	✎	All	Test	🗑
□	2	Example：172[redacted].108	Example：80	○	/	✎	None	Test	🗑

Figure 3-30 Automatic upload

Table 3-20 Parameters description

Parameter	Description
IP/Domain Name	The IP or domain name of the management platform.
Port	The port of the management platform.
HTTPS	Access the management platform through HTTPS. HTTPS secures communication over a computer network.
Authentication	Enable account authentication when you access the management platform. Login username and password are required.
Even Type	Select the type of event that will be pushed to the management platform. ● Before you use this function, go to **Communication Settings** > **Network Settings** > **Basic Service** to enable **Push Person Info**. ● Person information can only be pushed to one management platform and attendance records can be pushed to multiple management platforms.

Step 4 Click **Apply**.

3.10 Configuring the System

3.10.1 User Management

You can add or delete users, change users' passwords, and enter an email address for resetting the password when you forget your password.

3.10.1.1 Adding Administrators

You can add new administrator accounts, and then they can log in to the webpage of the Device.

Procedure

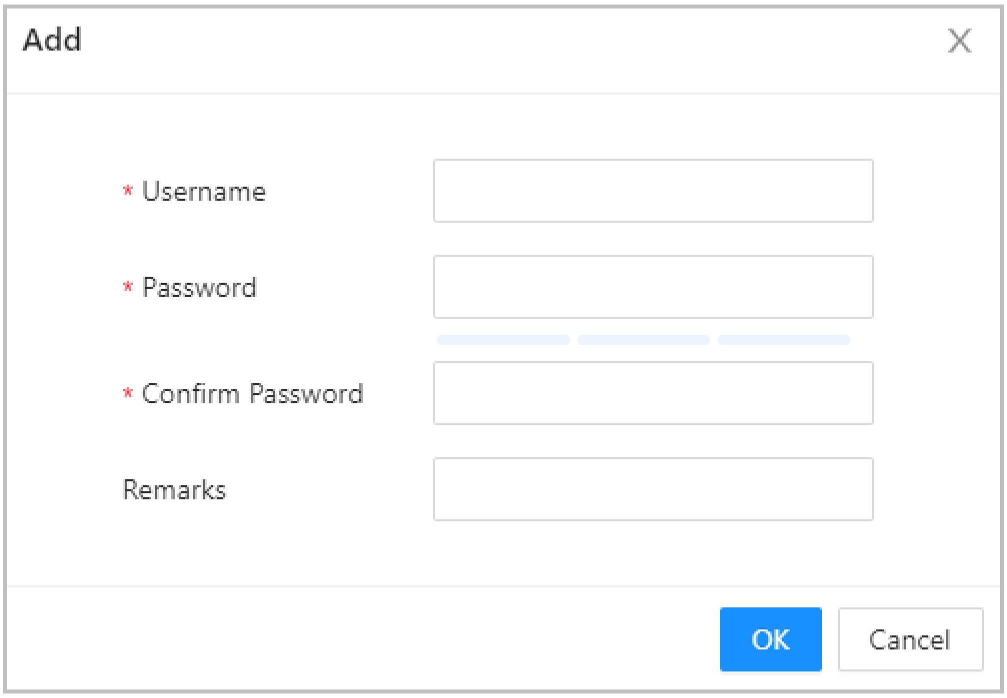
Step 1 On the home page, select **System** > **Account**.

Step 2 Click **Add**, and enter the user information.

- The username cannot be the same with existing account. The username consists of up to 31 characters and only allows for numbers, letters, underscores, midlines, dots, or @.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: Upper case, lower case, numbers, and special characters (excluding ' " ; : &).

  Set a high-security password by following the password strength prompt.

Figure 3-31 Add administrators



Step 3 Click **OK**.

Only admin account can change password and admin account cannot be deleted.

3.10.1.2 Adding ONVIF Users

Background Information

Open Network Video Interface Forum (ONVIF), a global and open industry forum that is established for the development of a global open standard for the interface of physical IP-based security products, which allows the compatibility from different manufactures. ONVIF users have their identities verified through ONVIF protocol. The default ONVIF user is admin.

Procedure

Step 1 On the home page, select **System** > **Account** > **ONVIF User**.

Step 2 Click **Add**, and then configure parameters.

Figure 3-32 Add ONVIF user

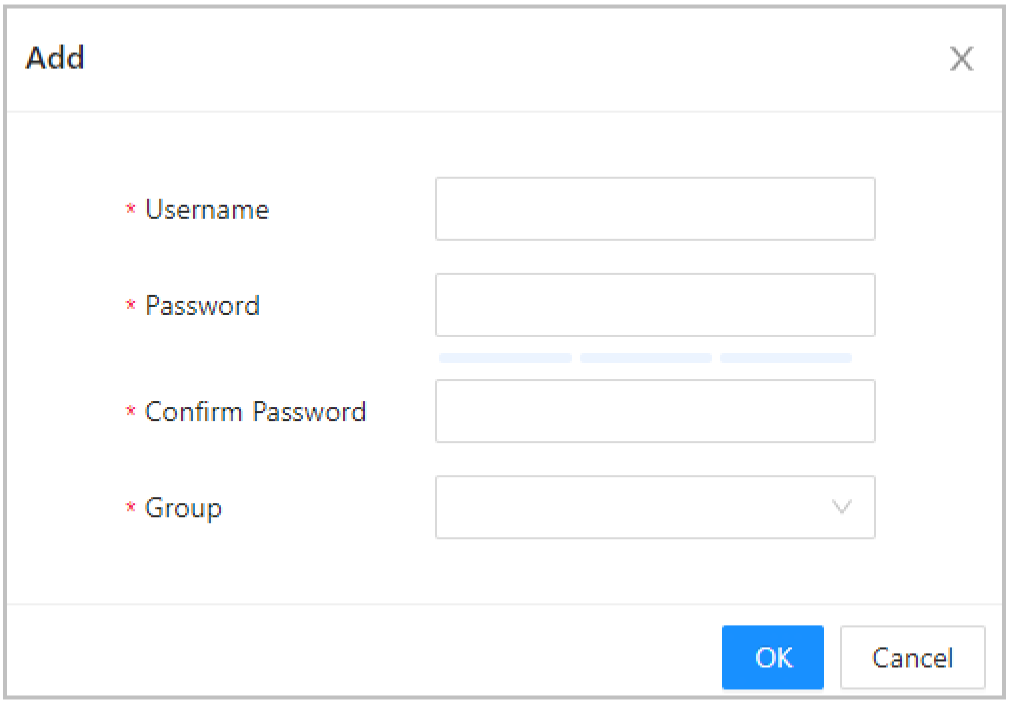


Table 3-21 ONVIF user description

Parameter	Description
Username	The username cannot be the same with existing account. The username consists of up to 31 characters and only allows for numbers, letters, underscores, midlines, dots, or @.
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: Upper case, lower case, numbers, and special characters (excluding ' " ; : &).

Parameter	Description
Group	There three permission groups which represents different permission levels. ● admin: You can view and manage other user accounts on the ONVIF Device Manager. ● Operator: You cannot view or manage other user accounts on the ONVIF Device Manager. ● User: You cannot view or manage other user accounts and system logs on the ONVIF Device Manager.

Step 3 Click **OK**.

3.10.1.3 Resetting the Password

Reset the password through the linked e-mail when you forget your password.

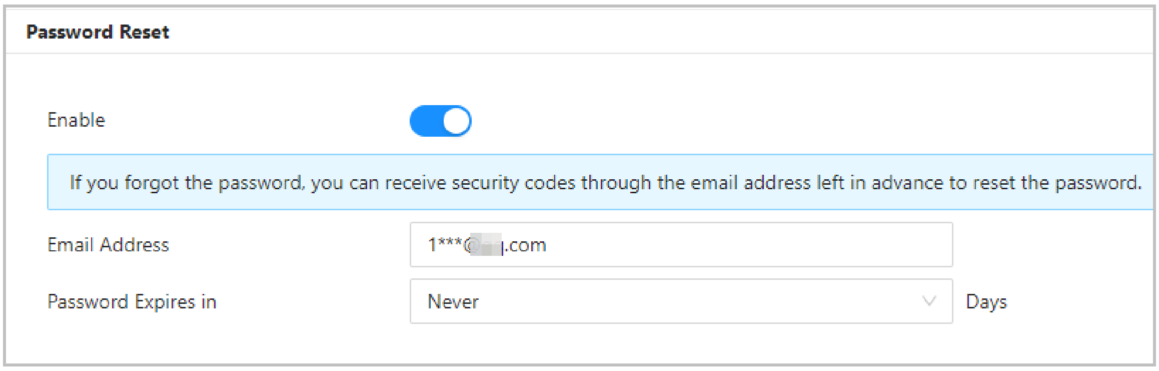
Procedure

Step 1 Select **System** > **Account**.

Step 2 Enter the email address, and set the password expiration time.

Step 3 Turn on the password reset function.

Figure 3-33 Reset Password



Password Reset

Enable

If you forgot the password, you can receive security codes through the email address left in advance to reset the password.

Email Address: 1***@[redacted].com

Password Expires in: Never Days

If you forgot the password, you can receive security codes through the linked email address to reset the password.

Step 4 Click **Apply**.

3.10.1.4 Viewing Online Users

You can view online users who currently log in to the webpage. On the home page, select **System** > **Online User**.

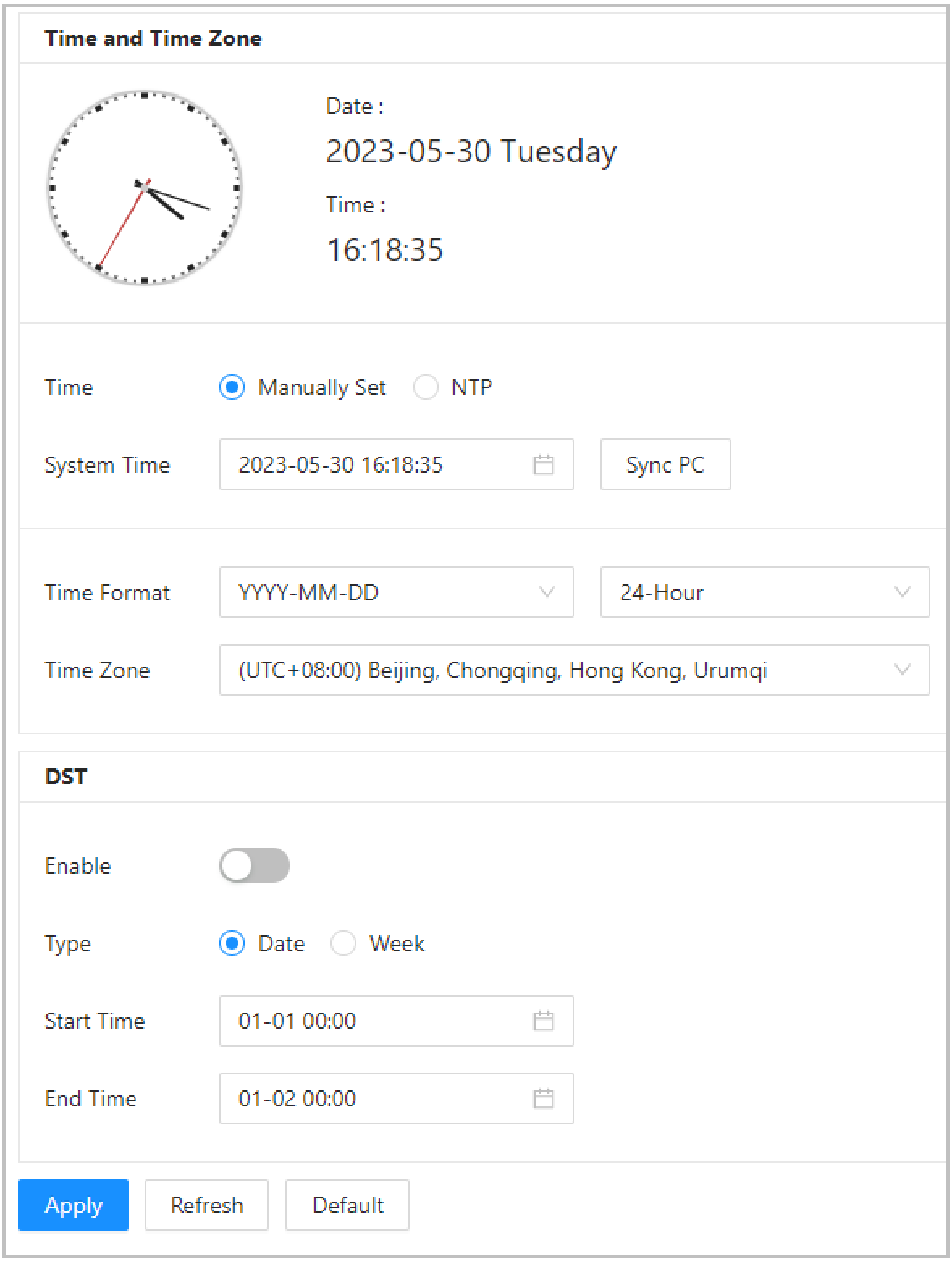
3.10.2 Configuring Time

Procedure

Step 1 On the home page, select **System** > **Time**.

