TIMEWATCH®

Presence perfect

Face Recognition Device

TrueFace1L

User Manual

V1.2.2

Foreword

General

This manual introduces the functions and operations of the Face Recognition Access Controller (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.
ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
ELECTRIC SHOCK	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
LASER RADIATION	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.2.2	Updated the attendance permissions settings.	June 2024
V1.2.1	Updated the intercom settings, access control settings and more.	May 2024
V1.2.0	Updated communication settings, access control settings and more.	November 2023
V1.1.0	Updated the manual.	October 2023

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Version	Revision Content	Release Time
V1.0.0	First Release.	June 2023

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Table of Contents

Foreword I
Important Safeguards and Warnings III
1 Overview 1
2 Local Operations 2
2.1 Basic Configuration Procedure 2
2.2 Common Icons 2
2.3 Standby Screen 3
2.4 Initialization 5
2.5 Logging In 6
2.6 Resetting the Password 6
2.7 Unlocking Methods 7
2.7.1 Unlocking by Cards 7
2.7.2 Unlocking by Face 7
2.7.3 Unlocking by User Password 8
2.7.4 Unlocking by Admin Password 8
2.7.5 Unlocking by QR code 8
2.7.6 Unlocking by Fingerprint 9
2.7.7 Unlocking by Temporary Password 9
2.8 Person Management 9
2.8.1 Adding Users 9
2.8.2 Viewing User Information 13
2.8.3 Configuring the Admin Unlock Password 14
2.9 Access Control Management 14
2.9.1 Configuring Unlock Method 14
2.9.1.1 Configuring Unlock Combinations 14
2.9.1.2 Configuring Unlock by Period 16
2.9.1.3 Configuring Unlock by Multiple Users 16
2.9.2 Configuring Alarms 16
2.9.3 Configuring the Door Status 19
2.9.4 Configuring the Verification Time Interval 20
2.10 Attendance Management 20
2.10.1 Configuring Departments 20
2.10.2 Configuring Shifts 21
2.10.3 Configuring Holiday Plans 24

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

2.10.4 Configuring Work Schedules 24
2.10.5 Configuring Attendance Modes 27
2.11 Communication Settings 29
2.11.1 Configuring Network 29
2.11.1.1 Configuring the IP Address 29
2.11.1.2 Configuring Auto Registration 30
2.11.1.3 Configuring Wi-Fi 31
2.11.1.4 Configuring Wi-Fi AP 32
2.11.2 Configuring Serial Port 33
2.11.3 Configuring Wiegand 35
2.12 System Settings 36
2.12.1 Configuring Time 36
2.12.2 Configuring Face Parameters 38
2.12.3 Setting the Volume 41
2.12.4 Configuring the Language 41
2.12.5 Screen Settings 41
2.12.6 (Optional) Configuring Fingerprint Parameters 42
2.12.7 Restoring Factory Defaults 42
2.12.8 Restarting the Device 42
2.13 Functions Settings 43
2.14 USB Management 47
2.14.1 Exporting to USB 47
2.14.2 Importing from USB 48
2.14.3 Updating the System 48
2.15 Record Management 48
2.16 System Information 48
2.16.1 Viewing Data Capacity 48
2.16.2 Viewing Device Version 49
3 Web Operations 50
3.1 Initialization 50
3.2 Logging In 50
3.3 Resetting the Password 51
3.4 Home Page 52
3.5 Person Management 53
3.6 Configuring Access Control 58
3.6.1 Configuring Access Control Parameters 58

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.6.1.1 Configuring Basic Parameters 58
3.6.1.2 Configuring Unlock Methods 59
3.6.2 Configuring Alarms 61
3.6.3 Configuring Alarm Linkages (Optional) 64
3.6.4 Configuring Alarm Event Linkage 66
3.6.5 Configuring Face Detection 67
3.6.6 Configuring Card Settings 71
3.6.7 Configuring QR Code 73
3.6.8 Configuring Schedules 74
3.6.8.1 Configuring Time Periods 74
3.6.8.2 Configuring Holiday Plans 75
3.6.9 Privacy Settings 77
3.6.10 Configuring Expansion Modules 78
3.6.11 Configuring Port Functions 78
3.6.12 Configuring Back-end Comparison 79
3.7 Configuring Intercom 79
3.7.1 Using the Device as the SIP Server 80
3.7.1.1 Configuring SIP Server 80
3.7.1.2 Configuring Local Parameters 81
3.7.1.3 Adding the Door Station 81
3.7.1.4 Adding the VTH 83
3.7.1.5 Adding the VTS 86
3.7.2 Using VTO as the SIP server 87
3.7.2.1 Configuring SIP Server 87
3.7.2.2 Configuring Local Parameters 88
3.7.3 Using the Platform as the SIP server 89
3.7.3.1 Configuring SIP Server 89
3.7.3.2 Configuring Local Parameters 91
3.7.3.3 Registration Management 92
3.7.4 Simple Mode 92
3.8 Attendance Configuration 93
3.8.1 Configuring Departments 93
3.8.2 Configuring Shifts 94
3.8.3 Configuring Holiday 97
3.8.4 Configuring Work Schedules 98
3.8.5 Configuring Attendance Modes 100

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.9 Configuring Audio and Video 102
3.9.1 Configuring Video 102
3.9.1.1 Configuring Channel 1 102
3.9.1.2 Configuring Channel 2 107
3.9.2 Configuring Audio Prompts 111
3.9.3 Configuring Motion Detection 112
3.9.4 Configuring Local Coding 113
3.10 Communication Settings 114
3.10.1 Network Settings 114
3.10.1.1 Configuring TCP/IP 114
3.10.1.2 Configuring Wi-Fi 116
3.10.1.3 Configuring Port 117
3.10.1.4 Configuring Basic Service 118
3.10.1.5 Configuring Cloud Service 120
3.10.1.6 Configuring Auto Registration 121
3.10.1.7 Configuring CGI Actively Registers 122
3.10.1.8 Configuring Auto Upload 123
3.10.2 Configuring RS-485 124
3.10.3 Configuring Wiegand 126
3.11 Configuring the System 127
3.11.1 User Management 127
3.11.1.1 Adding Administrators 128
3.11.1.2 Adding ONVIF Users 129
3.11.1.3 Resetting the Password 130
3.11.1.4 Viewing Online Users 131
3.11.2 Configuring Time 131
3.11.3 Configuring the Shortcuts 133
3.12 Personalization 135
3.12.1 Adding Resources 135
3.12.2 Configuring Themes 136
3.13 Management Center 139
3.13.1 One-click Diagnosis 139
3.13.2 System Information 140
3.13.2.1 Viewing Version Information 140
3.13.2.2 Viewing Legal Information 140
3.13.3 Data Capacity 140

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.13.4 Viewing Logs 140
3.13.4.1 System Logs 140
3.13.4.2 Unlock Records 141
3.13.4.3 Call History 141
3.13.4.4 Alarm Logs 141
3.13.4.5 Admin Logs 141
3.13.4.6 USB Management 142
3.13.5 Configuration Management 142
3.13.5.1 Exporting and Importing Configuration Files 142
3.13.5.2 Restoring the Factory Default Settings 143
3.13.6 Maintenance 143
3.13.7 Updating the System 144
3.13.7.1 File Update 144
3.13.7.2 Online Update 144
3.13.8 Advanced Maintenance 144
3.13.8.1 Exporting 144
3.13.8.2 Packet Capture 145
3.14 Security Settings(Optional) 145
3.14.1 Security Status 145
3.14.2 Configuring HTTPS 146
3.14.3 Attack Defense 147
3.14.3.1 Configuring Firewall 147
3.14.3.2 Configuring Account Lockout 148
3.14.3.3 Configuring Anti-DoS Attack 149
3.14.4 Installing Device Certificate 150
3.14.4.1 Creating Certificate 150
3.14.4.2 Applying for and Importing CA Certificate 151
3.14.4.3 Installing Existing Certificate 153
3.14.5 Installing the Trusted CA Certificate 153
3.14.6 Data Encryption 154
3.14.7 Security Warning 155
3.14.8 Security Authentication 156
4 Smart PSS Lite Configuration 157
4.1 Installing and Logging In 157
4.2 Adding Devices 157
4.2.1 Adding Device One by One 157

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

4.2.2 Adding Devices in Batches 159
4.3 User Management 160
4.3.1 Configuring Card Type 160
4.3.2 Adding Users 160
4.3.2.1 Adding Users One by One 160
4.3.2.2 Adding Users in Batches 165
4.3.3 Assigning Access Permission 167
4.3.4 Assigning Attendance Permissions 168
4.4 Access Management 170
4.4.1 Remotely Opening and Closing Door 170
4.4.2 Setting Always Open and Always Close 171
4.4.3 Monitoring Door Status 171
Appendix 1 Important Points of Face Registration 173
Appendix 2 Important Points of Intercom Operation 176
Appendix 3 Important Points of Fingerprint Registration Instructions 177
Appendix 4 Important Points of QR Code Scanning 179
Appendix 5 Security Recommendation 180

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

1 Overview

The Device is an access control panel that supports unlocking through faces, passwords, fingerprint, cards, QR code, and their combinations. Based on the deep-learning algorithm, it features faster recognition and higher accuracy. It can work with management platform which meets various needs of customers.

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.

Devices with non-touch screen must connect to a mouse to perform configurations. This manual uses the device with touch screen as an example.

Some models support connecting extension modules like QR code module, fingerprint module and more. The type of extension modules Device supports might differ, please refer to the actual product.

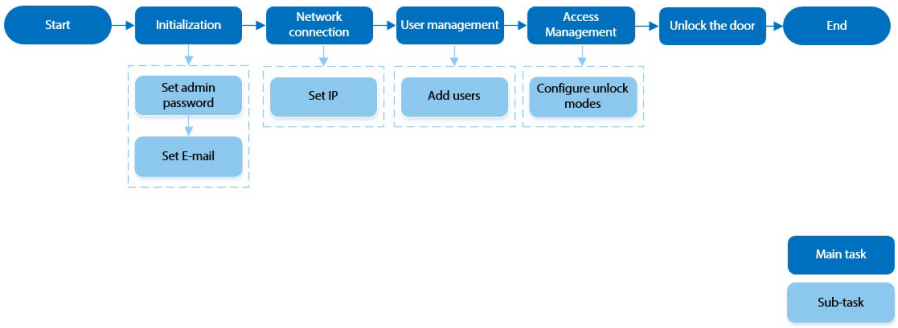
(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

2 Local Operations

Configurations might differ depending on the actual product.
Models with no-touch screen needs connecting a wired USB mouse. This section uses the models with touch screen as an example.
External expansion modules are only available on select models.
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 Basic Configuration Procedure

Figure 2-1 Basic configuration procedure



2.2 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.
	Turn on
	Turn off
	Delete

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Icon	Description
	Search

2.3 Standby Screen

You can unlock the door through faces, card, passwords, and QR code. You can also make calls through the intercom function. Unlock methods might differ depending on the models of the product.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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 2-2 Standby screen

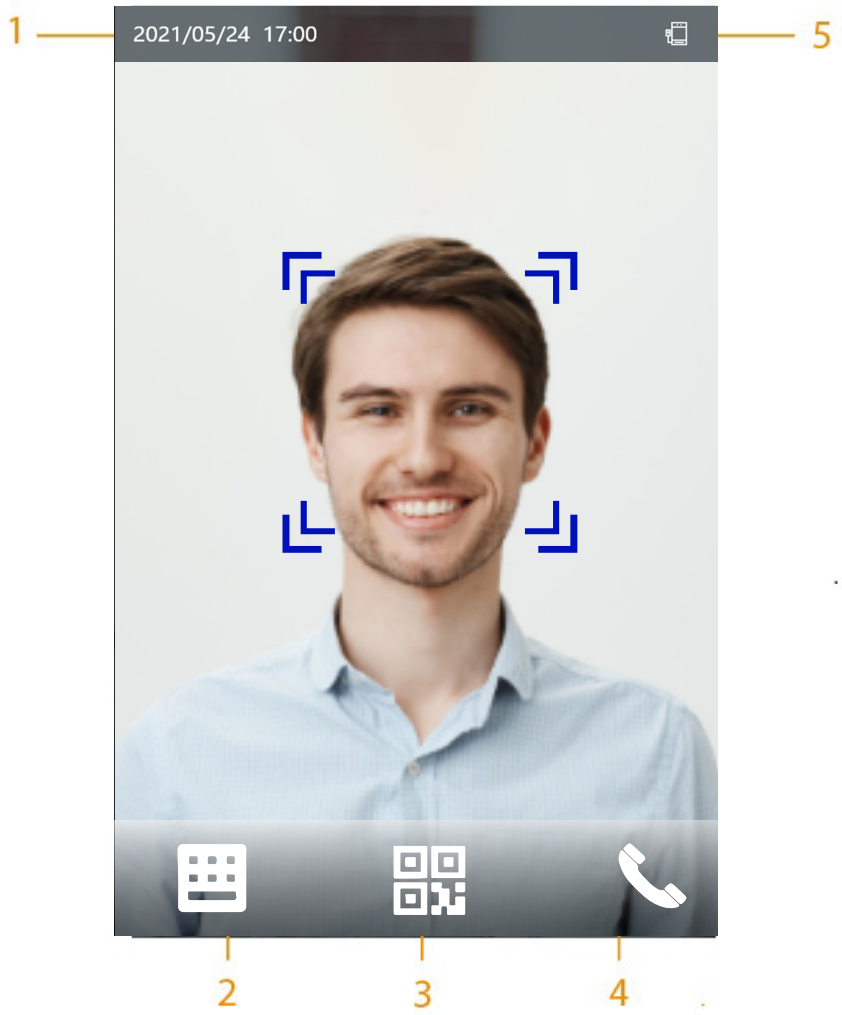


Table 2-2 Home screen description

No.	Name	Description
1	Date and time	Current date and time.
2	Password	Enter user password or administrator password or temporary password to unlock the door.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

No.	Name	Description
3	QR code	Tap the QR code icon and scan QR code to unlock the door. For models that have a standalone QR code module or connects a QR expansion module. The icon will be not displayed. You can simply place your QR code in front of the lens of Device or the expansion module, it will be automatically scanned.
4	Intercom	When the Device functions as a server, it can call the VTO and VTH. When the management platform functions as a server, the Device can call the VTO, VTS and the management platform. When it works with DMSS, it can call DMSS.
5	Status display	Displays status of Wi-Fi, network, extension module, USB and more. Wi-Fi and extension modules are only available on select models.You can tap to enter the Wi-Fi AP screen. For details, see "2.11.1.4 Configuring Wi-Fi AP"

2.4 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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 ' " ; : &).

2.5 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 1.5 seconds.

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

Face: Enter the main menu by face recognition.

Fingerprint: Enter the main menu by using fingerprint.

Fingerprint function is only available on select models.

Card Punch: Enter the main menu by swiping card.

PWD: Enter the user ID and password of the administrator account.

admin: Enter the admin password to enter the main menu.

2.6 Resetting the Password

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

Procedure

Step 1 Press and hold the standby screen for 1.5 seconds.

Step 2 Tap admin , and then tap once on the blank area of the screen.

Step 3 Click Forgot password .

Step 4 Read the on-screen prompt, and then click Enter .

Step 5 Tap QR Code , and then scan the QR code.

Step 6 Send the results of the scan to the designated e-mail address.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

You will receive a security code in your e-mail address.

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.

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.

Step 7 Enter the security code.

If the wrong security code is entered 5 times in a row, the administrator account will be frozen for 5 minutes.

Step 8 Click Next .

Step 9 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 10 Click OK .

2.7 Unlocking Methods

You can unlock the door through faces, passwords, fingerprints, cards, and more.

2.7.1 Unlocking by Cards

Place the card at the swiping area to unlock the door.

This function is only available on select models.

2.7.2 Unlocking by Face

Verify the identity of an individual by detecting their faces. Make sure that the face is centered on the face detection frame.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

2.7.3 Unlocking by User Password

Enter the user ID and password to unlock the door.

Procedure

Step 1 Tap on the standby screen.

Step 2 Tap Unlock by password , and then enter the user ID and password.

Step 3 Tap OK.

2.7.4 Unlocking by Admin Password

Enter only the admin password to unlock the door. The door can be unlocked through admin password except for always closed door. One device allows for only one admin password.

Prerequisites

The admin password was configured. For details, see "2.8.3 Configuring the Admin Unlock Password".

Procedure

Step 1 Tap on the standby screen.

Step 2 Tap Unlock through Admin Password , and then enter the admin password.

Step 3 Tap .

Admin password cannot be used to unlock when the door status is set to always closed status.

2.7.5 Unlocking by QR code

Procedure

Step 1 On the standby screen, tap .

The QR code icon is displayed only after you go to Functions > Face Recognition Interface Shortcut to enable QR code.

Step 2 Place your QR code in front of the lens.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

2.7.6 Unlocking by Fingerprint

Place you finger on the fingerprint scanner. This function is only available select models.

2.7.7 Unlocking by Temporary Password

Unlock the door by the temporary password.

Procedure

Step 1 Add the Device to DMSS.

DMSS will generate a temporary password, which allow you unlock the door before it expires.

Step 2 On the home screen, tap , and then tap Unlock by Temporary Password .

Step 3 Enter the temporary password, and then tap .

2.8 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.

2.8.1 Adding Users

Procedure

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

Step 2 Configure the parameters on the interface.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 2-3 Add new user

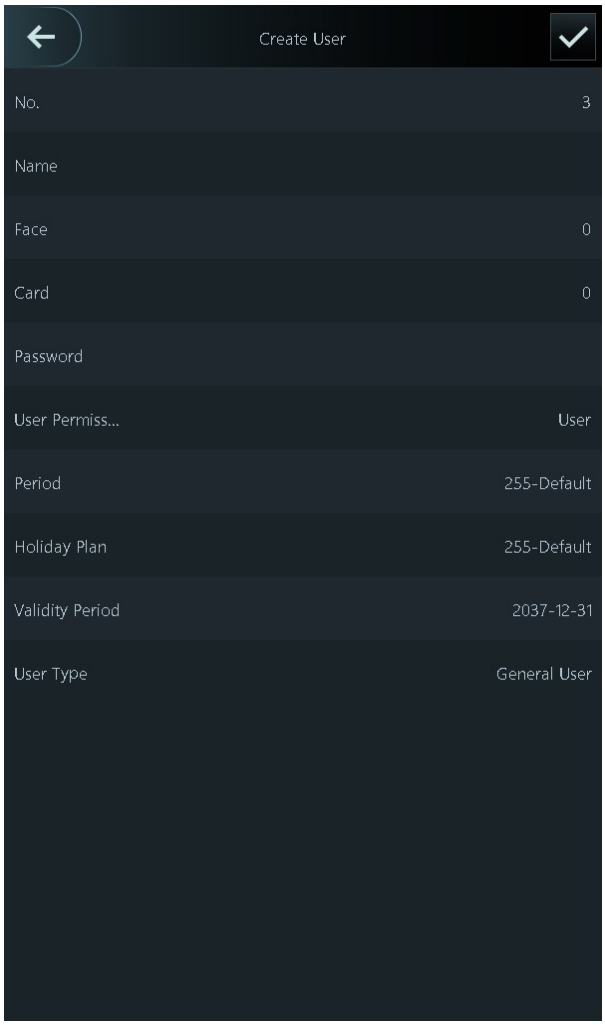


Table 2-3 Parameters description

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).

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
FP	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. Fingerprint function is only available on select models. We do not recommend you set the first fingerprint as the duress fingerprint. One user can only set one duress fingerprint. Fingerprint function is available if the Device supports connecting a fingerprint extension module.
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.
Card	A user can register up to 5 cards at most. Enter your card number or swipe your card, and then the card information will be read by the Device. You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door. This function is only available on select models. One user can only set one duress card.
Password	Enter the user password. The maximum length of the password is 8 digits. The duress password is adding 1 based on the last digit of the unlock password. For example, if the user password is 12345, the duress password will be 12346; if the user password is 789, and then the duress password is 780. A duress alarm will be triggered when a duress password is used to unlock the door.
User Permission	User : Users only have door access or time attendance permissions. Admin : Administrators can configure the Device besides door access and attendance permissions.
Period	People can unlock the door or take attendance during the defined period. For details on how to configure periods, see "3.6.8.1 Configuring Time Periods".

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Holiday Plan	People can unlock the door or take attendance during the defined holiday. For details on how to configure periods, see "3.6.8.2 Configuring Holiday Plans".
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.
User Type	General User : General users can unlock the door. Blocklist User : When users in the blocklist unlock the door, an blocklist alarm will be triggered. Guest User : Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. Patrol User : Patrol users can take attendance on the Device, but they do not have door permissions. VIP User : When VIP unlocks the door, service personnel will receive a notification. Other User : When they unlock the door, the door will stay unlocked for 5 more seconds. This function is not effective when remote verification is enabled. Custom User 1/Custom User 2 : Same with general users.
Department	Select departments, which is useful when configuring department schedules. For how to create departments, see "2.10.1 Configuring Departments". This function is only available on select models.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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 "2.10.4 Configuring Work Schedules". ◇ This function is only available on select models. ◇ 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 .

2.8.2 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.

: Unlock through password.

: Unlock through swiping card.

: Unlock through face recognition.

: Unlock through fingerprint.

Related Operations

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

Search for users: Tap and then enter the username or user ID.

Edit users: Tap the user to edit user information.

Delete users

◇ 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

2.8.3 Configuring the Admin Unlock Password

You can unlock the door by only entering the admin password. This password is not limited by user types. Only one admin unlock password is allowed for one device.

Procedure

Step 1 On the Main Menu screen, select User > Admin Unlock Password .

Step 2 Tap Admin Unlock Password , and then enter a password.

Step 3 Turn on the admin unlock function.

2.9 Access Control Management

You can configure settings for doors such as the unlocking mode, alarm linkage and door schedules. The available unlock modes might differ depending on the product model.

2.9.1 Configuring Unlock Method

2.9.1.1 Configuring Unlock Combinations

Use card, fingerprint, face, password or their combinations to unlock the door. The available unlock modes might differ depending on the product model.

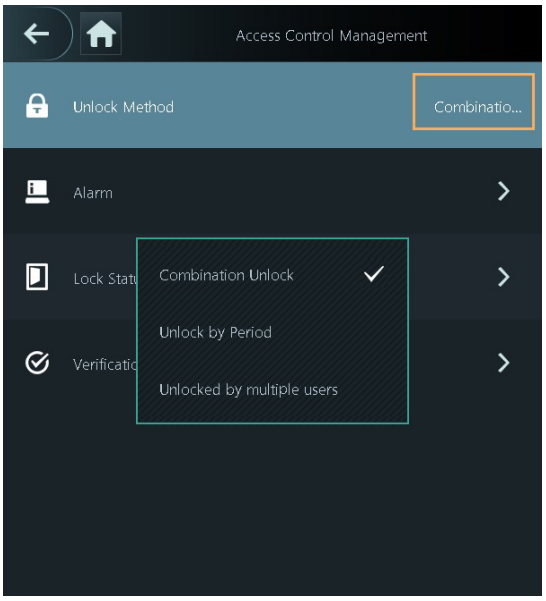
Procedure

Step 1 Select Access Control Management > Unlock Method .

Step 2 Tap Combination Unlock , and the select Combination Unlock form the list.

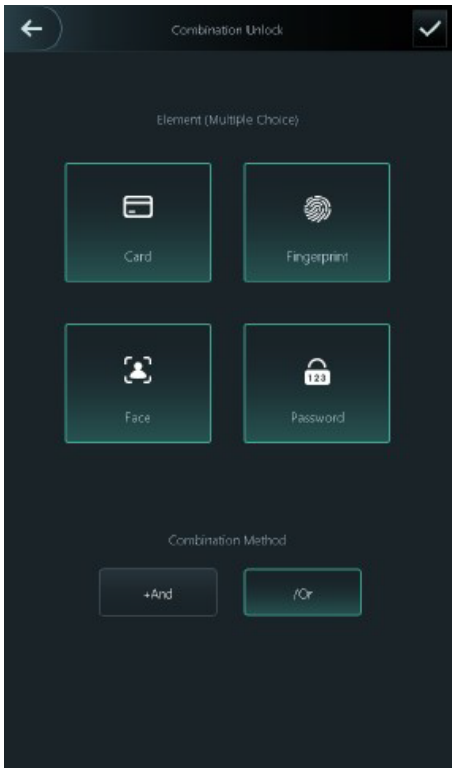
(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 2-4 Combination unlock



Step 3 Tap Unlock Method , and select unlock methods.

Figure 2-5 Combination method



Step 4 Tap + And or /Or to configure combinations.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

To cancel your selection, tap the selected method again.

+And : Verify all the selected unlock methods to open the door.

People have to complete verification in the order of card, fingerprint, face and password.

/Or : Verify one of the selected unlock methods to open the door.

Step 5 Tap ☑ to save changes.

2.9.1.2 Configuring Unlock by Period

Procedure

Step 1 Select Access Control Management > Unlock Method .

Step 2 Tap the right area of Unlock Method , and then select Unlock by Period form the list.

For details on how to configure unlock by period, see "3.6.1.2 Configuring Unlock Methods".

Step 3 Tap ☑ to save changes.

2.9.1.3 Configuring Unlock by Multiple Users

Procedure

Step 1 Select Access Control Management .

Step 2 Tap the right area of Unlock Method , and then select Unlock by multiple users from the list.

For details on how to configure unlock by period, see "3.6.1.2 Configuring Unlock Methods".

Step 3 Tap ☑ to save changes.

2.9.2 Configuring Alarms

An alarm will be triggered when the entrance or exit is abnormally accessed.

Procedure

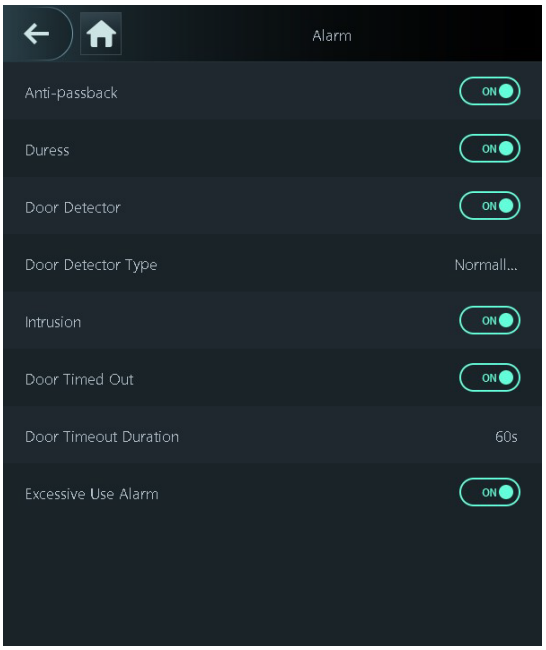
Step 1 Select Access Control Management > Alarm .

Step 2 Enable the alarm type.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Alarm types might differ depending on the models of the product.

Figure 2-6 Alarm



(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Table 2-4 Description of alarm parameters

Parameter	Description
Anti-passback	Users need to verify their identities both for entry and exit; otherwise an alarm will be triggered. This helps prevent card holders from being able to give their card to other people to allow them access. When anti-passback is enabled, the card holder must leave the secure area through an exit reader before the system will grant them access again. People need to swipe their card at the "in" reader to enter a secure area and swipe it at the "out" reader to get out of it. If a person enters after being verified, but exits without being verified, an alarm will be triggered if they attempt to enter again, and they will be denied access. If a person enters without being verified, but exits after being verified, an alarm will be triggered if they attempt to enter again, and they will be denied access. If the Device can only connect to one lock, verification through the Device means a person entered in the "in" direction, and verification through the external card reader means they exited in the "out" direction. This is the default.
Duress	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Door Detector	With the door detector wired to your device, alarms can be triggered when doors are opened or closed abnormally. There are 2 types of door detectors: NC detector and NO detector.
Door Detector Type	Normally Closed: The sensor is in a shorted position when the door or window is closed. Normally Open: An open circuit is created when the window or door is actually closed.
Intrusion	If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time.
Door Timed Out	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time. The door detector and door timed out function need to be enabled at the same time.
Door Timeout Duration	

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Excessive Use Alarm	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time.

2.9.3 Configuring the Door Status

Procedure

Step 1 On the Main Menu screen, select Access Control Management > Lock Status Config .

Step 2 Set door status.

Figure 2-7 Lock status

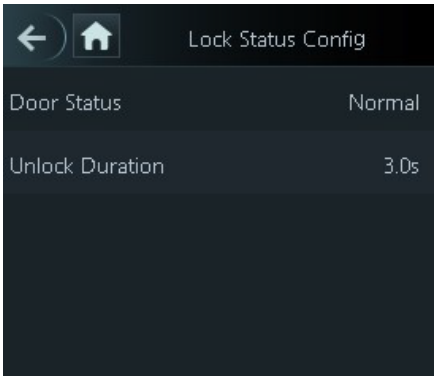


Table 2-5 Parameters description

Parameter	Description
Door Status	Normally Open : The door remains unlocked all the time. Normally Closed : The door remains locked all the time. Normal : If Normal is selected, the door will be locked and unlocked according to your settings.
Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

2.9.4 Configuring the Verification Time Interval

If you verify your identity multiple times within a set period, only the earliest verification will be considered valid, and the door will not open after the second or later verifications. From the moment the door fails to open, you must wait for the configured verification time interval before attempting to verify your identity again.

Procedure

Step 1 Select Access Control Management > Verification Interval (sec) .

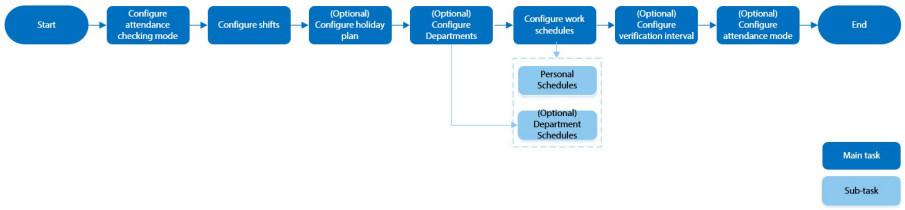
Step 2 Enter the time interval, and then tap ☑.

2.10 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.

This function is only available on select models (devices of 4.3-inch series).

Figure 2-8 Configuration flow chart of time attendance



2.10.1 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 2-9 Create departments

Step 3 Tap ☑.

2.10.2 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 Select a shift.

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

Step 3 Configure the parameters of the shift.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 2-10 Create shifts

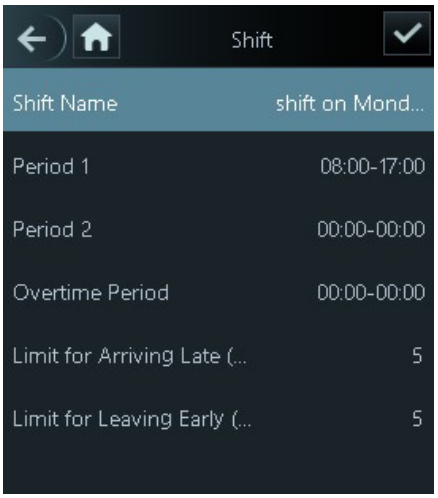


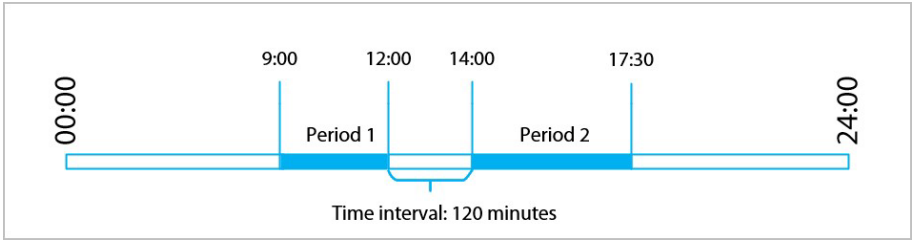
Table 2-6 Shift parameters description

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 2-11 Time interval (Even number)

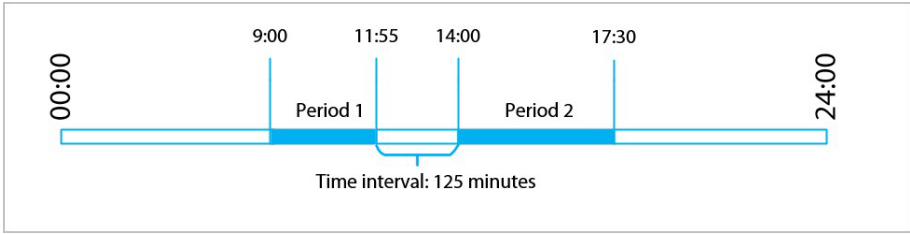


For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.

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 2-12 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 ☑.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

2.10.3 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 2-13 Create holiday plans

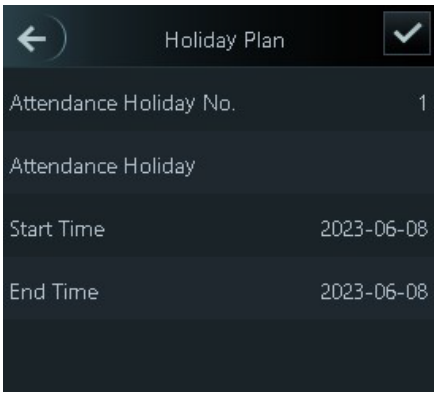


Table 2-7 Parameters description

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 ☑.

