Alarm Keypad

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

General

This manual introduces the functions and operations of the alarm keypad (hereinafter referred to as "the keypad").

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, lower performance, or unpredictable result.
🔑 TIPS	Provides methods to help you solve a problem or save you time.
📖 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	July 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and car 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 zone 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 Descriptions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

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

Operation Requirements

- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.
- Only use the device within the rated power range.
- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.

Installation Requirements

- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- Connect the device to the adapter before power on.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Connect class I electrical appliances to a power socket with protective earthing.

Table of Contents

1 Overview

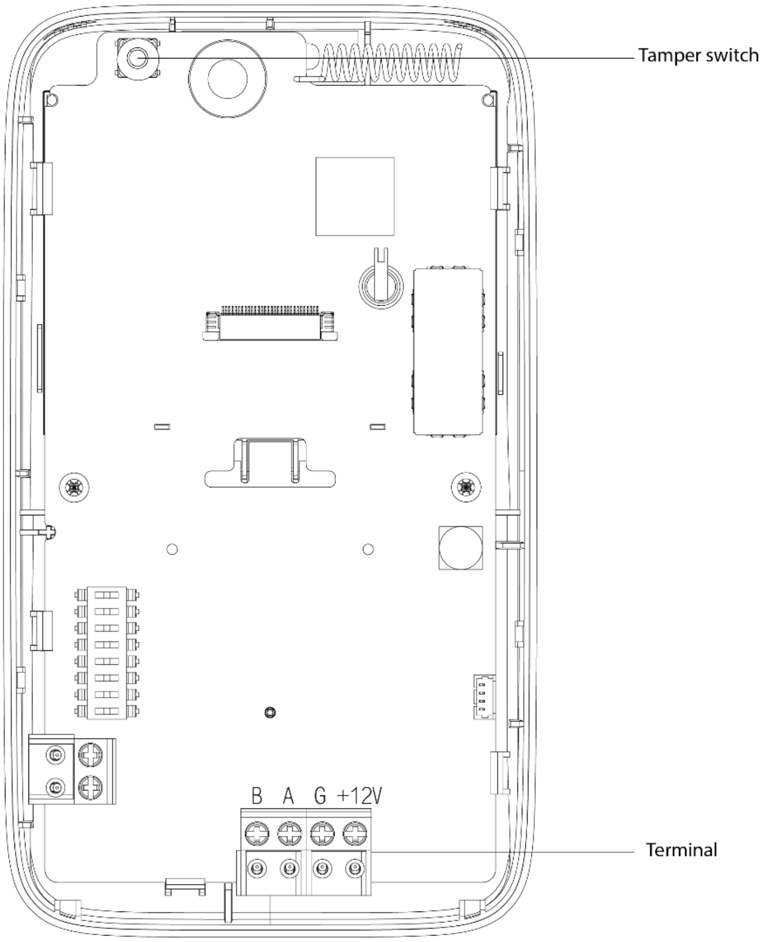
Specially designed to work with ARC9 and ARC2 series alarm controllers, the alarm keypad can configure arming and disarming settings, controller systems and can display the system status.

2 Wiring and Installation

2.1 Wiring

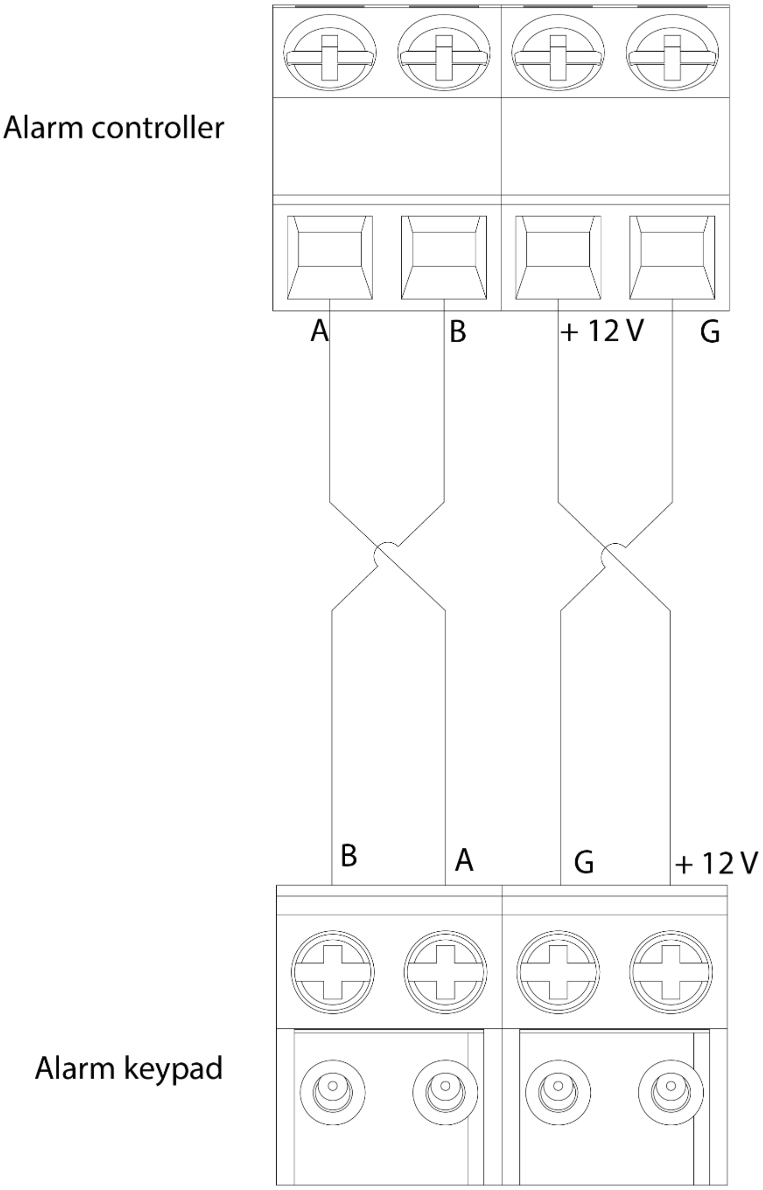
Step 1 Use a slotted screwdriver to remove the rear panel.