Step 2 Configure the time of the Platform.

Figure 3-34 Date settings



Time and Time Zone

Date : 2023-05-30 Tuesday

Time : 16:18:35

Time: ● Manually Set ○ NTP

System Time: 2023-05-30 16:18:35

Time Format: YYYY-MM-DD, 24-Hour

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

DST

Enable

Type: ● Date ○ Week

Start Time: 01-01 00:00

End Time: 01-02 00:00

Table 3-22 Time settings description

Parameter	Description
Time	● Manual Set: Manually enter the time or you can click **Sync Time** to sync time with computer. ● NTP: The Device will automatically sync the time with the NTP server. ◇ **Server** : Enter the domain of the NTP server. ◇ **Port** : Enter the port of the NTP server. ◇ **Interval** : Enter its time with the synchronization interval.
Time format	Select the time format.
Time Zone	Enter the time zone.
DST	1. (Optional) Enable DST. 2. Select **Date** or **Week** from the **Type**. 3. Configure the start time and end time of the DST.

Step 3 Click **Apply**.

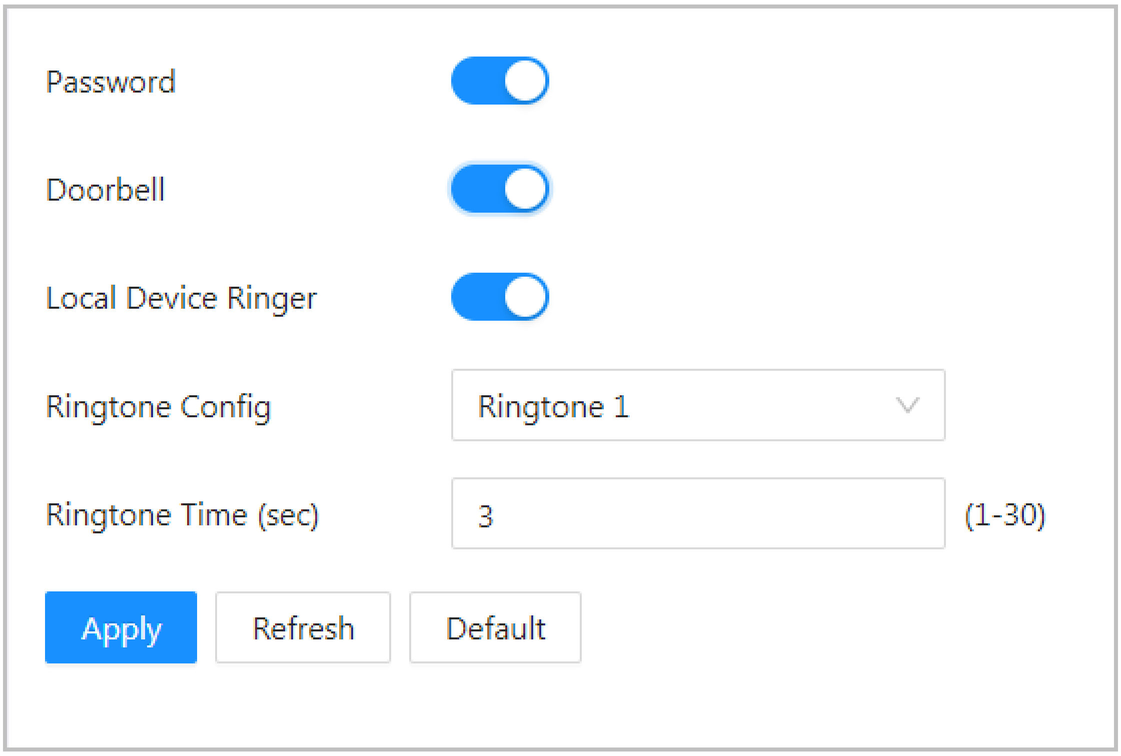
3.11 Configuring the Shortcuts

Procedure

Step 1 On the webpage, select **Personalization** > **Shortcut Settings**.

Step 2 Configure the shortcut parameters.

Figure 3-35 Shortcut Settings



Password ●

Doorbell ●

Local Device Ringer ●

Ringtone Config: Ringtone 1

Ringtone Time (sec): 3 (1-30)

Table 3-23 Parameters description

Parameter	Description
Password	The icon of the password is displayed on the standby screen.
Doorbell	After the doorbell function is turned on, doorbell icon is displayed on the standby screen. ● Local Device Ringer: Tap the ring bell icon on the standby screen, Device will ring. ● Ringtone Config: Select a ringtone. ● Ringtone Time (sec): Set ring time (1-30 seconds). The default value is 3.

3.12 Management Center

3.12.1 One-click Diagnosis

The system automatically diagnoses the configurations and the status of the device to improve its performance.

Procedure

Step 1 On the home page, select **Maintenance Center** > **One-click Diagnosis**.

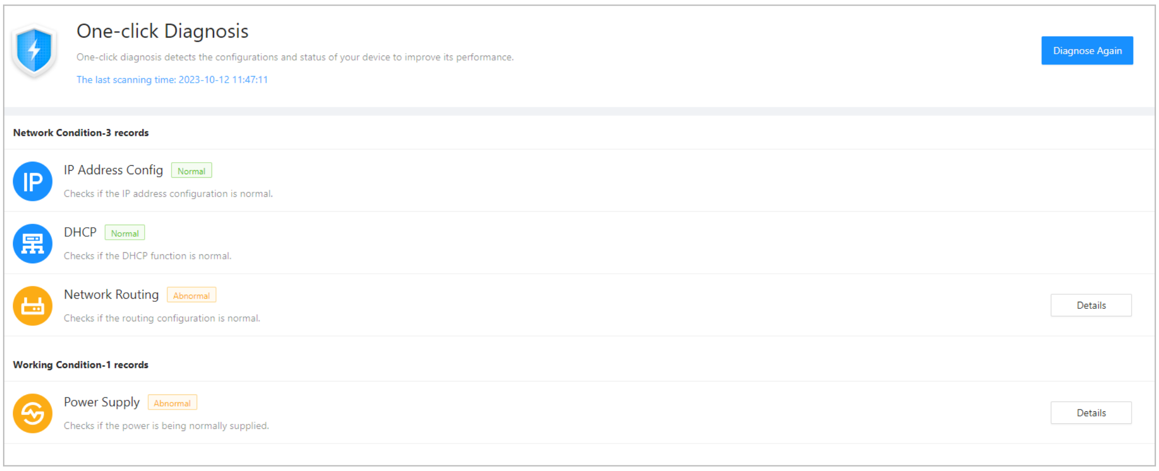
Step 2 Click **Diagnose**.

The system automatically diagnoses the configurations and the status of the device and display diagnosis results after it completes.

Step 3 (Optional) Click **Details** to view details of abnormal items.

You can ignore the abnormality or optimize it. You can also click **Diagnose Again** to perform automatic diagnosis again.

Figure 3-36 One-click diagnosis



One-click Diagnosis

One-click diagnosis detects the configurations and status of your device to improve its performance.

The last scanning time: 2023-10-12 11:47:11

Network Condition-3 records

IP Address Config Normal
Checks if the IP address configuration is normal.

DHCP Normal
Checks if the DHCP function is normal.

Network Routing Abnormal
Checks if the routing configuration is normal.

Working Condition-1 records

Power Supply Abnormal
Checks if the power is being normally supplied.

3.12.2 System Information

3.12.2.1 Viewing Version Information

On the webpage, select **System** > **Version**, and you can view version information of the Device.

3.12.2.2 Viewing Legal Information

On the home page, select **System** > **Legal Info**, and you can view the software license agreement, privacy policy and open source software notice.

3.12.3 Data Capacity

You can see how many users and face images that the Device can store.

Log in to the webpage and select **Data Capacity**.

3.12.4 Viewing Logs

View logs such as system logs, admin logs, and attendance records.

3.12.4.1 System Logs

View and search for system logs.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Log** > **Log**.

Step 3 Select the time range and the log type, and then click **Search**.

Related Operations

- click **Export** to export the searched logs to your local computer.
- Click **Encrypt Log Backup**, and then enter a password. The exported file can be opened only after entering the password.
- Click ▣ to view details of a log.

3.12.4.2 Attendance Records

Search for attendance records and export them.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Log** > **Attendance Records**.

Step 3 Select the time range and the type, and then click **Search**.

You can click **Export** to download the records.

3.12.4.3 Admin Logs

Search for admin logs by using admin ID.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Log** > **Admin Log**.

Step 3 Enter the admin ID, and then click **Search**.

Click **Export** to export admin logs.

3.12.4.4 USB Management

Export user information from/to USB.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Log** > **USB Management**.

- Make sure that a USB is inserted to the Device before you export data or update the system. To avoid failure, do not pull out the USB or perform any operation of the Device during the process.
- You have to use a USB to export the information from the Device to other devices. Face images are not allowed to be imported through USB.

Step 3 Select a data type, and then click **USB Import** or **USB Export** to import or export the data.

3.12.5 Configuration Management

When more than one Device need the same configurations, you can configure parameters for them by importing or exporting configuration files.

3.12.5.1 Exporting and Importing Configuration Files

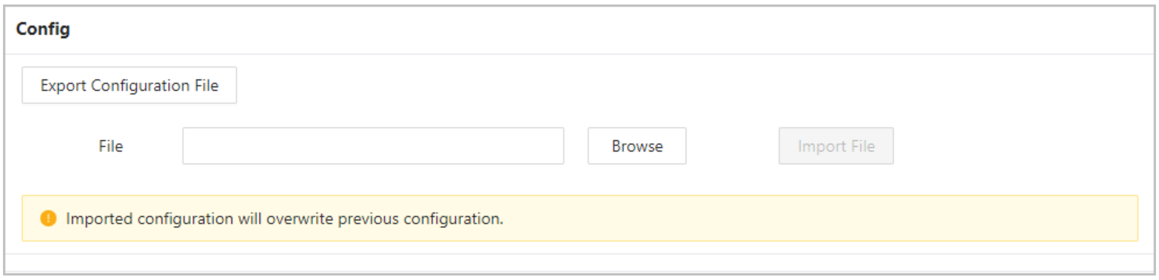
You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Manager** > **Config**.

Figure 3-37 Configuration management



Imported configuration will overwrite previous configuration.

Step 3 Export or import configuration files.

- Export the configuration file.

  Click **Export Configuration File** to download the file to the local computer.

  The IP will not be exported.

- Import the configuration file.
  1. Click **Browse** to select the configuration file.
  2. Click **Import configuration**.

     Configuration files can only be imported to devices that have the same model.

3.12.5.2 Restoring the Factory Default Settings

Procedure

Step 1 Select **Maintenance Center** > **Manager** > **Config**..

Restoring the **Device** to its default configurations will result in data loss. Please be advised.

Step 2 Restore to the factory default settings if necessary.

- **Factory Defaults** : Resets all the configurations of the Device and delete all the data.
- **Restore to Default (Except for User Info and Logs)** : Resets the configurations of the Device and deletes all the data except for user information and logs.

3.12.6 Maintenance

Regularly restart the Device during its idle time to improve its performance.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Manager** > **Maintenance**.

Step 3 Set the time, and then click **Apply**.

The Device will restart at the scheduled time, or you can click **Restart** to restart it immediately.

3.12.7 Updating the System

- Use the correct update file. Make sure that you get the correct update file from technical support.
- Do not disconnect the power supply or network, and do not restart or shutdown the Device during the update.

3.12.7.1 File Update

Procedure

Step 1 On the home page, **Maintenance Center** > **Update**.

Step 2 In **File Update** , click **Browse**, and then upload the update file.

The update file should be a .bin file.

<u>Step 3</u> Click **Update**.

The Device will restart after the update finishes.

3.12.7.2 Online Update

Procedure

<u>Step 1</u> On the home page, select **Maintenance Center** > **Update**.

<u>Step 2</u> In the **Online Update** area, select an update method.