2.10.4 Configuring Work Schedules

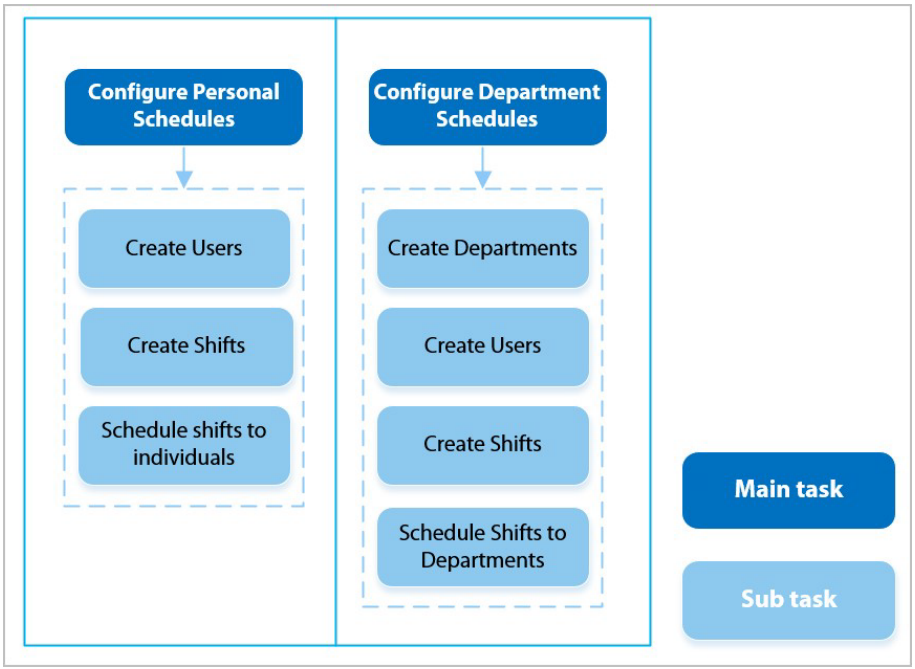
A work schedule generally refers to the days per month and the hours per day that an employee is expected to be at their job. You can create different types of work schedules based on different individuals or departments, and then employees must follow the established work schedules.

Background Information

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 2-14 Configuring work schedules



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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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

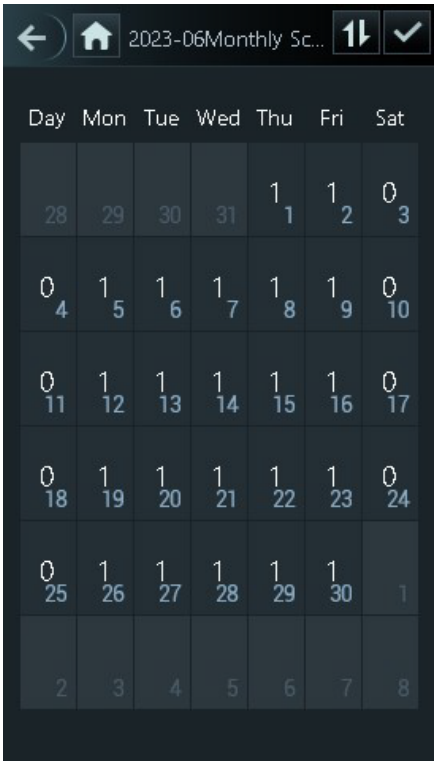
0 indicates break.

1 to 24 indicates the number of the per-defined shifts. For how to configure shifts, see "2.10.2 Configuring Shifts".

25 indicates business trip.

26 indicates leave of absence.

Figure 2-15 Schedule shifts to individuals



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.

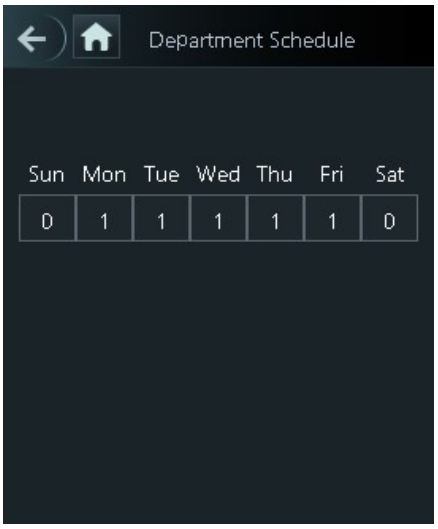
   1 to 24 indicates the number of the per-defined shifts. For how to configure shifts, see "2.10.2 Configuring Shifts".

   25 indicates business trip.

   26 indicates leave of absence.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 2-16 Schedule shifts to a department



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

Step 4 Tap ☑.

2.10.5 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 set the attendance mode.

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 2-17 Attendance mode

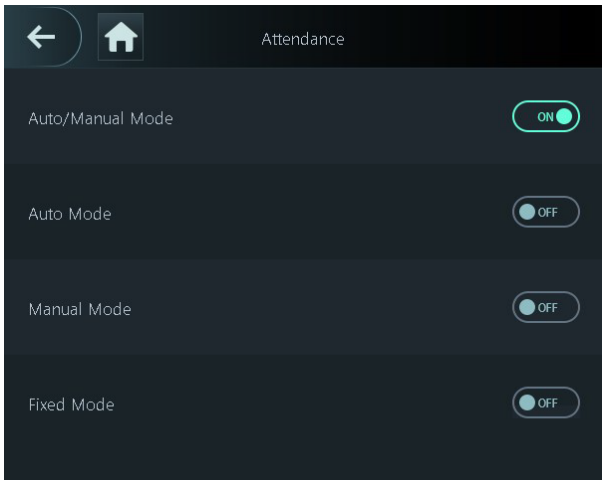


Table 2-8 Attendance mode

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 2-18 Auto Mode/manual mode

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 2-19 Fixed mode

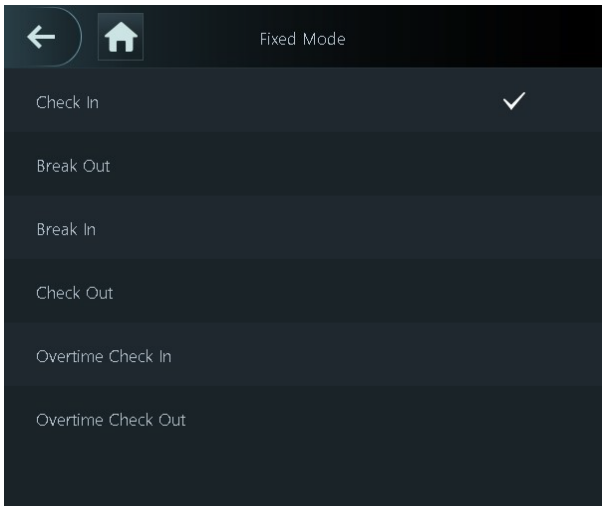


Table 2-9 Attendance mode parameters

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.

2.11 Communication Settings

Configure the network, serial port and Wiegand port to connect the Device to the network.

The serial port and the Wiegand port might differ depending on the models of Device.

2.11.1 Configuring Network

2.11.1.1 Configuring the IP Address

Set an IP address for the Device to connect it to the network. After that, you can log in to the webpage and the management platform to manage the Device.

Procedure

Step 1 On the Main Menu , select Communication Settings > Network > IP Address .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Step 2 Set the IP Address.

Figure 2-20 IP address configuration

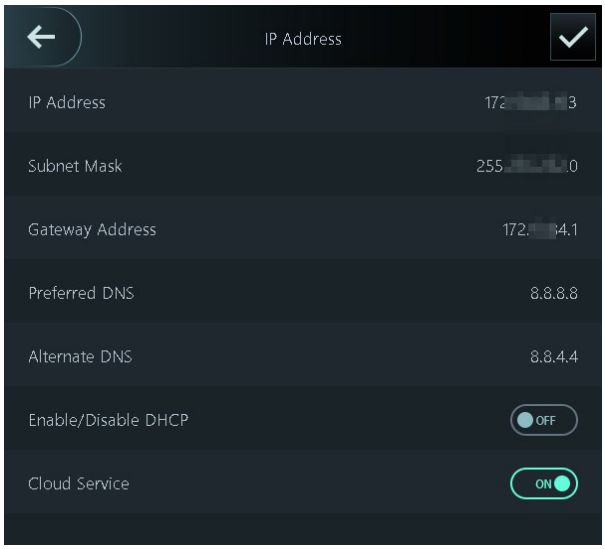


Table 2-10 IP configuration parameters

Parameter	Description
IP Address/Subnet Mask/Gateway Address	The IP address, subnet mask, and gateway IP address must be on the same network segment.
Preferred DNS	The IP of the DNS server.
Alternate DNS	The alternate IP of the DNS server.
Enable/Disable DHCP	It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Device will automatically be assigned an IP address, subnet mask, and gateway.
Cloud Service	Manage devices without applying for DDNS, set port mapping and deploy transit servers.

2.11.1.2 Configuring Auto Registration

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

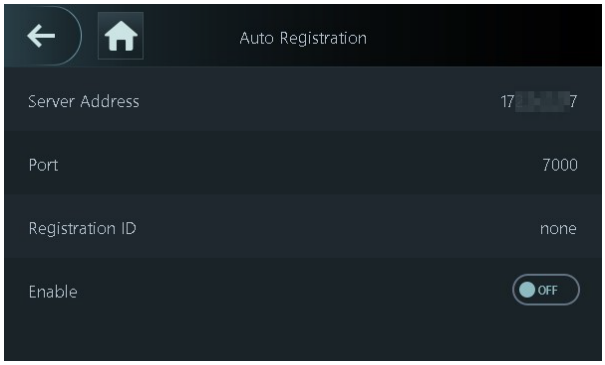
Procedure

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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

Figure 2-21 Active registration



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

Table 2-11 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.

2.11.1.3 Configuring Wi-Fi

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

Background Information

This function is only available on select models.

Procedure

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

Step 2 Turn on Wi-Fi.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

The Wi-Fi function is only available on select models.

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

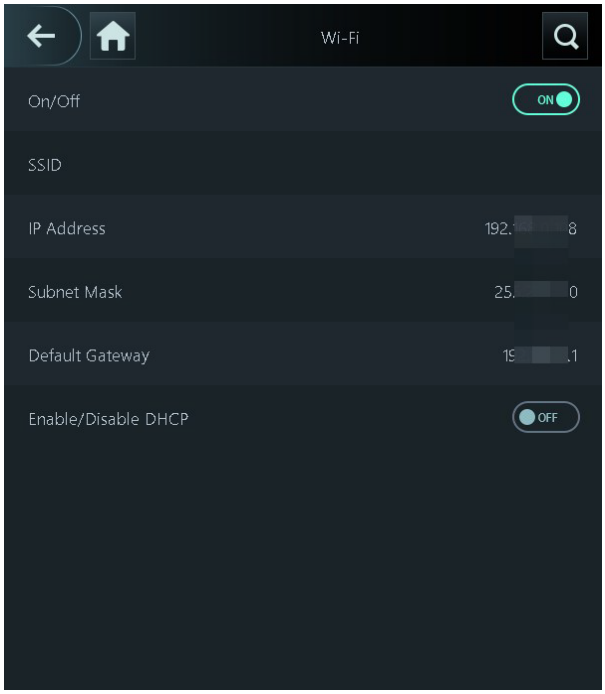
After Wi-Fi is enabled, wait about 1 minutes to connect Wi-Fi.

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 2-22 Connect to Wi-Fi



Related Operations

Enable/Disable DHCP: Enable this function, and the Device will automatically be assigned a Wi-Fi address.

2.11.1.4 Configuring Wi-Fi AP

This function is only available on select models.

Procedure

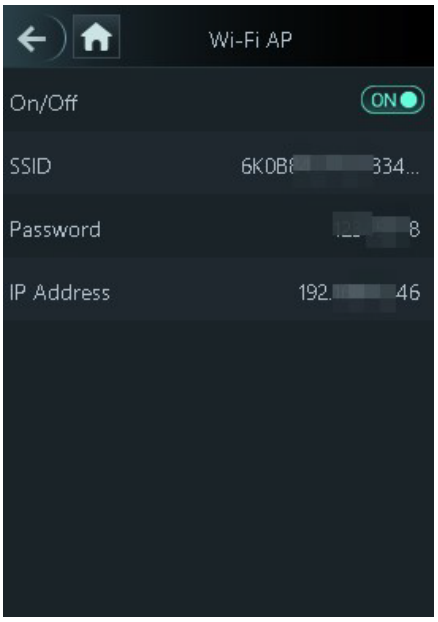
Step 1 On the Main Menu , select Communication Settings > Network > Wi-Fi AP .

Step 2 Turn on Wi-Fi AP.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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

Figure 2-23 Connect to Wi-Fi AP



Result

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

2.11.2 Configuring Serial Port

This function is only available on select models.

Procedure

Step 1 On the Main Menu , select Communication Settings > Serial Port .

Step 2 Select an external device.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 2-24 External device type

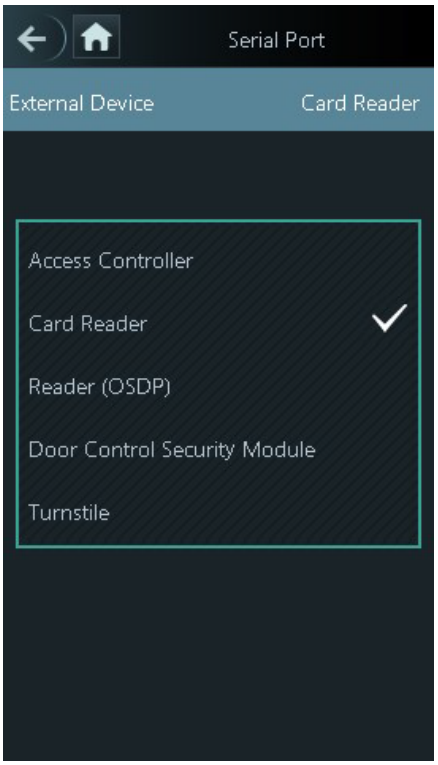


Table 2-12 Port description

External device	Description
Access Controller	The Device functions as a card reader and sends data to other external access controllers to control access. Output Data type: Card Number: Outputs data based on the card number when users swipe their cards to unlock doors; outputs data based on user's first card number when users use other unlock methods. No.: Outputs data based on the user ID.
Card Reader	The Device functions as an access controller, and connects to an external card reader.
Reader (OSDP)	The Device is connected to a card reader based on the OSDP protocol.
Door Control Security Module	After the security module is enabled, the door exit button, lock control and fire linkage of the Device become not effective, but the door exit button and lock control that connects to the security module become effective.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

External device	Description
Turnstile	When the Device is connected to a turnstile, and the access controller board of the turnstile is connected to an external QR code module or card swiping module, the board will transmit the verification data to the turnstile.

2.11.3 Configuring Wiegand

The Device allows for both Wiegand input and output mode.

This function is only available on select models.

Procedure

Step 1 On the webpage, select Communication Settings > Wiegand .

Step 2 Select a Wiegand.

Select Wiegand Input when you connect an external card reader to the Device.

When the Device connects to a third-party device through the Wiegand input port, and the card number read by the Device is in the reverse order from the actual card number. In this case, you can turn on Card No. Inversion function.

Select Wiegand Output when the Device functions as a card reader, and you need to connect it to a controller or another access terminal.

Figure 2-25 Wiegand output

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Table 2-13 Description of Wiegand output

Parameter	Description
Wiegand Output Type	Select a Wiegand format to read card numbers or ID numbers. Wiegand26 : Reads 3 bytes or 6 digits. Wiegand34 : Reads 4 bytes or 8 digits. Wiegand66 : Reads 8 bytes or 16 digits.
Pulse Width	Enter the pulse width and pulse interval of Wiegand output.
Pulse Interval	
Output Data Type	Select the type of output data. No. : The system outputs data based on the user ID. The data format is hexadecimal or decimal. Card Number : The system outputs data based on user's first card number.

2.12 System Settings

2.12.1 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 2-26 Time

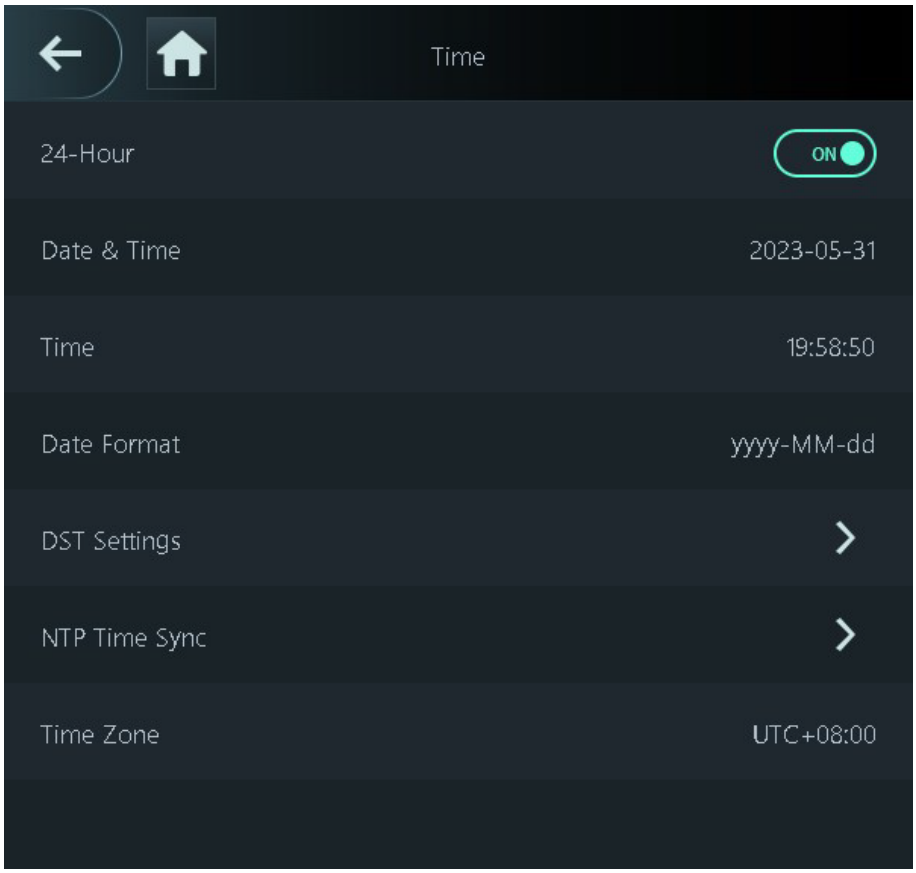


Table 2-14 Description of time parameters

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 ☑.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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.

2.12.2 Configuring Face Parameters

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

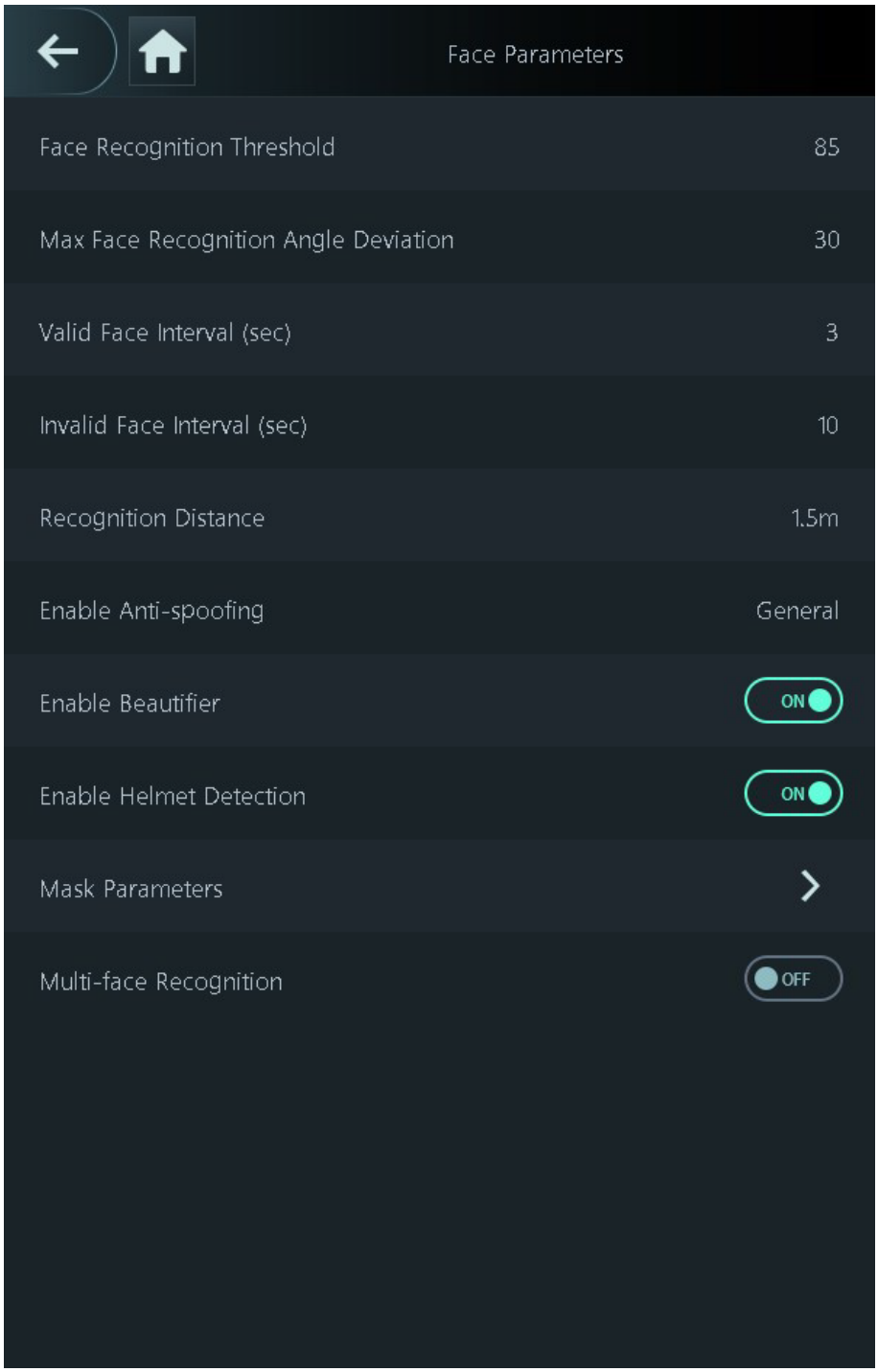
Procedure

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

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 2-27 Face parameter



(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Table 2-15 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.
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.
Recognition Distance	The distance between the face and the lens.
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.
Enable Helmet Detection	Detects safety helmets. The door will not unlock for persons that are not wearing their helmet.
Mask Parameters	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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Name	Description
Multi-face Recognition	Detects 4 to 6 face images at a time. Combination unlock cannot be used with this, and the door will be unlocked when one of the people are successfully verified. The number of face images which are supported might differ depending on the model of the product.
Illuminator Mode	Auto: The illuminator is turned on in low-light conditions. Disable: The illuminator is turned off all the time. This function is only available on select models.

2.12.3 Setting the Volume

Procedure

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

Step 2 Configure the parameters.

Table 2-16 Parameters description

Parameters	Description
Beep Volume	and then tap + or − to adjust the volume.
Microphone Volume	
Screen Tap Sound	When this function is enabled, touch screen devices will produce tap sound and non-touch screen devices will produce mouse click sound.

2.12.4 Configuring the Language

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

2.12.5 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 , Screen Off Settings or Screen Brightness Settings , and then tap

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

+ or − to adjust the time or screen brightness.

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.

2.12.6 (Optional) Configuring Fingerprint Parameters

Configure fingerprint detection accuracy. The higher the value, the higher the similarity threshold and accuracy is.

Background Information

This function is only available on select models, and some supports being connected to a fingerprint extension module.

Procedure

Step 1 On the Main Menu , select System Settings > Fingerprint Parameter Settings .

Step 2 Tap + or − to adjust the value.

2.12.7 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 and the type of the extension module.

Restore to Default Settings (except for user information and logs) : Resets all the configurations except for user information and logs.

2.12.8 Restarting the Device

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

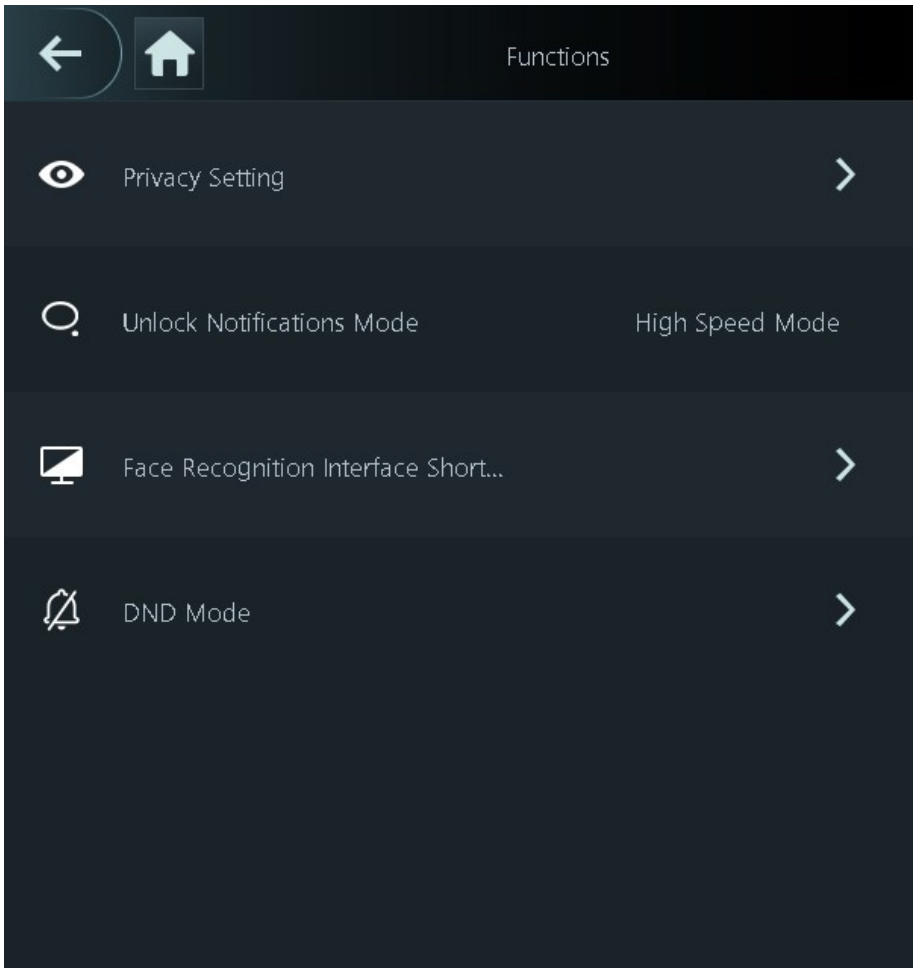
(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

2.13 Functions Settings

On the Main Menu screen, select Functions .

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

Figure 2-28 Functions



(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Table 2-17 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. Fingerprint Image: The fingerprint image is displayed when you unlock through fingerprint. This function is only available on select models. Capture: Face images will be captured automatically when people unlock the door. Clear All Snapshots: Delete all automatically captured photos.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Push Notifications	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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Face Recognition Interface Shortcut	Select identity verification methods on the standby screen. Password: It's icon is displayed on the standby screen. QR code: It's icon is displayed on the standby screen. This function is only available on select models. Doorbell: It's 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. ◇ Alarm: Tap the ring bell icon, and the external alarm device rings. This function is only available on select models. When the alarm cable and the doorbell cable are shared, make sure the functional interface is set to Doorbell . For details, see "3.6.11 Configuring Port Functions". Call: It's icon is displayed on the standby screen. Call Type: ◇ Call Room: Tap the call icon on the standby mode and enter the room number to make a call. ◇ Call Management Center: Tap the call icon on the standby mode, and then call the management center. ◇ Custom call room: Tap the call icon on the standby screen to call the pre-defined room. You can call DMSS only in this call type. SIP Server: You can turn on SIP to set the Device to SIP server.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Expansion Module	Select an expansion module, and the Device will restart. is displayed on the right corner on the standby screen, which means it was successfully set. is displayed on the right corner on the standby screen, which means setup failed. Expansion module is only available on select models. Expansion module does not support hot swapping. The configuration for the expansion module remains unchanged even after the system is restored to its factory settings.
DND Mode	No voice prompts during the set time when you verify your identity on the Device. You can set up to 4 periods.

2.14 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.

2.14.1 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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, card data, fingerprint data are encrypted when exporting.

2.14.2 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.

2.14.3 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.

2.15 Record Management

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

2.16 System Information

You can view data capacity and device version.

2.16.1 Viewing Data Capacity

On the Main Menu , select System Info > Data Capacity , you can view storage capacity of

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

each data type.

2.16.2 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.

Related Operations

Tap Product Material QR Code , scan the QR code with your phone to view the product documents.

This function is only available on select models.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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 (the default address is 192.168.1.108) 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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.

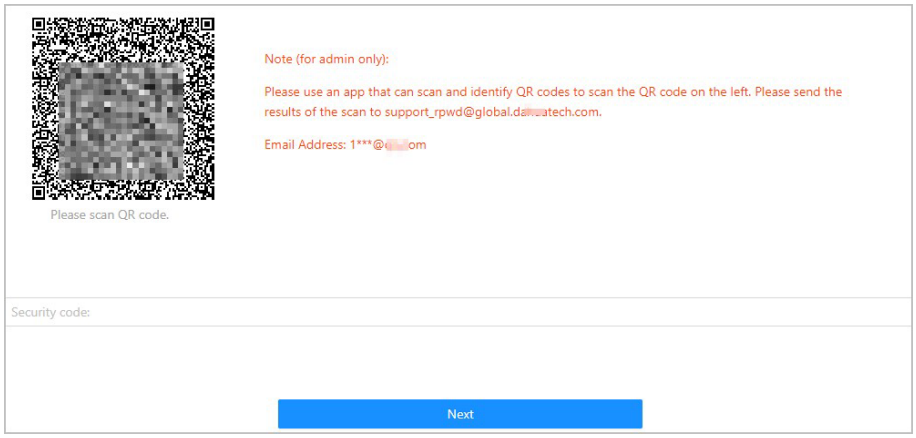
Procedure

Step 1 On the login page, click Forgot password .

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

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

Figure 3-1 Reset password



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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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

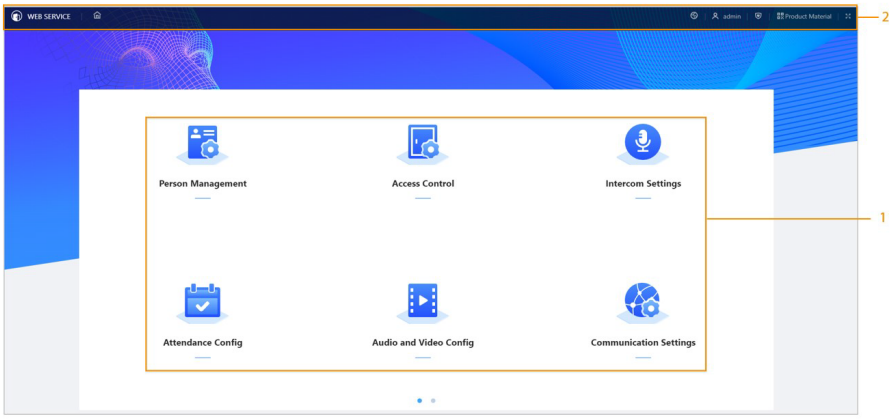


Table 3-1 Home page description

No.	Description
1	Main menu.
2	: Enter the home page. : Display in full screen. : Enter the Security page. Product Material: Scan the QR code with your phone to view the product documents. This function is only available on select models admin: Log out or restart the device. : Select a language on the device.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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

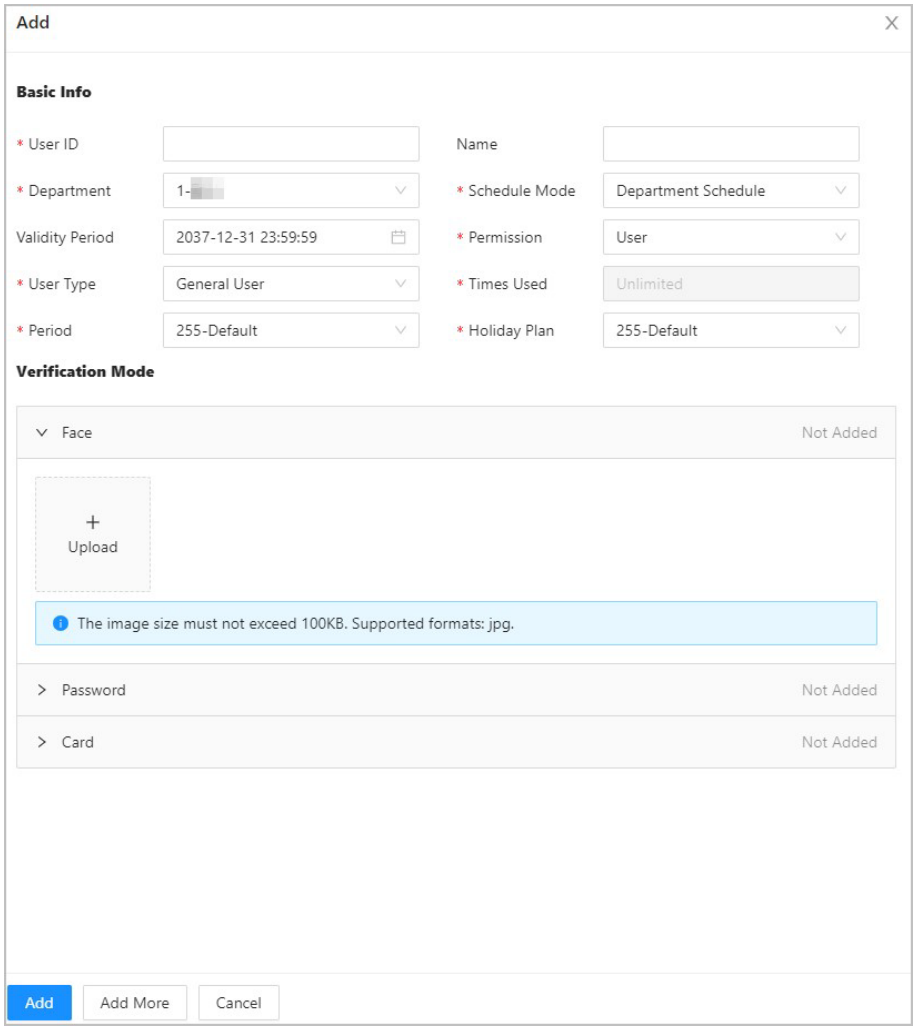


Table 3-2 Parameters description

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Name	The name can have up to 32 characters (including numbers, symbols, and letters).
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 "2.10.1 Configuring Departments".
Schedule Mode	Department Schedule: Assign department schedule to the user. For details, see "2.10.4 Configuring Work Schedules". Personal Schedule: Assign personal schedule to the user. For details, see "2.10.4 Configuring Work Schedules". ◇ This function is only available on select models. ◇ 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.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.
Permission	User : Users only have door access or time attendance permissions. Admin : Administrators can configure the Device besides door access and attendance permissions.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
User Type	General User : General users can unlock the door. Blocklist User : When users in the blocklist unlock the door, service personnel will receive a notification. Guest User : Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. Patrol User : Patrol users can take attendance on the Device, but they do not have door permissions. VIP User : When VIP unlock the door, service personnel will receive a notice. Other User : When they unlock the door, the door will stay unlocked for 5 more seconds. Custom User 1/Custom User 2: Same with general users.
Time Used	Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.
Period	People can unlock the door or take attendance during the defined period. You can select more than one period.
Holiday Plan	People can unlock the door or take attendance during the defined holiday. You can select more than one holiday.
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, jpeg, png format and must be less than 100 KB.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Card	This function is only available on select models. Enter the card number manually. 1. Click Add . 2. Enter the card number, and then click Add . Read the number automatically through the enrollment reader or the Device. 1. Click Add , and then click Modify to select an enrollment reader or the Device. 2. Click Read Card , and then swipe cards on the card reader. A 60-second countdown is displayed to remind you to swipe cards, and the system will read the card number automatically. If the 60-second countdown expires, click Read Card again to start a new countdown. 3. Click Add . A user can register up to 5 cards at most. Enter your card number or swipe your card, and then the card information will be read by the Device. You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door. : Set duress card. : Change card number. One user can only set one duress card.
Password	Enter the user password. The maximum length of the password is 8 digits. The duress password is the unlock password + 1. For example, if the user password is 12345, the duress password will be 12346. A duress alarm will be triggered when a duress password is used to unlock the door.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
FP	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. Enroll fingerprints through an enrollment reader or the Device. 1. Click Add , and then click Modify to select an enrollment reader or the Device. 2. Press finger on the scanner according to the on-screen instructions. 3. Click Add . Fingerprint function is only available on select models. We do not recommend you set the first fingerprint as the duress fingerprint. One user can only sets one duress fingerprint. Fingerprint function is available if the Device supports connecting a fingerprint module.