Figure 2-1 Rear panel



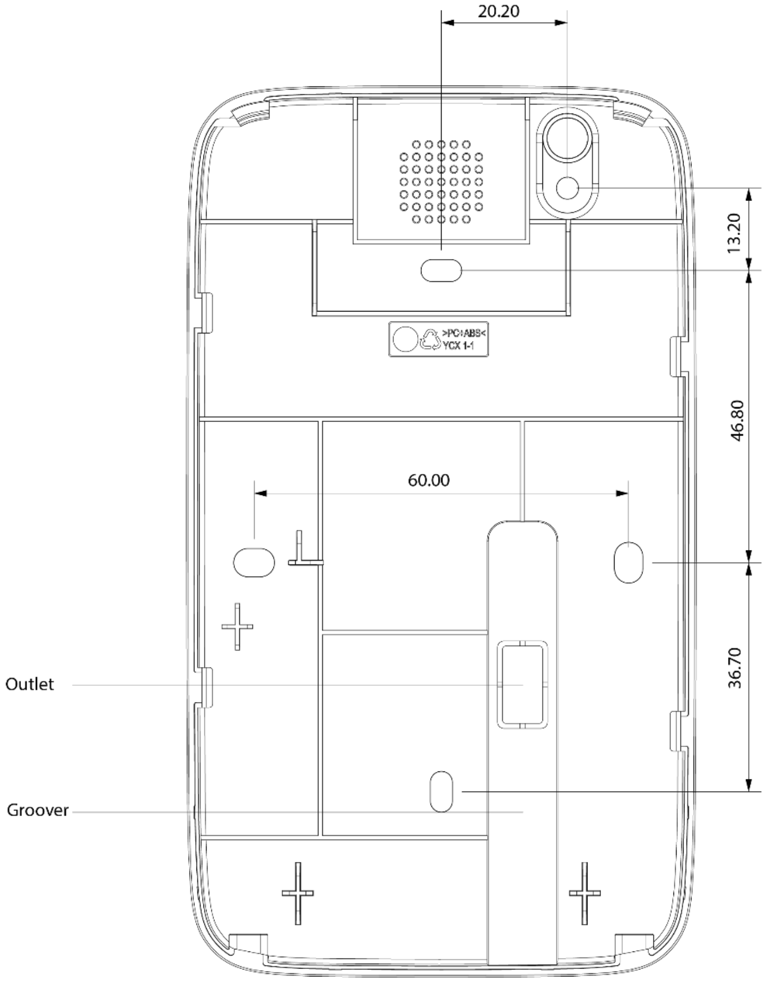
Step 2 Connect the wiring with the alarm controller and the keypad.

Figure 2-2 Wiring



2.2 Installation

Figure 2-3 Hole size (mm)



2.2.1 Surface Mount

Fix the keypad to the wall with screws.

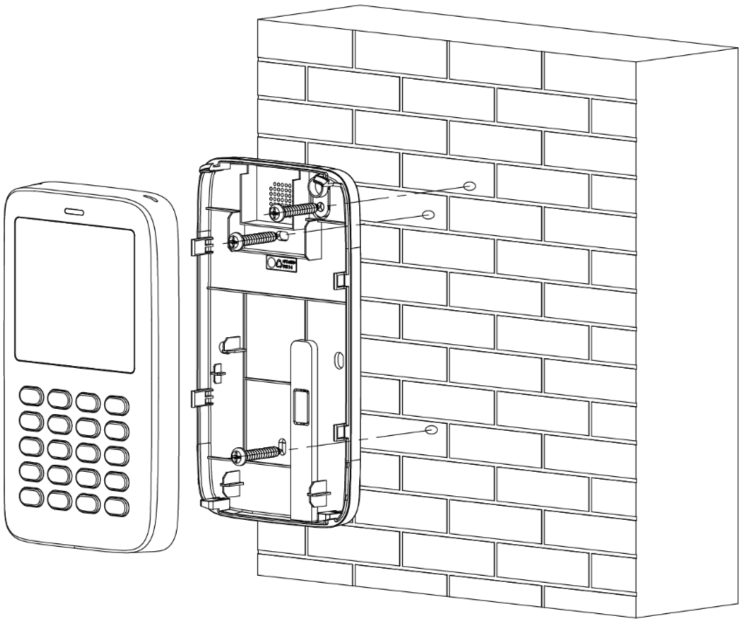
Step 1 Drill 3 holes into the wall according to the hole size.

Step 2 Pull the wires out the outlet, lead them along the groove, and connect them to the alarm controller.

Step 3 Attach the real panel to the wall with screws.

Step 4 Attach the front panel to the rear panel.

Figure 2-4 Surface mount



2.2.2 Flush Mount

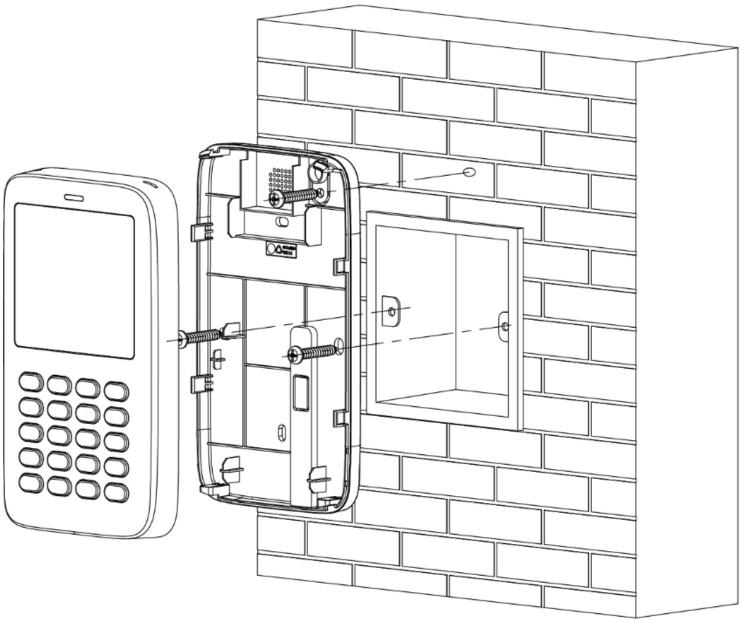
Install the keypad with 86 box.

Step 1 Pull the wires out the outlet, lead them along the groove, and connect them to the alarm controller.

Step 2 Attach the real panel to the 86 box with screws.

Step 3 Attach the front panel to the rear panel.

Figure 2-5 Install with 86 box



3 Operation

3.1 Initialization

Step 1 Power off the keypad while the controller is still powered on, and check if the controller works normally.

Supply independent power for each of them when multiple keypads are connected.

Step 2 Press and hold both ENTER and ENTER keys to power on the keypad. Release ENTER when the keypad lights up and displays operating language options (Chinese and English).

Step 3 Select a proper language through ∧ or ∨, and then press ENTER.

Step 4 Select **RS-485 Address** through ∧ or ∨, press ENTER, enter keypad address and then press ENTER.