- Select **Auto Check for Updates**, and the Device will automatically check for the latest version update.
- Select **Manual Check**, and you can immediately check whether the latest version is available.

<u>Step 3</u> (Optional) Click **Update Now** to update the Device immediately.

3.12.8 Advanced Maintenance

Acquire device information and capture packet to make easier for maintenance personnel to perform troubleshooting.

3.12.8.1 Exporting

Procedure

<u>Step 1</u> On the home page, select **Maintenance Center** > **Advanced Maintenance** > **Export**.

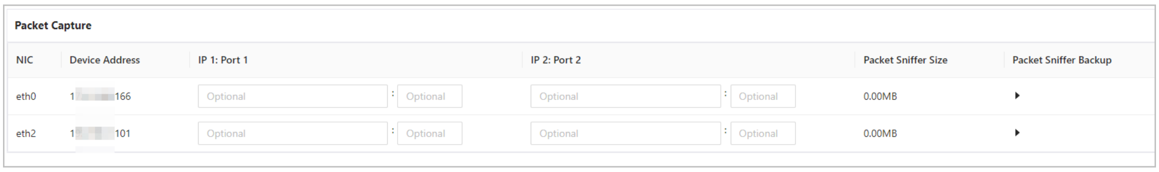
<u>Step 2</u> Click **Export** to export the serial number, firmware version, device operation logs and configuration information.

3.12.8.2 Packet Capture

Procedure

<u>Step 1</u> On the home page, select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.

Figure 3-38 Packet Capture



Packet Capture

NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Backup
eth0	1[redacted]166	Optional	Optional	Optional	Optional	0.00MB	▶
eth2	1[redacted]101	Optional	Optional	Optional	Optional	0.00MB	▶

<u>Step 2</u> Enter the IP address, click ▶.

▶ changes to ⏸.

<u>Step 3</u> After you acquired enough data, click ⏸.

Captured packets are automatically downloaded to your local computer.

3.13 Security Settings(Optional)

3.13.1 Security Status

Scan the users, service, and security modules to check the security status of the Device.

Background Information

- User and service detection: Check whether the current configuration conforms to recommendation.
- Security modules scanning: Scan the running status of security modules, such as audio and video transmission, trusted protection, securing warning and attack defense, not detect whether they are enabled.

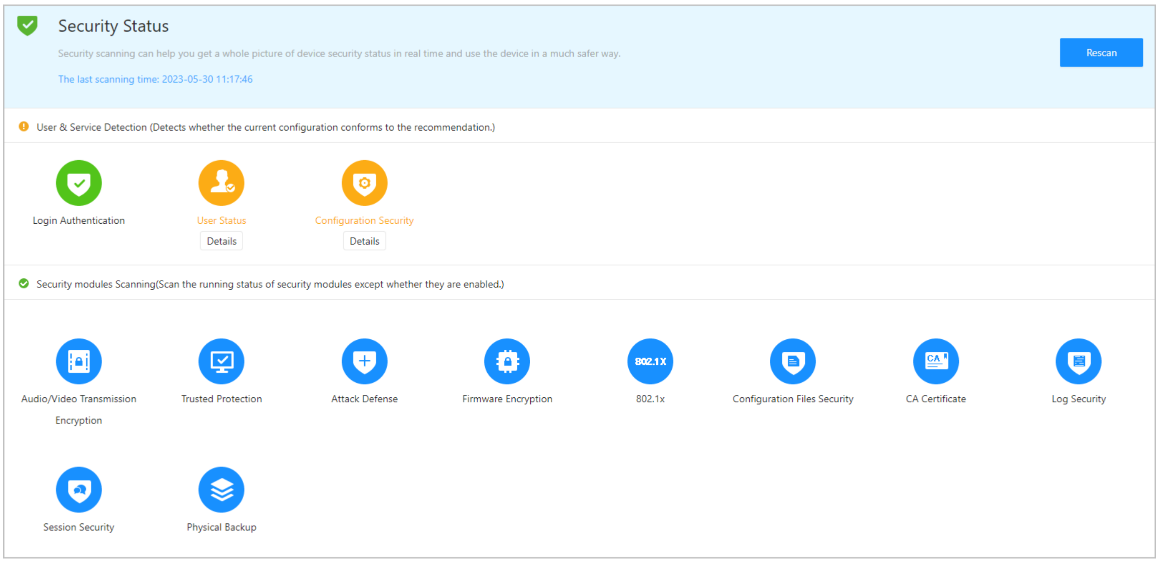
Procedure

Step 1 Select ⛉ > **Security Status**.

Step 2 Click **Rescan** to perform a security scan of the Device.

Hover over the icons of the security modules to see their running status.

Figure 3-39 Security Status



Security Status

Security scanning can help you get a whole picture of device security status in real time and use the device in a much safer way.

The last scanning time: 2023-05-30 11:17:46

User & Service Detection (Detects whether the current configuration conforms to the recommendation.)

Security modules Scanning(Scan the running status of security modules except whether they are enabled.)

Related Operations

After you perform the scan, the results will be displayed in different colors. Yellow indicates that the security modules are abnormal, and green indicates that the security modules are normal.

- Click **Details** to view the details on the results of the scan.
- Click **Ignore** to ignore the abnormality, and it will not be scanned. The abnormality that was ignored will be highlighted in grey.
- Click **Optimize** to troubleshoot the abnormality.

3.13.2 Configuring HTTPS

Create a certificate or upload an authenticated certificate, and then you can log in to the webpage through HTTPS on your computer. HTTPS secures communication over a computer network.

Procedure

Step 1 Select > **System Service** > **HTTPS**.

Step 2 Turn on the HTTPS service.

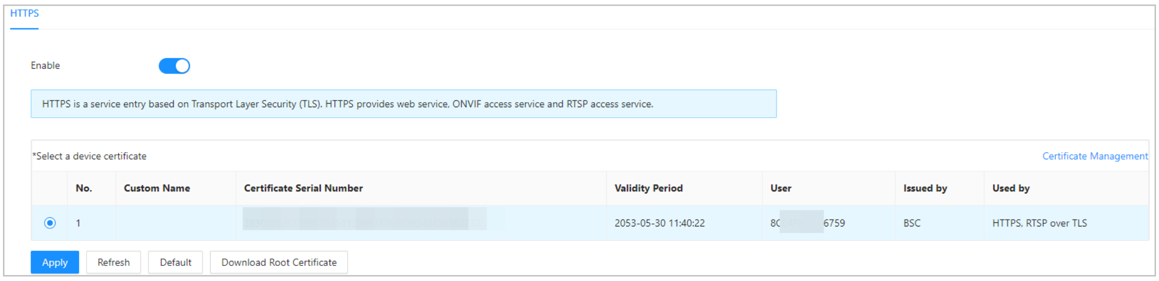
⚠

If you turn on the compatible with TLS v1.1 and earlier versions, security risks might occur. Please be advised.

Step 3 Select the certificate.

If there are no certificates in the list, click **Certificate Management** to upload a certificate.

Figure 3-40 HTTPS



HTTPS

Enable

HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access service and RTSP access service.

*Select a device certificate

Certificate Management

	No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
●	1		[redacted]	2053-05-30 11:40:22	8C[redacted]6759	BSC	HTTPS, RTSP over TLS

Step 4 Click **Apply**.

Enter “https://*IP address*: *httpsport*" in a web browser. If the certificate is installed, you can log in to the webpage successfully. If not, the webpage will display the certificate as wrong or untrusted.

3.13.3 Attack Defense

3.13.3.1 Configuring Firewall

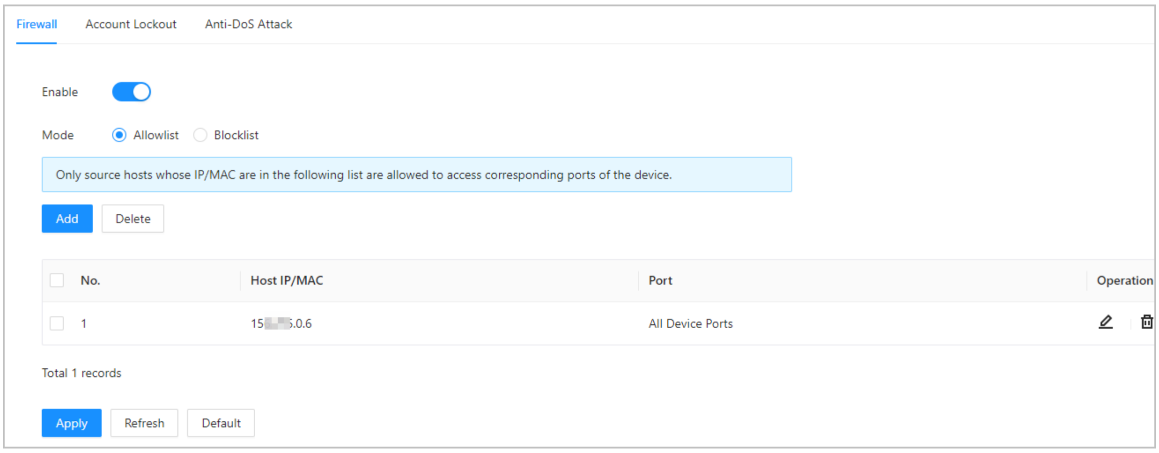
Configure firewall to limit access to the Device.

Procedure

Step 1 Select > **Attack Defense** > **Firewall**.

Step 2 Click to enable the firewall function.

Figure 3-41 Firewall



Enable: on

Mode: ● Allowlist ○ Blocklist

Only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device.

□	No.	Host IP/MAC	Port	Operation
□	1	15[redacted]5.0.6	All Device Ports	✎ 🗑

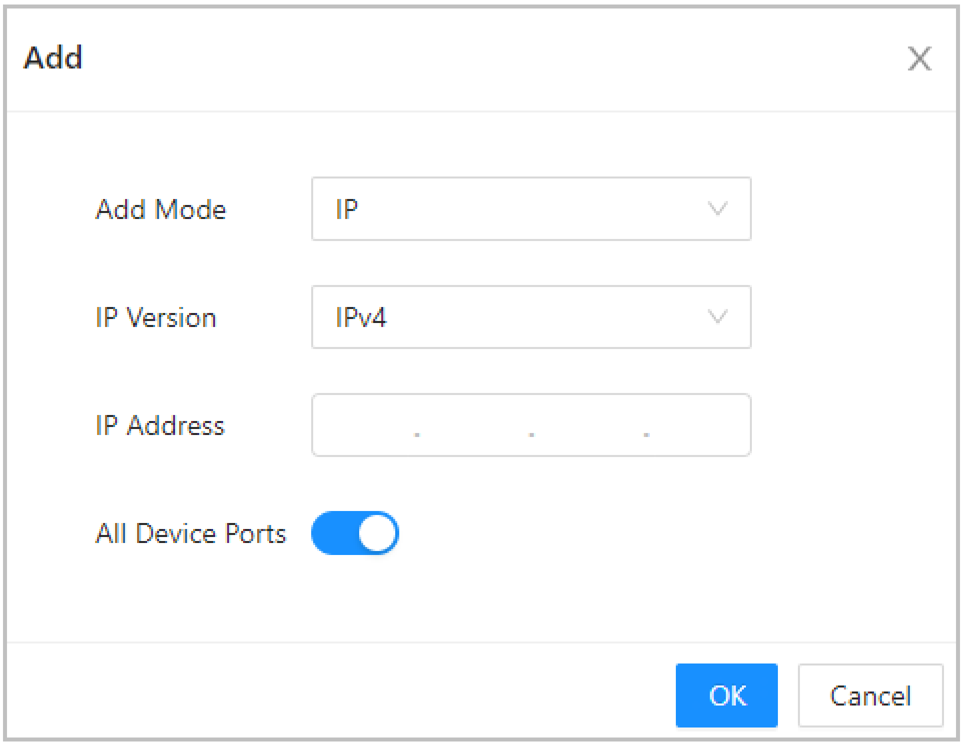
Total 1 records

Step 3 Select the mode: **Allowlist** and **Blocklist**.

- **Allowlist** : Only IP/MAC addresses on the allowlist can access the Device.
- **Blocklist** : The IP/MAC addresses on the blocklist cannot access the Device.

Step 4 Click **Add** to enter the IP information.

Figure 3-42 Add IP information



Add Mode: IP

IP Version: IPv4

IP Address: . . .

All Device Ports: on

Step 5 Click **OK**.

Related Operations

- Click ✎ to edit the IP information.
- Click 🗑 to delete the IP address.