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 file path, 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.

Search: Search by user name or user ID.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.6 Configuring Access Control

3.6.1 Configuring Access Control Parameters

3.6.1.1 Configuring Basic Parameters

Procedure

Step 1 Select Access Control > Access Control Parameters .

Step 2 In Basic Settings , configure basic parameters for the access control.

Figure 3-4 Basic parameters

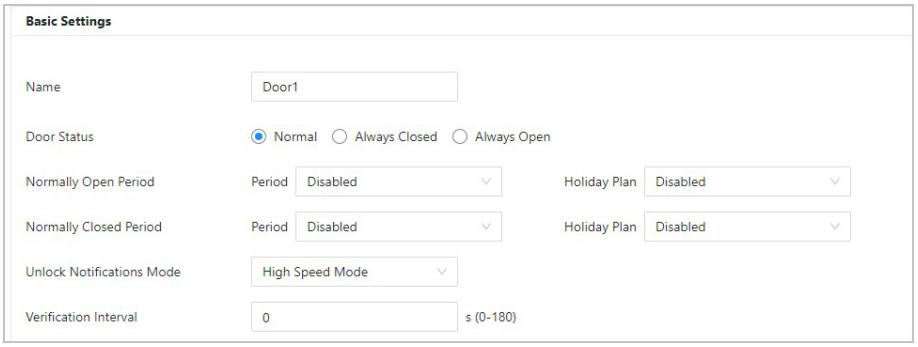


Table 3-3 Basic parameters description

Parameter	Description
Name	The name of the door.
Door Status	Set the door status. Normal: The door will be unlocked and locked according to your settings. Always Open: The door remains unlocked all the time. Always Closed: The door remains locked all the time.
Normally Open Period	When you select Normal , you can select a time template from

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Normally Closed Period	the drop-down list. The door remains open or closed during the defined time. For details on how to configure periods and holiday plans, see "3.6.8 Configuring Schedules". When normally open period conflicts with normally closed period, normally open period takes priority over normally closed period. When period conflict with holiday plan, holiday plans takes priority over periods.
Unlock Notification	Displays the notification on the screen when a person 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 granted; displays Not authorized and authorization time after access denied. Standard: Displays user's registered face image, user ID, name and verification time after access granted; displays Not authorized and verification time after access denied. Contrast Mode: Displays the captured face image and a registered face image of a user, user ID, name and authorization time after access granted; displays Not authorized and authorization time after access denied.
Verification Interval	If you verify your identity multiple times within a set period, only the earliest verification will be considered valid, and the door will not open after the second or later verifications. From the moment the door fails to open, you must wait for the configured verification time interval before attempting to verify your identity again.

Step 3 Click Apply .

3.6.1.2 Configuring Unlock Methods

You can use multiple unlock methods to unlock the door, such as fingerprint, card, and password. You can also combine them to create your own personal unlock method.

Procedure

Step 1 Select Access Control > Access Control Parameters .

Step 2 In Unlock Settings , select an unlock mode.

Combination unlock

1. Select Combination Unlock from the Unlock Mode list.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

2. Select Or or And .
   - Or: Use one of the selected unlock methods to open the door.
   - And: Use all the selected unlock methods to open the door.
3. Select unlock methods, and then configure other parameters.

Figure 3-5 Unlock settings

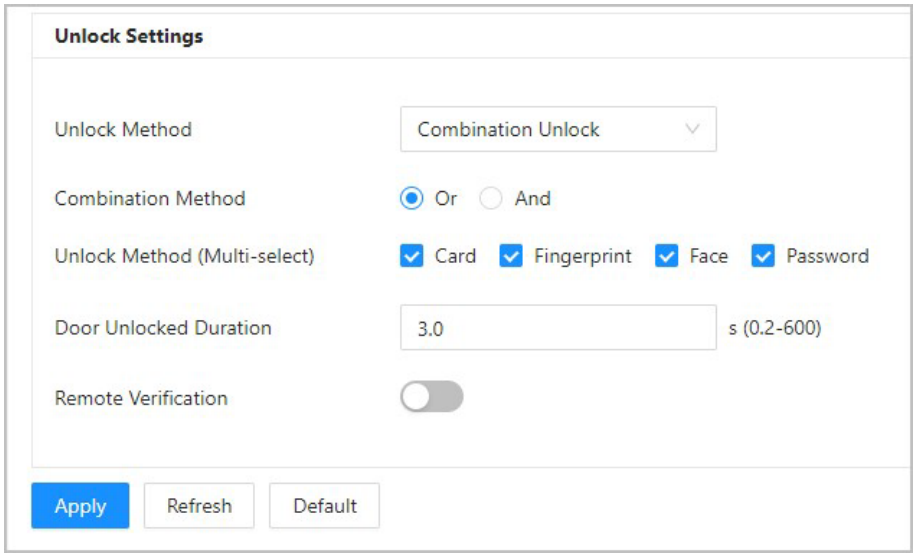


Table 3-4 Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Unlock methods might differ depending on the models of product.
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through. It ranges from 0.2 to 600 seconds.
Unlock Timeout	When the door detector and the unlock timeout alarm are enabled, a timeout alarm will be triggered if the door remains unlocked longer than the defined unlock time.
Remote Verification	Open the door remotely.

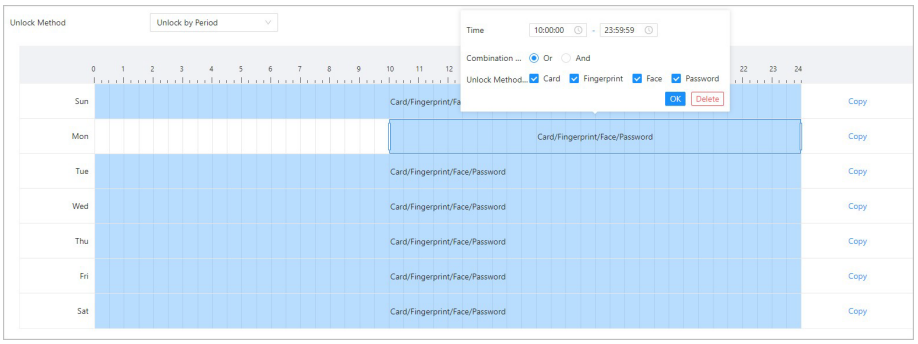
Unlock by period

1. In the Unlock Mode list, select Unlock by Period .
2. Drag the slider to adjust time period for each day.

   You can also click Copy to apply the configured time period to other days.
3. Select an unlock method for the time period, and then configure other parameters.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-6 Unlock by period



Unlock by multiple users.

1. In the Unlock Mode list, select Unlock by multiple users .
2. Click Add to add groups.
3. Select unlock method, valid number and user list.
   - If only one group is added, the door unlocks only after the number of people in the group who grant access equals the defined valid number.
   - If more than one groups are added, the door unlocks only after the number of people in each group who grant access equals the defined valid number.

- You can add up to 4 groups.
- The valid number indicates the number of people in each group who need to verify their identities on the Device before the door unlocks. For example, if the valid number is set to 3 for a group, any 3 people in the group need to verify their identities to unlock the door.

Step 3 Click Apply .

3.6.2 Configuring Alarms

An alarm will be triggered when an abnormal access event occurs.

Procedure

Step 1 Select Access Control > Alarm > Alarm .

Step 2 Configure alarm parameters.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-7 Alarm

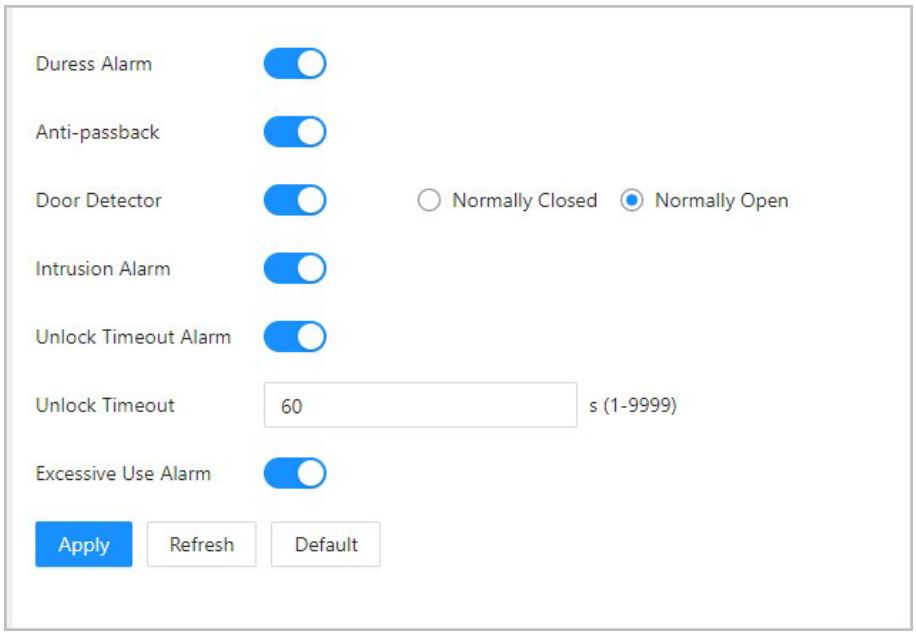


Table 3-5 Description of alarm parameters

Parameter	Description
Duress Alarm	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Anti-passback	Users need to verify their identities both for entry and exit; otherwise an alarm will be triggered. It helps prevents a card holder from passing an access card back to another person to gain entry. When anti-passback is enabled, the card holder must leave the secured area through an exit reader before system will grant another entry. If a person enters after authorization and exits without authorization, an alarm will be triggered when they attempt to enter again, and access is denied at the same time. If a person enters without authorization and exits after authorization, an alarm will be triggered when they attempt to enter again, and access is denied at the same time. If the Device can only connect one lock, verifying on the Device means entry direction, and verifying on the external card reader means exit direction by default. You can modify the setting on the management platform.
Door Detector	With the door detector wired to your device, alarm can be triggered when doors are opened or closed abnormally. The door detector includes 2 types, including NC detector and NO detector. Normally Closed: The sensor is in a shorted position when the door or window is closed. Normally Open: An open circuit is created when the window or door is actually closed.
Intrusion Alarm	If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time. The door detector and intrusion need to be enabled at the same time.
Unlock Timeout Alarm	When the door remains unlocked for longer than the

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Unlock Timeout	defined timeout duration, the door timeout alarm will be triggered and last for the defined time. The door detector and door timed out function need to be enabled at the same time.
Excessive Use Alarm	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time.

Step 3 Click Apply .

3.6.3 Configuring Alarm Linkages (Optional)

You can configure alarm linkages.

Procedure

Step 1 Select Access Control > Alarm > Alarm Linkage Setting .

If the Device is added to a management platform, the alarm settings will be synchronized to the platform.

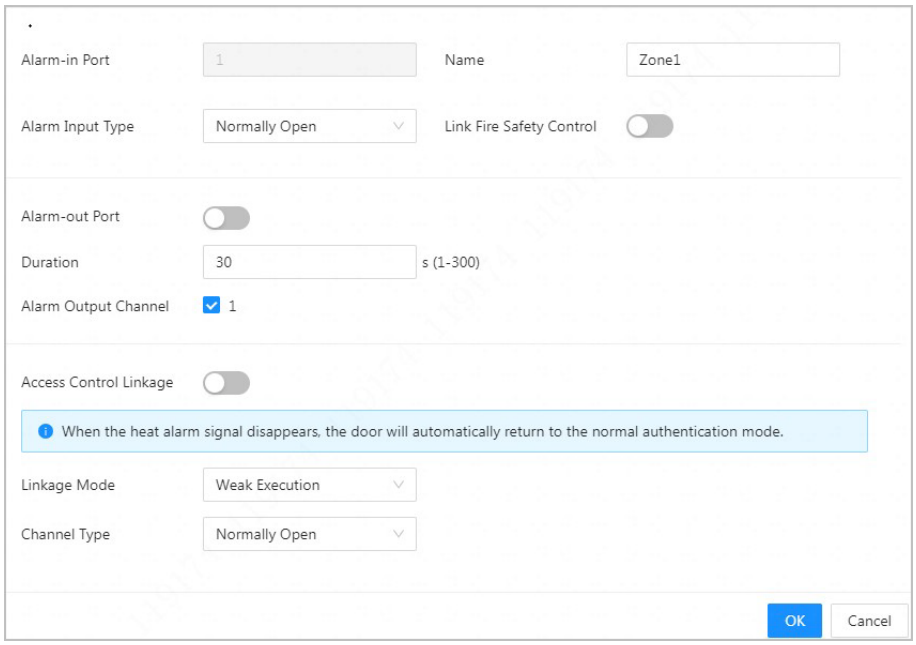
This function is only available on models that have alarm input and alarm output ports.

The number of alarm input and output ports differs depending on models of the product.

Step 2 Click to configure alarm.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-8 Alarm linkage



Step 3 Create a name for the alarm zone.

Step 4 Enable Link Fire Safety Control , and select a type for the alarm input device.

Normally Closed: The alarm input is in a normally closed (NC) circuit state when the alarm has not been tripped. Opening a normally closed circuit sets off the alarm.

Normally Open: The alarm input device is in a normally open (NO) circuit state when the alarm has not been tripped. Closing the circuit sets off the alarm.

Step 5 If you want to link access control when the fire alarm is triggered, enable Access Control Linkage .

This function takes effect only after Link Fire Safety Control is enabled.

Step 6 Select a linkage mode.

Strong Execution: When the fire alarm signal disappears, the door remains the current status. Please manually changes to its previous door status settings if you want to.

Weak Execution: When the fire alarm signal disappears, the door automatically returns to its previous door status.

Step 7 Select a channel type.

Normally Open: The door automatically opens when fire alarm is triggered.

Normally Closed: The door automatically closes when fire alarm is triggered.

Step 8 Click OK.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.6.4 Configuring Alarm Event Linkage

Procedure

Step 1 On the Main Menu , select Access Control > Alarm > Alarm Event Linkage .

Step 2 Configure alarm event linkages.

Figure 3-9 Alarm event linkage

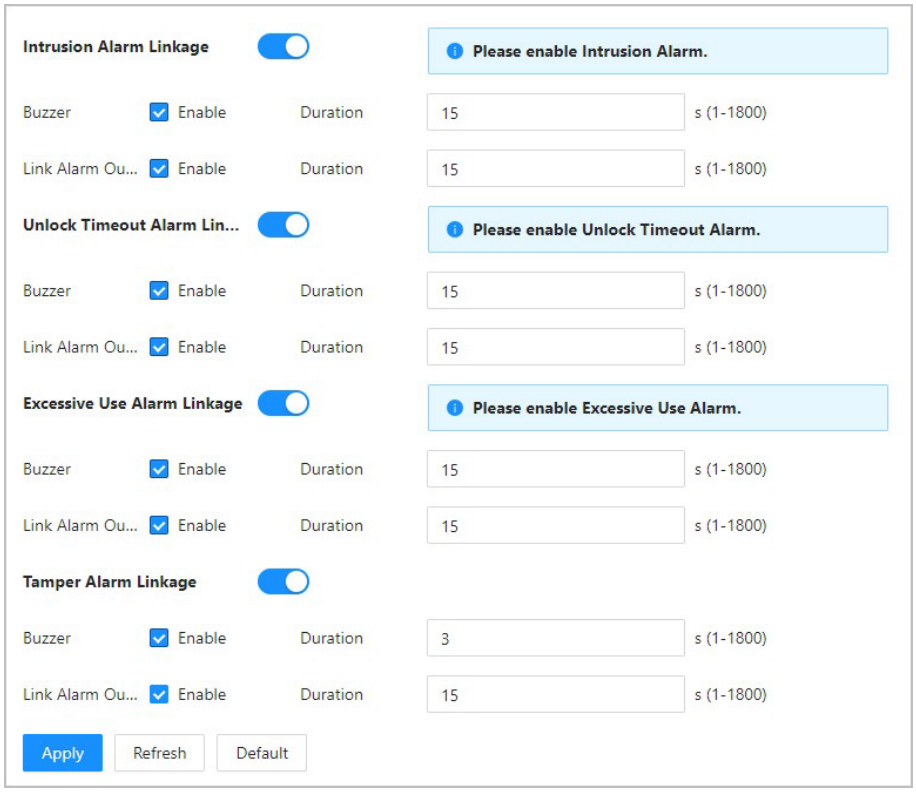


Table 3-6 Alarm event linkage

Parameter	Description
Intrusion Alarm Linkage	If the door is opened abnormally, an intrusion alarm will be triggered. Buzzer: The buzzer sounds when an intrusion alarm is triggered. You can configure the alarm duration. Link Alarm Output: The external alarm device generates alarms when the intrusion alarm is triggered. You can configure the alarm duration.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Unlock Timeout Alarm Linkage	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time. Buzzer: The buzzer sounds when the unlock timeout alarm is triggered. You can configure the alarm duration. Local Alarm Output: The external alarm device generates alarms when the unlock timeout alarm is triggered. You can configure the alarm duration.
Excessive Use Alarm Linkage	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time. Buzzer: The buzzer sounds when the excessive use alarm is triggered. You can configure the alarm duration. Local Alarm Output: The external alarm device generates alarms when the unlock timeout alarm is triggered. You can configure the alarm duration.
Tamper Alarm Linkage	The tamper alarm is triggered when someone has tried to physically damage the Device. Buzzer: The buzzer sounds when the tamper alarm is triggered. You can configure the alarm duration. Local Alarm Output: The external alarm device generates alarms when the tamper alarm is triggered. You can configure the alarm duration.

3.6.5 Configuring Face Detection

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

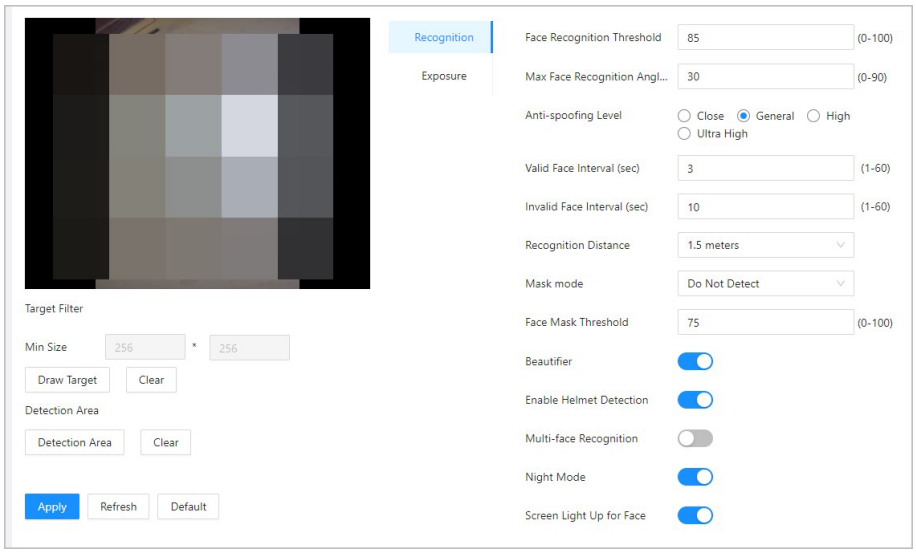
Procedure

Step 1 Log in to the webpage.

Step 2 Select Access Control > Face Detection .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-10 Face detection parameters



Step 3 Configure the parameters.

Table 3-7 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.
Illuminator	Auto: The illuminator is turned on in low-light conditions. Disable: The illuminator is turned off all the time. This function is only available on select models.
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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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.
Recognition Distance	The distance between the face and the lens.
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.
Enable Helmet Detection	Detects safety hats. The door will not unlock if the a person does not wear a helmet.
Multi-face Recognition	Detects 4 to 6 face images at a time. Combination unlock cannot be used with this, and the door will be unlocked when one of the people are successfully verified. 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 or QR code.
Screen Light Up for Face	In the screen-off status, the screen will light up when a face is detected.

Step 4 Configure the exposure parameters.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-11 Exposure parameters

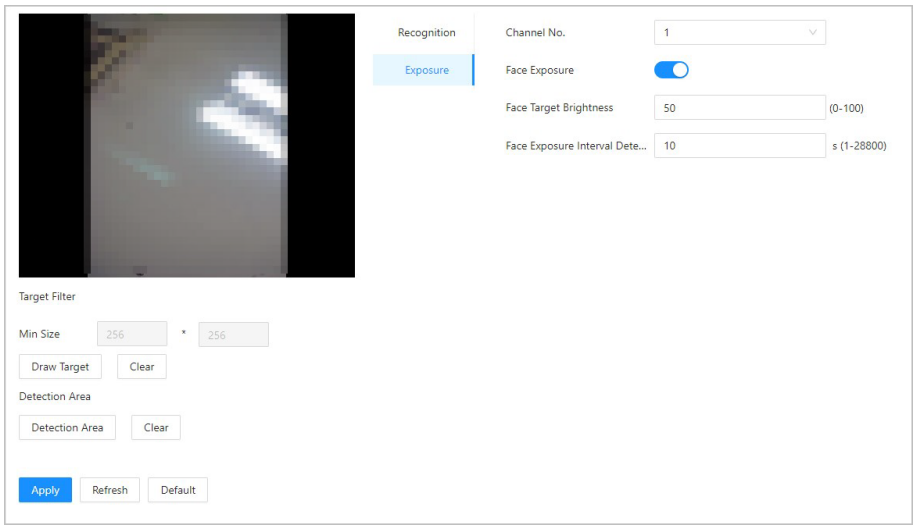


Table 3-8 Exposure parameters description

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 5 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 6 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 7 Draw the detection area.

Step 8 Click OK.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.6.6 Configuring Card Settings

Background Information

This function is only available on select models.

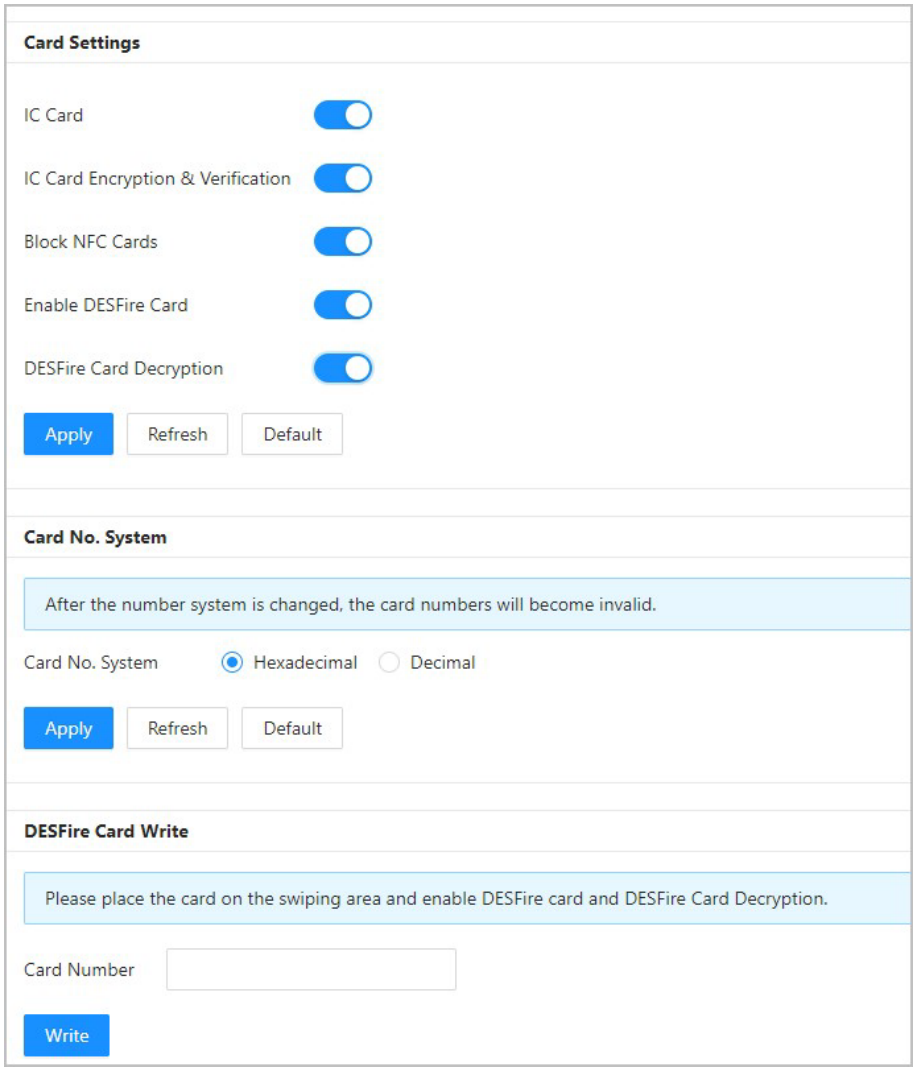
Procedure

Step 1 Log in to the webpage.

Step 2 Select Access Control > Card Settings .

Step 3 Configure the card parameters.

Figure 3-12 Card parameters



(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Table 3-9 Card parameters description

Item	Parameter	Description
Card Settings	IC Card	The IC card can be read when this function is enabled. This function is only available on select models.
	IC Card Encryption & Verification	The encrypted card can be read when this function is enabled. Make sure IC Card is enabled.
	Block NFC Cards	Prevent unlocking through duplicated NFC card after this function is enabled. This function is only available on models that support IC cards. Make sure IC Card is enabled. NFC function is only available on select models of phones.
	Enable Desfire Card	The Device can read the card number of Desfire card when this function is enabled. This function is only available on models that support IC cards. Only supports hexadecimal format.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Item	Parameter	Description
	Desfire Card Decryption	Information in the Desfire card can be read when Enable Desfire Card and Desfire Card Decryption are enabled at the same time. This function is only available on models that support IC cards. Make sure that Desfire card is enabled.
Card No. System	Card No. System	Select decimal format or hexadecimal format for the card number when Wiegand card reader is connected. The card No. system is the same for both card number input and output.
DESFire Card Write	Card Number	Place the card on the reader, enter the card number, and then click Write to write card number to the card. Desfire card function must be enabled. Only supports hexadecimal format. Supports up to 8 characters.

Step 4 Click Apply .

3.6.7 Configuring QR Code

Procedure

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-13 QR code

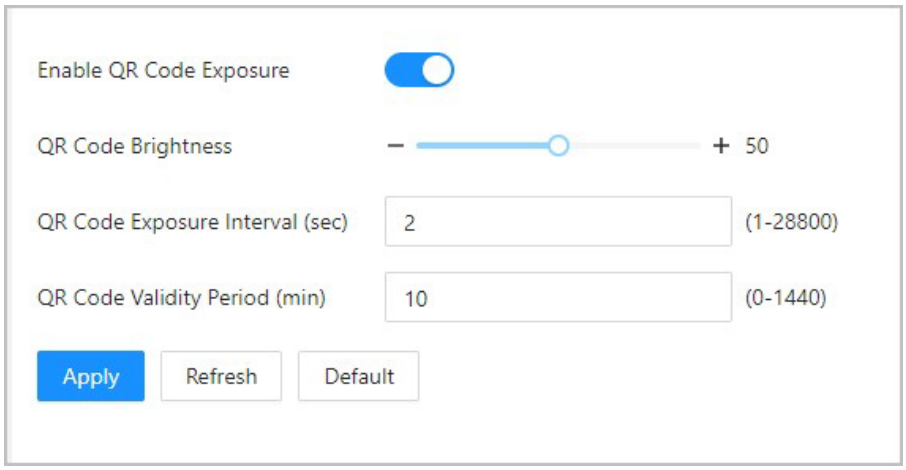


Table 3-10 QRR code parameters

Parameters	Description
Enable QR Code Exposure	The QR code will be exposed at the defined brightness, and the QR code can be detected and read clearly.
QR Code Brightness	
QR Code Exposure Interval (sec)	The QR code will be exposed only once during the defined interval.
QR Code Validity Period (min)	After the QR code is generated, and the validity of your QR codes will last for a defined time before it expires.

3.6.8 Configuring Schedules

Configure time sections and holiday plans, and then you can define when a user has the permissions to unlock doors.

3.6.8.1 Configuring Time Periods

You can configure up to 128 periods (from No.0 through No.127) of time periods. In each period, you need to configure door access schedules for a whole week. People can only unlock the door during the scheduled time.

Procedure

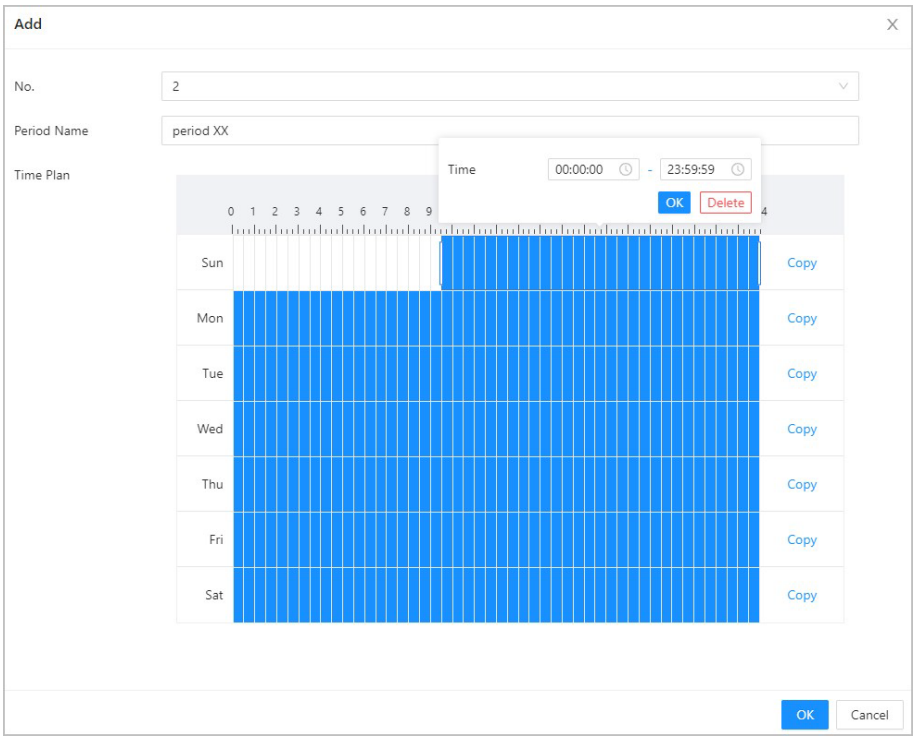
Step 1 Log in to the webpage.

Step 2 Select Access Control > Period Config > Period .

Step 3 Click Add .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-14 Configure time periods



Step 4 Drag the time slider to configure time for each day.

Step 5 (Optional) Click Copy to copy the configuration to the rest of days.

Step 6 Click OK.

3.6.8.2 Configuring Holiday Plans

You can configure up to 128 holiday groups (from No.0 through No.127), and for each holiday group, you can add up to 16 holidays in it. After that, you can assign the configured holiday groups to the holiday plan. Users can only unlock the door during the defined time of the holiday plan.

Procedure

Step 1 Log in to the webpage.

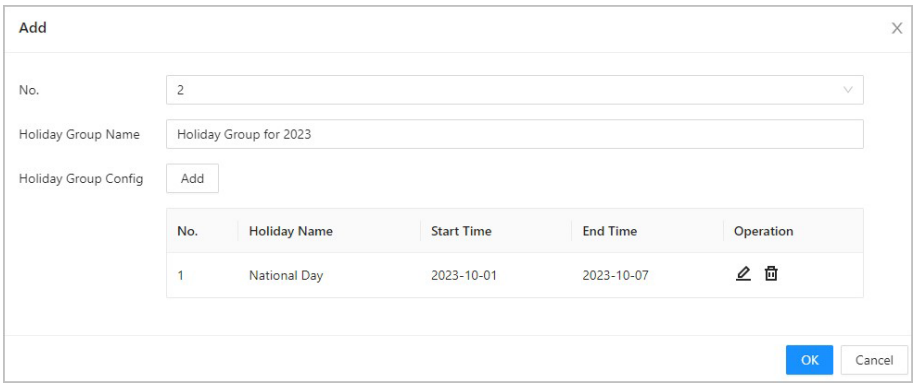
Step 2 Select Access Control > Period Config > Holiday Plan .

Step 3 Click Holiday Management , and then click Add .