Step 5 Restart the keypad

3.2 Function Key

Figure 3-1 Function key

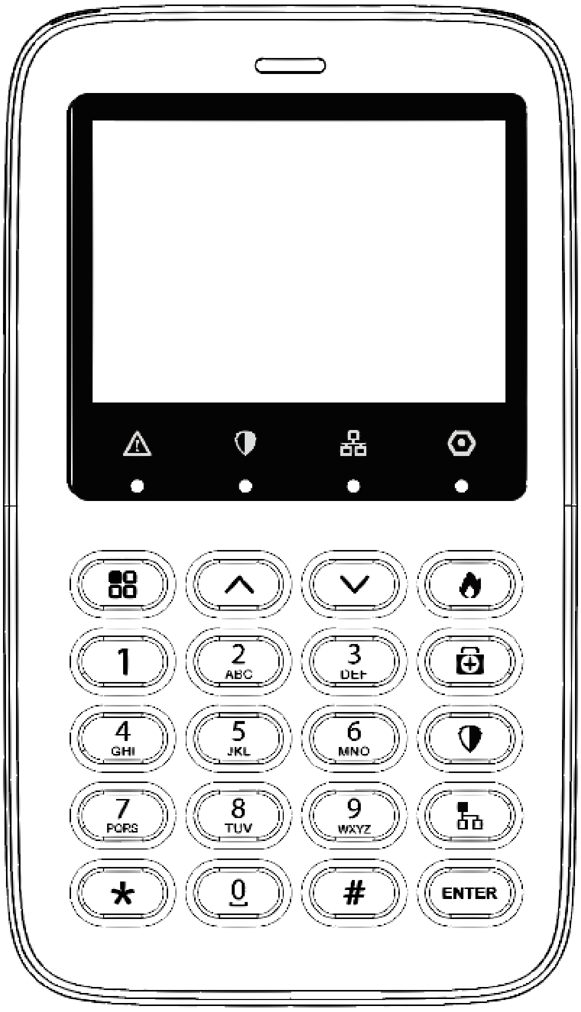


Table 3-1 Function key description

key/Icon	Name	Description
⚠	Fault	● System fault: Solid red. ● Normal: Light off.
🛡	Arming and disarming indicator	● Arming: Solid green. ● Disarming: Light off.
🖧	Network indicator	● Connected successfully: Solid green. ● Failed to connect: Light off.
⬡	Communication indicator	● Successfully registered the keypad to the alarm controller: Solid green. ● Failed to register the keypad to the alarm controller: Light off.
⊞	Menu	● Enters the menu interface. ● Returns to the previous menu.

key/Icon	Name	Description
		● On the input interface, press the key to clear the previous code. ● On the main interface, press the key to view the zone status.
∧	Up	● On the menu interface, press the key to go to the previous page. ● On the main interface, press the key to view the arming and disarming status of the sub system.
∨	Down	● On the menu interface, press the key to go to the next page. ● On the main interface, press the key to view fault status of the device.
0 - 9	Arabic numerals.	Number.
*	*	● Character. ● Under global mode, press and hold the key for 3 seconds to view device information. Press ∧ and ∨ to turn the page.
#	#	Character.
🔥	Fire	Press and hold this key for 3 seconds, and then the keypad will send fire alarm messages to the hub. 📖 You can press 🔥 under any mode.
⊕	Medical	Press and hold this key for 3 seconds, and then the keypad will send medical alarm messages to the hub. 📖 You can press ⊕ under any mode.
◐	Arm	Press and hold this key for 3 seconds, and then all the subsystems will be armed. 📖 You can press ◐ under any mode.
⊞	Bypass	Bypass the zone. 📖

key/Icon	Name	Description
		You can press 🖧 in any mode.
ENTER	Enter	Press to confirm.

3.3 Operation Modes and Passcodes

Use the keypad by directly entering command under operation mode. Operation mode is divided into programming and walk test modes which cannot be logged into at the same time. When exiting from the programming mode, the keypad returns to global mode by default. When there are no operations for 3 minutes under programming mode, the keypad returns to global mode automatically.

The default passcode is different for each user type, which includes administrator, installer, manufacturer and operator.

- The default passcode of admin is 1234.
- The default passcode of installer is 9090.
- The default passcode of manufacturer 2008.

3.4 User Permissions

Permissions vary for different users.

Table 3-2 Description of user permissions

User	Description
Administrator	Arm, disarm, cancel alarm, unbypass, bypass, isolate, configure forced arm, manage users, add or edit configuration parameters.
Installer	All permissions of the admin (including walk test) except disarming.
Manufacturer	Manage users, edit basic programs, such as updating program.
Operator	Arm, disarm, cancel alarm, unbypass.

3.5 Global Mode

- The zone number contains 3 digits, ranging from 001 to 256. It uses 0 as placeholder in front when there are less than 3 digits (e.g. 10 becomes 010).
- The subsystem number contains 2 digits, ranging from 001 to 256. It uses 0 as placeholder in front when there are less than 2 digits (e.g. 8 becomes 08).
- The relay number contains 3 digits, ranging from 01 to 08. It uses 0 as placeholder in front when there are less than 3 digits (e.g. 10 becomes 010).
- All objects with the consecutive operation function support up to 16 operations in a row. For

example, bypass zone can bypass up to 16 zones at the same time.

3.5.1 Arming and Disarming

Description

- Arming: When the controller and the detectors work properly, arm the zone, and then the controller will respond to alarm signals in the zone.
- Disarming: Disarm the zone when it is in the armed status.

Command

- Switch system status: Enter passcode.
- Disarm subsystem: Enter passcode + * + 2 + * + subsystem number.
- Away arm subsystem: Enter passcode + * + 3 + * + subsystem number.
- Forced away arm subsystem: Enter passcode + * + 4 + * + subsystem number.
- Home arm subsystem: Enter passcode + * + 5 + * + subsystem number.
- Forced home arm subsystem: Enter passcode + * + 6 + * + subsystem number.
- Arm single zone: Enter passcode + * + 10 + * + zone number.
- Disarm single zone: Enter passcode + * + 11 + * + zone number.

Switching system status means that you can switch the arming/disarming status of each active subsystem. For example, if the current subsystem is in the armed status, enter the command and the subsystem changes to the disarmed status.

Example

Admin (default passcode is 1234) performs away arming on subsystem1.

Step 1 Under global mode, enter 1234*3*01.

Step 2 Press **Enter**.

3.5.2 Cancel Alarm

Description

Cancel the alarm through the keypad when an alarm is triggered.

Command

- Cancel all alarms: Enter passcode + * + 1.
- Cancel zone alarm: Enter passcode + * + 1 + * + zone number.
- Cancel subsystem alarm: Enter passcode + * + 23 + * + subsystem number.

Example

Admin (default passcode is 1234) cancels all alarms.

Step 1 Under global mode, enter 1234*1.

Step 2 Press **Enter**.

3.5.3 Bypass and Isolate

Description

When the whole system fails to be armed due to detector faults or human activities in some zones, users are allowed to bypass these zones by selectively removing detectors from the security system. For example, a detector may be bypassed in order to arm the perimeter with a window open.

- Bypass: If one or more zones are bypasses, they are disabled for one arming cycle. After one arming cycle, they are automatically unbypassed.
- Isolate: If one or more zones are isolated, they are disabled until they are unbypassed.
- Unbypass: Manually restores a zone to normal functioning by removing a bypass condition.

Command

- Unbypass: Enter passcode + * + 7 + * + zone number.
- Bypass: Enter passcode + * + 8 + * + zone number.
- Isolate: Enter passcode + * + 9 + * + zone number.

Example

Admin (default passcode is 1234) bypass zone1.

Step 1 Under the global mode, enter 1234*8*001.

Step 2 Press **Enter**.

3.5.4 Relay

Description

Manually turn on or off the relay output.

Command

- Manually turn on the relay output: Enter passcode + * + 13 + * + relay number.
- Manually turn off the relay output: Enter passcode + * + 14 + * + relay number.

The 3-digit relay number ranges from 001 to 256, and it uses 0 as placeholder in front when there are less than 3 digits (e.g. 10 becomes 010).