3.13.3.2 Configuring Account Lockout

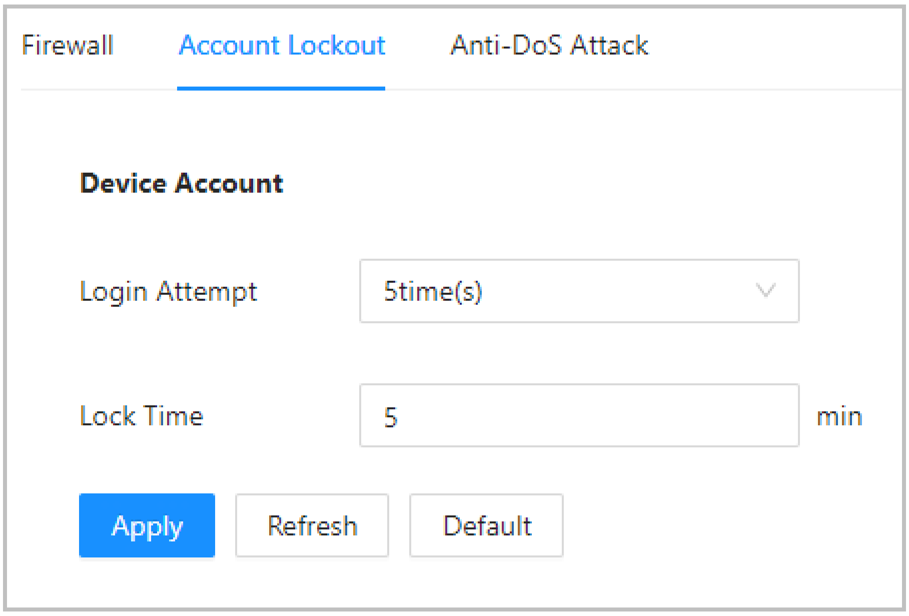
If the incorrect password is entered for a defined number of times, the account will be locked.

Procedure

Step 1 Select > **Attack Defense** > **Account Lockout**.

Step 2 Enter the number of login attempts and the time the administrator account and ONVIF user will be locked for.

Figure 3-43 Account lockout



Device Account

Login Attempt: 5time(s)

Lock Time: 5 min

- Login Attempt: The limit of login attempts. If the incorrect password is entered for a defined number of times, the account will be locked.
- Lock Time: The duration during which you cannot log in after the account is locked.

Step 3 Click **Apply**.

3.13.3.3 Configuring Anti-DoS Attack

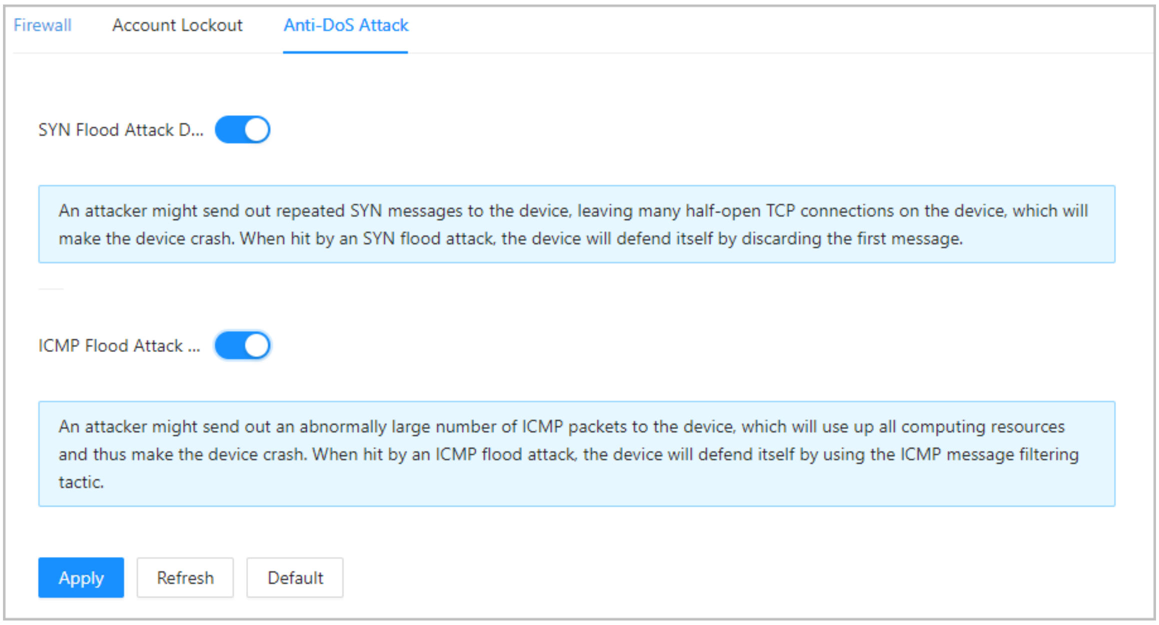
You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Device against Dos attacks.

Procedure

Step 1 Select > **Attack Defense** > **Anti-DoS Attack**.

Step 2 Turn on **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to protect the Device against Dos attack.

Figure 3-44 Anti-DoS attack



SYN Flood Attack D... ●

An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.

ICMP Flood Attack ... ●

An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

Step 3 Click **Apply**.

3.13.4 Installing Device Certificate

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS on your computer.

3.13.4.1 Creating Certificate

Create a certificate for the Device.

Procedure

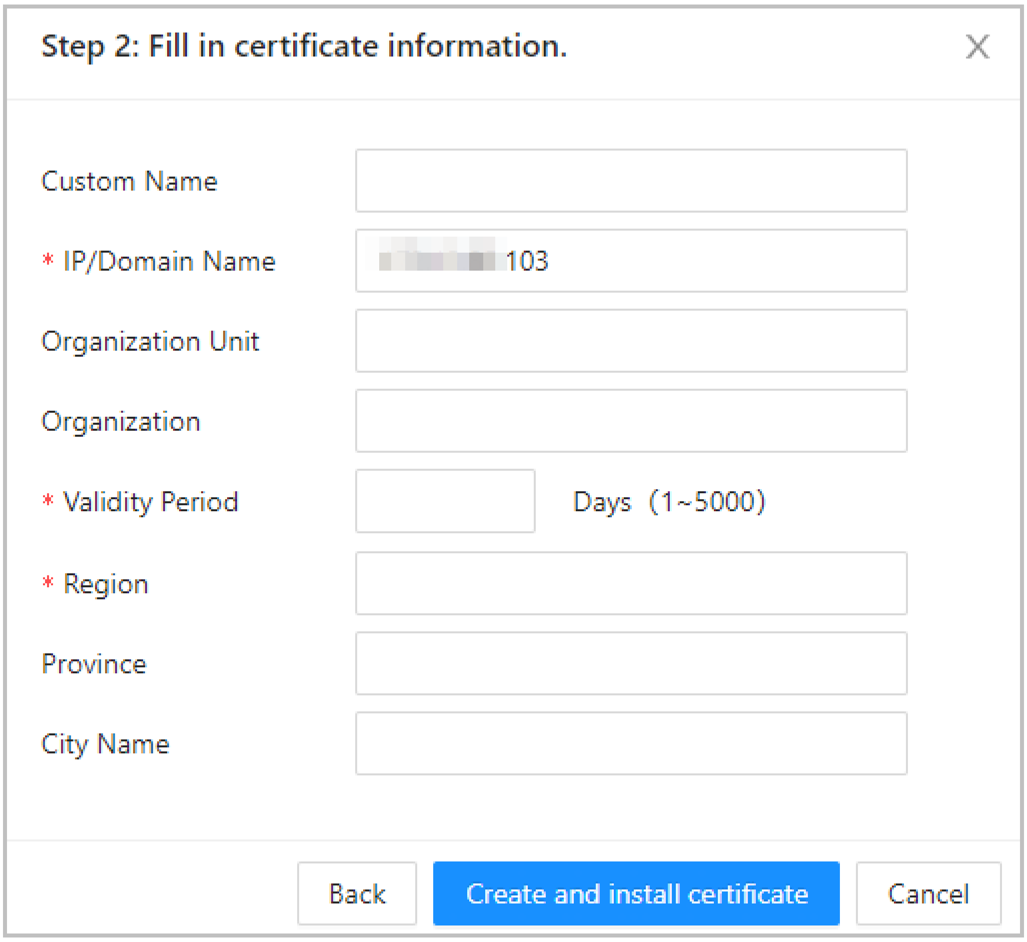
Step 1 Select 🛡 > **CA Certificate** > **Device Certificate**.

Step 2 Select **Install Device Certificate**.

Step 3 Select **Create Certificate** , and then click **Next**.

Step 4 Enter the certificate information.

Figure 3-45 Certificate information



Step 2: Fill in certificate information.

Custom Name

* IP/Domain Name [redacted]103

Organization Unit

Organization

* Validity Period Days (1~5000)

* Region

Province

City Name

The name of region cannot exceed 2 characters. We recommend entering the abbreviation of the name of the region.

Step 5 Click **Create and install certificate**.

The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click ⤓ to download the certificate.
- Click 🗑 to delete the certificate.

3.13.4.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the Device.

Procedure

Step 1 Select 🛡 > **CA Certificate** > **Device Certificate**.

Step 2 Click **Install Device Certificate**.

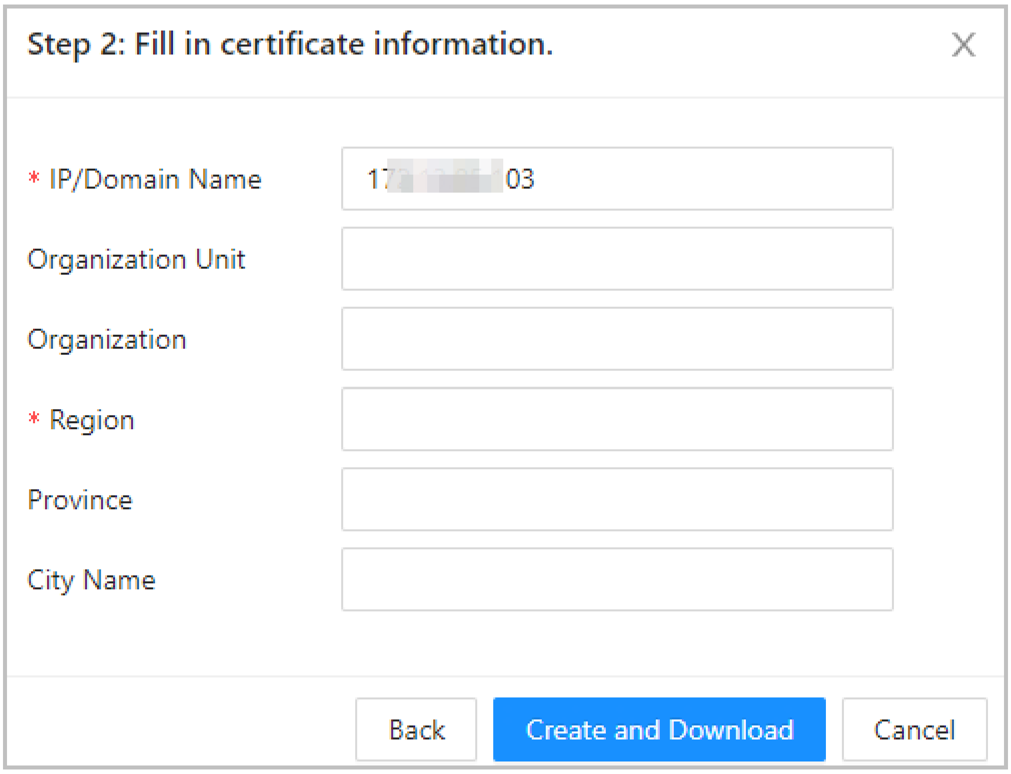
Step 3 Select **Apply for CA Certificate and Import (Recommended)** , and click **Next**.

Step 4 Enter the certificate information.

- IP/Domain name: the IP address or domain name of the Device.

- Region: The name of region must not exceed 3 characters. We recommend you enter the abbreviation of region name.

Figure 3-46 Certificate information (2)



Step 2: Fill in certificate information.

* IP/Domain Name: 17[redacted]03

Organization Unit

Organization

* Region

Province

City Name

Step 5 Click **Create and Download**.

Save the request file to your computer.

Step 6 Apply to a third-party CA authority for the certificate by using the request file.

Step 7 Import the signed CA certificate.

1. Save the CA certificate to your computer.
2. Click **Installing Device Certificate**.
3. Click **Browse** to select the CA certificate.
4. Click **Import and Install**.