Step 4 Select a number for the holiday group, and then enter a name for the group.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

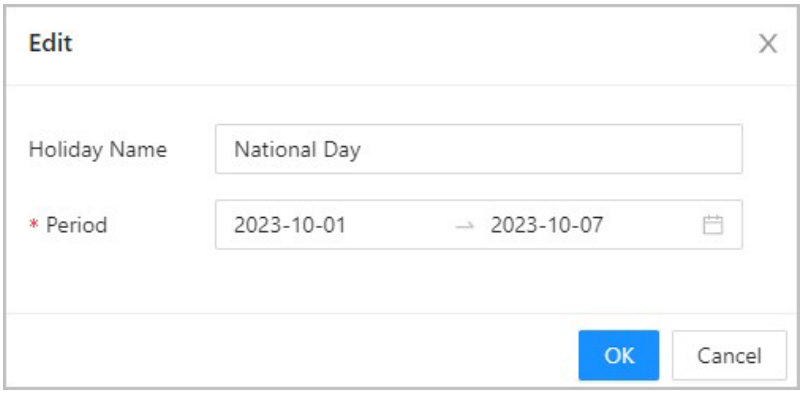
Figure 3-15 Add a holiday group



Step 5 Click Add , and then add a holiday to a holiday group.

Step 6 Click OK .

Figure 3-16 Add a holiday to a holiday group



Step 7 Click Plan Management , and then click Add .

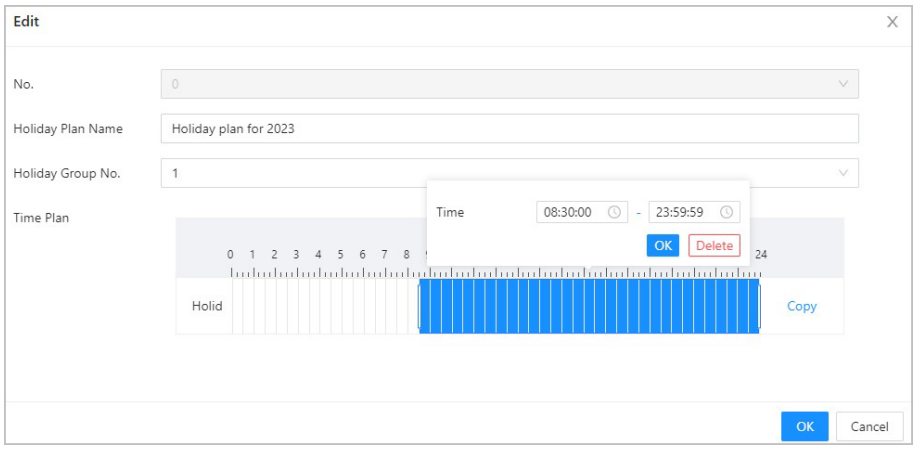
Step 8 Select a number for the holiday plan, and then enter a name for it.

Step 9 Select a holiday group, and then drag the slider to configure time for each day.

Supports adding up to 4 time sections on a day.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-17 Add holiday plan



Step 10 Click OK.

3.6.9 Privacy Settings

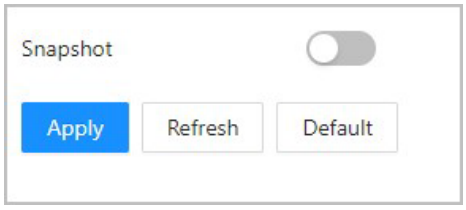
Procedure

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

Step 2 Enable snapshot function.

Face images will be captured automatically when people unlock the door.

Figure 3-18 Enable snapshot



Step 3 Click Apply .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.6.10 Configuring Expansion Modules

For Device that supports connecting expansion modules, configure the type of the module that the Device supports.

Background Information

The type the expansion module might differ depending on models of the Device.

The settings of expansion module remain after restoring the Device to factory defaults.

Procedure

Step 1 On the webpage, select Access Control > Expansion Module .

Step 2 Select the type of the module that the Device supports.

Step 3 Click Apply .

The configurations become effective after Device is restarted.

is displayed on the right corner of the Device is the setting is effective.

is displayed on the right corner of the Device, which means the type of the expansion module you configured does not match the actual expansion module that is connected to Device.

If None is selected and no expansion module is connected to the Device, the expansion module icon will not be displayed.

3.6.11 Configuring Port Functions

Some ports can function as different ports, you can set them to different ports based on the actual needs.

Background Information

This function is only available on select models.

Ports might differ depending on the models of the product.

Procedure

Step 1 On the webpage, select Access Control > Port Config .

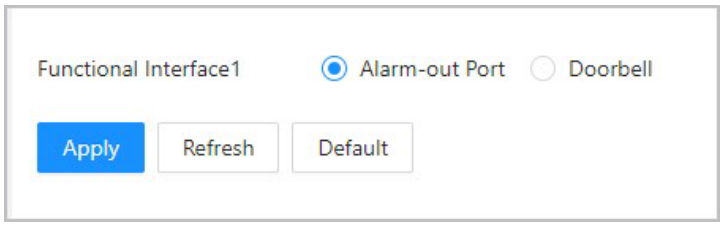
Step 2 Select the type of the port.

When the alarm cable and the doorbell cable are shared, configure the interface to Doorbell to make sure the doorbell will ring.

Step 3 Click Apply .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-19 Configure ports



3.6.12 Configuring Back-end Comparison

Directly pass data such as QR code or card number to the third-party platform for data validation rather than validating data on the Device.

Select Access Control > Back-end Comparison .

Figure 3-20 Back-end comparison

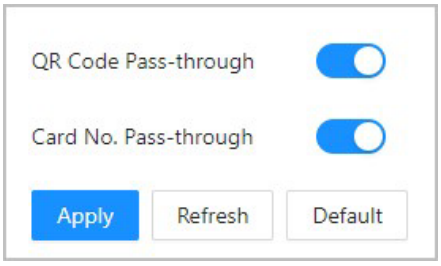


Table 3-11 Back-end comparison

Parameters	Description
QR Code Pass-through	After it is enabled, the scanned QR code is passed to the third-party platform for data validation.
Card No. Pass-through	After it is enabled, the card number passed to the third-party platform for data validation.

3.7 Configuring Intercom

The Device can function as a door station to realize video intercom.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Intercom function is only available on select models.

3.7.1 Using the Device as the SIP Server

3.7.1.1 Configuring SIP Server

When the Device functions as the SIP server, it can connect up to 500 VTHs.

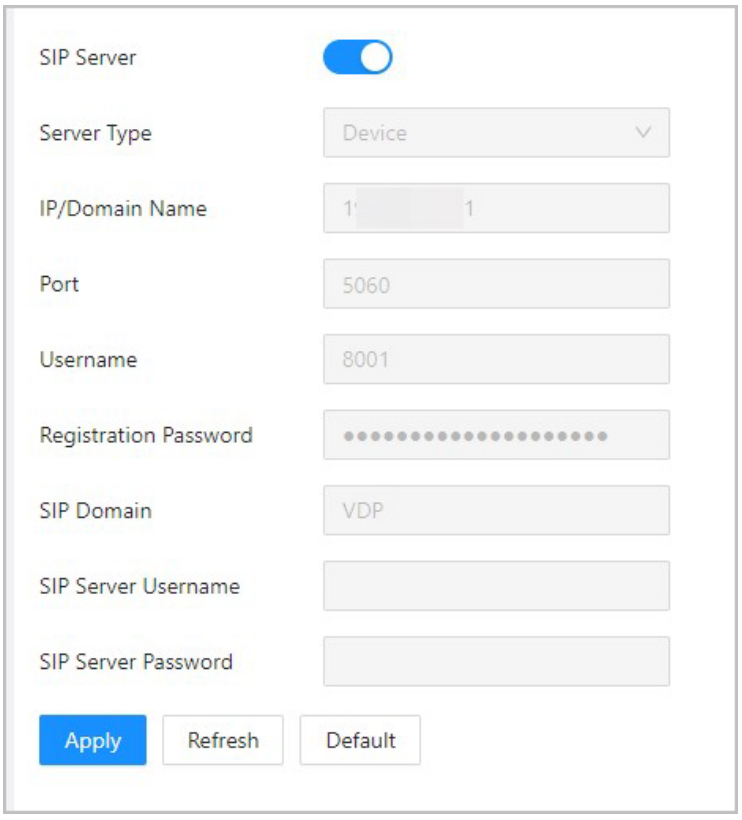
Procedure

Step 1 Select Intercom Settings > SIP Server .

Step 2 Turn on SIP Server .

The device settings will be automatically restored to factory defaults if the SIP server status changes.

Figure 3-21 Use the Device as the SIP server



Step 3 Click Apply .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.7.1.2 Configuring Local Parameters

When the Device functions as the SIP server, configure the parameters of the Device.

Procedure

Step 1 Select Intercom Settings > Local Device Config .

Step 2 Configure the parameters.

Figure 3-22 Basic parameters

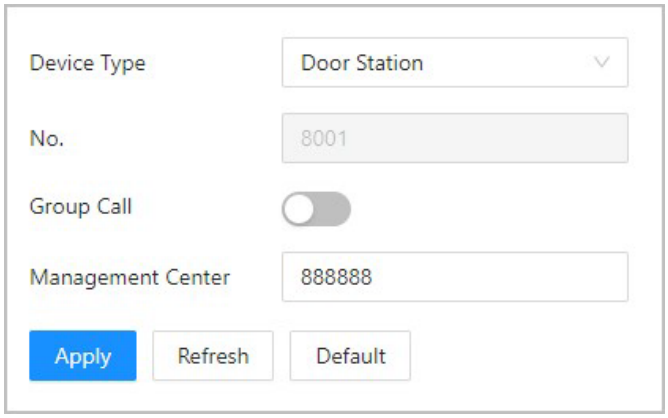


Table 3-12 Basic parameters description

Parameter	Description
Device Type	Select Door Station .
No.	Cannot be set.
Group Call	When you turn on the group call function, the door station calls the main VTH and the extensions at the same time. The setup is effective after the door station restarts.
Management Center	The default call number of the management center is 888888+VTS No. For the VTS No, go to the Project Setting > General of the management center.

Step 3 Click Apply .

3.7.1.3 Adding the Door Station

When the Device functions as the SIP Server, you need to add door station to the SIP server to make sure they can call each other.

Procedure

Step 1 On the webpage of the Device, select Intercom Settings > Device Setting .

Step 2 Click Add , and then configure the door station.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-23 Add door station

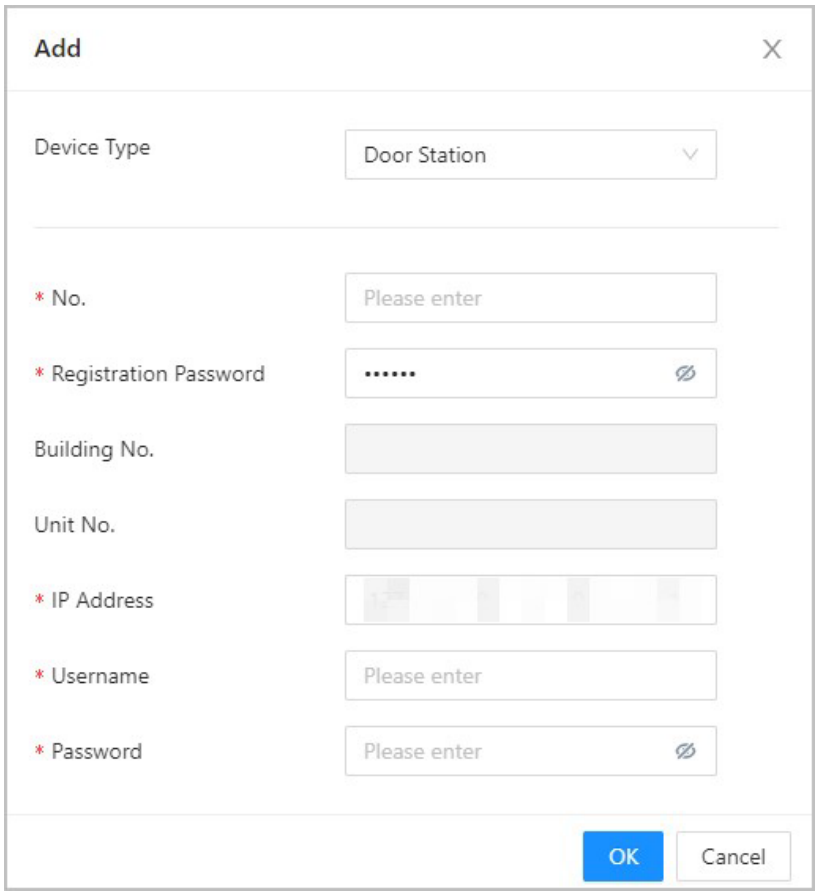


Table 3-13 Add VTO configuration

Parameter	Description
Device Type	Select Door Station .
No.	To view the number of the door station, go to the Device screen of the door station, and then enter the number of door station on this page.
Registration Password	Keep it default.
Building No.	Cannot be configured.
Unit No.	
IP Address	The IP address of the added door station.
Username	The username and password that are used to log in to the webpage of the added door station.
Password	

Step 3 Click OK.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.7.1.4 Adding the VTH

When the Device functions as the SIP Server, you can add all VTHs in the same unit to the SIP server to make sure that they can call each other.

Background Information

When there are main VTH and extension, you need to turn on the group call function first, and then add main VTH and extension on the VTH Management page. For how to turn on the group call function, refer to "3.7.1.2 Configuring Local Parameters".
Extension cannot be added when the main VTHs are not added.

Procedure

Step 1 On the home page, select Intercom Settings > Device Setting .

Step 2 Add the VTH.

Add one by one.

1. Click Add .
2. Configure parameters, and then click OK .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-24 Add one by one

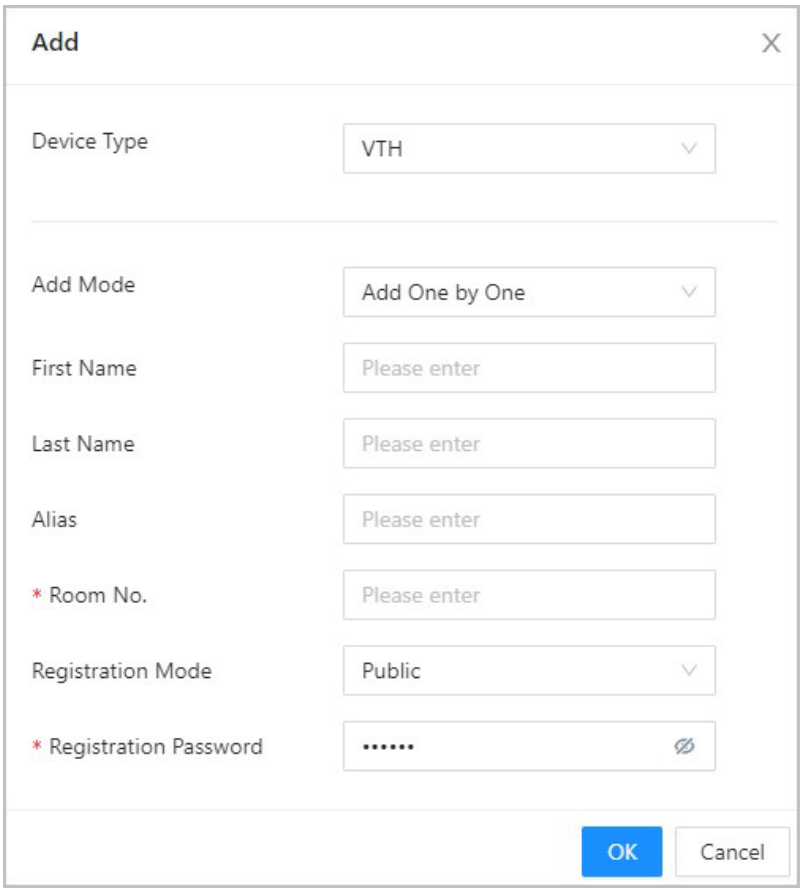


Table 3-14 Room information

Parameter	Description
First Name	Enter the name of the VTH to help you differentiate VTHs.
Last Name	
Alias	
Room No.	Enter the room number of the VTH. The room number consists of 1-5 digits, and must conform to the configured room number on the VTH. When there are main VTH and extensions, the room number of main VTH ends with -0 and the room number of extension ends with -1, -2 or -3. For example, the main VTH is 101-0, and the room number of the extension is 101-1, 101-2... If the group call function is not turned on, room number in the format of 9901-xx cannot be set.

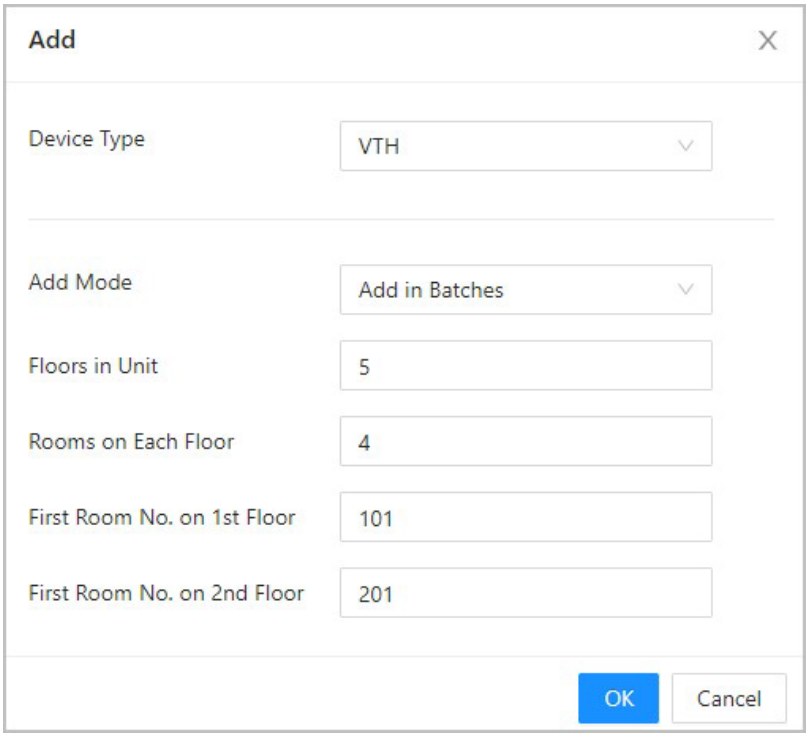
(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Room No.	Enter the room number of the VTH. The room number consists of 1-5 digits, and must conform to the configured room number on the VTH. When there are main VTH and extensions, the room number of main VTH ends with -0 and the room number of extension ends with -1, -2 or -3. For example, the main VTH is 101-0, and the room number of the extension is 101-1, 101-2... If the group call function is not turned on, room number in the format of 9901-xx cannot be set.
Registration Mode	Keep them as defaults.
Registration Password	

Add in batches.

1. Click Add in Batches .
2. Configure the parameters.
3. Click Add .

Figure 3-25 Batch add



(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Table 3-15 Add in batches

Parameter	Description
Floors in Unit	The number of floors of the building, which ranges from 1 to 99.
Rooms on Each Floor	The number of rooms on each floor, which ranges from 1 to 99.
First Room No. on 1st Floor	The first room on the first floor.
First Room No. on 2nd Floor	The first room number on the 2nd floor = The first digit of the first room number on the 1st floor plus 1. For example, if the first room number on the first floor is 101, the first room number on the 2nd floor must be 201.

3.7.1.5 Adding the VTS

When the Device functions as the SIP Server, you can add VTSs to the SIP server to make sure they can call each other.

Procedure

Step 1 On the Homepage, select Intercom Settings > Device Setting .

Step 2 Click Add , and then set parameters.

Figure 3-26 VTS management

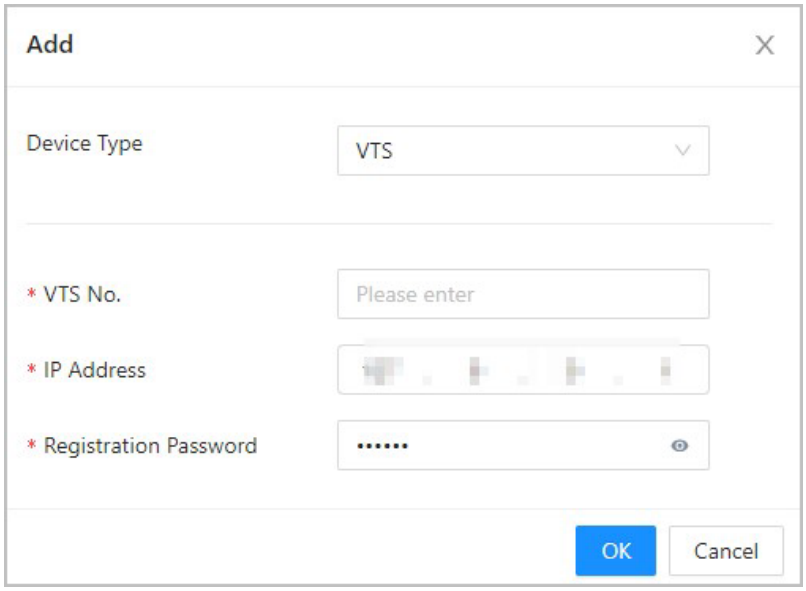


Table 3-16 VTS parameters

Parameter	Description
VTS No.	Enter 888888+ VTS No, which can include up to 9 digits. For the VTS No, go to Device screen on the VTS.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
IP Address	The IP address of the VTS.
Registration Password	Keep it as default.

Step 3 Click OK.

3.7.2 Using VTO as the SIP server

3.7.2.1 Configuring SIP Server

Use another VTO as the SIP server.

Procedure

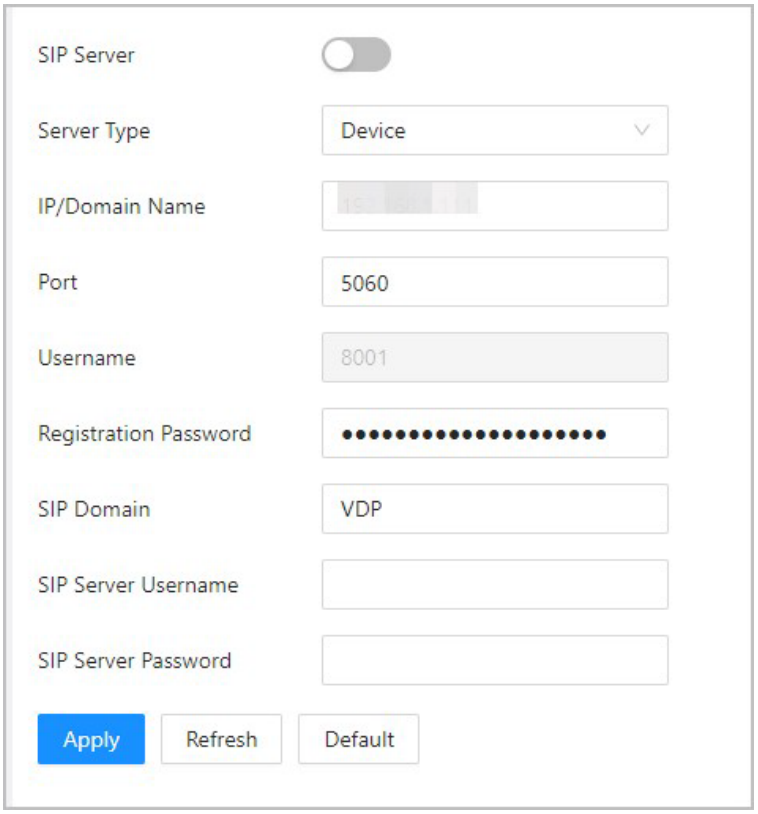
Step 1 Select Intercom Settings > SIP Server .

Step 2 Select Device from the Server Type .

Do not enable SIP server .

Step 3 Configure the parameters, and then click OK.

Figure 3-27 Use VTO as the SIP server



(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Table 3-17 SIP server configuration

Parameter	Description
IP/Domain Name	IP address or domain name of the VTO.
Port	5060 by default when VTO works as SIP server.
Username	Leave them as default.
Registration Password	
SIP Domain	VDP.
SIP Server Username	The login username and password of the SIP server.
SIP Server Password	

Step 4 Click Apply .

3.7.2.2 Configuring Local Parameters

Configure the parameters of the Device when you use another VTO as the SIP server.

Procedure

Step 1 Select Intercom Settings > Local Device Config .

Step 2 Configure the parameters.

Figure 3-28 Configure the parameters

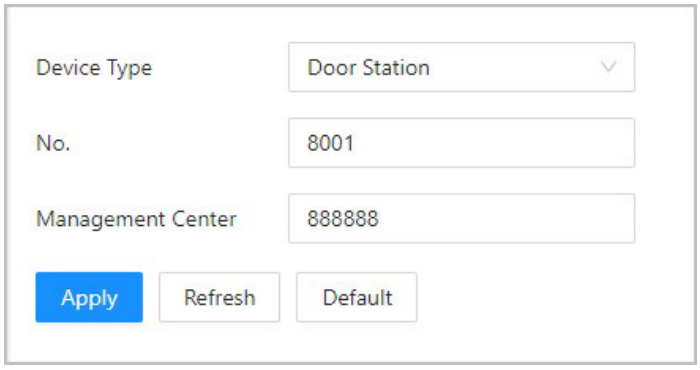


Table 3-18 Parameters description

Parameter	Description
Device Type	Select Door Station .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
No.	The number of the VTO. The number must have 4 digits. The first 2 digits must be 80, and the last 2 digits start from 01. For example, 8001. If multiple VTOs exist in one unit, the VTO No. cannot be repeated.
Management Center	The call number for the management center is 888888. Keep it as default.

Step 3 Click Apply .

3.7.3 Using the Platform as the SIP server

3.7.3.1 Configuring SIP Server

The management platform is used as the SIP server.

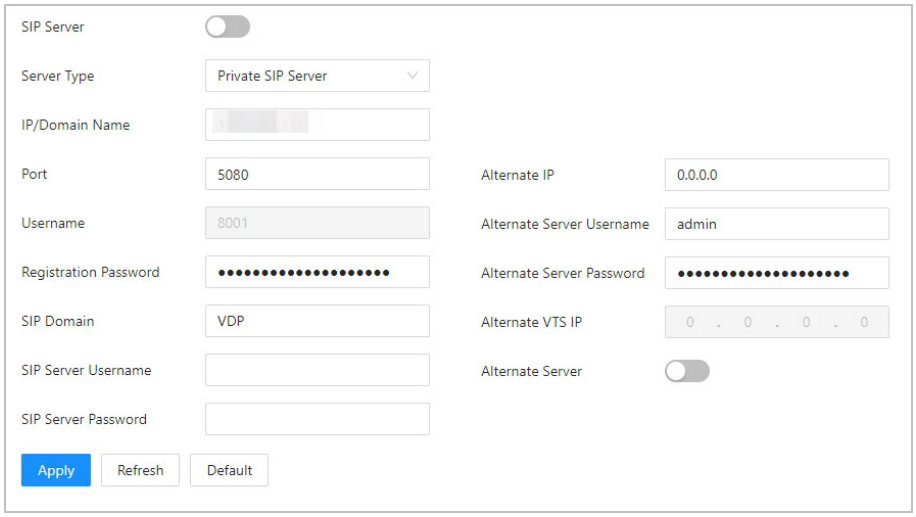
Procedure

Step 1 Select Intercom Settings > SIP Server .

Step 2 Select Private SIP Server from the Server Type .

Do not enable SIP Server .

Figure 3-29 Use the management platform as the SIP server



(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Table 3-19 SIP server configuration

Parameter	Description
IP/Domain Name	IP address or domain name of the platform.
Port	5080 by default when the platform works as SIP server.
Username	Leave them as default.
Registration Password	
SIP Domain	Leave it as default.
SIP Server Username	The login username and password of the platform.
SIP Server Password	
Alternate IP	The alternate server will be used as the SIP server when the platform does not respond. If you turn on the Alternate Server function, you will set the Device as the alternate server. If you want another VTO to function as the alternate server, you need to enter the IP address, username, password of the VTO. Do not enable Alternate Server in this case. We recommend you set the main VTO as the alternate server.
Alternate Server Username	After you set the alternate server, when the management platform does not respond, the alternate server will be activated to make sure VTO and VTH can each other. If Alternate Server is enabled, the Device is set as the alternate server. If Alternate Server is not enabled, enter the IP of the alternate server, its username and password to set VTO as the alternate server. We recommend you set the main VTO as the alternate server.
Alternate Server Password	
Alternate Server	
Alternate VTS IP	Enter the IP address of the alternate VTS. When the management platform does not respond, the alternate VTS will be activated to make sure VTO, VTH and VTS can each other.

Step 3 Click Apply .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.7.3.2 Configuring Local Parameters

Configure the parameters of the Device when the platform is used as the SIP server.

Procedure

Step 1 Select Intercom Settings > Local Device Config .

Step 2 Configure the parameters.

Figure 3-30 Basic parameter

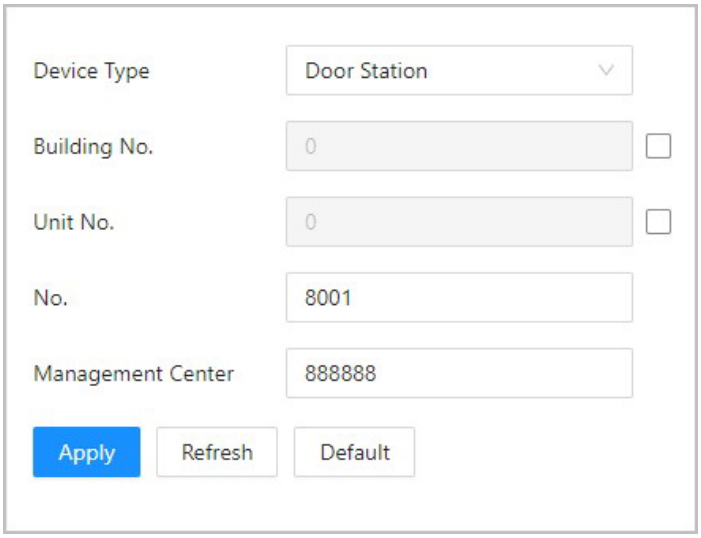


Table 3-20 Parameters description

Parameter	Description
Device Type	Select fence station or door station based on its installation site.
Building No.	Select the checkbox and then enter the number of the building where the unit door station is installed.
Unit No.	Select the checkbox, and then enter the number of the unit where the unit door station is installed.
No.	The number must have 4 digits. The first 2 digits must be 80, and the last 2 digits start from 01. For example, 8001. If multiple VTOs exist in one unit, the VTO No. cannot be repeated.
Management Center	The default phone number is 888888 when the VTO calls the VTS. Keep it as default.

Step 3 Click Apply .

After settings, the username in Intercom > SIP page is automatically refreshed. Make sure the username is same to the call number when you add the device to the management platform.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.7.3.3 Registration Management

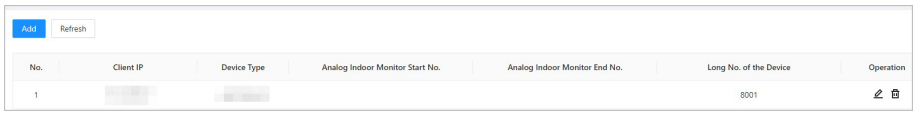
When the management platform works as the SIP server, you can view and manage all devices that registered to SIP server.

Procedure

Step 1 Select Intercom Settings > Registration Management .

Step 2 You can view and edit the devices.

Figure 3-31 View and manage devices



3.7.4 Simple Mode

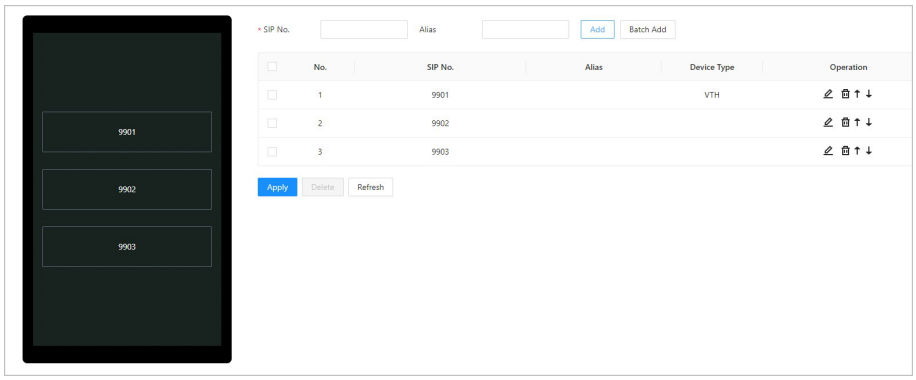
One-touch call to VTH or VTS on the Device.

Procedure

Step 1 On the webpage, select Intercom Settings > Simple Mode .

The call list preview window is different depending on models of the product.
The Device in 4.3-inch horizontal screen series does not supports call list preview.
Only when the Device is set as the SIP server, and VTH and VTS are added to the SIP server on the Device Setting page, the corresponding device type is displayed.

Figure 3-32 Simple mode



Step 2 Add VTH and VTS one by one or in batches.

If the VTH has extensions (such as 9901-0, 9901-1, and 9901-2) and the SIP number is 9901, and then you can simply call the SIP number, and 9901-0, 9901-1, and 9901-2 will be called at the same time.

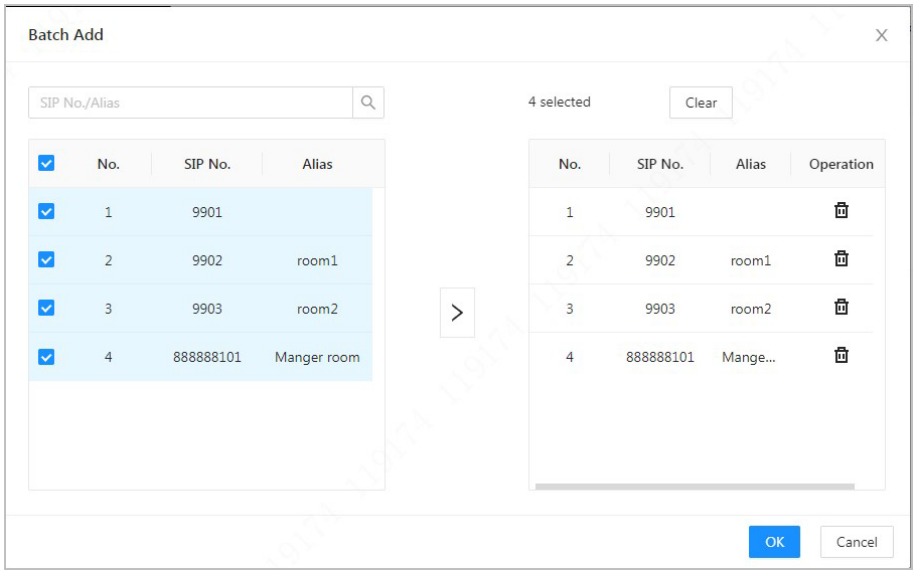
Add one by one: Enter the SIP number, and then click Add .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Add in batches: This function is only available when the Device is set as the SIP server, and VTH and VTS are added to the SIP server on the Device Setting page.