Example

Installer (default passcode is 1234) turns off the relay1 output function.

Step 1 Under global mode, enter 1234*14*001.

Step 2 Press **Enter**.

3.5.5 PSTN Test

Description

- With the correct configuration, the controller tries to send a test message to the configured alarm receiving center after executing the PSTN manual test command. The successful test prompt only means that the command was sent successfully, but not that the alarm receiving center received the message.
- After executing SMS or the call manual test command, the controller sends a test message or makes a test call to the phone to check whether the 2G/4G module, or SMS and call functions of the controller are available.

Command

- PSTN manual test: Enter passcode + * + 15.
- SMS manual test: Enter passcode + * + 16 + * + phone number.
- Call manual test: Enter passcode + * + 17 + * + phone number.

Example

Installer (default passcode is 1234) manually tests PSTN.

Step 1 Under global mode, enter 1234*15.

Step 2 Press **Enter**.

3.5.6 Restarting Controller

Description

Restart the alarm controller.

Command

Enter passcode + * + 20.

Example

Admin (default passcode is 1234) restarts the controller.

Step 1 Under global mode, enter 1234*20.

Step 2 Press **Enter**.

3.5.7 Initializing Controller

Description

Initialize the alarm controller.

Due to the inconvenience of entering letters on the keypad, the passcode of the admin account which initializes the controller uses the following rules.

- After executing the command with a digital passcode (3–27 digits) to successfully initialize the controller, the actual passcode is admin + the digital passcode.
- If the passcode is a mix of numbers and letters (8–32), after successful initialization, the actual passcode is the mixed passcode.

Command

Enter passcode * + 21 + * + passcode of admin.

Example

Admin (default passcode is 1234) initializes the controller, and sets the admin user passcode to admin123.

Step 1 Under global mode, enter 1234*21*123.

Step 2 Press **Enter**.

3.5.8 Restoring to Default

Description

Restore parameters to default settings, including alarm, alarm output, alarm subsystem, keypad, arm/disarm, main battery failure, undervoltage, tamper alarm, call alarm receiving center, PSTN offline, subsystem status, network disconnection, IP conflict, MAC conflict and emergency alarm.

Command

Enter passcode + * + 22.

Example

Admin (default passcode is 1234) restores the controller to default settings.

Step 1 Under the global mode, enter 1234*22.

Step 2 Press **Enter**.

3.6 Programming Mode

3.6.1 Entering Programming Mode

Description

When the alarm controller enters programming mode, you can manage users, configure alarm output settings, and network settings of the alarm controller.

Command

Enter admin default passcode or installer default passcode or manufacturer passcode or operator passcode + * + 12.

- The default passcode of the admin user is 1234.
- The default passcode of the installer is 9090.
- The default passcode of the manufacturer is 2008.

Example

The admin user enters programming mode. The default passcode of the admin user is 1234.

Step 1 Under global mode, enter 1234*12.

Step 1 Press **Enter**.

Programming Mode is displayed on the screen.

3.6.2 User Management

3.6.2.1 Adding User

Description

Add a new user.

Command

Figure 3-2 Add a user

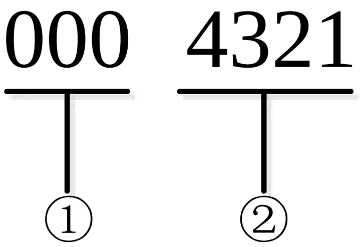


Table 3-3 Add a user

Number	Description
1	The encoding address. The command operation means adding the user.
2	User passcode. Passcodes can contain 4 to 6 digits.

Example

The admin user adds a new operator. The default password of the operator is 4321.

Step 1 The admin user enters 0004321 under programming mode.

Step 2 Press **Enter**.

3.6.2.2 Deleting Users

Description

Delete a user.

📖

- Only the admin user can delete the operators.
- Both admin users and installers cannot be deleted.

Command

Figure 3-3 Delete a user

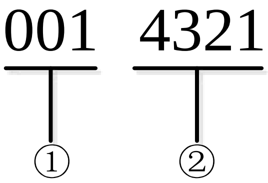


Table 3-4 Delete a user

Number	Description
1	The encoding address. The command operation means deleting the user.

Number	Description
2	User passcode. Passcodes can contain 4 to 6 digits.

Example

The admin user deletes a user. The default password of the operator is 4321.

Step 1 The admin user enters 0014321 under programming mode.

Step 2 Press **Enter**.

3.6.2.3 Configuring Permissions

Description

Grant permissions to keypad users.

📖

The permissions can be represented by passcodes, which contain 2 digits. If the passcode is less than 2 digits, you must add 0 to the front. For example, 1 becomes 01.

Command: Adding User Permissions

Enter 002 + user passcode + * + permission passcode.

Command: Deleting User Permissions

Enter 003 + user passcode + * + permission passcode.

Table 3-5 Permissions

Permission	Passcode	Permission	Passcode
Arm	01.	View logs	07.
Forced arming	02.	Soak mode	08.
Disarm	03.	Update	09.
Bypass	04.	System settings	10.
Isolate	05.	Alarm user management	11.
Cancel alarm	06.	—	—

Example

The admin user grants permissions of **Arm** to the user. The default passcode of the admin user is 1234, and the passcode of the user is 4321.

Step 1 The admin user enters 0024321*01 under programming mode.

Step 2 Press **Enter**.

3.6.2.4 Changing Passcode

Description

Change user passcode.

Command

Enter 004 + user old passcode + * + user new passcode.

Example

The admin user edits user passcode. The old password of the user is 4321, and the new one is 1234.

Step 1 The admin user enters 0044321*1234 under programming mode.

Step 2 Press **Enter**.

3.6.2.5 Linking Subsystems

Description

The keypad users link subsystems.

Command

Enter 005 + user passcode + * + subsystem number.

📖

The subsystem number comprises 2 digits, and the range is from 01 to 08.

Example

The admin user links subsystem 01. The passcode of the user is 4321.

Step 1 The admin user enters 0054321*01 under programming mode.

Step 2 Press **Enter**.

3.6.2.6 Cancelling Linking Subsystems

Description

The keypad users cancel linking subsystems.

Command

Enter 006 + user passcode + * + subsystem number.

The subsystem number contains 2 digits, and the range is from 01 to 08.

Example

The admin user cancels linking subsystem 01. The passcode of the user is 4321.

Step 1 The admin user enters 0064321*01 under programming mode.

Step 2 Press **Enter**.

3.6.3 Zones

3.6.3.1 Sensor Type

Description

You can select from **NO** and **NC**.

Command

Figure 3-4 Sensor type

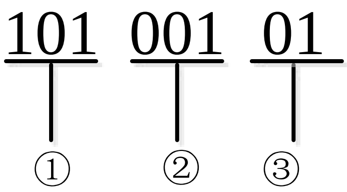


Table 3-6 Sensor type

Number	Description
1	The encoding address. The command operation means configuring the sensor type.
2	Zone. ● ARC9 series: 001-256. ● ARC2 series ◇ ARC2008 series: 001-072. ◇ ARC2016 series: 001-080.
3	● 01: **NO**. ● 02: **NC**.