   The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

   - Click **Recreate** to create the request file again.
   - Click **Import Later** to import the certificate at another time.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click ⤓ to download the certificate.
- Click 🗑 to delete the certificate.

3.13.4.3 Installing Existing Certificate

If you already have a certificate and private key file, import the certificate and private key file.

Procedure

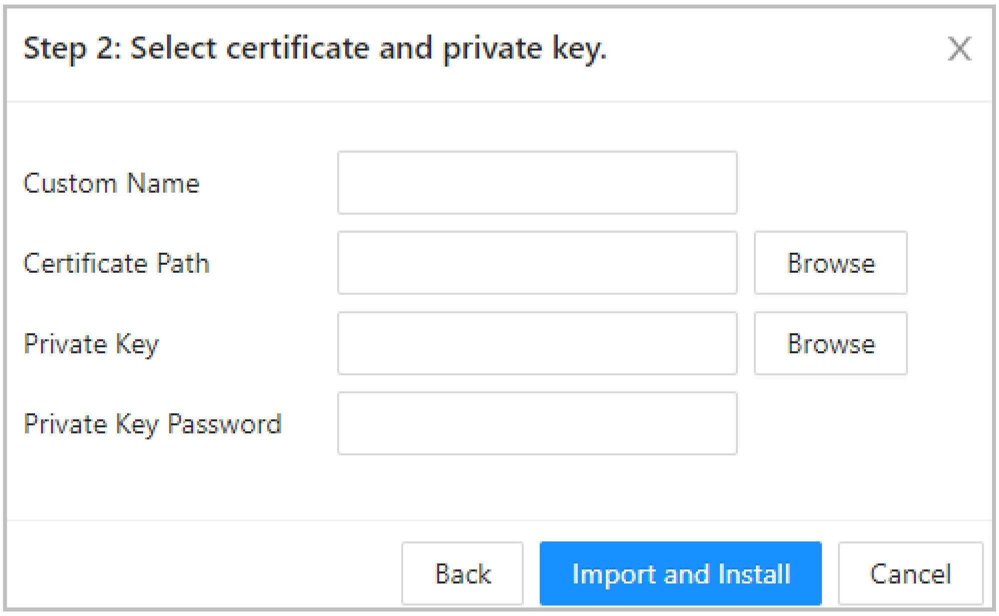
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Click **Install Device Certificate**.

Step 3 Select **Install Existing Certificate** , and click **Next**.

Step 4 Click **Browse** to select the certificate and private key file, and enter the private key password.

Figure 3-47 Certificate and private key



Step 2: Select certificate and private key.

Custom Name	
Certificate Path	
Private Key	
Private Key Password	

Step 5 Click **Import and Install**.

The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click ⬇ to download the certificate.
- Click 🗑 to delete the certificate.

3.13.5 Installing the Trusted CA Certificate

A trusted CA certificate is a digital certificate that is used for validating the identities of websites and servers. For example, when 802.1x protocol is used, the CA certificate for switches is required to authenticate its identity.

Background Information

802.1X is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them access to the network.

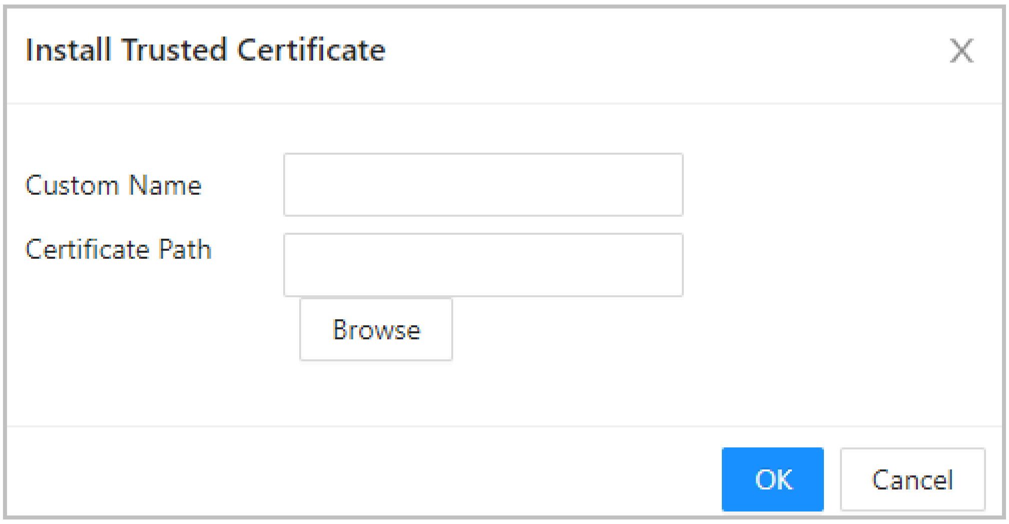
Procedure

Step 1 Select 🛡 > **CA Certificate** > **Trusted CA Certificates**.

Step 2 Select **Install Trusted Certificate**.

Step 3 Click **Browse** to select the trusted certificate.

Figure 3-48 Install the trusted certificate


Install Trusted Certificate

Custom Name

Certificate Path

Step 4 Click **OK**.

The newly installed certificate is displayed on the **Trusted CA Certificates** page after the certificate is successfully installed.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click 📥 to download the certificate.
- Click 🗑 to delete the certificate.

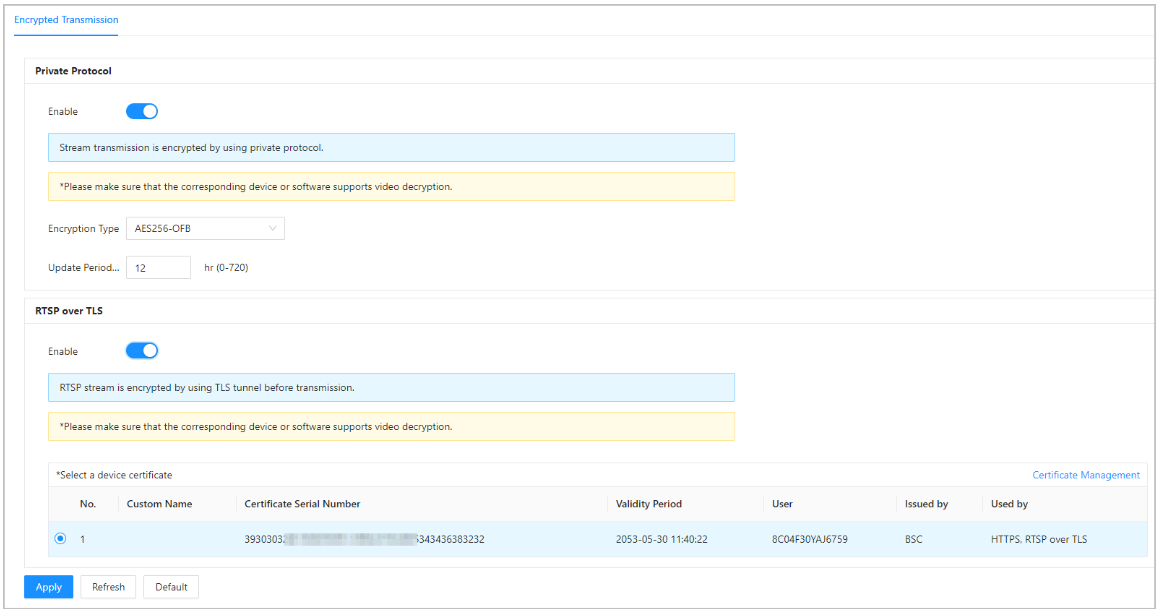
3.13.6 Data Encryption

Procedure

Step 1 Select 🛡 > **Data Encryption**.

Step 2 Configure the parameters.

Figure 3-49 Data encryption



Private Protocol

Enable: ●

Stream transmission is encrypted by using private protocol.

*Please make sure that the corresponding device or software supports video decryption.

Encryption Type: AES256-OFB

Update Period...: 12 hr (0-720)

RTSP over TLS

Enable: ●

RTSP stream is encrypted by using TLS tunnel before transmission.

*Please make sure that the corresponding device or software supports video decryption.

*Select a device certificate

	No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
◉	1		3930303[redacted]343436383232	2053-05-30 11:40:22	8C04F30YAJ6759	BSC	HTTPS, RTSP over TLS

Table 3-24 Data encryption description

	Parameter	Description
Private Protocol	Enable	Streams are encrypted during transmission through private protocol.
	Encryption Type	Keep it as default.
	Update Period of Secret Key	Ranges from 0 h -720 h. 0 means never update the secret key.
RTSP over TLS	Enable	RTSP stream is encrypted during transmission through TLS tunnel.
	Certificate Management	Create or import certificate. For details, see "3.13.4 Installing Device Certificate". The installed certificates are displayed in the list.

3.13.7 Security Warning

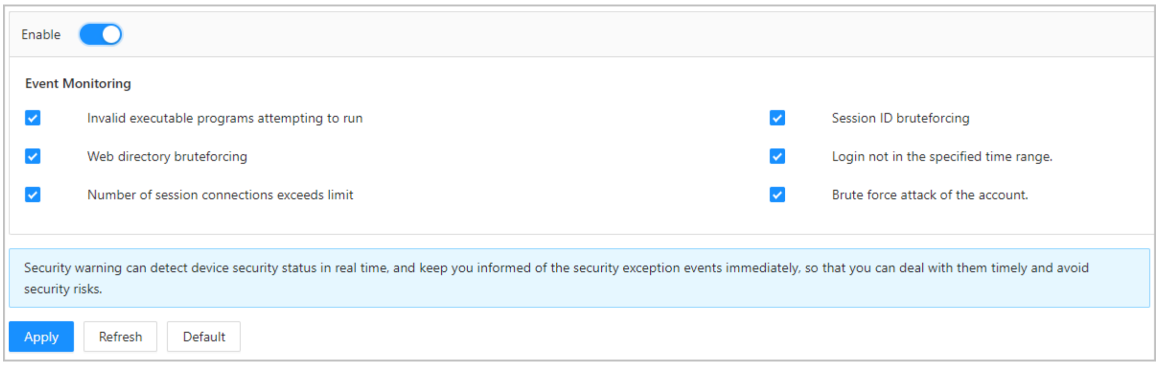
Procedure

Step 1 Select 🛡 > **Security Warning**.

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

Figure 3-50 Security warning



Enable ●

Event Monitoring

☑ Invalid executable programs attempting to run	☑ Session ID bruteforcing
☑ Web directory bruteforcing	☑ Login not in the specified time range.
☑ Number of session connections exceeds limit	☑ Brute force attack of the account.

Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.

Step 4 Click **Apply**.

3.13.8 Security Authentication

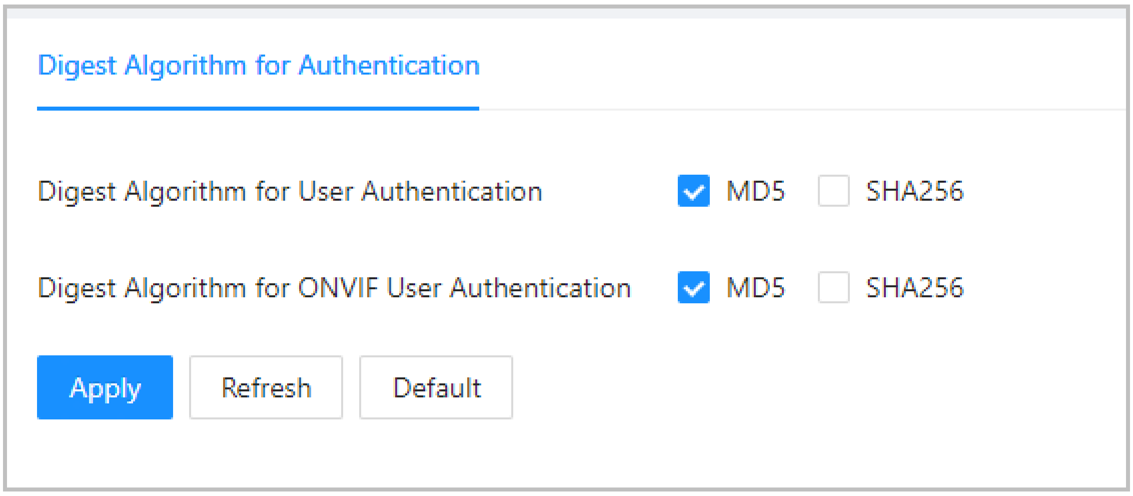
Procedure

Step 1 Select **Security** > **Security Authentication**.

Step 2 Select a message digest algorithm.

Step 3 Click **Apply**.