1. Click Batch Add .
2. Select added VTS or VTH, and then click OK .

Figure 3-33 Add in batches



Step 3 (Optional) Click ↑↓ to adjust the order of the devices, or you can simple drag the devices on the preview window.

Related Operations

Click to eidt the alias of the device.

Click to delete the device.

3.8 Attendance Configuration

This function is only available on select models.

3.8.1 Configuring Departments

Procedure

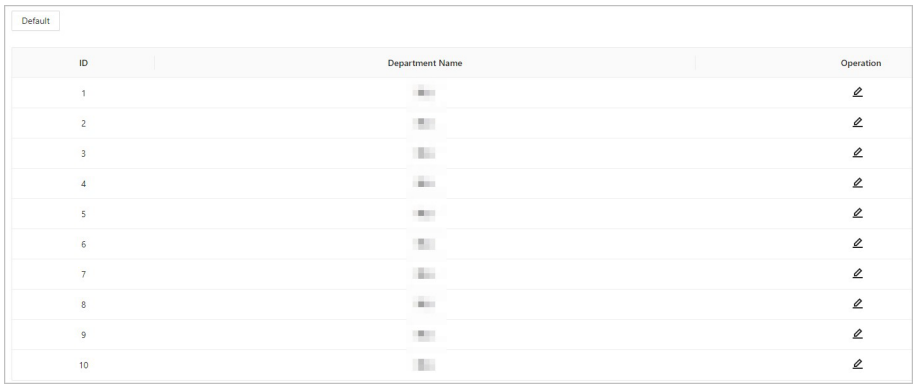
Step 1 Select Attendance Config > Department Settings .

Step 2 Click to rename the department.

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-34 Create departments



Related Operations

You can click Default to restore departments to default settings.

3.8.2 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-35 Create shifts

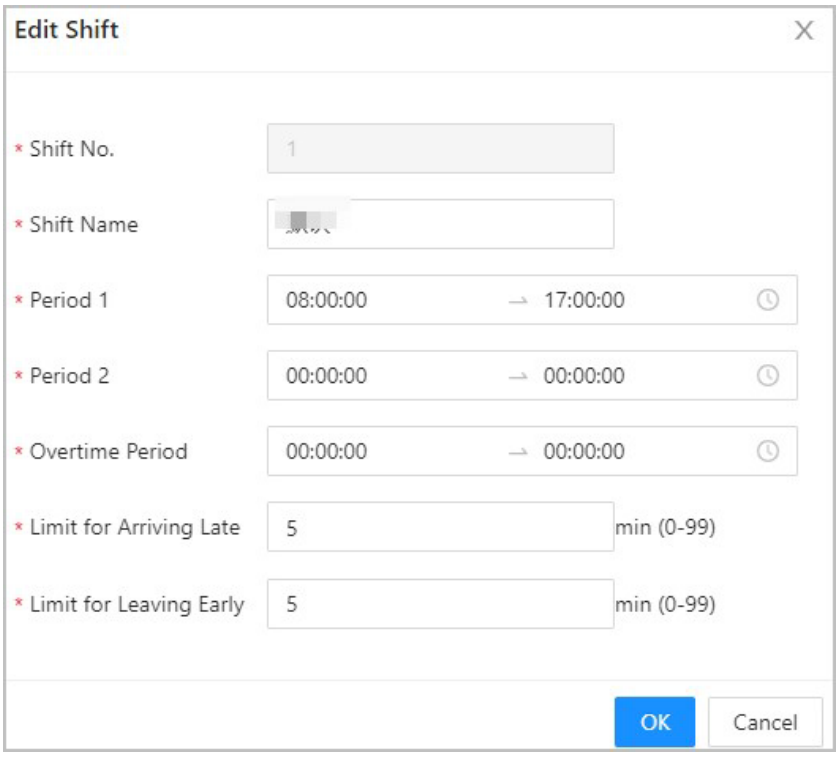


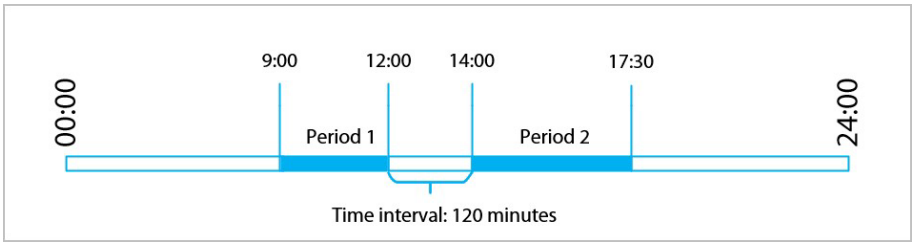
Table 3-21 Shift parameters description

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)	

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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 3-36 Time interval (even number)

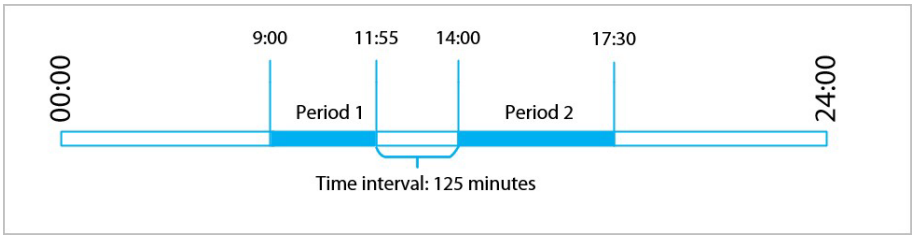


For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.

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 3-37 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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.

3.8.3 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 3-38 Create holiday plans

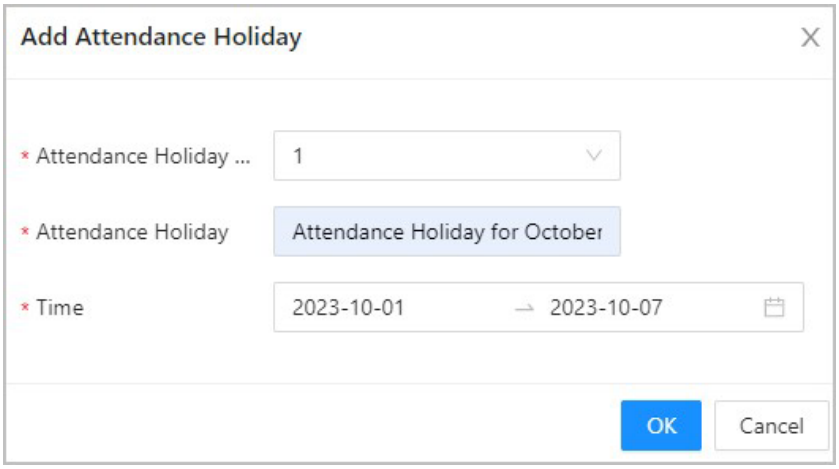


Table 3-22 Parameters description

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
End Time	

Step 4 Click OK.

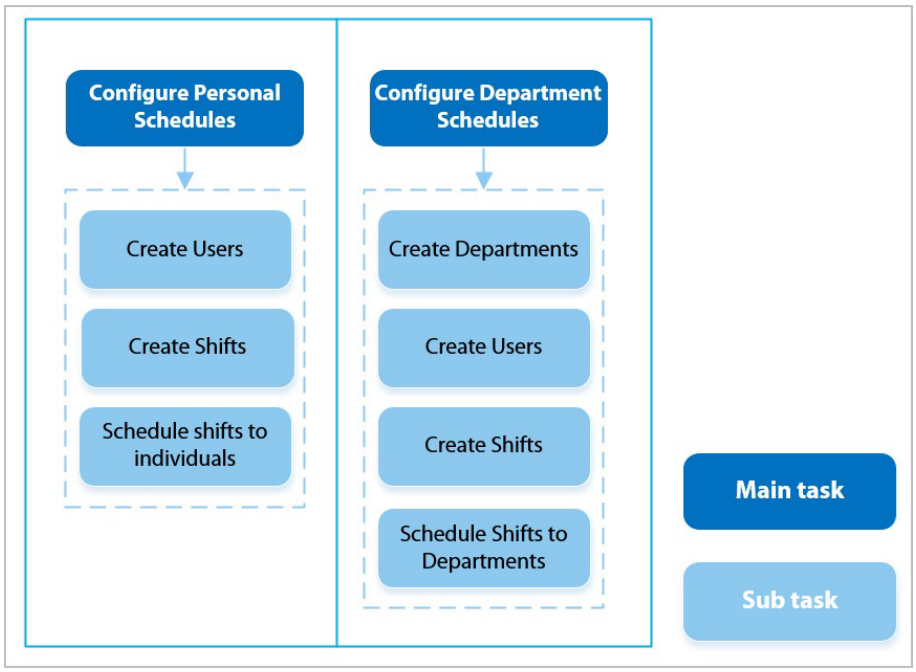
3.8.4 Configuring Work Schedules

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 3-39 Configuring work schedules



Procedure

Step 1 Select Attendance Config > Schedule Config .

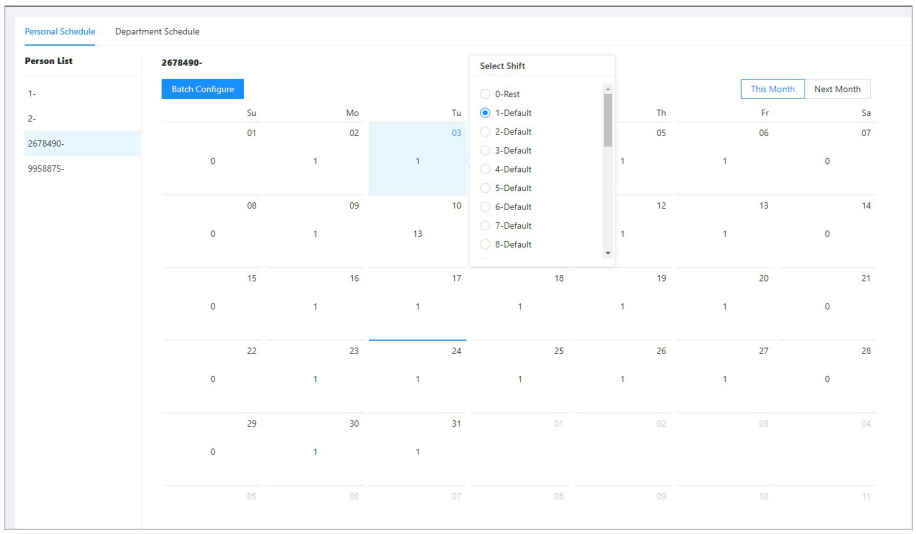
Step 2 Set work schedules for individuals.

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-40 Personal schedule



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 "2.10.2 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.

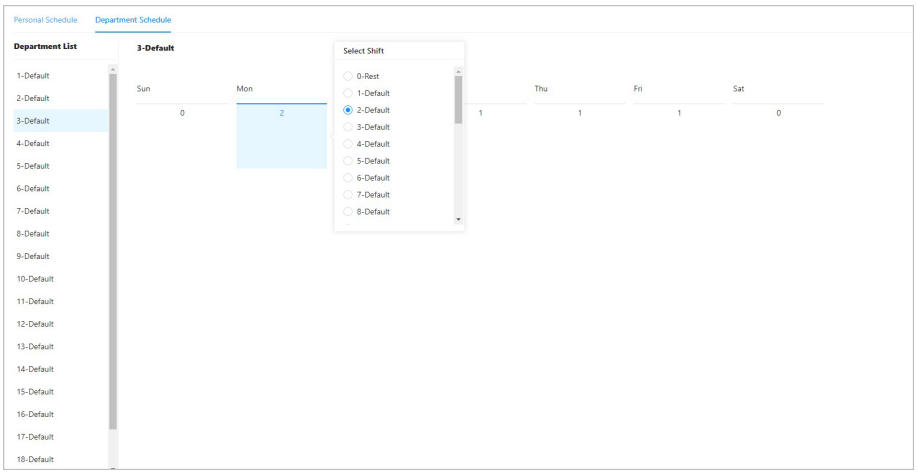
   1 to 24 indicates the number of the per-defined shifts. For how to configure shifts, see "2.10.2 Configuring Shifts".

   25 indicates business trip.

   26 indicates leave of absence.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-41 Schedule shifts to a department



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

3.8.5 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-42 Attendance modes

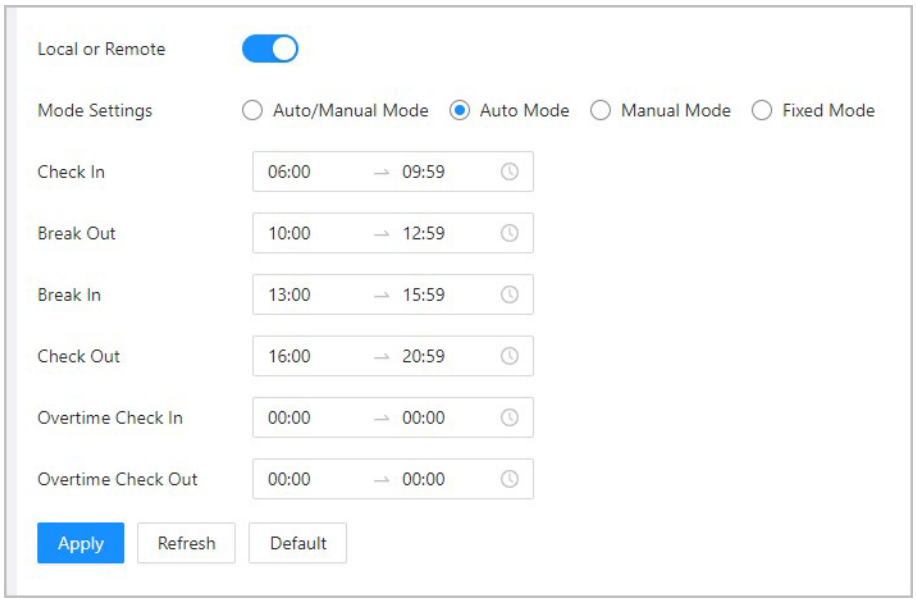


Table 3-23 Attendance mode

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
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.

3.9 Configuring Audio and Video

3.9.1 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.

3.9.1.1 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-43 Date rate

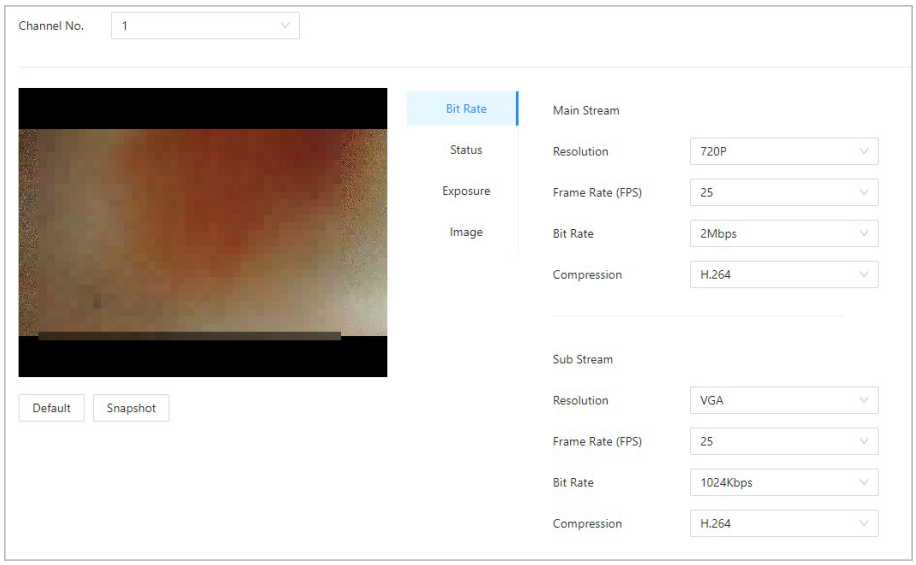


Table 3-24 Bit rate description

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter		Description
	Compression	Video compression standard to deliver good video quality at lower bit rates.

Step 4 Configure the status.

Figure 3-44 Status

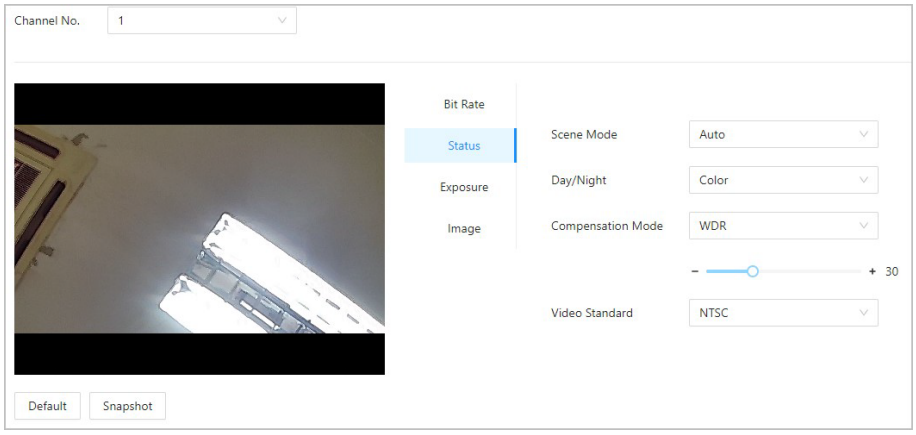


Table 3-25 Parameters description of status

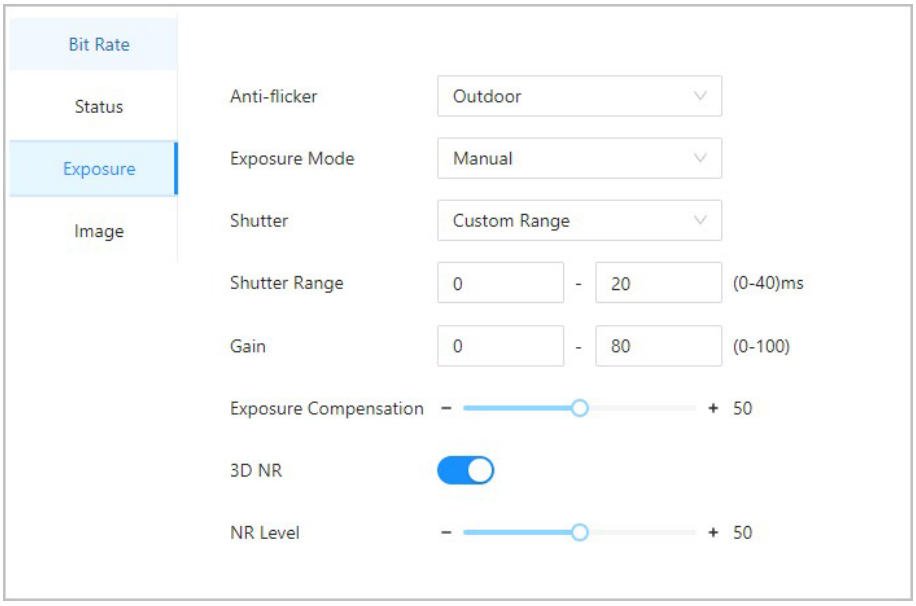
Parameter	Description
Scene Mode	The image hue is different in different scene mode. Close : Scene mode function is turned off. Auto : The system automatically adjusts the scene mode based on the photographic sensitivity. Sunny : In this mode, image hue will be reduced. Night : In this mode, image hue 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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 3-45 Exposure



(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Table 3-26 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.
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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-46 Image

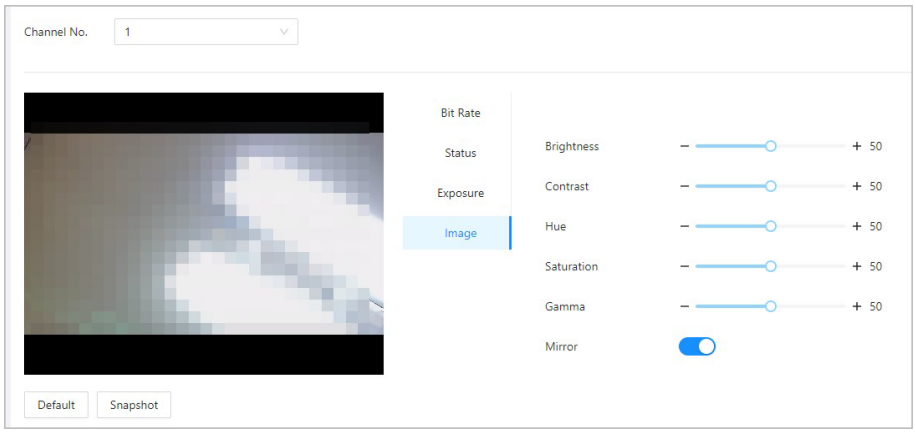


Table 3-27 Image description

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.
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.

3.9.1.2 Configuring Channel 2

Procedure

Step 1 Select Audio and Video Config > Video .

Step 2 Select 2 from the Channel No. list.

Step 3 Configure the video status.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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

Figure 3-47 Configure status

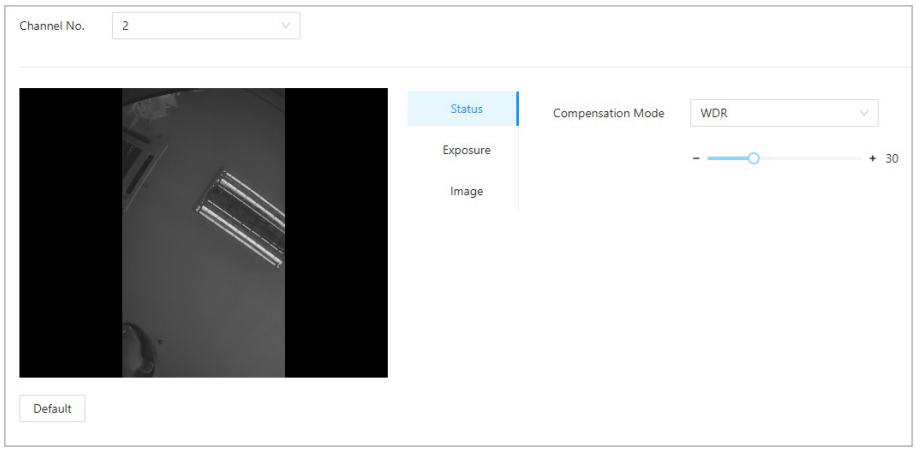


Table 3-28 Status description

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 4 Configure the exposure parameters.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-48 Exposure parameter

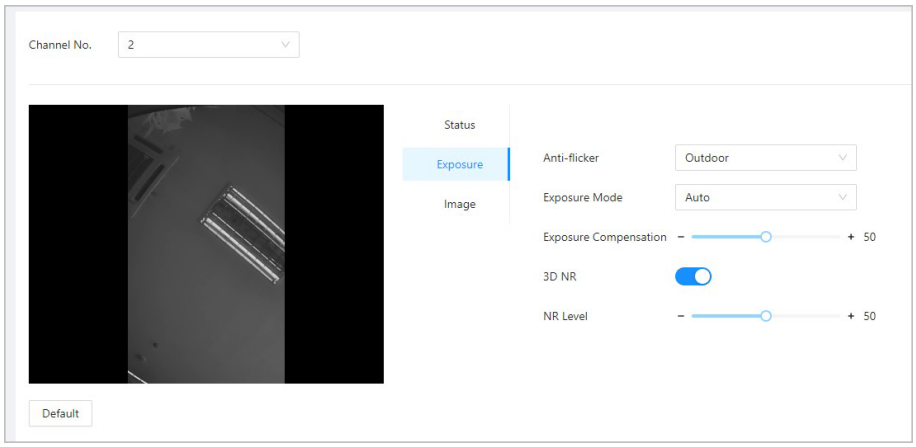


Table 3-29 Exposure parameter description

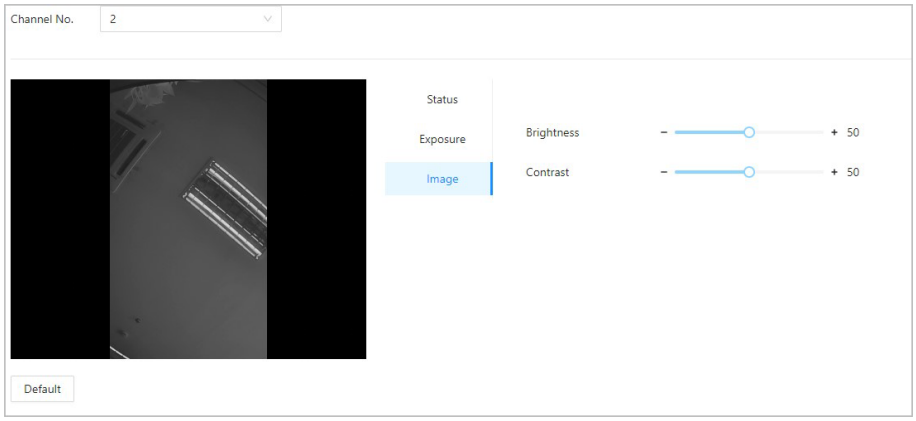
Parameter	Description
Anti-flicker	Set anti-flicker to reduce flicker and decrease or reduce uneven colors or exposure. 50Hz : When the mains electricity is 50 Hz, the exposure is automatically adjusted based on brightness of the surroundings to prevent the appearance of horizontal lines. 60Hz : When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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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 5 Configure the image parameters.

Figure 3-49 Image parameters



(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Table 3-30 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.

3.9.2 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 3-50 Configure audio parameters

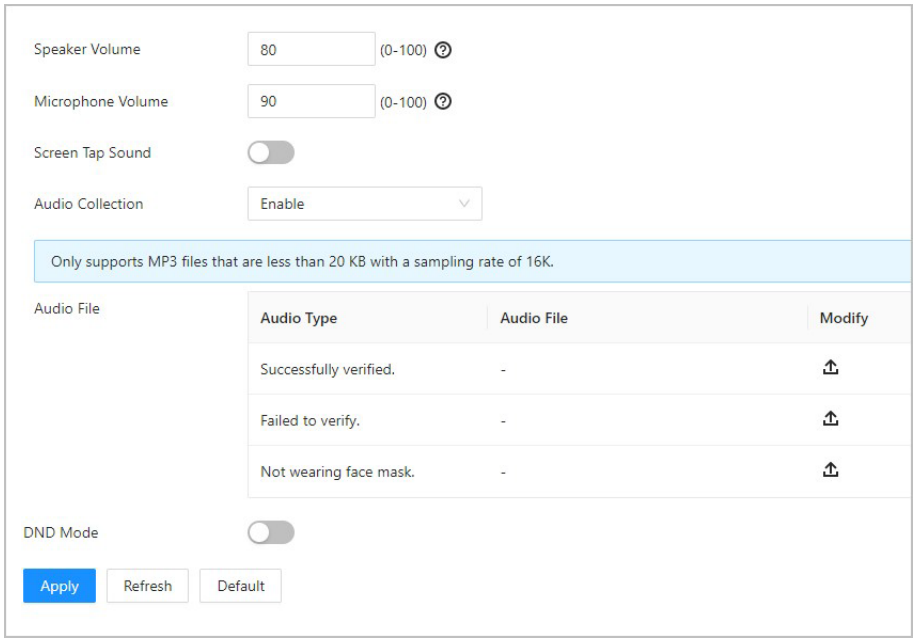


Table 3-31 Parameters description

Parameters	Description
Speaker	Set the volume of the speaker.
Microphone Volume	Set the volume of the microphone.
Screen Tap Sound	When this function is enabled, touch screen devices will produce tap sound and non-touch screen devices will produce mouse click sound.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameters	Description
Audio Collection	The audio will not be recorded during video talk when this function is not enabled.
Audio File	Click Upload audio files to the platform.
DND Mode	No voice prompts during the set time when you verify your identity on the Device. You can set up to 4 periods.

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 16K.

Step 4 Click Apply .

3.9.3 Configuring Motion Detection

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

Background Information

This function is only available on select models.

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.

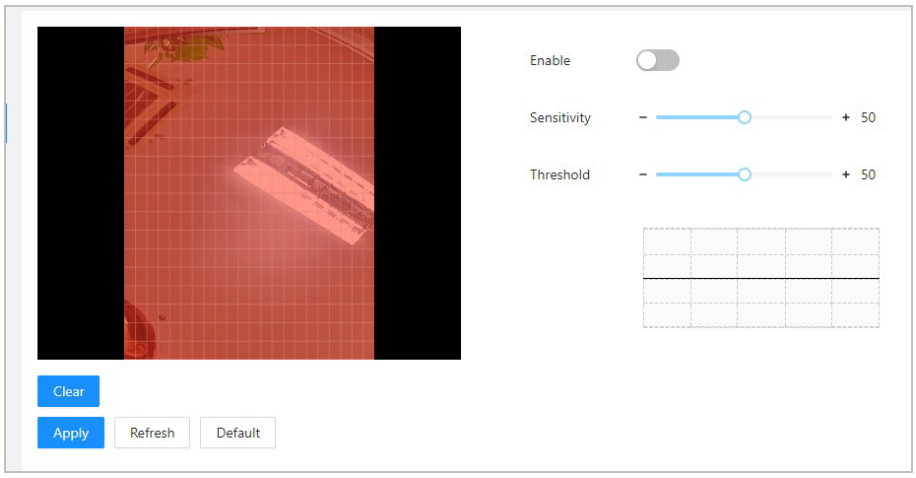
(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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 3-51 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.

3.9.4 Configuring Local Coding

Set the view area in the video talk and preview.

Background Information

This function is only available on select models.

This function is enabled by default when it works with a VTH. The preview might be not accessible when this function is disabled.

Procedure

Step 1 Log in to the webpage.

Step 2 Select Audio and Video Config > Local Code .

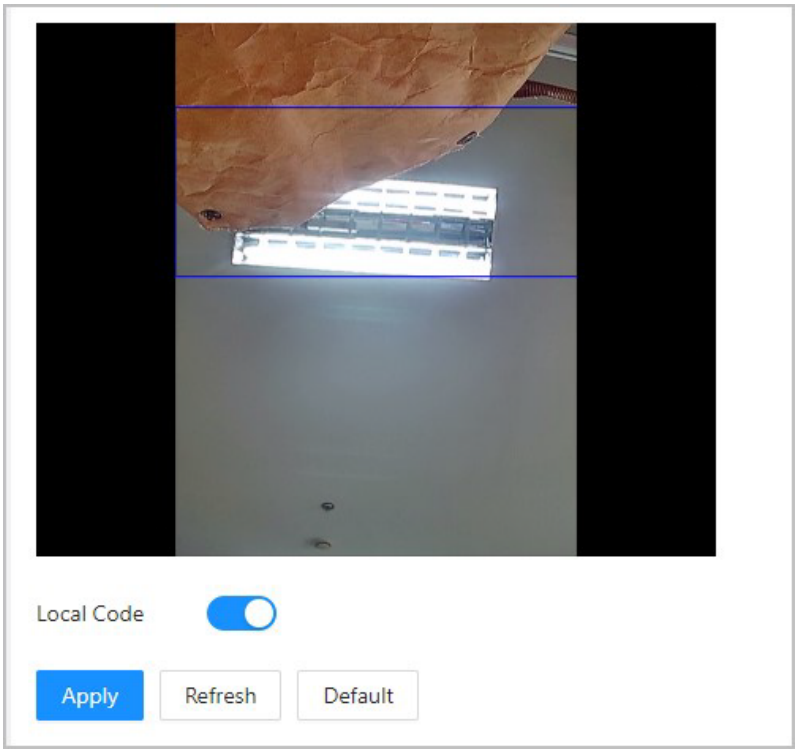
(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Step 3 Select Enable to turn on the function.

Step 4 Drag the box to a designated position.

The box indicates the preview area during the video talk.

Figure 3-52 Local coding



Step 5 Click Apply .

3.10 Communication Settings

3.10.1 Network Settings

3.10.1.1 Configuring TCP/IP

You need to configure IP address of Device to make sure that it can communicate with other devices.

Procedure

Step 1 Select Communication Settings > Network Setting > TCP/IP .