Example

The admin user configures the sensor type of zone 1 as **NO**.

Step 1 The admin user enters 10100101 under programming mode.

Step 2 Press **Enter**.

3.6.3.2 Zone Type

Description

Select zone type as needed.

Command

Figure 3-5 Zone type

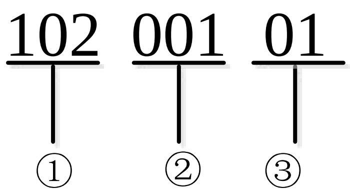


Table 3-7 Zone type

Number	Description
1	The encoding address. The command operation means configuring the zone type.
2	Zone. ● ARC9 series: 001-256. ● ARC2 series ◇ ARC2008 series: 001-072. ◇ ARC2016 series: 001-080.
3	● 01: **Instant Zone**. ● 02: **Delayed Zone**. ● 04: **Fire Zone**. ● 05: **Burglar Zone**. ● 06: **24-hour Audible Zone**. ● 07: **24-hour Silent Zone**. ● 08: **24-hour Vibration Zone**. ● 09: **24-hour Auxiliary Zone**. ● 10: **Interior Zone**. ● 11: **Perimeter Zone**. ● 12: **Key Zone**. ● 13: **Not Alarm Input**.

Example

The admin user configures zone 1 as an **Instant Zone**.

Step 1 The admin user enters 10200101 under programming mode.

Step 2 Press **Enter**.

3.6.3.3 Sensing Type

Description

Configure sensing type as needed.

Command

Figure 3-6 Sensing type

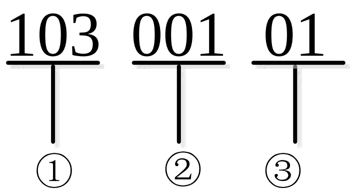


Table 3-8 Sensing type

Number	Description
1	The encoding address. The command operation means configuring the sensing type.
2	Zone. ● ARC9 series: 001-256. ● ARC2 series ◇ ARC2008 series: 001-072. ◇ ARC2016 series: 001-080.
3	● 01: **Door Sensor**. ● 02: **PIR Sensor**. ● 03: **Active Infrared Sensor**. ● 04: **Smoke Sensor**. ● 05: **Glass Break Sensor**. ● 06: **Vibration Sensor**. ● 07: **Dual-technology (IR + Microwave)**. ● 08: **Emergency Button**. ● 09: **Panic Button**. ● 10: **Temperature**. ● 11: **Humidity**. ● 12: **Gas Sensor**. ● 13: **Water Leak Sensor**.

Example

The admin user configures the sensing type of zone 1 as **Door Sensor**.

Step 1 The admin user enters 10300101 under programming mode.

Step 2 Press **Enter**.

3.6.3.4 Entry Delay Time

Description

A programmed delay in the system alarm response that allows an individual to enter an armed area through the correct detector and disarm the area. If the system is not disarmed before the delay time expires, the system will initiate an alarm response which may include sending reports to the central station.

Command

Figure 3-7 Enter delay time

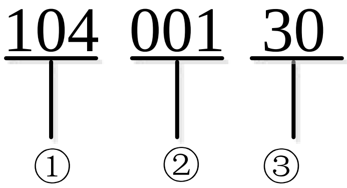


Table 3-9 Entry delay time

Number	Description
1	The encoding address. The command operation means configuring entry delay time.
2	Zone. ● ARC9 series: 001-256. ● ARC2 series ◇ ARC2008 series: 001-072. ◇ ARC2016 series: 001-080.
3	Entry delay time. The entry delay time can be set between 1 to 300 seconds.

Example

The admin user configures the entry delay time of zone 1 as 30 s.

Step 1 The admin user enters 10400130 under programming mode.

Step 2 Press **Enter**.

3.6.3.5 Exit Delay Time

Description

A programmed delay in the system alarm response that allows an individual to exit after arming an area. Failure to exit before the delay time expires, causes entry delay to begin. The system must then be disarmed. If it is not disarmed before the delay time expires, the system will produce an alarm response that might include the sending of reports to the central station.

Command

Figure 3-8 Exit delay time

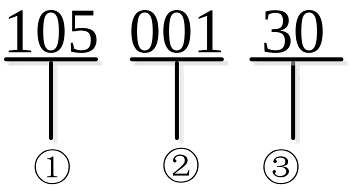


Table 3-10 Exit delay time

Number	Description
1	The encoding address. The command operation means configuring the exit delay time.
2	Zone. ● ARC9 series: 001-256. ● ARC2 series: ◇ ARC2008 series: 001-072. ◇ ARC2016 series: 001-080.
3	Exit delay time. The exit delay time can be set as 1 to 300 seconds.

Example

The admin user configures the exit delay time of zone 1 as 30 seconds.

Step 1 The admin user enters 10500130 under programming mode.

Step 2 Press **Enter**.

3.6.3.6 Module Type

Description

Configure module type as needed.

Command

Figure 3-9 Module type

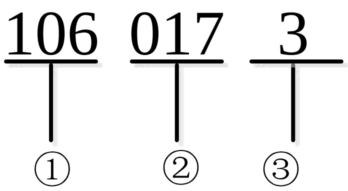


Table 3-11 Module type

Number	Descriptions
1	The encoding address. The command operation means configuring the module type.
2	Zone. ● ARC9 series: 001-256. ● ARC2 series ◇ ARC2008 series: 001-072. ◇ ARC2016 series: 001-080.
3	Module type. ● 0: **Local Zone**. ● 1: **M-Bus**. ● 2: **ARM808-RS** ● 3: **ARM708-RS**.

Example

The admin user configures the module type of zone 17 as **ARM708-RS**.

Step 1 The admin user enters 1060173 under programming mode.

Step 2 Press **Enter**.

3.6.3.7 Module Address

Description

Configure module address as needed. We recommend configuring the address starting from 0, going up in sequential order.

Command

Figure 3-10 Module address

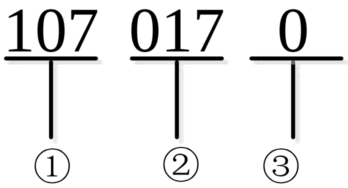


Table 3-12 Module address

Number	Descriptions
1	The encoding address. The command operation means configuring the module address.
2	Zone. ● ARC9 series: 001-256. ● ARC2 series ◇ ARC2008 series: 001-072. ◇ ARC2016 series: 001-080.
3	Module address: 000-254.

Example

The admin user configures the module address of zone 17 as 0.

Step 1 The admin user enters 107017000 under programming mode.

Step 2 Press **Enter**.

3.6.3.8 Module Channel No.

Description

Configure module channel number as needed.

Command

Figure 3-11 Module channel No.

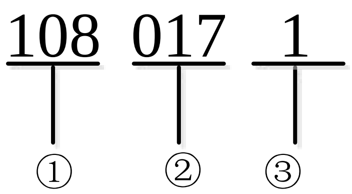


Table 3-13 Module channel No.

Number	Description
1	The encoding address. The command operation means configuring the module channel number.
2	Zone. ● ARC9 series: 001-256. ● ARC2 series ◇ ARC2008 series: 001-072. ◇ ARC2016 series: 001-080.
3	Module channel No.: 01-16.