Figure 3-51 Security Authentication



Digest Algorithm for Authentication

Digest Algorithm for User Authentication ☑ MD5 □ SHA256

Digest Algorithm for ONVIF User Authentication ☑ MD5 □ SHA256

4 Smart PSS Lite Configuration

This section introduces how to manage and configure the device through Smart PSS Lite. For details, see the user's manual of Smart PSS Lite.

4.1 Installing and Logging In

Install and log in to Smart PSS Lite. For details, see the user manual of Smart PSS Lite.

Procedure

Step 1 Get the software package of the Smart PSS Lite from the technical support, and then install and run the software according to instructions.

Step 2 Initialize Smart PSS Lite when you log in for the first time, including setting password and security questions.

📖

> Set the password is for the first-time use, and then set security questions to reset your password when you forgot it.

Step 3 Enter your username and password to log in to Smart PSS Lite.

4.2 Adding Devices

You need to add the Device to Smart PSS Lite. You can add them in batches or individually.

4.2.1 Adding Device One By One

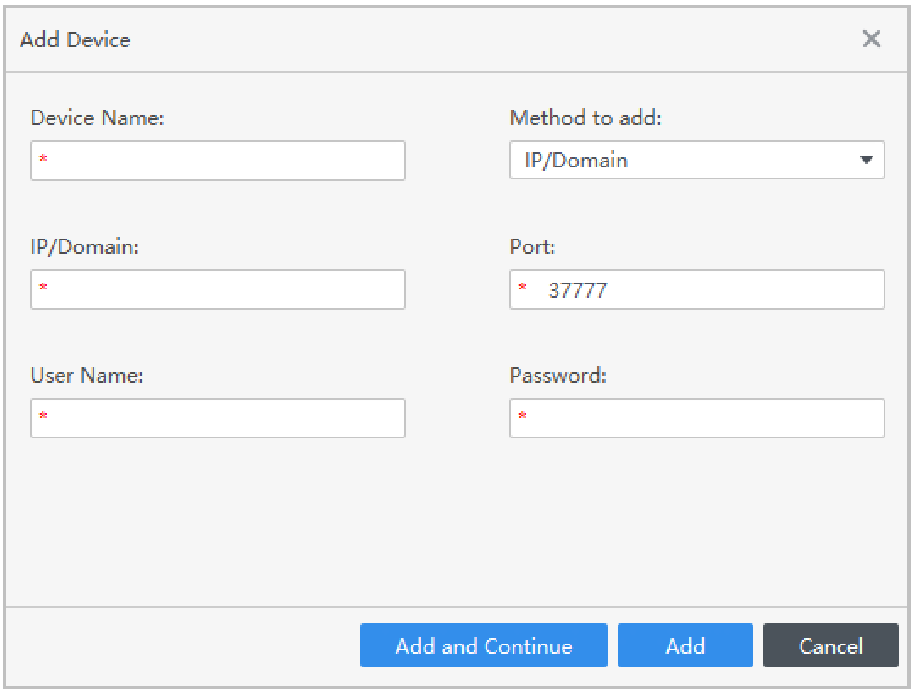
You can add devices one by one through entering their IP addresses or domain names.

Procedure

Step 1 On the **Device Manager** page, click **Add**.

Step 2 Configure the information of the device.

Figure 4-1 Add devices



Add Device

Device Name:

Method to add: IP/Domain

IP/Domain:

Port: 37777

User Name:

Password:

Table 4-1 Parameters of IP adding

Parameter	Description
Device Name	We recommend you name devices with the monitoring area for easy identification.
Method to add	Select **IP/Domain**. ● IP/Domain: Enter the IP address or domain name of the device. ● SN: Enter the serial number of the device.
Port	Enter the port number, and the port number is 37777 by default. The actual port number might differ according to different models.
User Name	Enter the username of the device.
Password	Enter the password of the device.

Step 3 Click **Add**.

You can click **Add and Continue** to add more devices.

4.2.2 Adding Devices in Batches

Background Information

- We recommend you add devices by automatically search when you need to add devices in batches within the same network segment, or when the network segment is known but the exact IP addresses of devices are not known.
- Close ConfigTool and DSS when you configure devices; otherwise, you may not be able to find all devices.

Procedure

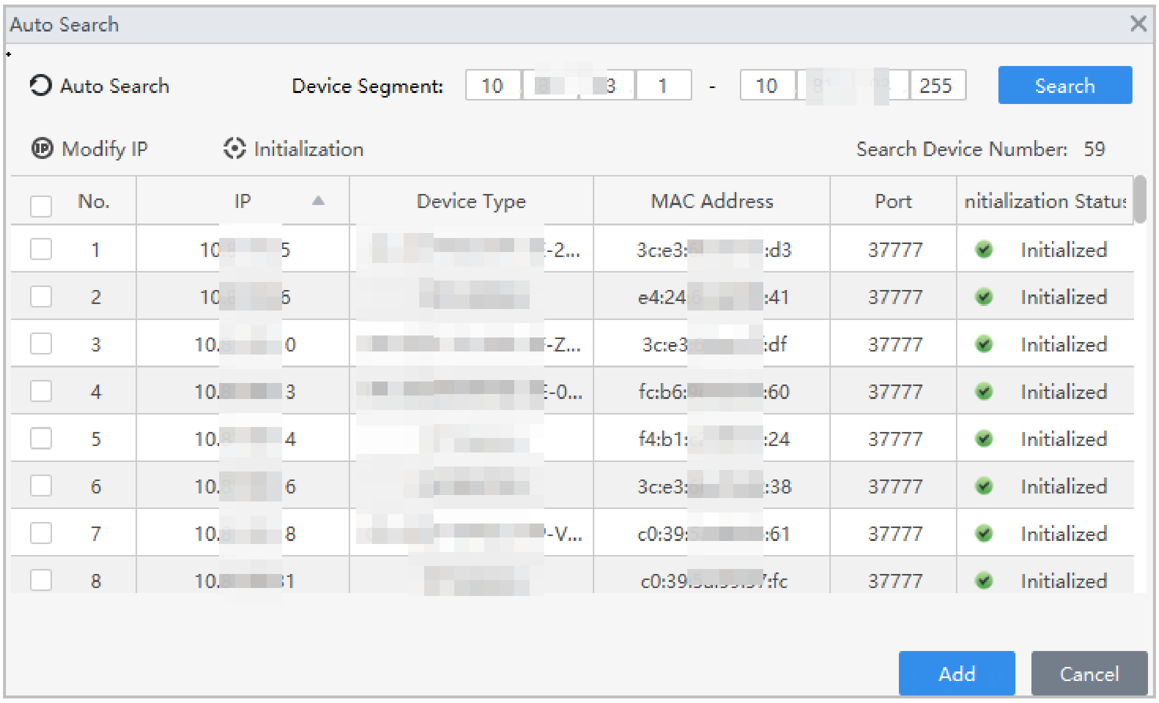
Step 1 On the **Device Manager** page, click **Auto Search**.

Step 2 Select a search method.

- Auto Search: Enter the username and the password of the device. The system will automatically search for devices that are on the same network to your computer.
- Device Segment Search: Enter the username and the password of the device, and then define the start IP and the end IP. The system will automatically search for devices in this IP range.

You can select both methods for the system to automatically search for devices on the network your computer is connected to and other networks.

Figure 4-2 Search for devices



Auto Search

Auto Search   Device Segment: 10 [redacted] 3 1 - 10 [redacted] 255   Search

Modify IP   Initialization   Search Device Number: 59

☐	No.	IP	Device Type	MAC Address	Port	nitialization Statu:
☐	1	10[redacted]5	[redacted]-2...	3c:e3:[redacted]:d3	37777	✓ Initialized
☐	2	10[redacted]5	[redacted]	e4:24[redacted]:41	37777	✓ Initialized
☐	3	10.[redacted]0	[redacted]-Z...	3c:e3[redacted]:df	37777	✓ Initialized
☐	4	10.[redacted]3	[redacted]-0...	fc:b6:[redacted]:60	37777	✓ Initialized
☐	5	10.[redacted]4	[redacted]	f4:b1:[redacted]:24	37777	✓ Initialized
☐	6	10.[redacted]6	[redacted]	3c:e3:[redacted]:38	37777	✓ Initialized
☐	7	10.[redacted]8	[redacted]-V...	c0:39:[redacted]:61	37777	✓ Initialized
☐	8	10.[redacted]1	[redacted]	c0:39[redacted]:fc	37777	✓ Initialized

Add   Cancel

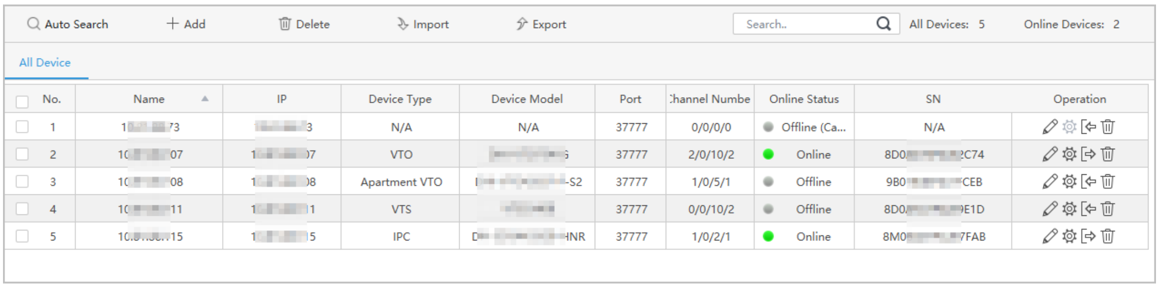
Step 3 Click devices, and then click **Add**.

Step 4 Enter the login user name and password, and then click **OK**.

Results

After the devices are successfully added, they are displayed on this page.

Figure 4-3 Added devices



All Devices: 5   Online Devices: 2

All Device

☐	No.	Name	IP	Device Type	Device Model	Port	:hannel Numbe	Online Status	SN	Operation
☐	1	1[redacted]73	[redacted]3	N/A	N/A	37777	0/0/0/0	● Offline (Ca...	N/A	
☐	2	10[redacted]07	1[redacted]07	VTO	[redacted]	37777	2/0/10/2	● Online	8D0[redacted]2C74	
☐	3	10[redacted]08	1[redacted]08	Apartment VTO	[redacted]-S2	37777	1/0/5/1	● Offline	9B0[redacted]CEB	
☐	4	10[redacted]11	1[redacted]1	VTS	[redacted]	37777	0/0/10/2	● Offline	8D0[redacted]9E1D	
☐	5	10.[redacted]15	1[redacted]5	IPC	D[redacted]HNR	37777	1/0/2/1	● Online	8M0[redacted]7FAB	