Step 2 Configure the parameters.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-53 TCP/IP

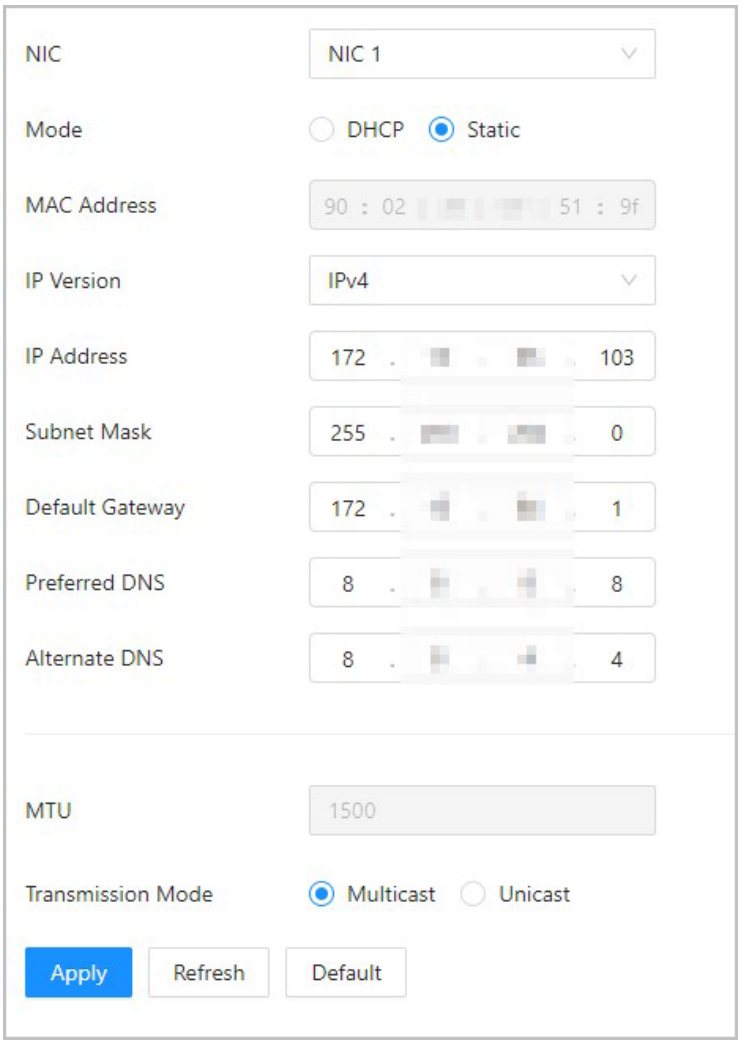


Table 3-32 Description of TCP/IP

Parameter	Description
Mode	Static: Manually enter IP address, subnet mask, and gateway. DHCP: It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Device will automatically be assigned with IP address, subnet mask, and gateway.
MAC Address	MAC address of the Device.
IP Version	IPv4 or IPv6.
IP Address	If you set the mode to Static , configure the IP address, subnet mask and gateway.
Subnet Mask	

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Default Gateway	IPv6 address is represented in hexadecimal. IPv6 version do not require setting subnet masks. The IP address and default gateway must be in the same network segment.
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
MTU	MTU (Maximum Transmission Unit) refers to the maximum size of data that can be transmitted in a single network packet in computer networks. A larger MTU value can improve network transmission efficiency by reducing the number of packets and associated network overhead. If a device along the network path is unable to handle packets of a specific size, it can result in packet fragmentation or transmission errors. In Ethernet networks, the common MTU value is 1500 bytes. However, in certain cases such as using PPPoE or VPN, smaller MTU values may be required to accommodate the requirements of specific network protocols or services. The following are recommended MTU values for reference: 1500: Maximum value for Ethernet packets, also the default value. This is a typical setting for network connections without PPPoE and VPN, some routers, network adapters, and switches. 1492: Optimal value for PPPoE 1468: Optimal value for DHCP. 1450: Optimal value for VPN.
Transmission Mode	Multicast: Ideal for video talk. Unicast: Ideal for group call.

Step 3 Click OK.

3.10.1.2 Configuring Wi-Fi

Procedure

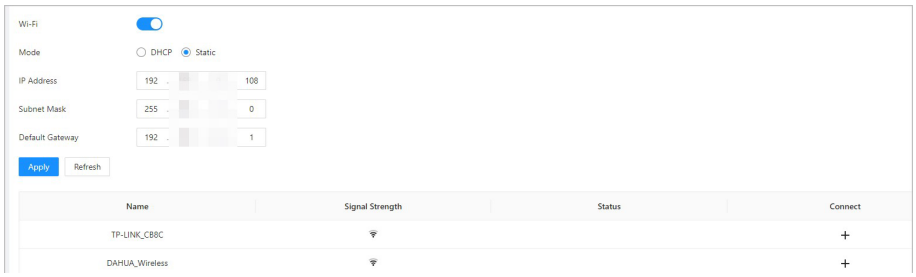
Step 1 Select Communication Settings > Network Setting > Wi-Fi .

Step 2 Turn on Wi-Fi.

All available Wi-Fi are displayed.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-54 Wi-Fi



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

Wi-Fi function is only available on select models.

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

The Wi-Fi is connected.

Related Operations

DHCP: Enabled this function and click Apply , the Device will automatically be assigned a Wi-Fi address.

Static: Enable this function, manually enter a Wi-Fi address, and then click Apply , the Device will connect to the Wi-Fi.

3.10.1.3 Configuring Port

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

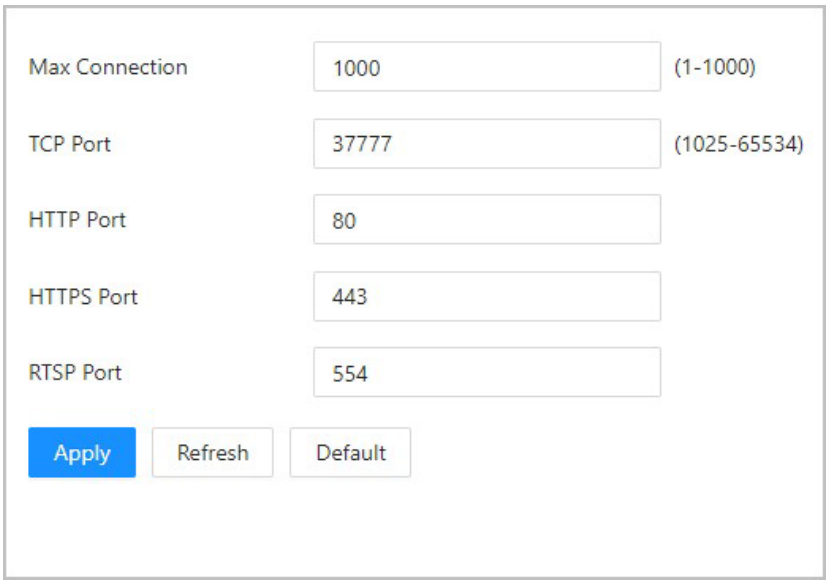
Procedure

Step 1 Select Communication Settings > Network Setting > Port .

Step 2 Configure the ports.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-55 Configure ports



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

Table 3-33 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 .

3.10.1.4 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 Communication Settings > Network Settings > Basic Services .

Step 2 Configure the basic service.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-56 Basic service

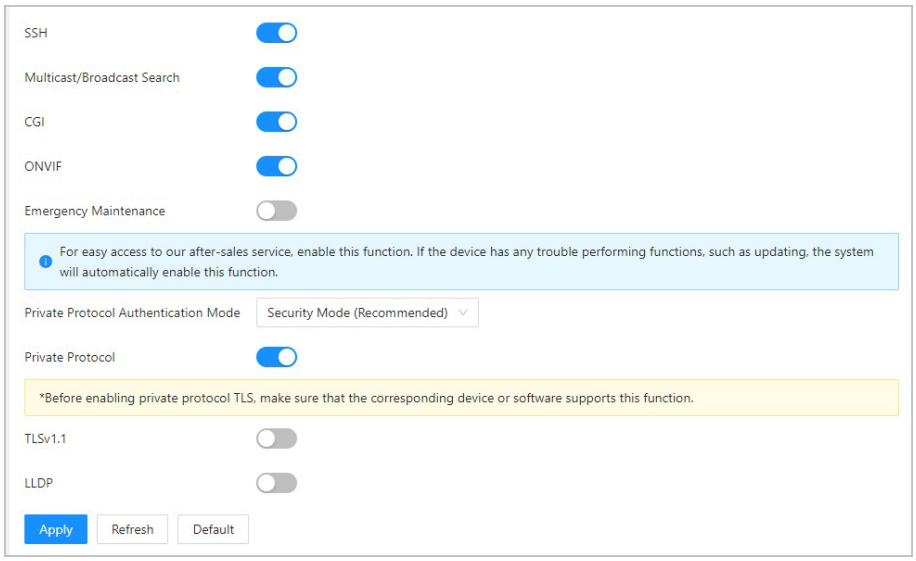


Table 3-34 Basic service parameter description

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.
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.
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 private protocol.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
TLSv1.1	TLSv1.1 refers to Transport Layer Security version 1.1. TLS is a cryptographic protocol designed to provide secure and authenticated communication over a computer network.  Security risks might present when TLSv1.1 is enabled. Please be advised.
LLDP	LLDP is the abbreviation for Link Layer Discovery Protocol, which is a data link layer protocol. It allows network devices, such as switches, routers, or servers, to exchange information about their identities and capabilities with each other. The LLDP protocol helps network administrators gain a better understanding of network topology and provides a standardized way to automate the discovery and mapping of connections between network devices. This makes it easier to perform network configuration, troubleshoot issues, and optimize performance.

Step 3 Click Apply .

3.10.1.5 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

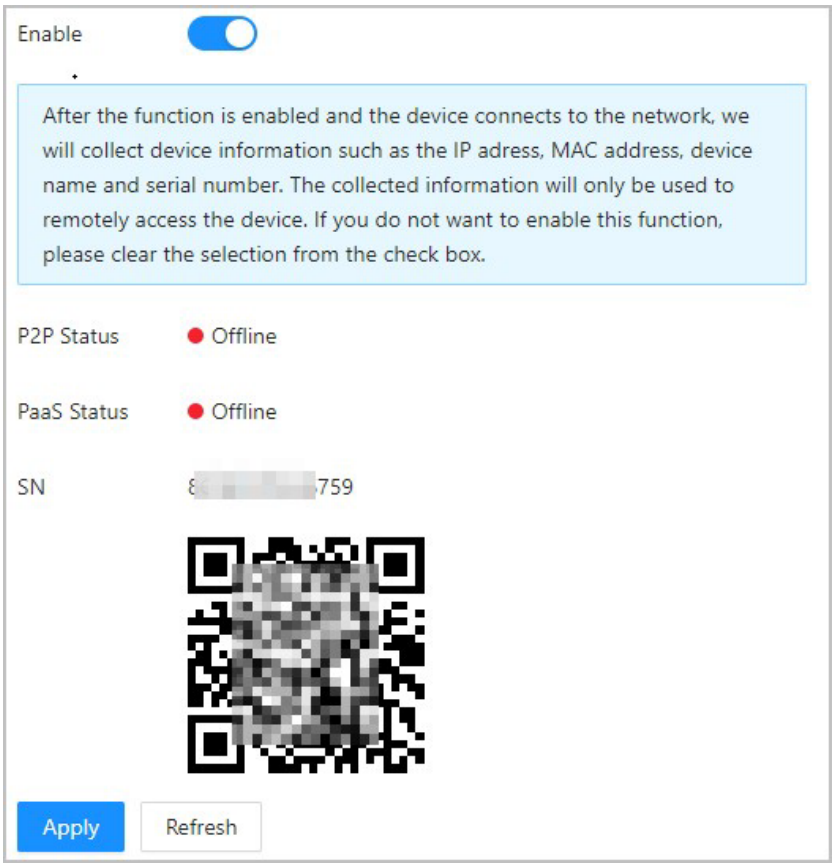
Step 1 On the home page, select Communication Settings > Network Setting > Cloud Service .

Step 2 Turn on the cloud service function.

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-57 Cloud service



Step 3 Click Apply .

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

3.10.1.6 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 Network Setting > Auto Registration .

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-58 Auto Registration

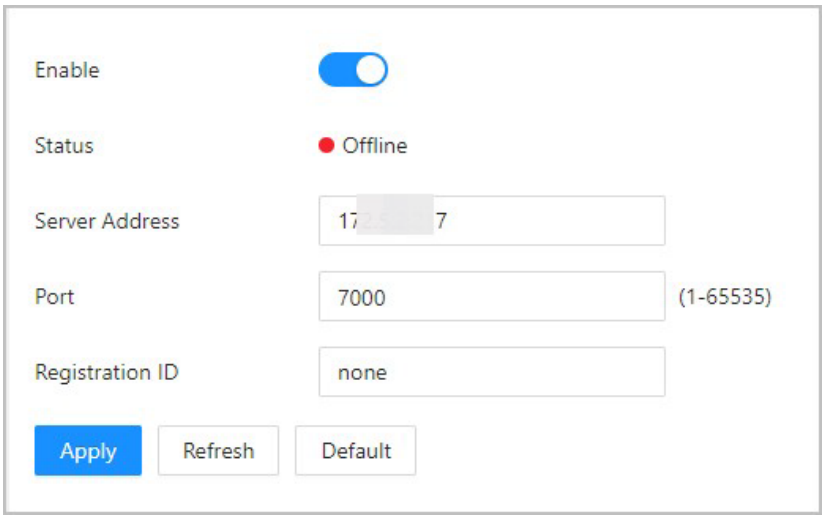


Table 3-35 Automatic registration description

Parameter	Description
Status	Displays the connection status of auto registration.
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 .

3.10.1.7 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-59 CGI active registration

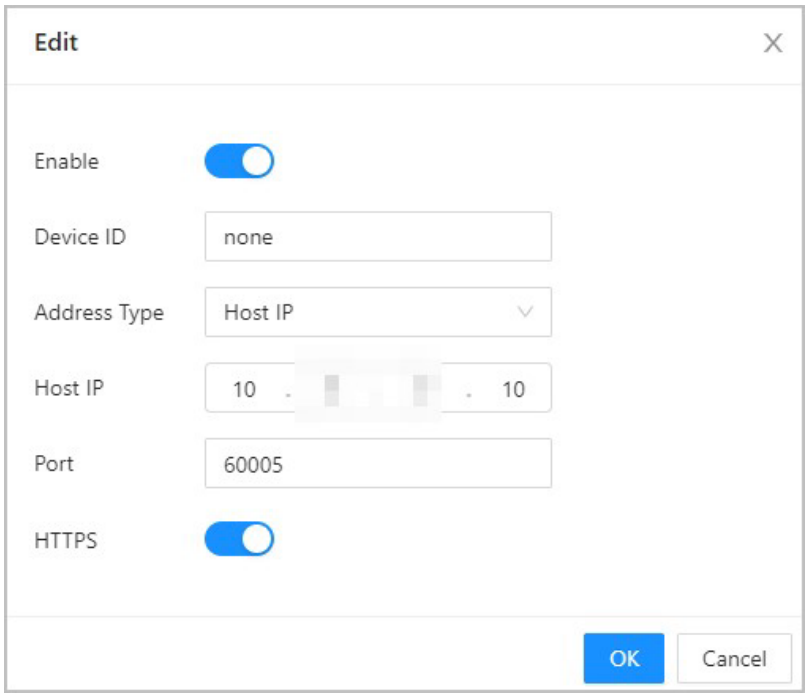


Table 3-36 Automatic registration description

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 .

3.10.1.8 Configuring Auto Upload

Send user information and unlock records through to the management platform.

Procedure

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

Step 2 (Optional) Enable 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Step 3 Enable HTTP upload mode.

Step 4 Click Add , and then configure parameters.

Figure 3-60 Automatic upload

Table 3-37 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, enable Push Person Info . Person information can only be pushed to one management platform and unlock records can be pushed to multiple management platforms.

Step 5 Click Apply .

3.10.2 Configuring RS-485

Configure the RS-485 parameters if you connect an external device to the RS-485 port.

Procedure

Step 1 Select Communication Settings > RS-485 Settings .

Step 2 Configure the parameters.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-61 Configure parameters

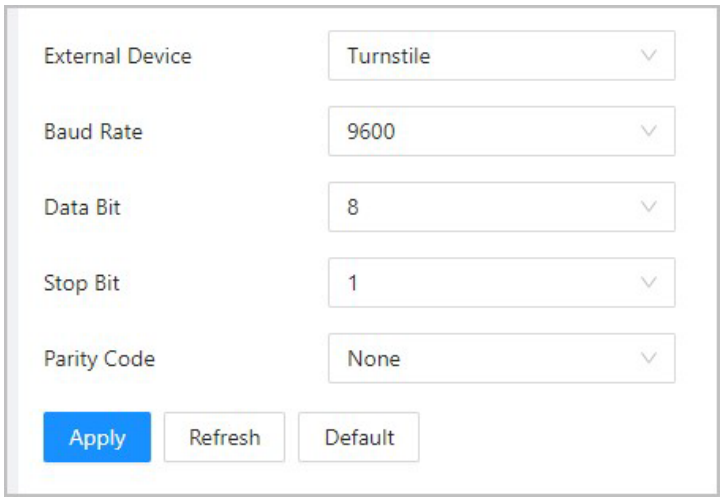


Table 3-38 Configure the Wiegand format

Parameter	Description
External Device	Access Controller Select Access Controller when the Device functions as a card reader, and sends data to other external access controllers to control access. Output Data type: ◇ Card Number: Outputs data based on card number when users swipe card to unlock door; outputs data based on user's first card number when they use other unlock methods. ◇ No.: Outputs data based on the user ID. Card Reader: The Device functions as an access controller, and connects to an external card reader. Reader (OSDP): The Device is connected to a card reader based on OSDP protocol. Door Control Security Module: The door exit button, lock and fire linkage is not effective after the security module is enabled. Turnstile: When the Device connects to a turnstile, and the access controller board of the turnstile connects to an external QR code module or card swiping module, the board will transmit the verification data to the turnstile.
Data Bit	The number of bits used to transmit the actual data in a serial communication. It represents the binary digits that carry the information being transmitted.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Stop Bit	A bit sent after the data and optional parity bits to indicate the end of a data transmission. It allows the receiver to prepare for the next byte of data and provides synchronization in the communication protocol.
Parity Code	An additional bit sent after the data bits to detect transmission errors. It helps verify the integrity of the transmitted data by ensuring a specific number of logical high or low bits.

Step 3 Click Apply .

3.10.3 Configuring Wiegand

Supports access Wiegand devices. Configure the mode and the transmission mode according to your actual devices.

Procedure

Step 1 Select Communication Settings > Wiegand .

Step 2 Select a Wiegand type, and then configure parameters.

Select Wiegand Input when you connect an external card reader to the Device.

When the Device connects to a third-party device through the Wiegand input port, and the card number read by the Device is in the reverse order from the actual card number. In this case, you can turn on Card No. Inversion function.

Select Wiegand Output when the Device functions as a card reader, and you need to connect it to another access controller.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-62 Wiegand output

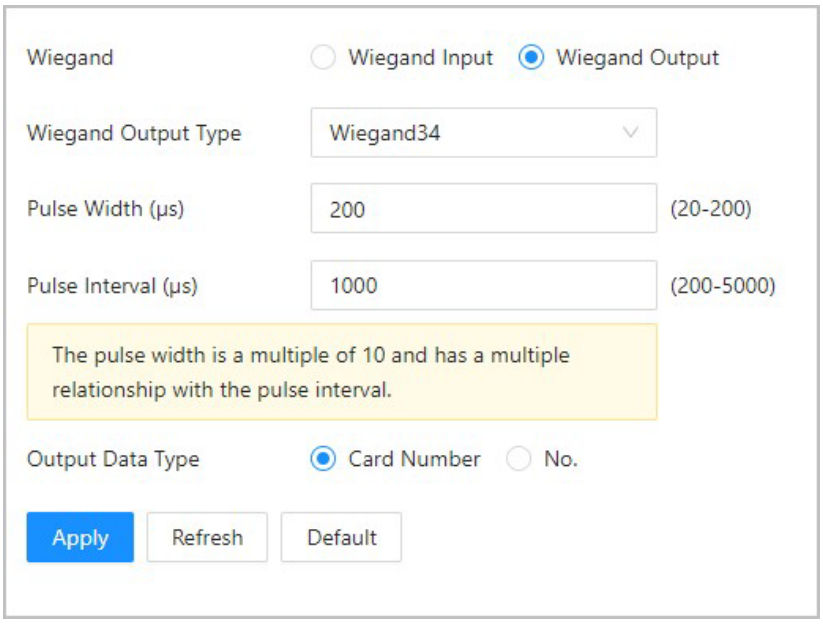


Table 3-39 Description of Wiegand output

Parameter	Description
Wiegand Output Type	Select a Wiegand format to read card numbers or ID numbers. Wiegand26 : Reads 3 bytes or 6 digits. Wiegand34 : Reads 4 bytes or 8 digits. Wiegand66 : Reads 8 bytes or 16 digits.
Pulse Width	Enter the pulse width and pulse interval of Wiegand output.
Pulse Interval	
Output Data Type	Select the type of output data. No. : Outputs data based on user ID. The data format is hexadecimal or decimal. Card Number : Outputs data based on user's first card number.

Step 3 Click Apply .

3.11 Configuring the System

3.11.1 User Management

You can add or delete users, change users' passwords, and enter an email address for resetting

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

the password when you forget your password.

3.11.1.1 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 .

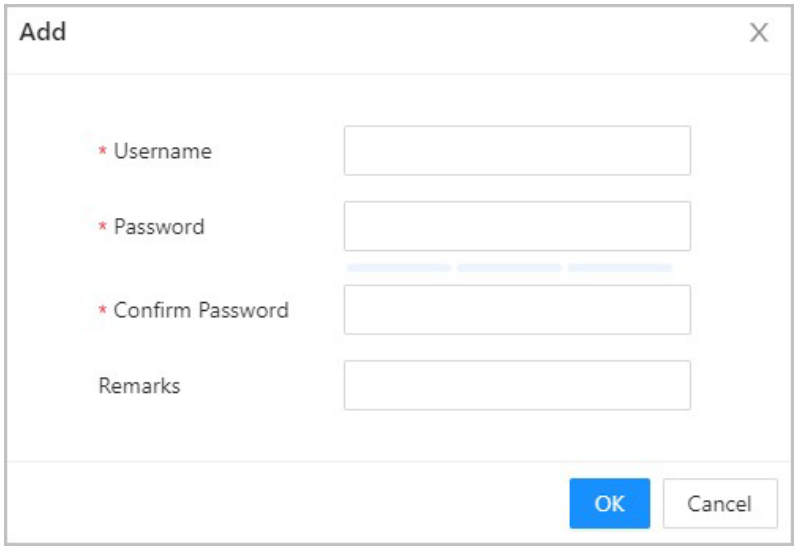
Step 2 Click Add , and enter the user information.

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 3-63 Add administrators



Step 3 Click OK .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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

3.11.1.2 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 3-64 Add ONVIF user

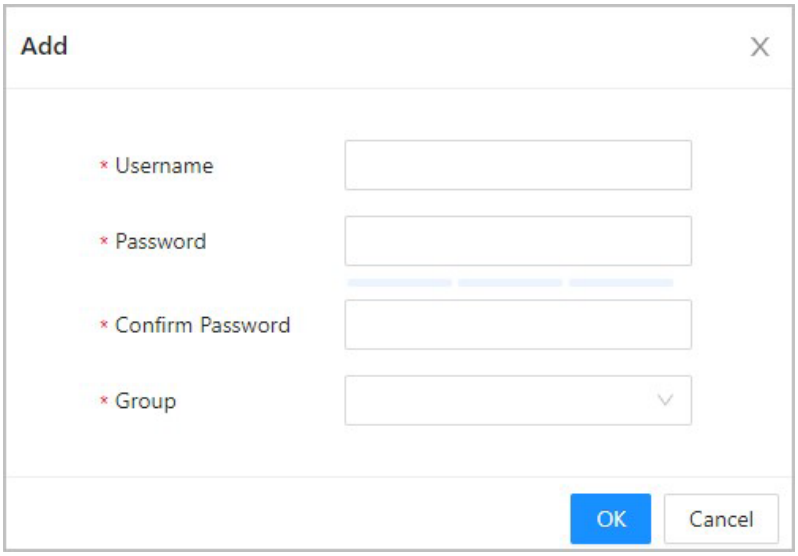


Table 3-40 ONVIF user description

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 ' " ; : &).

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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.

3.11.1.3 Resetting the Password

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

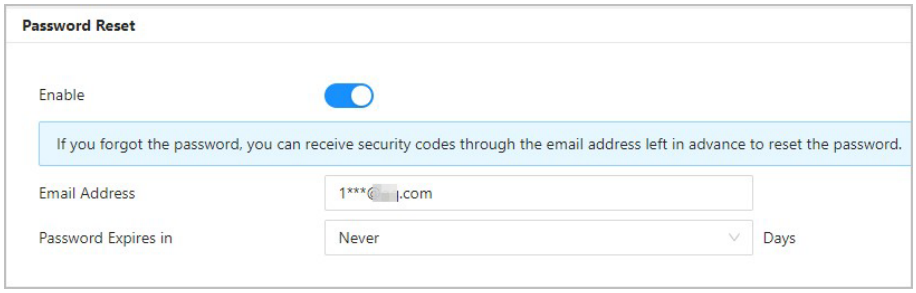
Procedure

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 3-65 Reset Password



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

Step 4 Click Apply .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.11.1.4 Viewing Online Users

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

3.11.2 Configuring Time

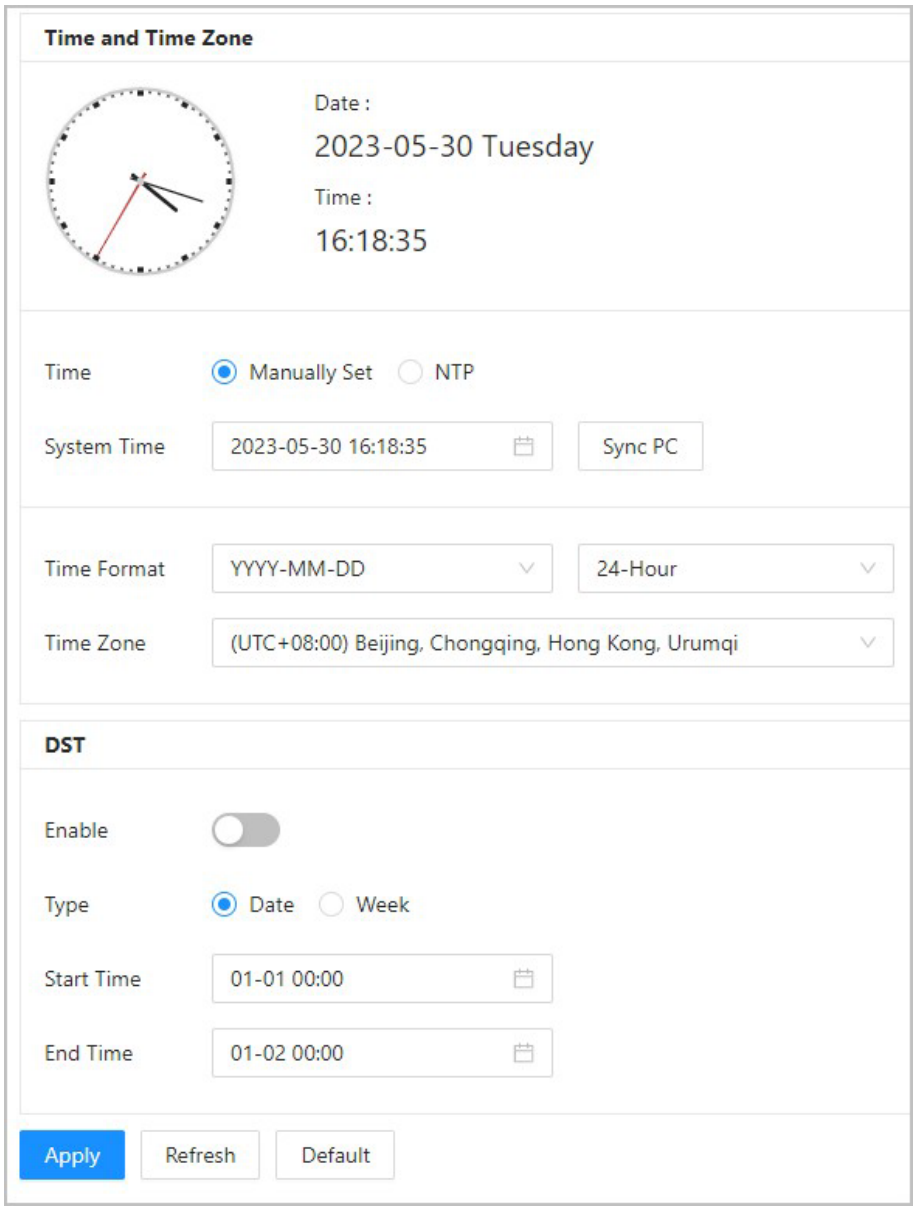
Procedure

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

Step 2 Configure the time of the Platform.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-66 Date settings



(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Table 3-41 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 .

3.11.3 Configuring the Shortcuts

Procedure

Step 1 On the webpage, select System > Shortcut Settings .

Step 2 Configure the shortcut parameters.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-67 Shortcut Settings

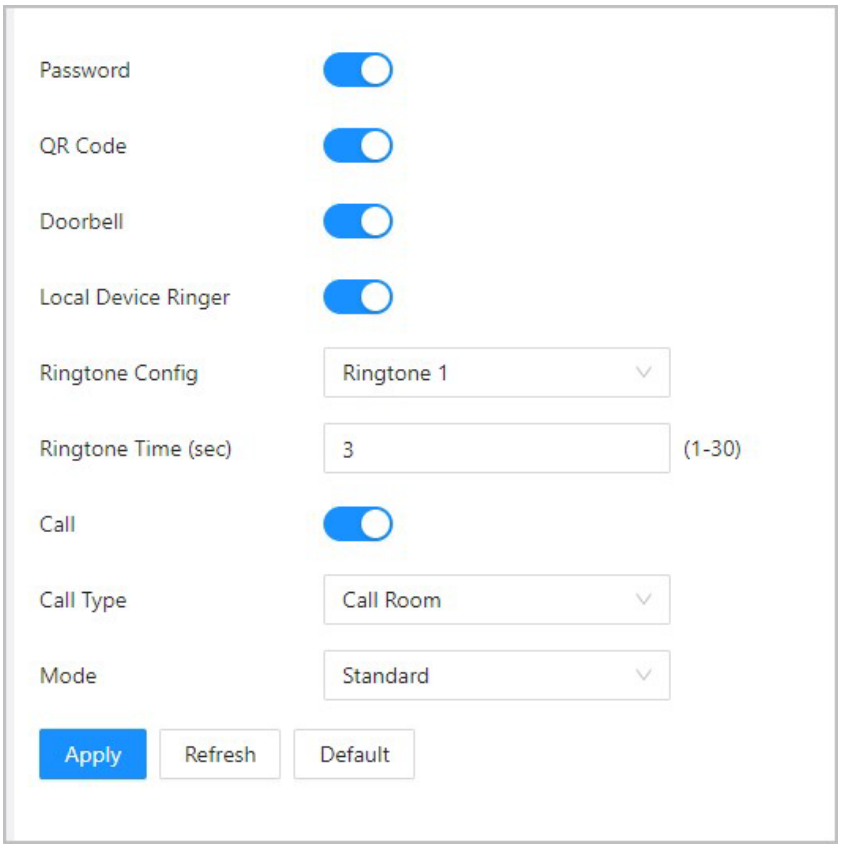


Table 3-42 Parameters description

Parameter	Description
Password	The icon of the password unlock method is displayed on the standby screen.
QR code	The QR code icon is displayed on standby screen. This function is not available for Device with a standalone QR code module.
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. This function is only available on select models.
Call	The icon of call is displayed on the standby screen.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Parameter	Description
Call Type	Call Room: Tap the call icon on the standby mode and enter the room number to make calls. Call Management Center: Tap the call icon on the standby mode, and then call the management center. Custom Call room: Enter the number of room, and then you can tap the call icon on the standby screen to call the pre-defined room number. You can call DMSS only in this call type.

3.12 Personalization

Configure themes and add video or image resources to the Device.

3.12.1 Adding Resources

Add images or videos to be displayed on the standby screen of the Device.

Background Information

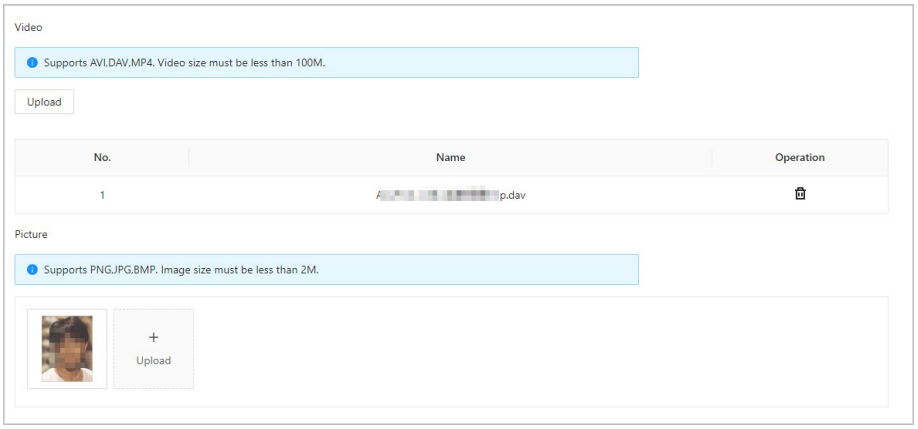
This function is only available on select models.

Procedure

Step 1 On the home page, select Personalization > Advertisement > Ad Resources .

Step 2 Add videos or images.

Figure 3-68 Add videos or images



(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Add videos.

1. Click Upload .
2. Click Browse , select the video file, and then click Next .
   The video is automatically uploaded to the platform after transcoding.

   - You can upload up to 5 video files.
   - Supports DAV, AVI, MP4. Video size must be less than 100 M.
   - Only supports latest version of Firefox and Chrome to upload video files.

Add images.

1. Click +.
2. Select image from the local and upload it.

   Supports PNG, JPG, BMP. Image size must be less than 2 M.

Related Operations

Click to delete uploaded images or videos.

Videos and images in use cannot be deleted.

3.12.2 Configuring Themes

Background Information

This function is only available on select models.

Procedure

Step 1 On the home page, select Personalization > Advertisement > Subject .

Step 2 Select the theme.

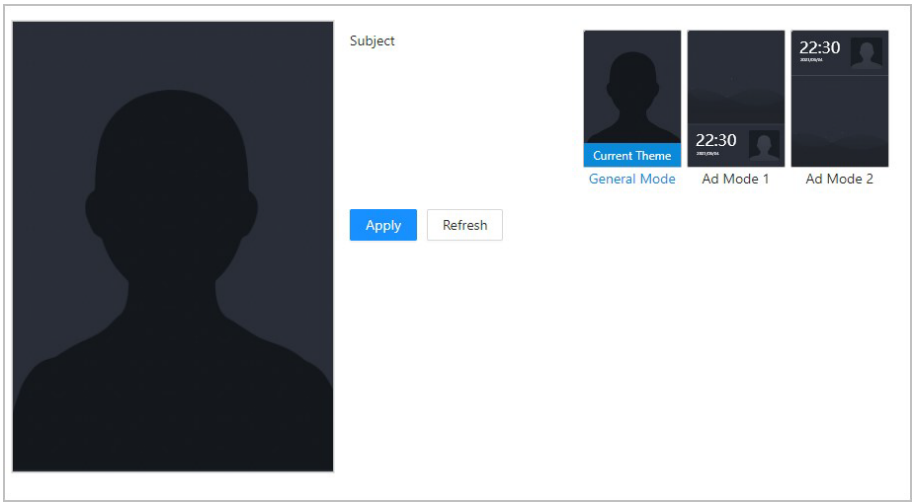
General Theme: Displays the face image in full screen.