Example

The admin user configures the module channel number of zone 17 as 1.

Step 1 The admin user enters 10801701 under programming mode.

Step 2 Press **Enter**.

3.6.3.9 Resistance

Description

Configure resistance.

Command

Figure 3-12 Resistance

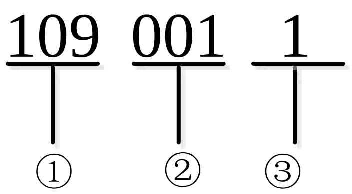


Table 3-14 Resistance

Number	Description
1	The encoding address. The command operation means configuring the resistance.
2	Zone. ● ARC9 series: 001-256. ● ARC2 series ◇ ARC2008 series: 001-072. ◇ ARC2016 series: 001-080.
3	10 K can be selected for **M-Bus**. Select the resistance as needed for other modules. ● 1：**2.7 K**. ● 2：**4.7 K.** ● 3：**6.8 K**. ● 4：**10 K**.

Example

The admin user selects 2.7 k for zone 1.

Step 1 The admin user enters 1090011 under programming mode.

Step 2 Press **Enter**.

3.6.4 Relay

3.6.4.1 Output Time

Description

Configure relay output time.

Command

Figure 3-13 Output time

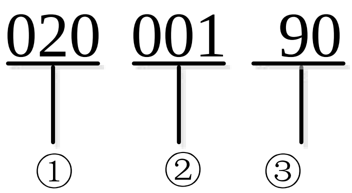


Table 3-15 Output time

Number	Description
1	The encoding address. The command operation means configuring output time for relay.
2	Relay. ● ARC9 series: 001-256. ● ARC2 series: 001-084.
3	Output time. The relay output time can be set between 90 seconds to 900 seconds.

Example

The relay output time is set as 90 seconds.

Step 1 The admin user enters 02000190 under programming mode.

Step 2 Press **Enter**.

3.6.4.2 Module Type

Description

Configure relay output module type as needed.

Command

Figure 3-14 Module type

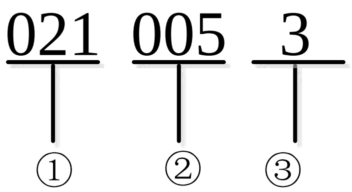


Table 3-16 Module type

Number	Description
1	The encoding address. The command operation means configuring the module type.
2	Relay. ● ARC9 series: 001-256. ● ARC2 series: 001-084.
3	Module type. ● 0: **Local Zone**. ● 1: **M-Bus**. ● 2: **ARM808-RS** ● 3: **ARM708-RS**.

Example

The admin user configures the module type of relay 5 as **ARM708-RS**.

Step 1 The admin user enters 0210053 under programming mode.

Step 2 Press **Enter**.

3.6.4.3 Module Address

Description

Configure relay module address as needed. We recommend configuring the address from 0 in sequential order.

Command

Figure 3-15 Module address

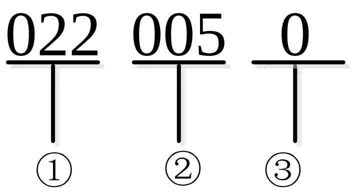


Table 3-17 Module address

Number	Description
1	The encoding address. The command operation means configuring the module address.
2	Relay. ● ARC9 series: 001-256. ● ARC2 series: 001-084.

Number	Description
3	Module address: 000-254.

Example

The admin user configures the module address of relay 5 as 0.

Step 1 The admin user enters 0220050 under programming mode.

Step 2 Press **Enter**.

3.6.4.4 Module Channel No.

Description

Configure module channel number as needed.

Command

Figure 3-16 Module channel No.

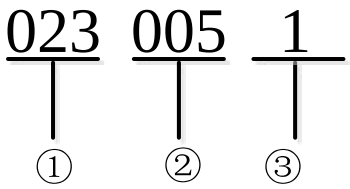


Table 3-18 Module channel No.

Number	Description
1	The encoding address. The command operation means configuring the module channel number.
2	Relay. ● ARC9 series: 001-256. ● ARC2 series: 001-084.
3	Module channel No.: 01-16.

Example

The admin user configures the module channel number of relay 5 as 1.

Step 1 The admin user enters 02300501 under programming mode.

Step 2 Press **Enter**.

3.6.5 Siren

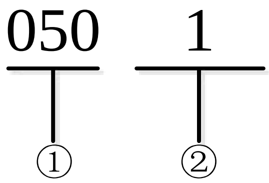
3.6.5.1 Enabling Siren

Description

Enable or disable siren function.

Command

Table 3-19 Enable siren



0: Disable; 1: Enable.

Example

The installer disables the siren.

Step 1 The admin user enters 0500 under programming mode.

Step 2 Press **Enter**.

3.6.5.2 Duration

Description

Configure alarm duration for the siren.

Command

Figure 3-17 Duration

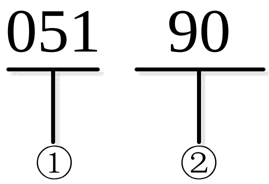


Table 3-20 Duration

Number	Description
1	The encoding address. The command operation means configuring siren duration.

Number	Description
2	Duration. The siren duration can be set between 90 seconds to 900 seconds.

Example

The admin user configures duration as 90 seconds.

Step 1 The admin user enters 05190 under programming mode.

Step 2 Press **Enter**.

3.6.6 Alarm Receiving Center

3.6.6.1 Sending Strategy

Description

Configure sending strategies.

Command

Figure 3-18 Sending strategy

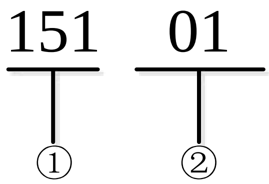


Table 3-21 Sending strategy

Number	Description
1	The encoding address. The command operation means configuring sending strategy.
2	Sending strategy. ● 01: **PSTN Only**. ● 02: **2G/4G Only**. ● 03: **PSTN Preferred**. Select 2G/4G when PSTN is unavailable. ● 04: **2G/4G Preferred**. Select PSTN when 2G/4G is unavailable.

Example

The admin user selects **PSTN Only** as a sending strategy for the alarm receiving center.

Step 1 The admin user enters 15101 under programming mode.

Step 2 Press **Enter**.

3.6.6.2 Dial Attempts

Description

Configure dial attempts. Assume that dial attempts is set to 3. If you send data to the alarm receiving center, and it fails 3 times to be sent, then the system will register that the CID message failed to send.

Command

Figure 3-19 Dial attempts

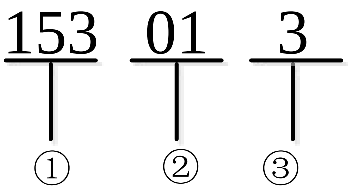


Table 3-22 Dial attempts

Number	Description
1	The encoding address. The command operation means configuring dial attempts.
2	Alarm receiving center: 01-02.
3	Dial attempt: 1-9.

Example

The admin user configures dial attempt for alarm receiving center 1 as 3.

Step 1 The admin user enters 153013 under programming mode.

Step 1 Press **Enter**.