4.3 User Management

4.3.1 Adding Users

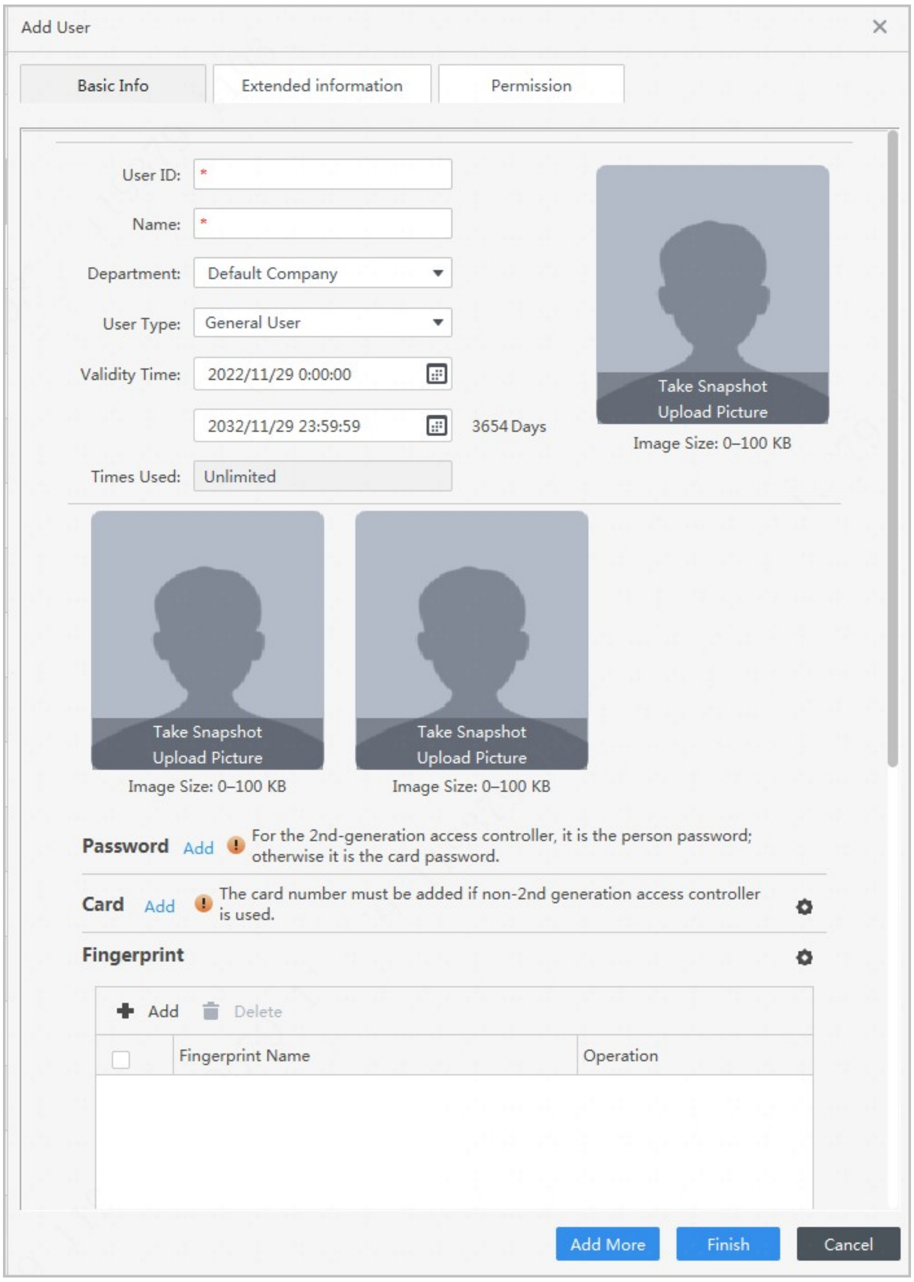
Procedure

Step 1 Select **Personnel** > **Personnel Manager** > **Add**.

Step 2 Enter basic information of staff.

1. Select **Basic Info**.
2. Add basic information of staff.

Figure 4-4 Add basic information



User ID: *

Name: *

Department: Default Company

User Type: General User

Validity Time: 2022/11/29 0:00:00

2032/11/29 23:59:59 3654 Days

Times Used: Unlimited

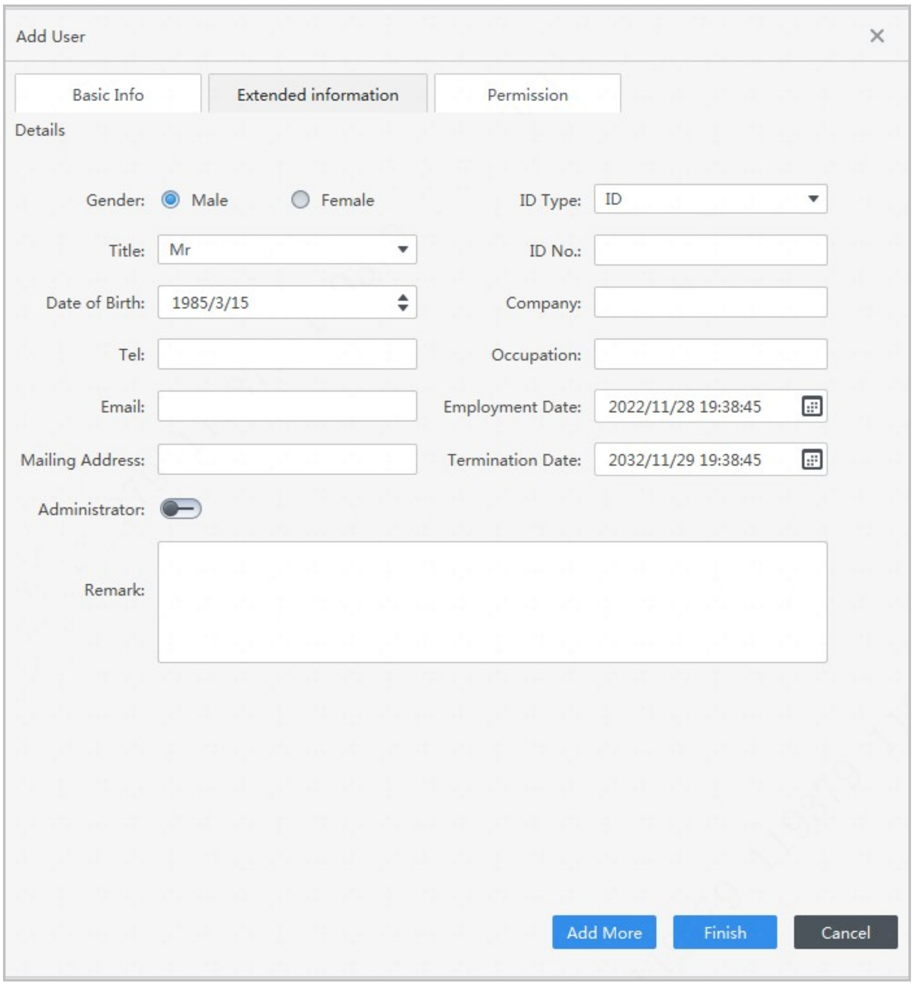
Password Add For the 2nd-generation access controller, it is the person password; otherwise it is the card password.

Card Add The card number must be added if non-2nd generation access controller is used.

Fingerprint

Step 3 Click **Extended information** to add extended information of the personnel, and then click **Finish** to save.

Figure 4-5 Add extended information



Gender: ● Male ○ Female

Title: Mr

Date of Birth: 1985/3/15

Tel:

Email:

Mailing Address:

Administrator:

Remark:

ID Type: ID

ID No.:

Company:

Occupation:

Employment Date: 2022/11/28 19:38:45

Termination Date: 2032/11/29 19:38:45

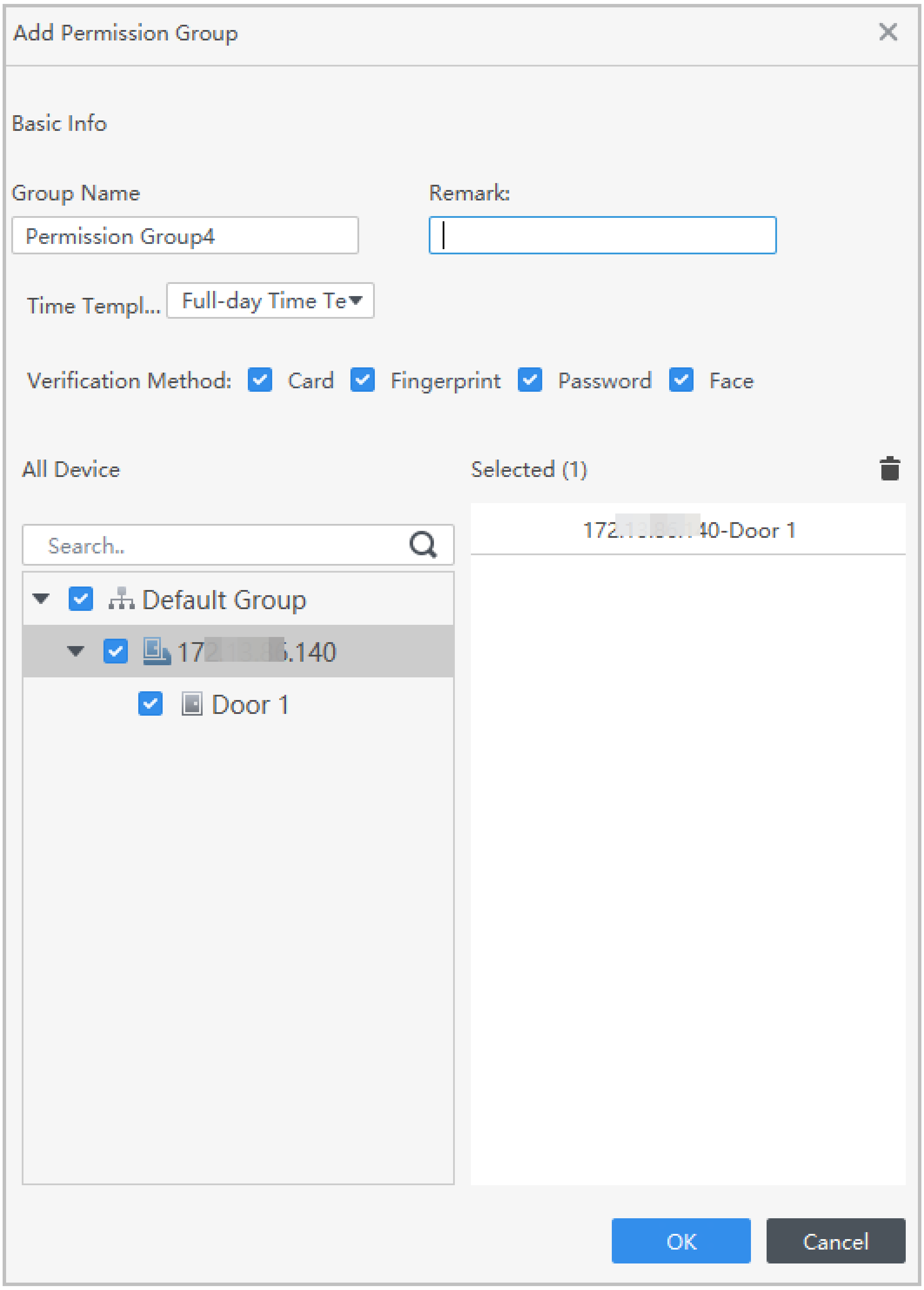
Step 4 Configure permissions.

1. Click + .
2. Enter the group name, remarks (optional), and select a time template.
3. Select verification methods and doors.

Step 5 Configure permissions. For details, see "4.3.2 Assigning Attendance Permissions".

1. Select **Group**.
2. Enter the group name, remarks (optional), and select a time template.
3. Select verification methods and doors.
4. Click **OK**.

Figure 4-6 Configure permission groups



Add Permission Group

Basic Info

Group Name: Permission Group4

Remark:

Time Templ...: Full-day Time Te

Verification Method: ☑ Card ☑ Fingerprint ☑ Password ☑ Face

All Device

Search..

☑ Default Group
- ☑ 17[redacted].140
  - ☑ Door 1

Selected (1)

172.[redacted]40-Door 1

Step 6 Click **Finish**.

After completing adding, you can click ✎ to modify information or add details in the list of staff.

4.3.2 Assigning Attendance Permissions

Create a permission group that is a collection of time attendance permissions, and then associate employees with the group so that they can punch in/out through defined verification methods.

Procedure

Step 1 Log in to the Smart PSS Lite.

Step 2 Click **Access Solution** > **Personnel Manger** > **Permission configuration**.