Ad Mode 1: The upper area displays the advertisements, and the lower area displays the time and the face detection box.

Ad Mode 2: The upper area displays the time and the face detection box, and the lower area displays the advertisements.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-69 Theme

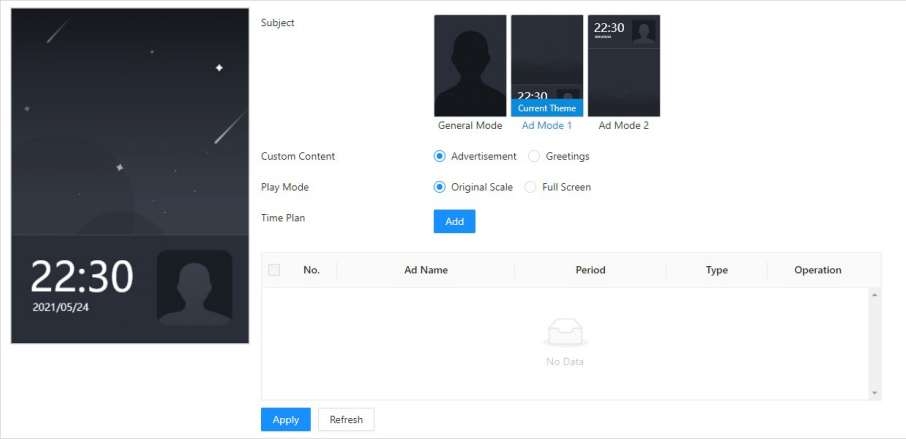


Step 3 Select the voice prompt for successful identity verification.

Step 4 Set advertisement display.

1. Select Ad mode 1 or Ad mode 2, and then select Advertisement .

Figure 3-70 Advertisement mode



2. Select the display mode.

   Original Scale: Plays the image and video in the original size.

   Full Screen: Plays the image and video in full screen.

3. Click Add to add time schedules.

   You can add up to 10 schedules.

4. Enter the name of the advertisement.

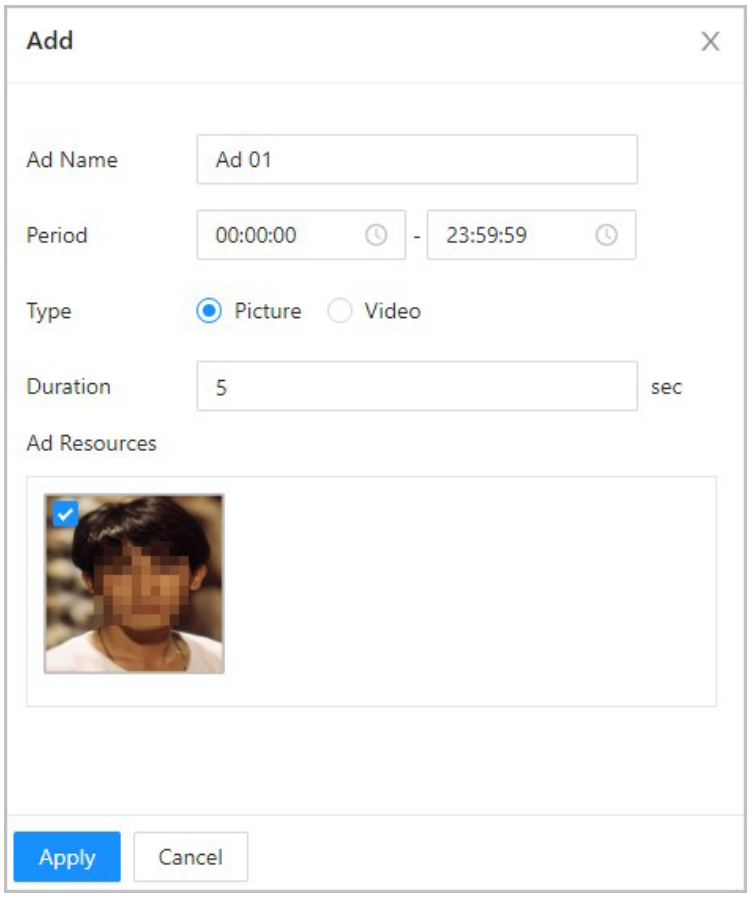
5. Select the time section, file type and file.

6. Enter the duration, and then click Apply .

   Set the duration for a single picture when pictures are played in a loop. The duration ranges from 1 s to 20 s and it is 5 s by default.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-71 Add time schedules

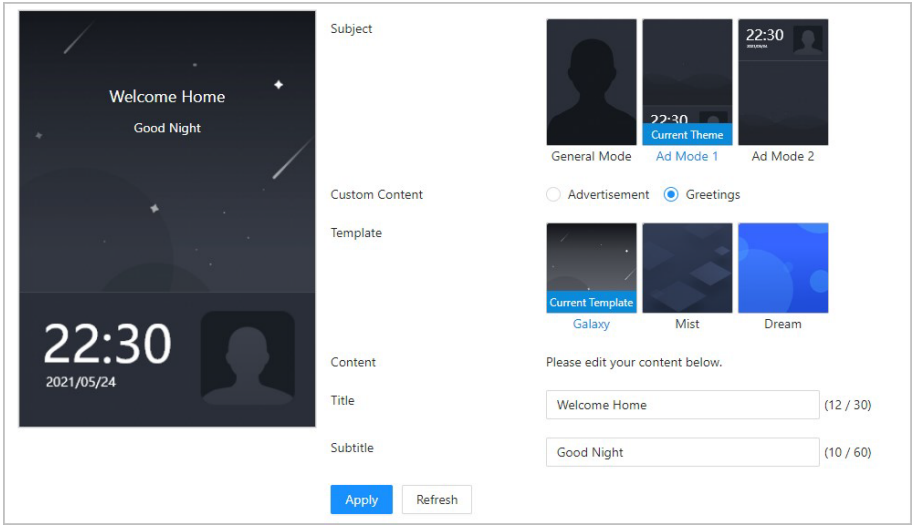


Step 5 Configure greetings.

1. Select Greetings from the Custom Content .
2. Select the template.
3. Enter the title and subtitle.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-72 Greetings



4. Click Apply .

3.13 Management Center

3.13.1 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 .

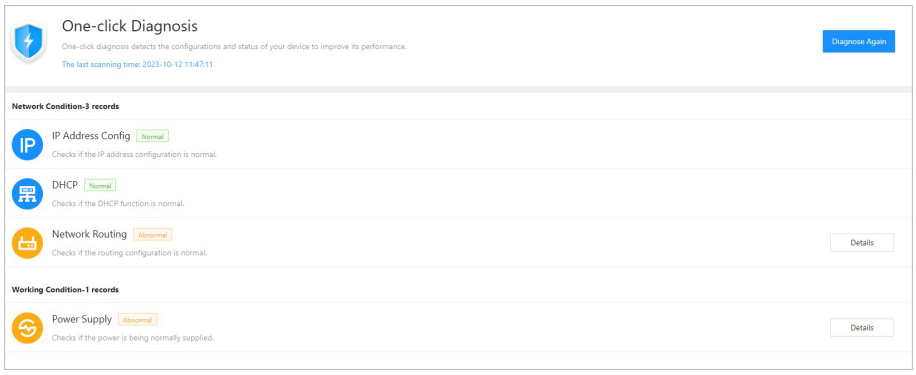
The system automatically diagnoses the configurations and the status of the device and display diagnosis results after it completes.

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-73 One-click diagnosis



3.13.2 System Information

3.13.2.1 Viewing Version Information

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

3.13.2.2 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.

3.13.3 Data Capacity

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

Log in to the webpage and select Data Capacity .

3.13.4 Viewing Logs

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

3.13.4.1 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 .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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.

3.13.4.2 Unlock Records

Search for unlock records and export them.

Procedure

Step 1 Log in to the webpage.

Step 2 Select Log > Unlock Records .

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

You can click Export to download the log.

3.13.4.3 Call History

View call logs.

Procedure

Step 1 Log in to the webpage.

Step 2 Select Log > Call History .

3.13.4.4 Alarm Logs

View alarm logs.

Procedure

Step 1 Log in to the webpage.

Step 2 Select Log > Alarm Log .

Step 3 Select the type and the time range.

Step 4 Enter the admin ID, and then click Search .

3.13.4.5 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.13.4.6 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.

3.13.5 Configuration Management

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

3.13.5.1 Exporting and Importing Configuration Files

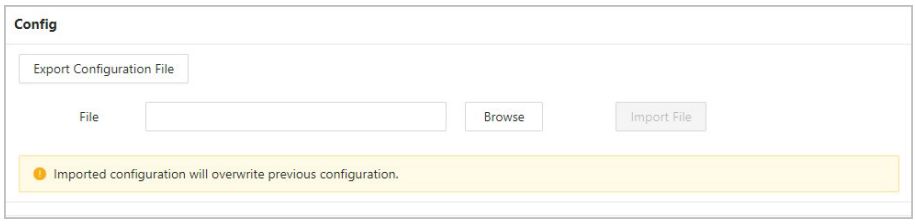
You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

Step 2 Select System > Config .

Figure 3-74 Configuration management



Step 3 Export or import configuration files.

Export the configuration file.

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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.

3.13.5.2 Restoring the Factory Default Settings

Procedure

Step 1 Select System > 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.

3.13.6 Maintenance

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

Procedure

Step 1 Log in to the webpage.

Step 2 Select System > 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.13.7 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.

3.13.7.1 File Update

Procedure

Step 1 On the home page, select System > Update .

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

📖

The update file should be a .bin file.

Step 3 Click Update .

The Device will restart after the update finishes.

3.13.7.2 Online Update

Procedure

Step 1 On the home page, select System > Update .

Step 2 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.

Step 3 (Optional) Click Update Now to update the Device immediately.

3.13.8 Advanced Maintenance

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

3.13.8.1 Exporting

Procedure

Step 1 On the home page, select Maintenance Center > Advanced Maintenance > Export .

Step 2 Click Export to export the serial number, firmware version, device operation logs and

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

configuration information.

3.13.8.2 Packet Capture

Procedure

Step 1 On the home page, select Maintenance Center > Advanced Maintenance > Packet Capture .

Figure 3-75 Packet Capture

Step 2 Enter the IP address, click .

changes to .

Step 3 After you acquired enough data, click .

Captured packets are automatically downloaded to your local computer.

3.14 Security Settings(Optional)

3.14.1 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

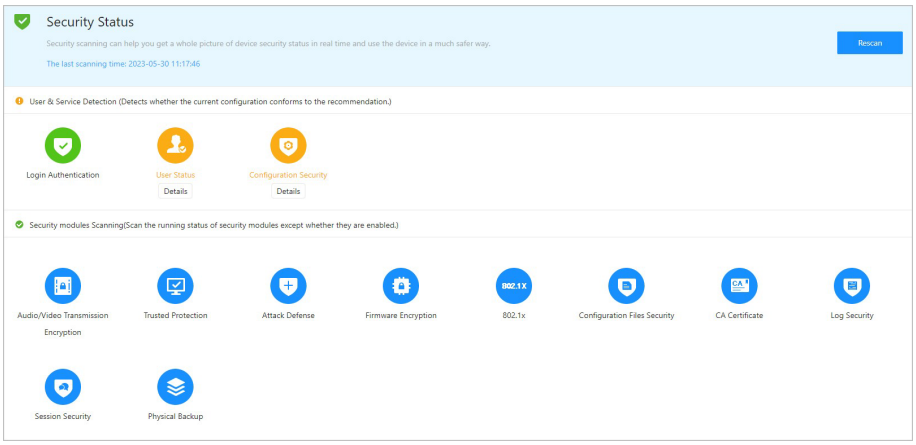
Step 1 Select > Security Status .

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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

Figure 3-76 Security Status



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.

3.14.2 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.

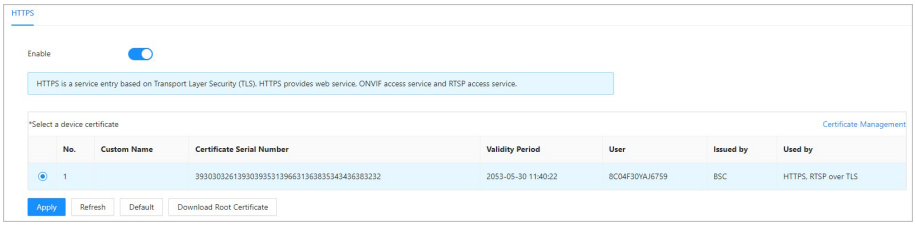
If you turn on the compatible with TLS v1.1 and earlier versions, security risks might occur. Please be advised.

Step 3 Select the certificate.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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

Figure 3-77 HTTPS



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.

3.14.3 Attack Defense

3.14.3.1 Configuring Firewall

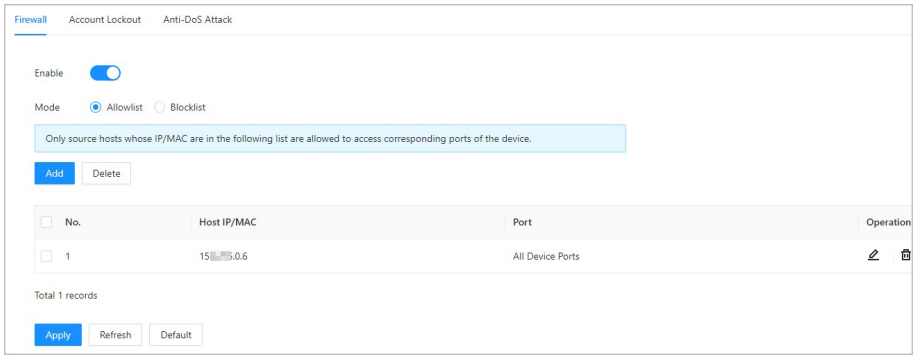
Configure firewall to limit access to the Device.

Procedure

Step 1 Select > Attack Defense > Firewall .

Step 2 Click to enable the firewall function.

Figure 3-78 Firewall



Step 3 Select the mode: Allowlist and Blocklist .

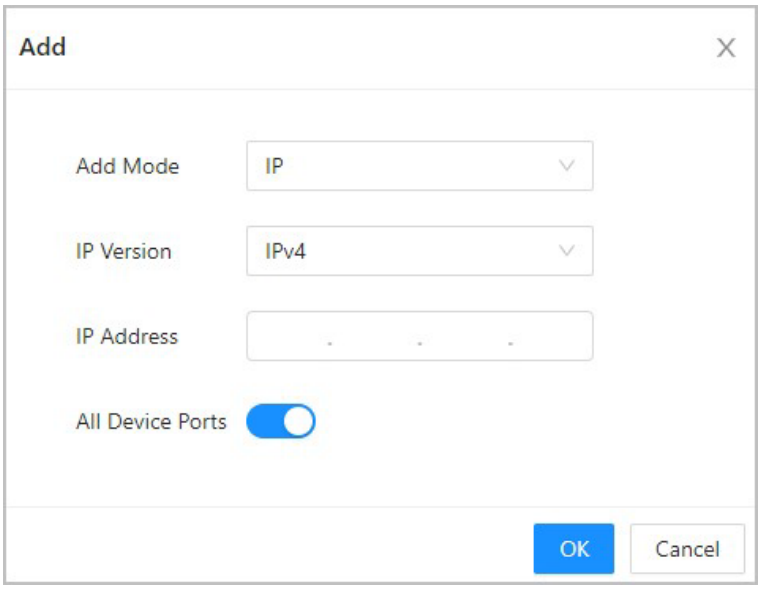
Allowlist : Only IP/MAC addresses on the allowlist can access the Device.

Blocklist : The IP/MAC addresses on the blocklist cannot access the Device.

Step 4 Click Add to enter the IP information.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-79 Add IP information



Step 5 Click OK.

Related Operations

Click to edit the IP information.

Click to delete the IP address.

3.14.3.2 Configuring Account Lockout

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

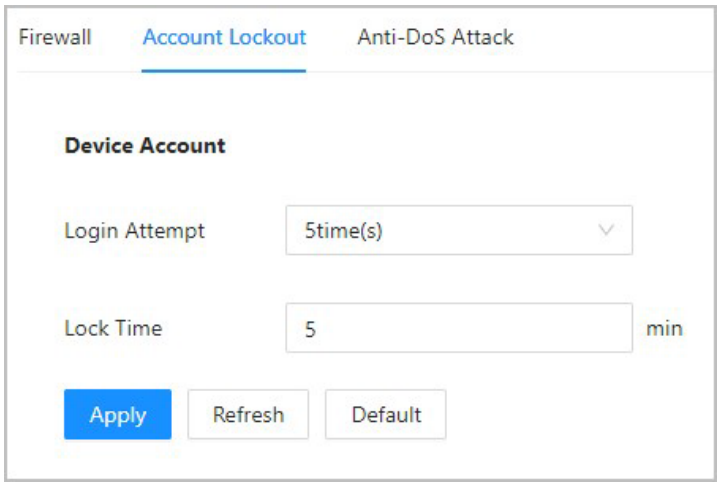
Procedure

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-80 Account lockout



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 .

3.14.3.3 Configuring Anti-DoS Attack

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

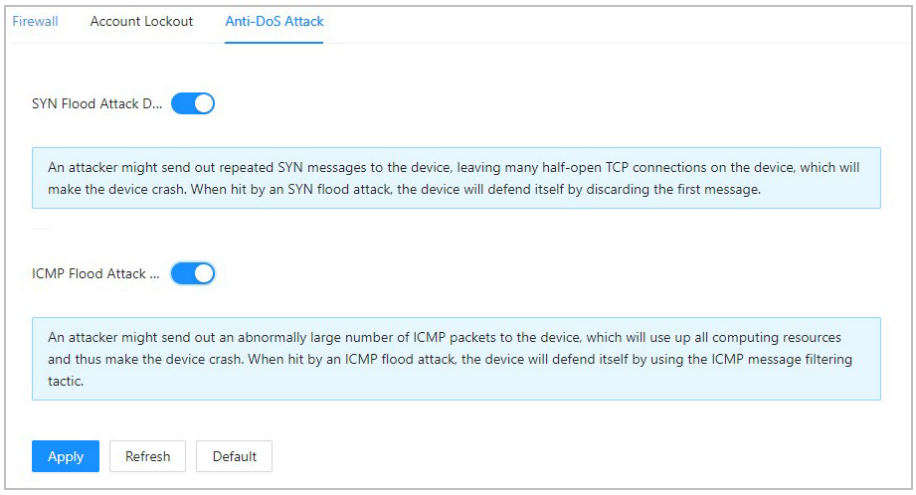
Procedure

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-81 Anti-DoS attack



Step 3 Click Apply .

3.14.4 Installing Device Certificate

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

3.14.4.1 Creating Certificate

Create a certificate for the Device.

Procedure

Step 1 Select > CA Certificate > Device Certificate .

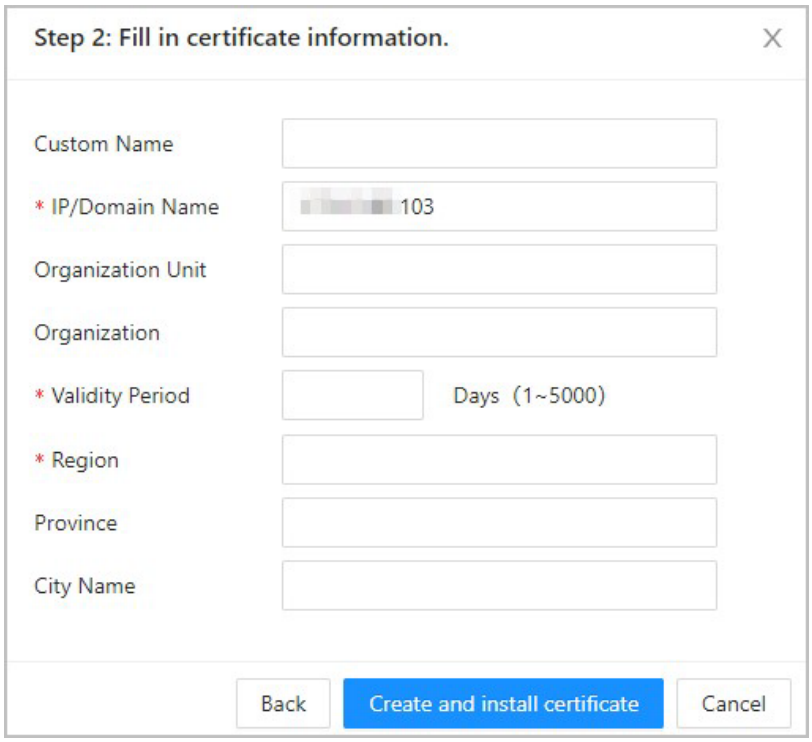
Step 2 Select Install Device Certificate .

Step 3 Select Create Certificate , and click Next .

Step 4 Enter the certificate information.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-82 Certificate information



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.

3.14.4.2 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 .

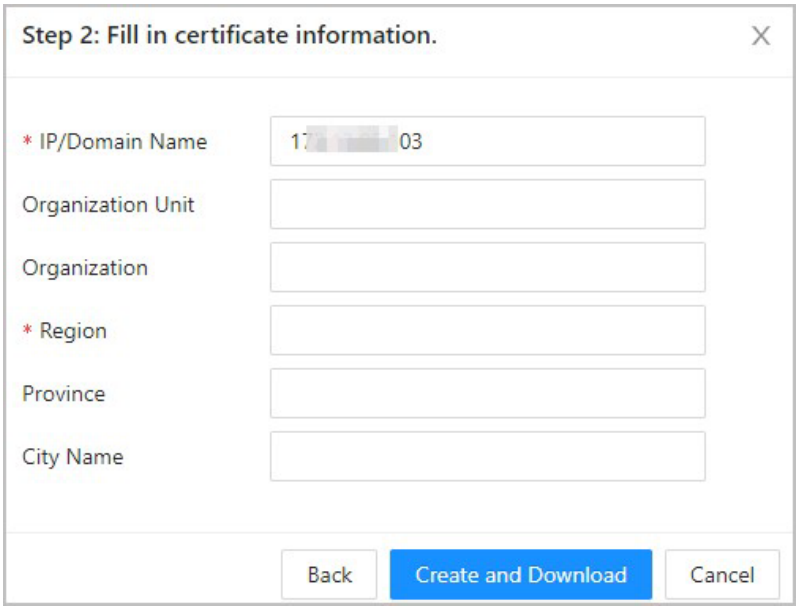
Step 4 Enter the certificate information.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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 3-83 Certificate information (2)



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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

3.14.4.3 Installing Existing Certificate

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

Procedure

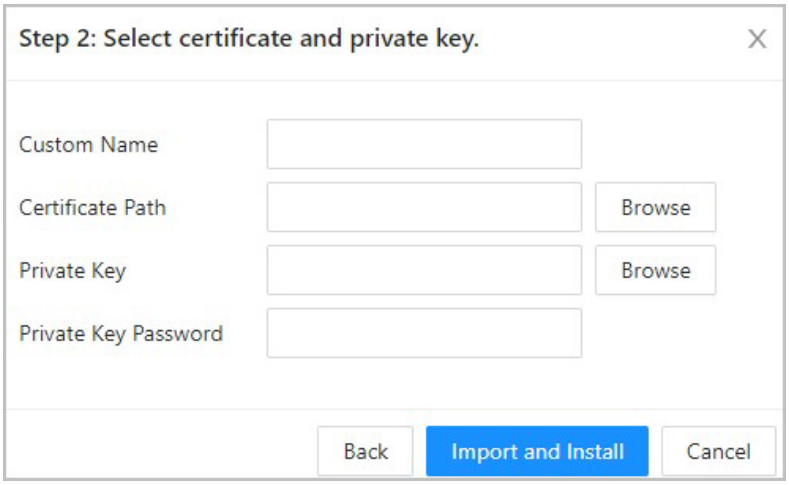
Step 1 Select Security > CA Certificate > Device Certificate .

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 3-84 Certificate and private key



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.

3.14.5 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

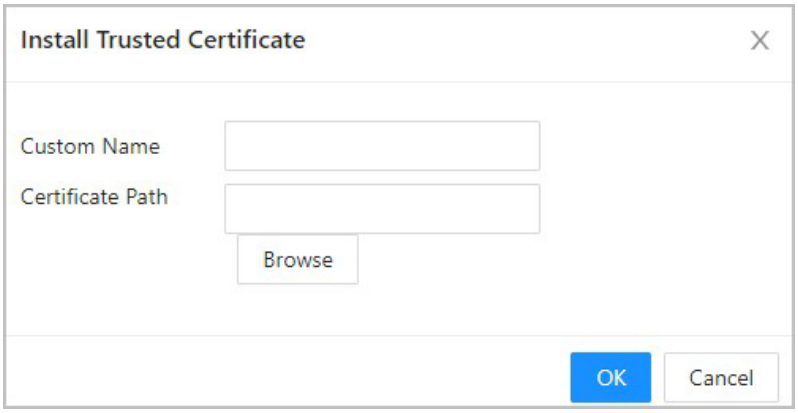
Procedure

Step 1 Select > CA Certificate > Trusted CA Certificates .

Step 2 Select Install Trusted Certificate .

Step 3 Click Browse to select the trusted certificate.

Figure 3-85 Install the trusted certificate



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.

3.14.6 Data Encryption

Procedure

Step 1 Select > Data Encryption .

Step 2 Configure the parameters.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-86 Data encryption

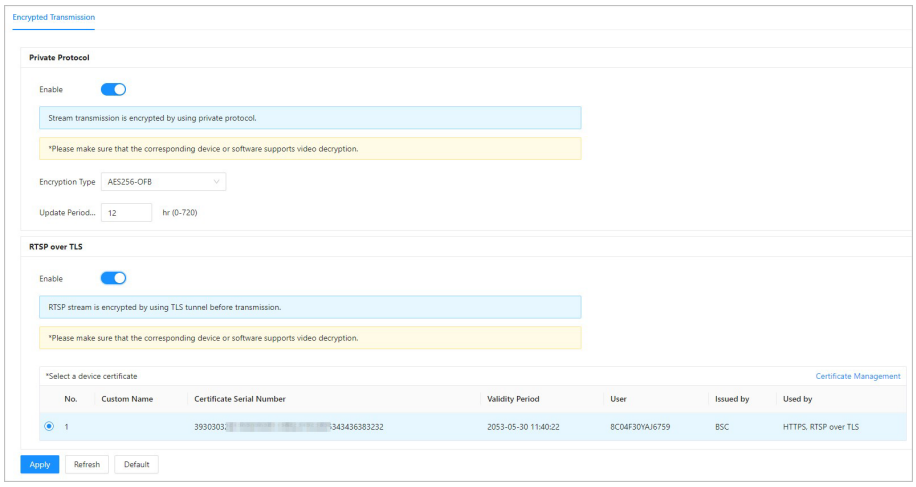


Table 3-43 Data encryption description

	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"3.14.4 Installing Device Certificate". The installed certificates are displayed in the list.

3.14.7 Security Warning

Procedure

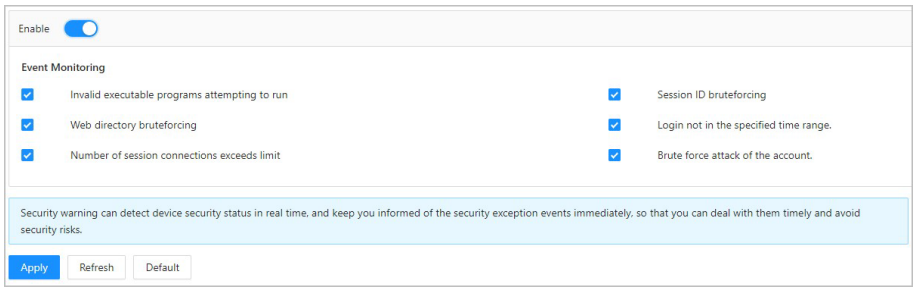
Step 1 Select > Security Warning .

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 3-87 Security warning



Step 4 Click Apply .

3.14.8 Security Authentication

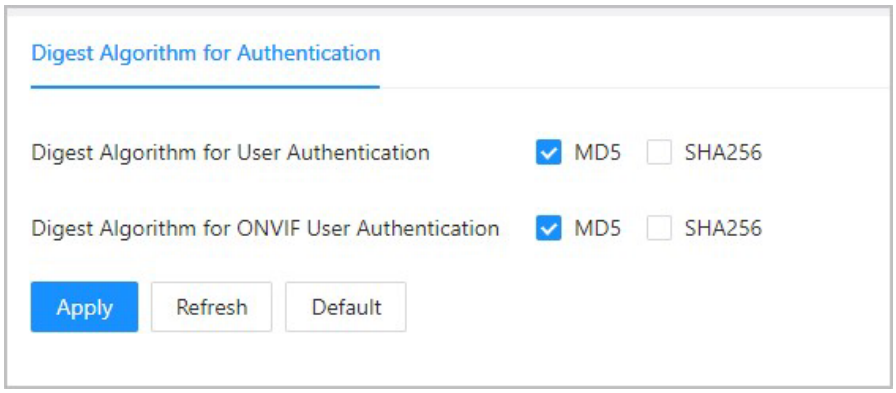
Procedure

Step 1 Select Security > Security Authentication .

Step 2 Select a message digest algorithm.

Step 3 Click Apply .

Figure 3-88 Security Authentication



(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 4-1 Add devices

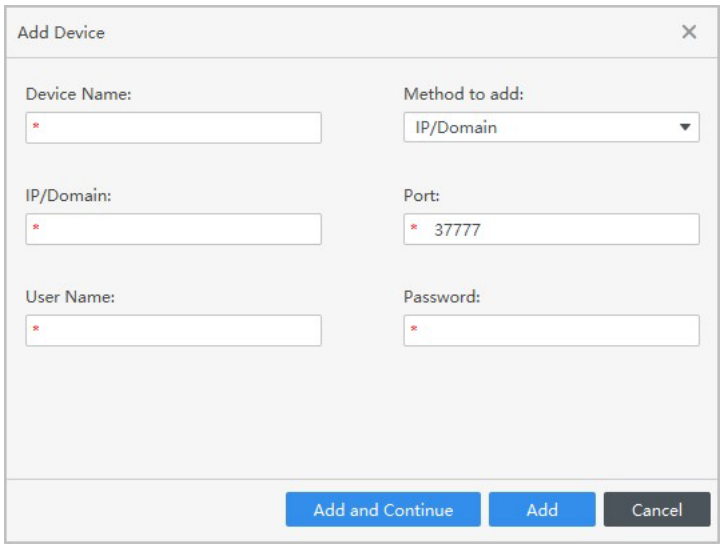


Table 4-1 Parameters of IP adding

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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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 .

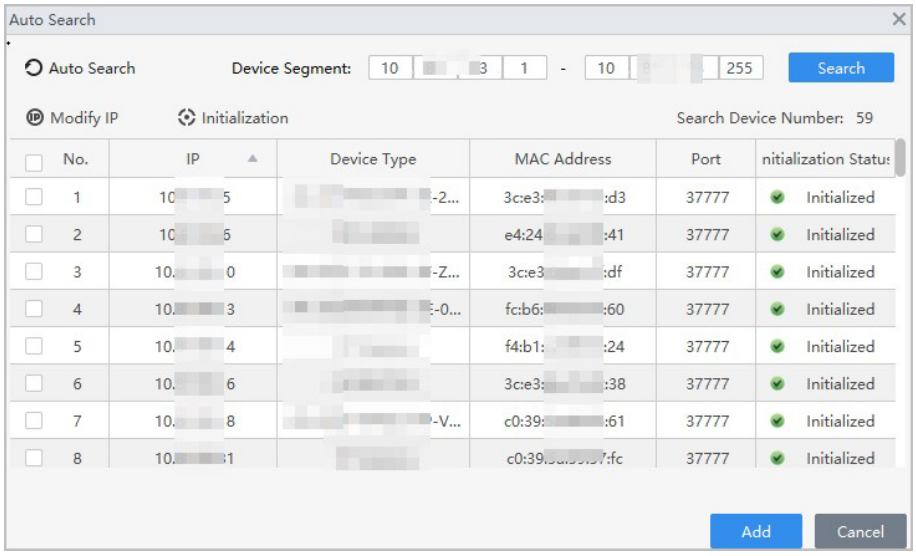
Step 2 Select a search method.

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



Step 3 Click devices, and then click Add .

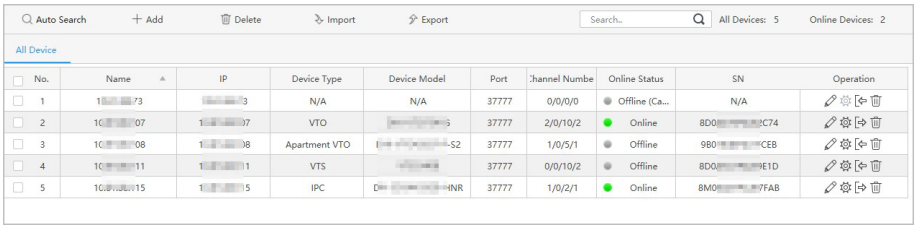
Step 4 Enter the login user name and password, and then click OK .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Result

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

Figure 4-3 Added devices



4.3 User Management

Add users, assign cards to them, and configure their access permissions.

4.3.1 Configuring Card Type

Set the card type before you assign cards to users. For example, if the assigned card is an ID card, set card type to ID card.

Procedure

Step 1 Log in to Smart PSS Lite.

Step 2 Click Access Solution > Personnel Manager > User .

Step 3 On the Card Issuing Type and then select a card type.

Make sure that the card type is same to the actually assigned card; otherwise, the card number cannot be read.

Step 4 Click OK .

4.3.2 Adding Users

4.3.2.1 Adding Users One by One

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.
3) Take snapshot or upload picture, and then click Finish .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

The card number can be read automatically or filled in manually. To automatically read card number, select the card reader next to Card No. , and then place the card on the card reader. The card number will be read automatically.

You can select multiple USB cameras to snap pictures.

Set password

Click Add to add the password.

Configure card

a. Click to select Device or Card issuer as card reader.
b. Add cards.
c. After adding, you can select the card as main card or duress card, or replace the card with a new one, or delete the card.
d. Click to display the QR code of the card.