3.6.6.3 Dial Delay

Description

Dial delay must be set to work with dial attempts. If you fail after dialing, you can dial again after the defined dial delay period.

Command

Figure 3-20 Dial delay

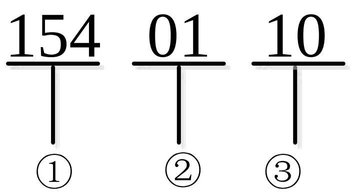


Table 3-23 Dial delay

Number	Description
1	The encoding address. The command operation means configuring dial delay.
2	Alarm receiving center: 01-02.
3	Dial delay: 1-255.

Example

The admin user configures dial delay for alarm receiving center 1 as 10 seconds.

Step 1 The admin user enters 1540110 under programming mode.

Step 2 Press **Enter**.

3.6.6.4 Alarm Receiver Number

Description

Configure alarm receiver number.

Command

Figure 3-21 Alarm receiver number

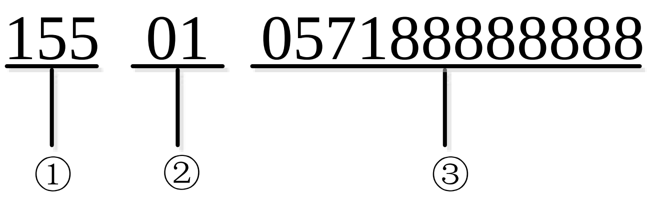


Table 3-24 Alarm receiver number

Number	Description
1	The encoding address. The command operation means configuring alarm receiver number.
2	Alarm receiving center: 01-02.
3	Alarm receiver number. Contains 1 to 24 digits.

Example

The admin user configures alarm receiver number of alarm receiving center 1 as 057188888888.

Step 1 The admin user enters 15501057188888888 under programming mode.

Step 2 Press **Enter**.

3.6.6.5 User Code

Description

Configure user code, which is a unique code for the device to send data to the alarm receiving center. The default user code is 0000.

Command

Figure 3-22 User code

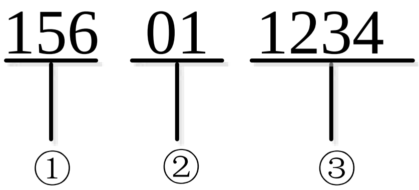


Table 3-25 User code

Number	Description
1	The encoding address. The command operation means configuring user code.
2	Alarm receiving center: 01-02.
3	User code. ● User code can be comprised of two character types: letters or digits. Letters in upper cases (B-F), and digits (0-9). ● User code must consist of 4 characters when selecting protocol type as **Contact ID Protocol**. For example, 0000, BBBB, or B000.

Example

The admin user configures user code for alarm receiving center 1 as 1234.

Step 1 The admin user enters 156011234 under programming mode.

Step 2 Press **Enter**.

3.6.6.6 Configuring Call Alarm Receiving Center

Description

Configure dial attempts, dial delays and user code for call alarm receiving center.

Command

Figure 3-23 Call alarm receiving center

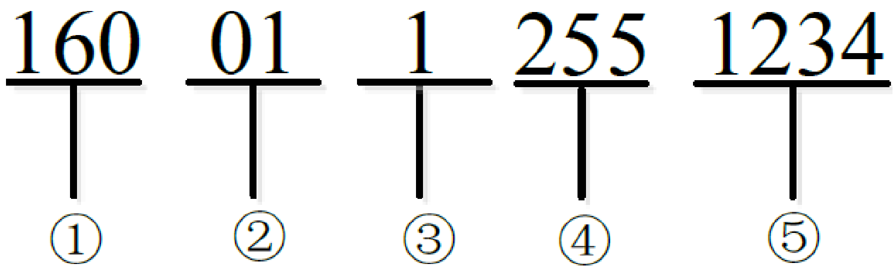


Table 3-26 Call alarm receiving center

Number	Description
1	The encoding address. The command operation means configuring parameters for call alarm receiving center.
2	Alarm receiving center: 01-02.
3	Dial attempt: 1-9.
4	Dial delay: 1-255.
5	User code. ● User code can be comprised of two character types: letters or digits. Letters in upper cases (B-F), and digits (0-9). ● User code must consist of 4 characters when selecting protocol type as **Contact ID Protocol**. For example, 0000, BBBB, or B000.

Example

The admin user configures dial attempt for alarm receiving center 1as 1, dial delay as 255 seconds, user code as 1234.

Step 1 The admin user enters 1600112551234 under programming mode.

Step 2 Press **Enter**.

3.6.7 Test Report

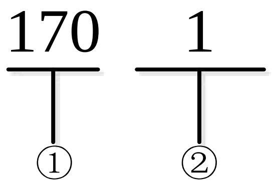
3.6.7.1 Enabling Test Report

Description

Enable or disable test report function.

Command

Figure 3-24 Test report



0: Disable; 1: Enable.

Example

The admin user enables **Test Report.**

Step 1 The admin user enters 1701 under programming mode.

Step 2 Press **Enter**.

3.6.7.2 Report Period

Description

Configure report periods.

Command

Figure 3-25 Report period

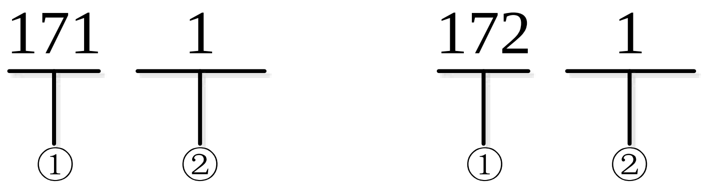


Table 3-27 Report period

Number	Description
1	The encoding address. The command operation means configuring report period for

Number	Description
	PSTN.
2	Report period. ● 171: 1 h-24 h. ● 172: 1 day-31 days.

Example

The admin user configures report period as 1 hour.

Step 1 The admin user enters 1711 under programming mode.

Step 2 Press **Enter**.

3.6.7.3 Enabling Alarm Receiving Center

Description

Enable or disable alarm receiving center function.

Command

Figure 3-26 Alarm receiving center

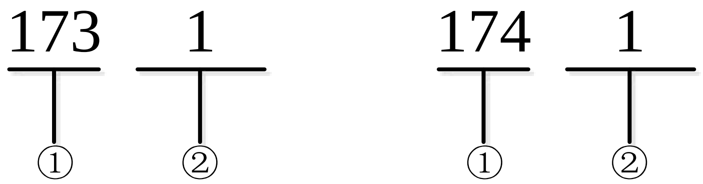


Table 3-28 Alarm receiving center

Number	Description
1	Enable or disable **Scheduled Test Report** for alarm receiving center. ● 173: Enable. ● 174: Disable.
2	Alarm receiving center: 1 or 2.

Example

The admin user enables scheduled test report for alarm receiving center 1.

Step 1 The admin user enters 1731 under programming mode.

Step 2 Press **Enter**.

3.6.7.4 Uploading First Test Report

Description

Configure time for uploading first test report.