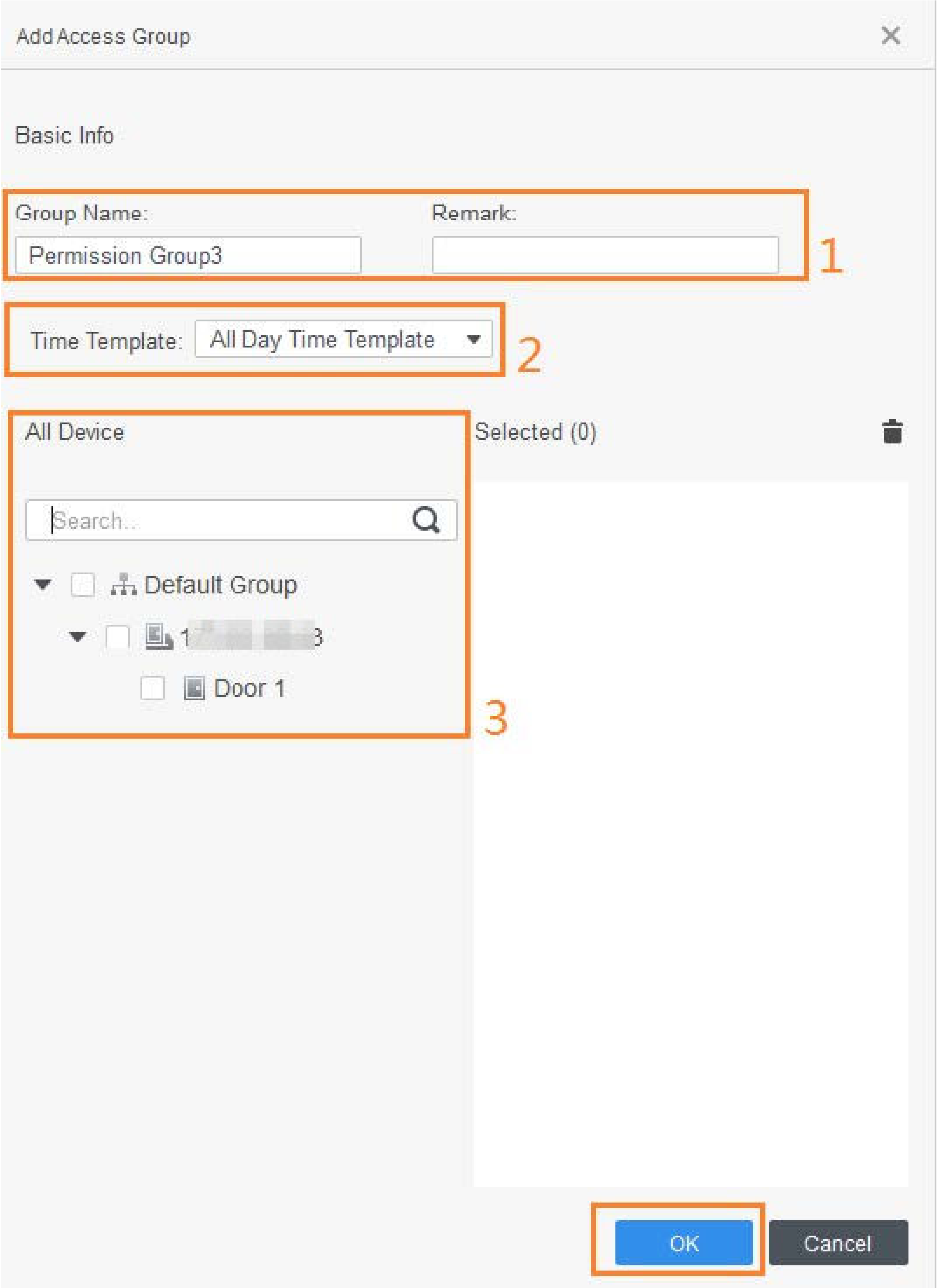
Step 3 Click + .

Step 4 Enter the group name, remarks (optional), and select a time template.

Step 5 Select the access control device.

Step 6 Click **OK**.

Figure 4-7 Create a permission group



Add Access Group

Basic Info

Group Name: Permission Group3

Remark:

Time Template: All Day Time Template

All Device

Search...

□ Default Group

□ 1[redacted]3

□ Door 1

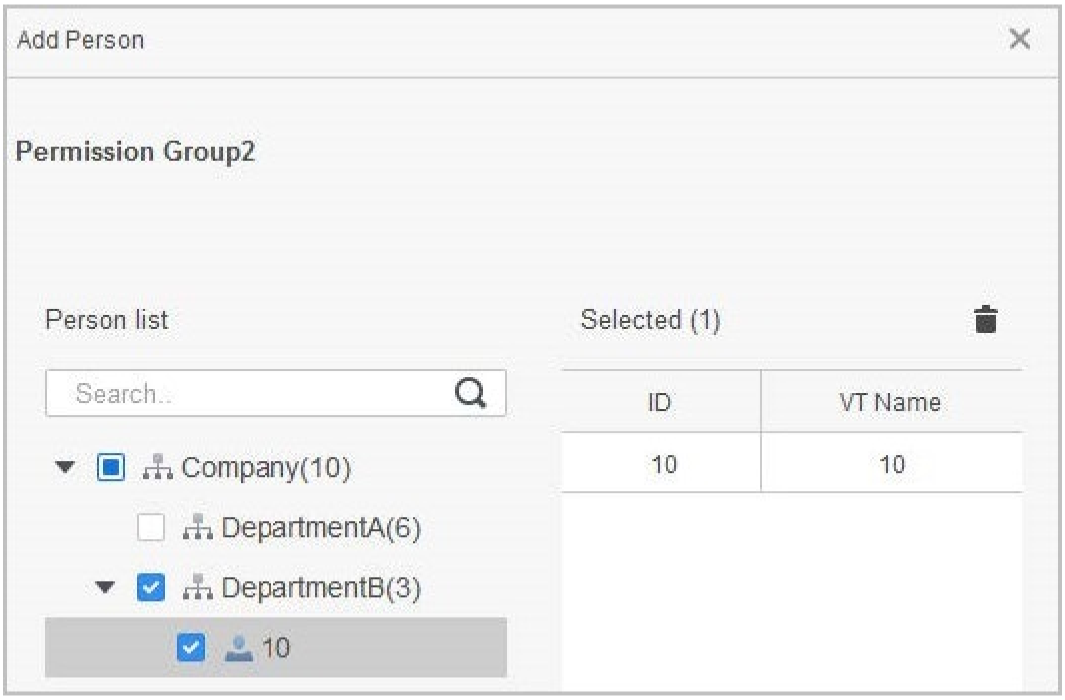
Selected (0)

The Time & Attendance only supports punch-in/out through password and face attendance.

Step 7 Click 👤 of the permission group you added.

Step 8 Select users to associate them with the permission group.

Figure 4-8 Add users to a permission group



Add Person

Permission Group2

Person list

Search..

- ■ Company(10)
  - □ DepartmentA(6)
  - ☑ DepartmentB(3)
    - ☑ 10

Selected (1)

ID	VT Name
10	10

Step 9 Click **OK**.

Appendix 1 Important Points of Face Registration

Before Registration

- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eyebrows when wearing hats.
- Do not change your beard style greatly if you use the Device; otherwise face recognition might fail.
- Keep your face clean.
- Keep the Device at least 2 meters away from light source and at least 3 meters away from windows or doors; otherwise backlight and direct sunlight might influence face recognition performance of the access controller.

During Registration

- You can register faces through the Device or through the platform. For registration through the platform, see the platform user manual.
- Make your head center on the photo capture frame. The face image will be captured automatically.

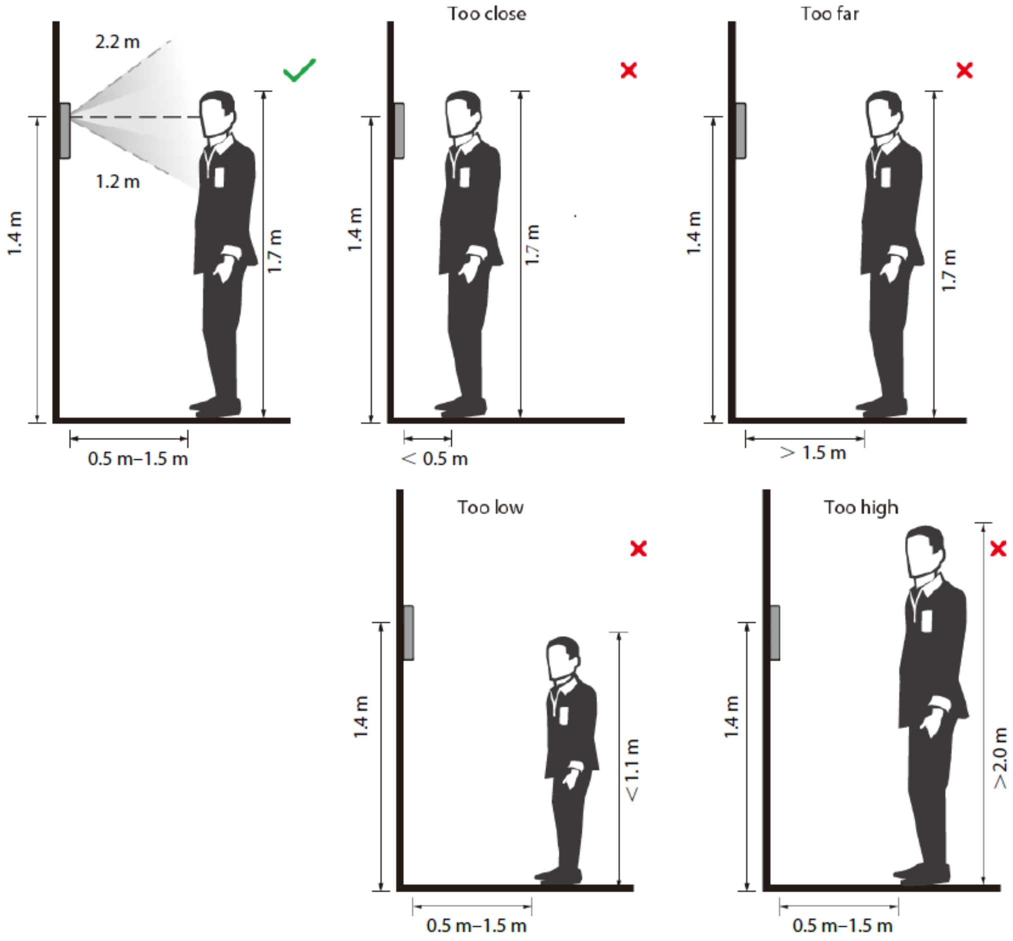
- Do not shake your head or body, otherwise the registration might fail.
- Avoid 2 faces appear in the capture frame at the same time.

Face Position

If your face is not at the appropriate position, face recognition accuracy might be affected.

The face position below is for reference only, and might differ from the actual situation.

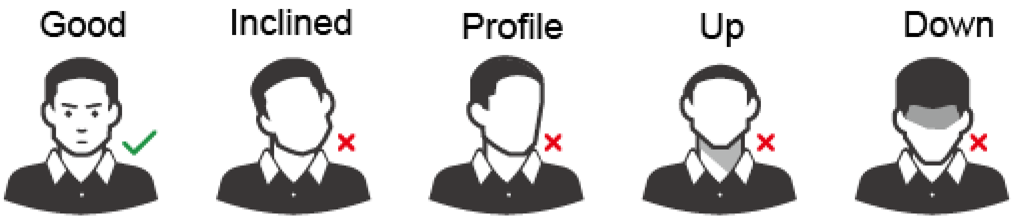
Appendix Figure 1-1 Appropriate face position



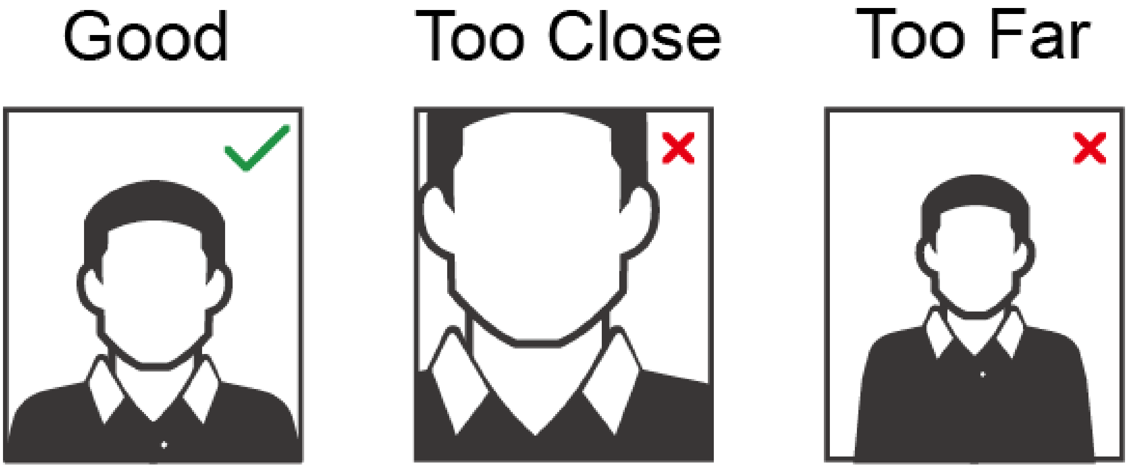
Requirements of Faces

- Make sure that the face is clean and forehead is not covered by hair.
- Do not wear glasses, hats, heavy beards, or other face ornaments that influence face image recording.
- With eyes open, without facial expressions, and make your face toward the center of camera.
- When recording your face or during face recognition, do not keep your face too close to or too far from the camera.

Appendix Figure 1-2 Head position



Appendix Figure 1-3 Face distance



- When importing face images through the management platform, make sure that image resolution is within the range 150 × 300 pixels–600 × 1200 pixels; image pixels are more than 500 × 500 pixels; image size is less than 100 KB, and image name and person ID are the same.
- Make sure that the face takes up more than 1/3 but no more than 2/3 of the whole image area, and the aspect ratio does not exceed 1:2.

Appendix 2 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.
2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.
3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.
4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.
5. **Set and update password reset information in a timely manner**

   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.
3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.
2. **Update client software in time**

   It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).