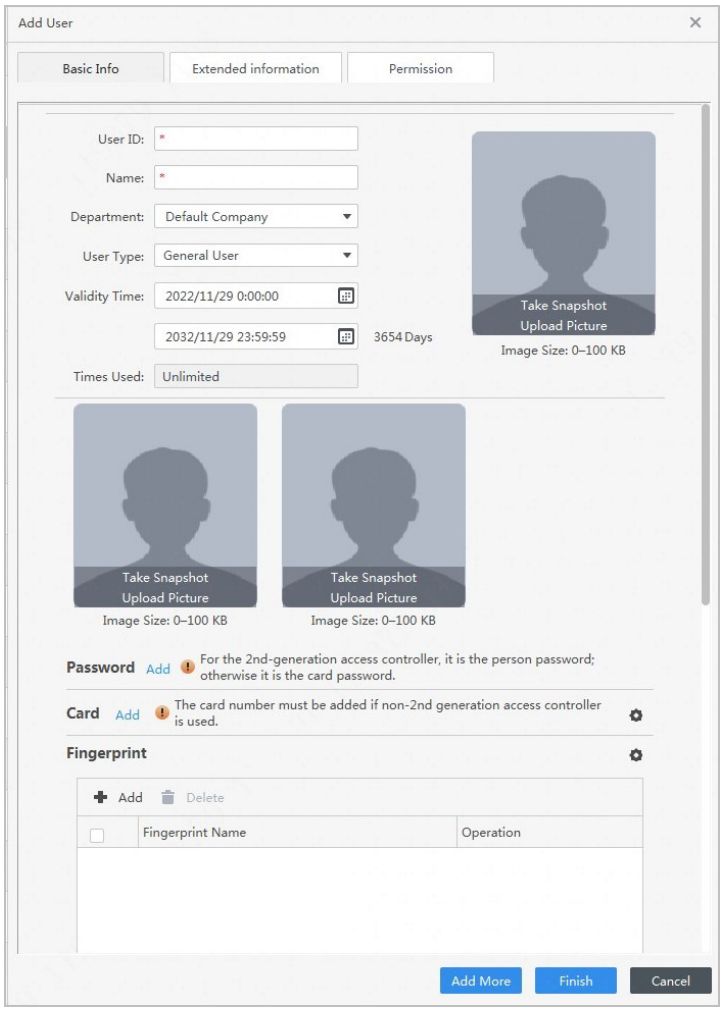
Only 8-digit card number in hexadecimal mode can display the QR code of the card.

Configure fingerprint

a. Click to select Device or Fingerprint Scanner as the fingerprint collector.
b. Add fingerprint. Select Add > Add Fingerprint , and then press finger on the scanner for three times continuously.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

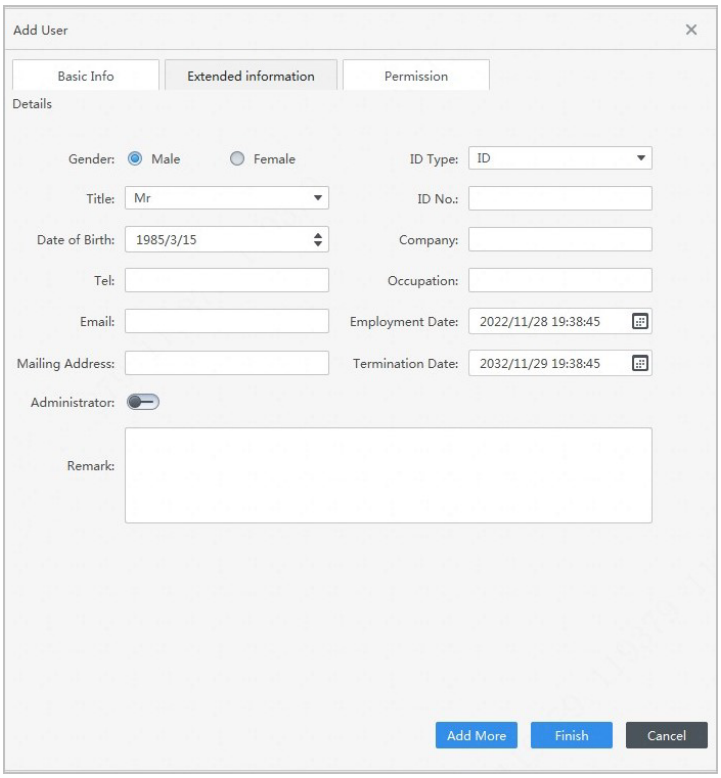
Figure 4-4 Add basic information



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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 4-5 Add extended information



Step 4 Configure permissions.

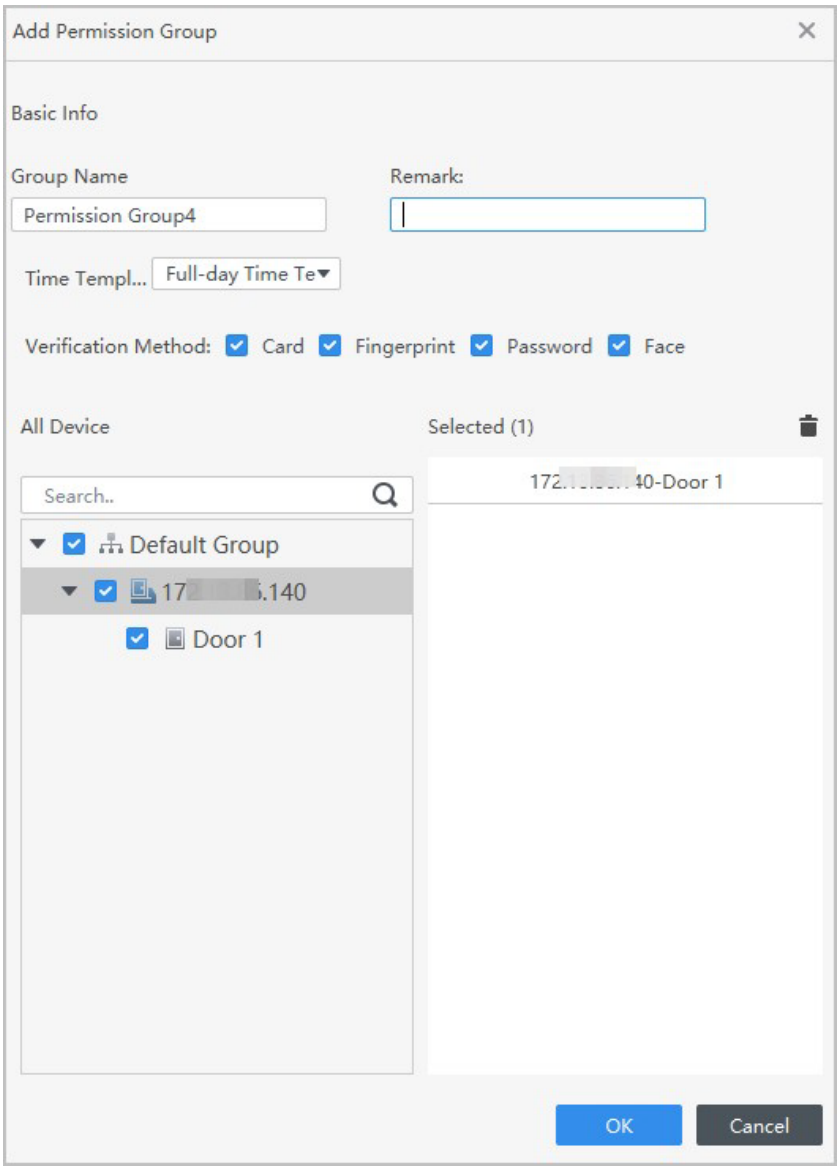
1) Click + .
2) Enter the group name, remarks (optional), and select a time template.
3) Select verification methods and doors.

Step 5 Configure permissions. For details, see "4.3.3 Assigning Access Permission".

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 4-6 Configure permission groups



Step 6 Click Finish .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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

4.3.2.2 Adding Users in Batches

Procedure

Step 1 Click Personnel Manger > Batch Update > Batch Add .

Step 2 Select Card issuer or Device from the Device list, and then configure the parameters.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 4-7 Add users in batches

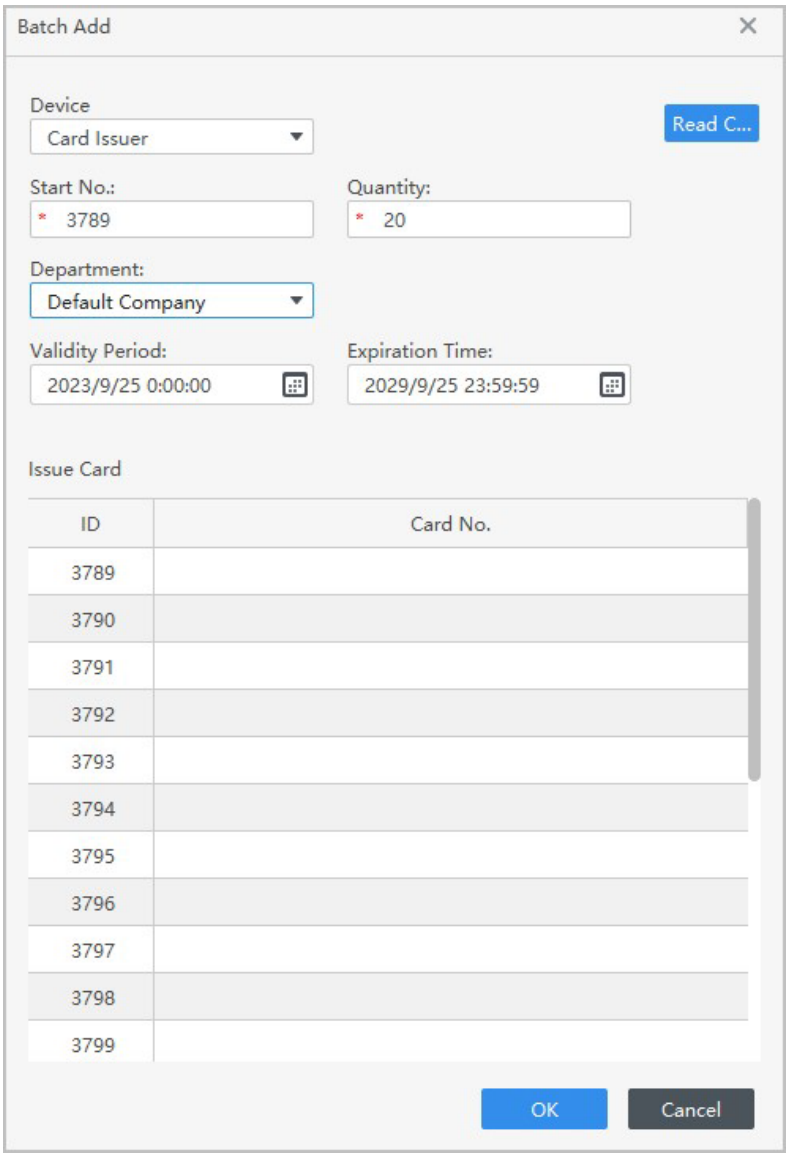


Table 4-2 Add users in batches parameters

Parameter	Description
Start No.	The user ID starts with the number you defined.
Quantity	The number of users you want to add.
Department	Select the department that the user belongs to.
Effective Time/Expired Time	The users can unlock the door within the defined period.

Step 3 Click Read Card No. , and swipe cards on the card reader.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

The card number will be read automatically.

Step 4 Click OK.

4.3.3 Assigning Access Permission

Create a permission group that is a collection of door access permissions, and then link users with the group so that users can unlock doors associated with the permission group.

Procedure

Step 1 Click Access Solution > Personnel Manger > Permission .

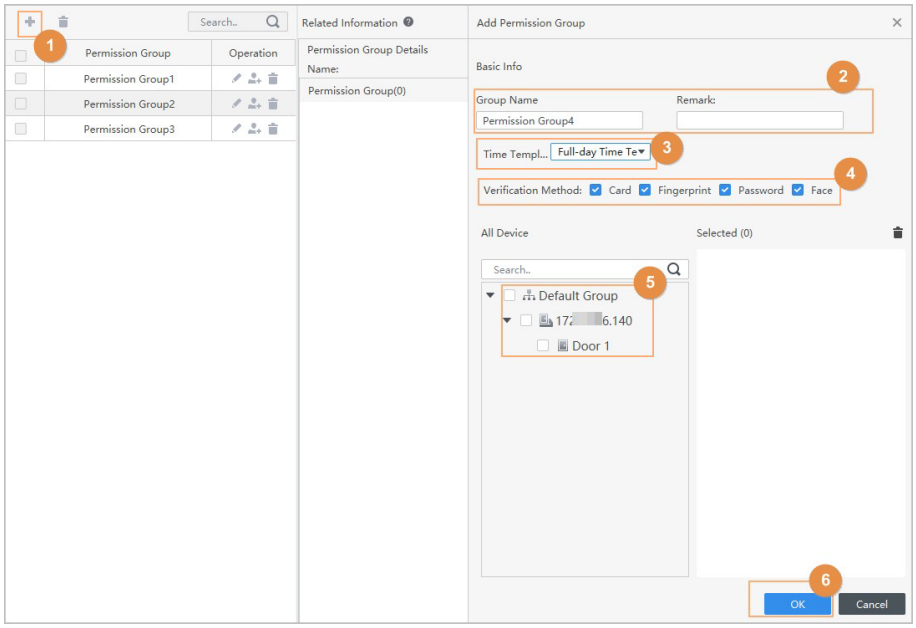
Step 2 Click .

Step 3 Enter the group name, remarks (optional), and select a time template.

Step 4 Select verification methods and doors.

Step 5 Click OK.

Figure 4-8 Create a permission group

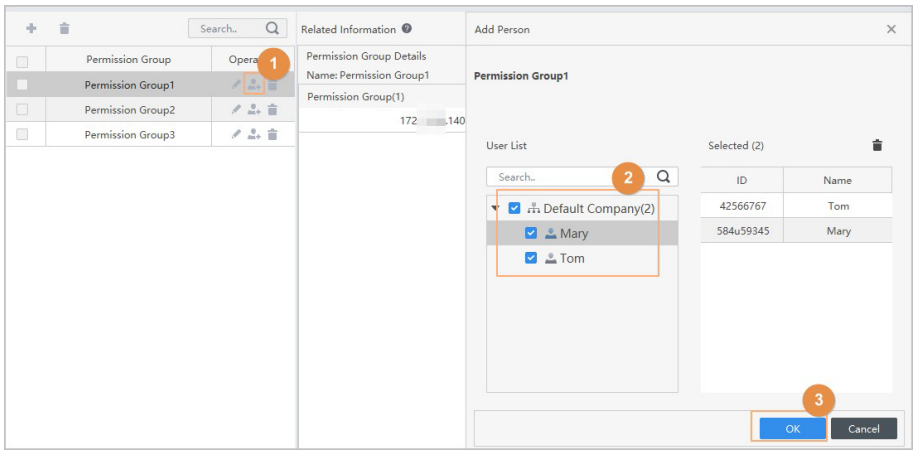


Step 6 Click of the permission group.

Step 7 Select users to associate them with the permission group.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 4-9 Add users to a permission group



Step 8 Click OK.

Users can unlock the door in this permission group after valid identity verification.

4.3.4 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 + .

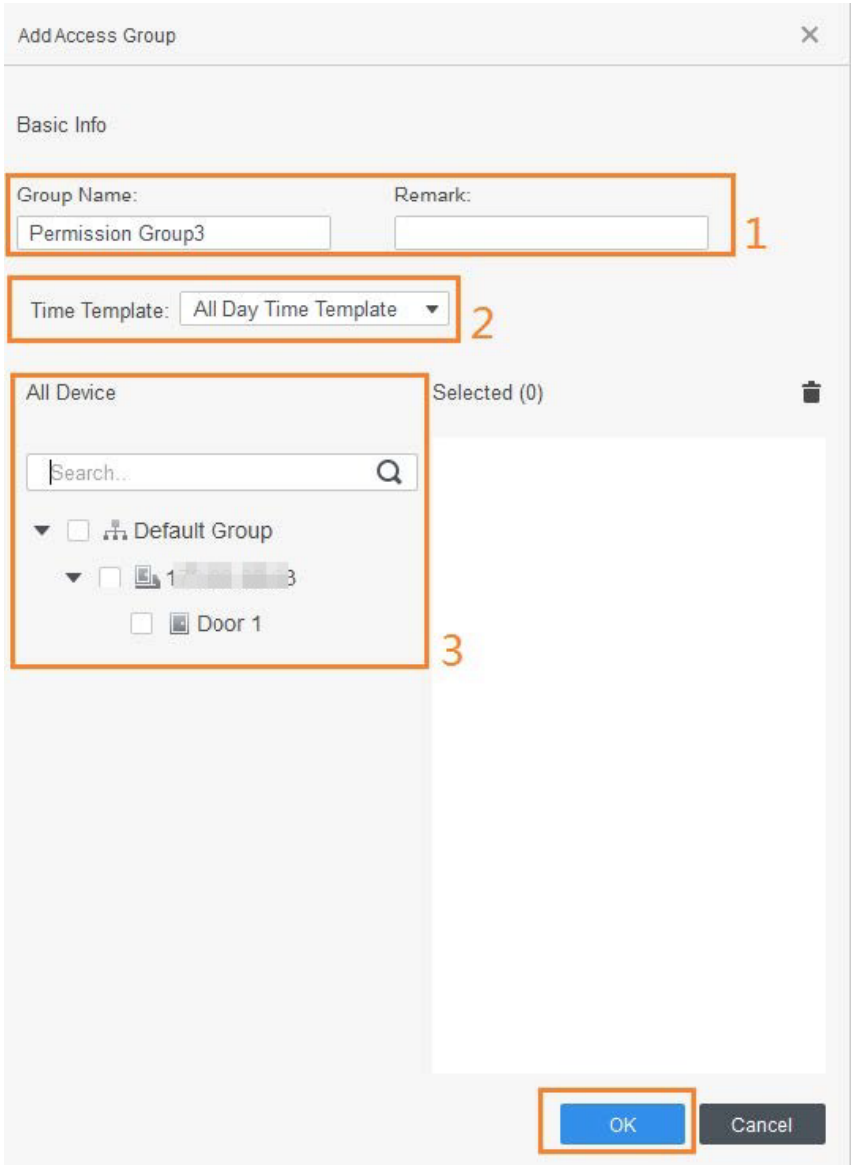
Step 4 Enter the group name, remarks (optional), and select a time template.

Step 5 Select the access control device.

Step 6 Click OK.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 4-10 Create a permission group



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

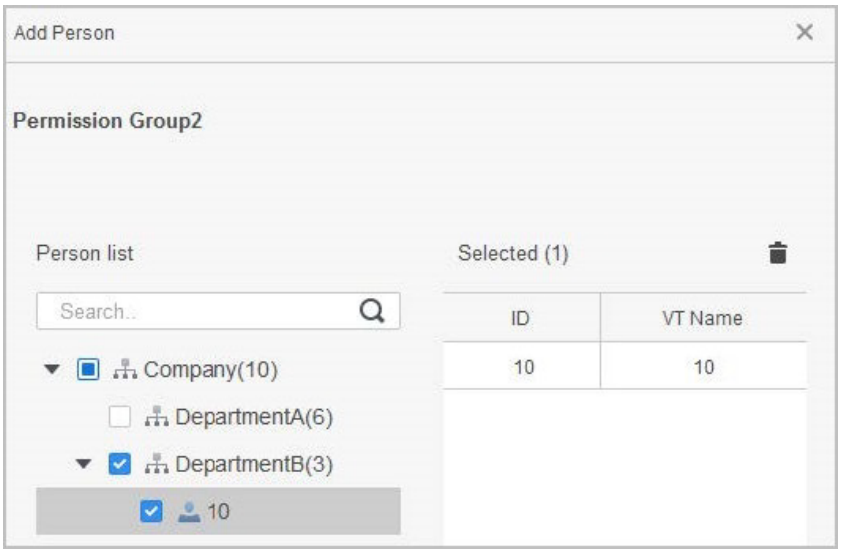
Card and fingerprint attendance are available on select models.

Step 7 Click of the permission group you added.

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Figure 4-11 Add users to a permission group



Step 9 Click OK.

4.4 Access Management

4.4.1 Remotely Opening and Closing Door

You can remotely monitor and control door through the platform. For example, you can remotely open or close the door.

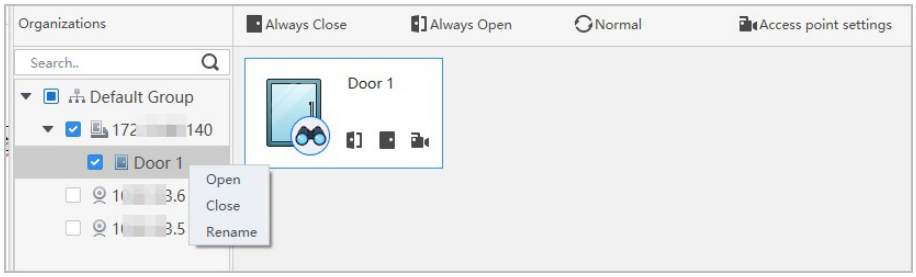
Procedure

Step 1 Click Access Solution > Access Manager on the home page.

Step 2 Remotely control the door.

Select the door, right click and select Open or Close to open or close the door.

Figure 4-12 Open door



: Open or close the door.

: View the live video of the door.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Related Operations

Event filtering: Select the event type in the Event Info , and the event list displays the selected event type, such as alarm events and abnormal events.

Event refresh locking: Click to lock the event list, and then event list will stop refreshing. Click to unlock.

Event deleting: Click to clear all events in the event list.

4.4.2 Setting Always Open and Always Close

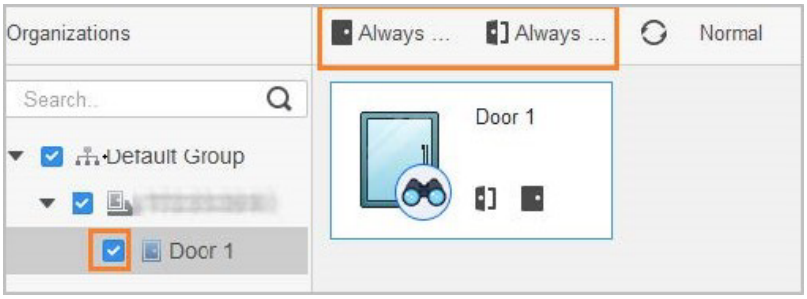
After setting always open or always close, the door remains open or closed all the time.

Procedure

Step 1 Click Access Solution > Access Manager on the Home page.

Step 2 Click Always Open or Always Close to open or close the door.

Figure 4-13 Always open or close



The door will remain open or closed all the time. You can click Normal to restore the access control to normal status, and then the door will be open or closed based on the configured verification methods.

4.4.3 Monitoring Door Status

Procedure

Step 1 Click Access Solution > Access Manager on the home page.

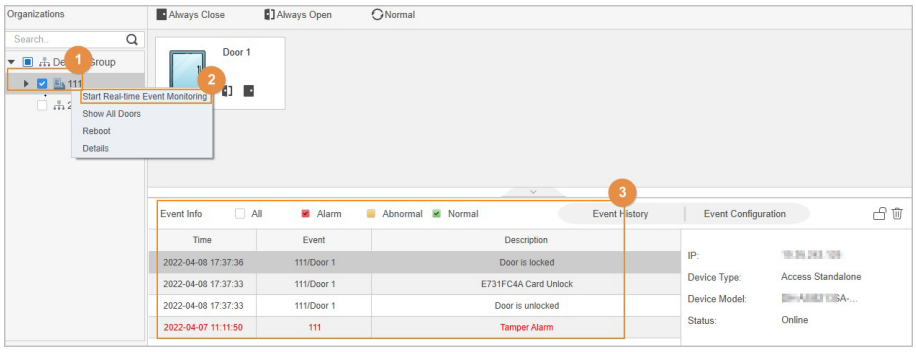
Step 2 Select the device in the device tree, and right click the device and then select Start Real-time Event Monitoring .

Real-time access control events will display in the event list.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Click Stop Monitor , real-time access control events will not display.

Figure 4-14 Monitor door status



Related Operations

Show All Door: Displays all doors controlled by the Device.

Reboot: Restart the Device.

Details: View the device details, such as IP address, model, and status.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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.

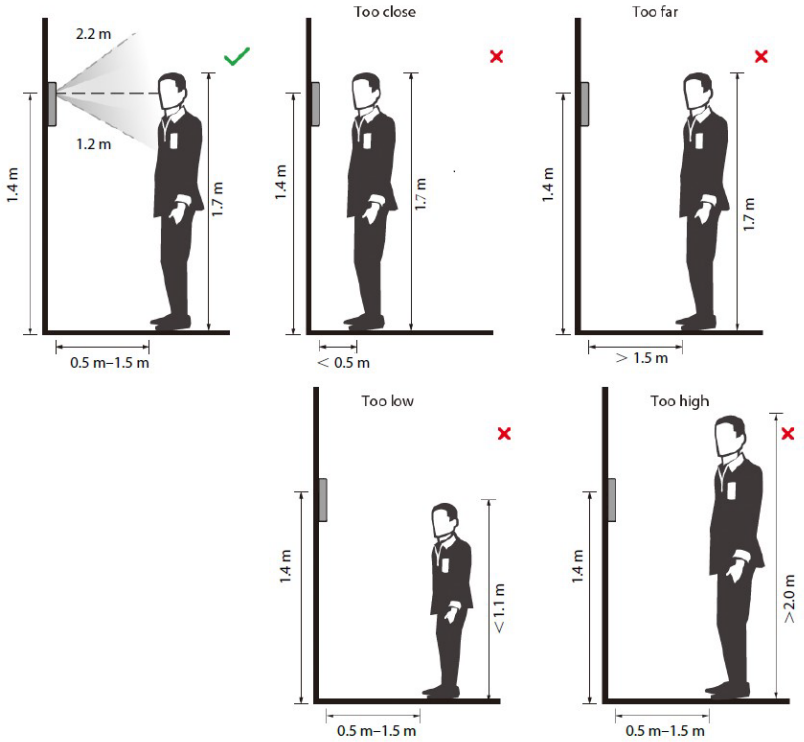
Face Position

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Appendix Figure 1-3 Face distance

When importing face images through the management platform, make sure that image resolution is within the range from 150 × 300 pixels to 600 × 1200 pixels. It is recommended that the resolution be greater than 500 × 500 pixels, the image size be less than 100 KB, and the image name and person ID be 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Appendix 2 Important Points of Intercom Operation

The Device can function as VTO to realize intercom function.

Prerequisites

The intercom function is configured on the Device and VTO.

Procedure

Step 1 On the standby screen, tap .

Step 2 Enter the room No, and then tap .

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Appendix 3 Important Points of Fingerprint Registration Instructions

When you register the fingerprint, pay attention to the following points:

Make sure that your fingers and the scanner surface are clean and dry.

Press your finger on the center of the fingerprint scanner.

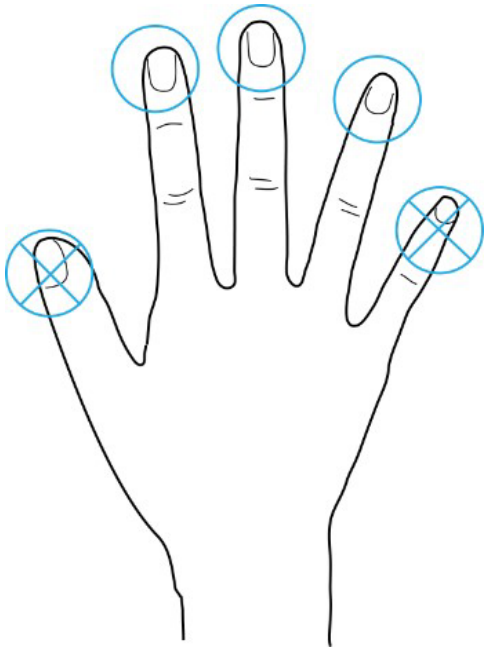
Do not put the fingerprint sensor in a place with intense light, high temperature, and high humidity.

If your fingerprints are unclear, use other unlocking methods.

Fingers Recommended

Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

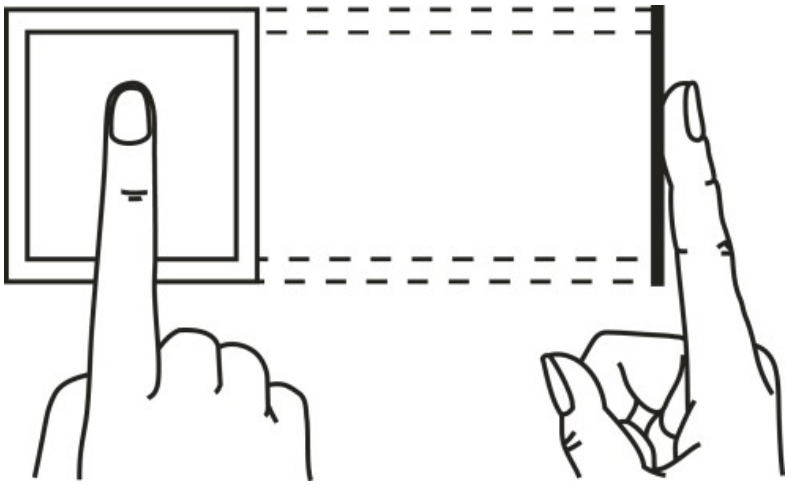
Appendix Figure 3-1 Recommended fingers



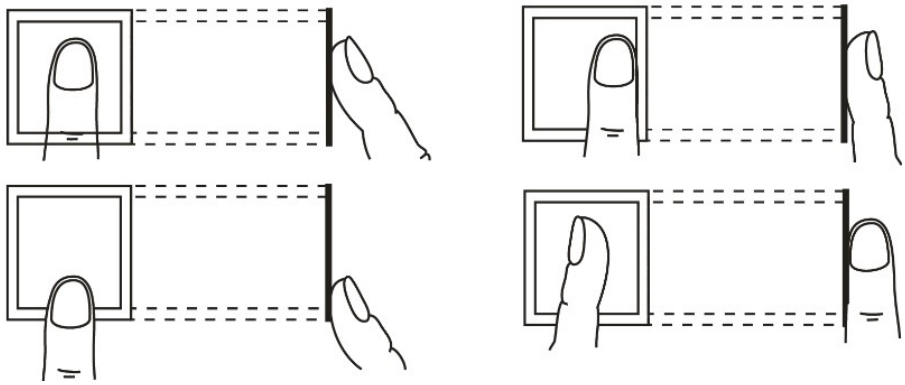
(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

How to Press Your Fingerprint on the Scanner

Appendix Figure 3-2 Correct placement



Appendix Figure 3-3 Wrong placement



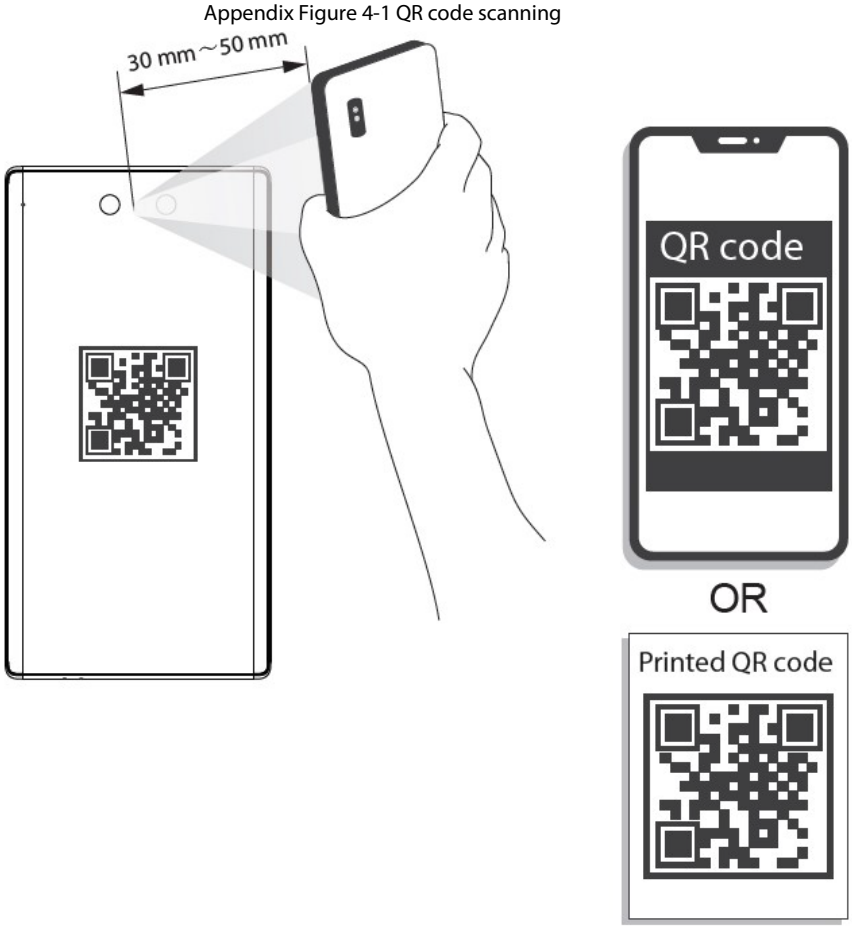
(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Appendix 4 Important Points of QR Code Scanning

Place the QR code on your phone at a distance of 30 mm–50 mm away from the QR code scanning lens. It supports QR code that is larger than 30 mm× 30 mm and less than 128 bytes in size.

QR code detection distance differs depending on the bytes and size of QR code.
Make sure the QR code is aligned with the lens, and avoid direct sunlight.

Appendix Figure 4-1 QR code scanning



(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

Appendix 5 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.

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

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).

(+91)-11-41916615
+91-95999-53923
D-162, Okhla Industrial Area
Phase I, New Delhi, 110020
sales@timewatchindia.com
www.timewatchindia.com

TIMEWATCH®
Presence perfect

Contact Us

D-162, Okhla Industrial Area, Phase-I, Delhi 110020
Email: sales@timewatchindia.com
Phone: +91-11-41916615
Mobile No: +91-95999-53923

New Delhi - NCR | Mumbai | Ahmedabad | Bengaluru | Chennai | Kolkata | Dubai

www.timewatchindia.com