Command

Figure 3-27 Upload first time report

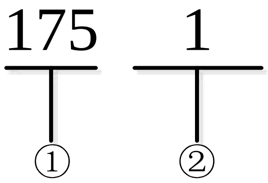


Table 3-29 Upload first time report

Number	Description
1	The encoding address. The command operation means configuring uploading time for the first report.
2	**Upload First Test Report**: 0 minute-3600 minutes.

Example

The admin user configures **Upload First Test Report** as 1 hour.

Step 1 The admin user enters 1751 under programming mode.

Step 2 Press **Enter**.

3.6.8 CID Linkage

3.6.8.1 Protocol Types

Description

Configuring protocol types.

Command

Figure 3-28 Protocol types

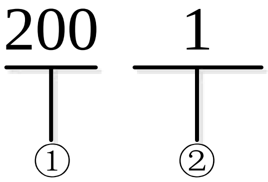


Table 3-30 Protocol types

Number	Description
1	The encoding address. The command operation means configuring protocol types for the events.
2	1: **Contact ID Protocol**.

Example

The admin user configures protocol type as **Contact ID Protocol**.

Step 1 The admin user enters 2001 under programming mode.

Step 2 Press **Enter**.

3.6.8.2 Reporting Restored Events

Description

Enable or disable **Report Restored Event**.

Command

Table 3-31 Report restored events

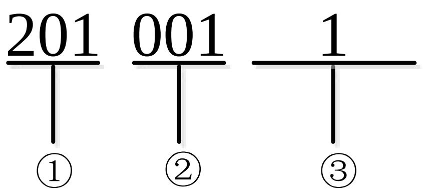


Table 3-32 Report restored events

Number	Description
1	The encoding address. The command operation means configuring whether or not to report restored event.
2	Event No.: 001-100.
3	● 0: Not report. ● 1: Report.

Example

The admin user disables **Report Restored Event** for event 1.

Step 1 The admin user enters 2010011 under programming mode.

Step 2 Press **Enter**.

3.6.8.3 Linking CID Events with Alarm Receiving Center

Description

Enable linking events with the alarm receiving center.

Command

Figure 3-29 Link events with the alarm receiving center

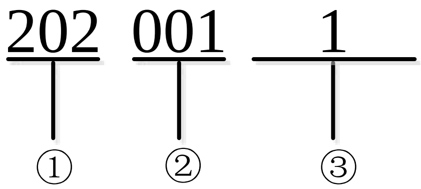


Table 3-33 Link events with the alarm receiving center

Number	Description
1	The encoding address. The command operation means linking events with the alarm receiving center.
2	Event No.: 001-100.
3	● 1: Alarm receiving center 1. ● 2: Alarm receiving center 2.

Example

The admin user links event 1 with the alarm receiving center 1.

Step 1 The admin user enters 2020011 under programming mode.

Step 2 Press **Enter**.

3.6.8.4 Disabling Linking Events with Call Alarm Receiving Center

Description

Disable linking events with the call alarm receiving center.

Command

Figure 3-30 Disable linking events with the alarm receiving center

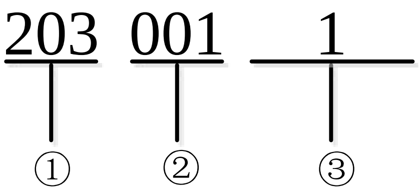


Table 3-34 Disable linking events with the alarm receiving center

Number	Description
1	The encoding address. The command operation means disabling linking events with the alarm receiving center.
2	Event No.: 001-100.
3	● 1: Alarm receiving center 1. ● 2: Alarm receiving center 2.

Example

The admin user disables linking event 1 with the alarm receiving center 1.

Step 1 The admin user enters 2030011 under programming mode.

Step 2 Press **Enter**.

3.6.8.5 Modifying Event Code

Description

Modify event codes.

Command

Figure 3-31 Modify event codes

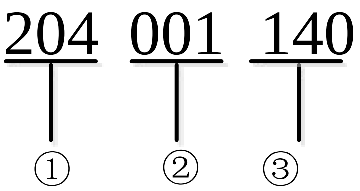


Table 3-35 Modify event code

Number	Description
1	The encoding address. The command operation means configuring whether or not to modify event codes.
2	Event No.: 001-100.
3	1: Alarm receiving center 1. 2: Alarm receiving center 2.

Example

The admin user modifies the event code 001 to 140.

Step 1 The admin user enters 204001140 under programming mode.

Step 2 Press **Enter**.

3.6.9 Printer

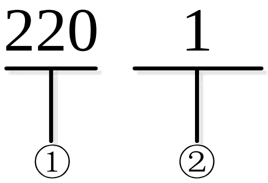
3.6.9.1 Enabling Printer

Description

Enable or disable printer.

Command

Figure 3-32 Enable printer



0: Disable; 1: Enable.

Example

The admin user enables **Printer**.

Step 1 The admin user enters 2201 under programming mode.

Step 2 Press **Enter**.

3.6.9.2 Printing Zone Alarm Event

Description

Configure to print zone alarm events and zone alarm restored events.

Command

Figure 3-33 Print zone alarm events

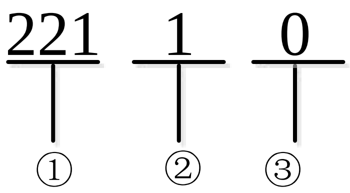


Table 3-36 Print zone alarm events

Number	Description
1	The encoding address. The command operation means printing alarm events.
2	**Zone Alarm Event**. ● 1: Print. ● 0: Not Print.
3	**Zone Alarm Restored**. ● 1: Print. ● 0: Not Print.

Example

The admin user configures the system to print **Zone Alarm** events, but not to print **Zone Alarm Restored** events.

Step 1 The admin user enters 22110 under programming mode.

Step 2 Press **Enter**.

3.6.9.3 Printing System Events

Description

When system faults occur, the printer will be linked to print the system events.

Command

Figure 3-34 Print system events

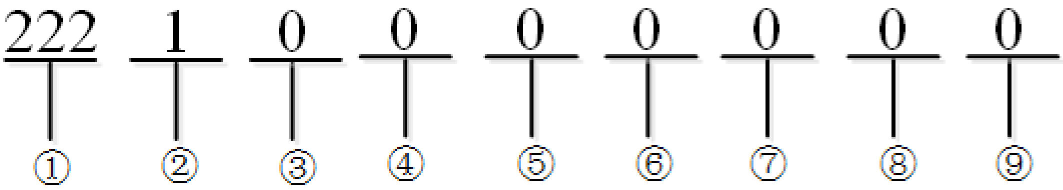


Table 3-37 Print system events

Number	Description
1	The encoding address. The command operation means printing system events.
2	**Power Failure**. ● 1: Print. ● 0: Not Print.
3	**Battery Undervoltage**. ● 1: Print. ● 0: Not Print.
4	**PSTN Offline**. ● 1: Print. ● 0: Not Print.
5	**Controller Tamper**. ● 1: Print. ● 0: Not Print.
6	**Keypad offline**. ● 1: Print. ● 0: Not Print.
7	**Disconnected Wireless Network**. ● 1: Print. ● 0: Not Print.
8	**Disconnected Wired Network**. ● 1: Print. ● 0: Not Print.
9	**Expansion Module Offline**. ● 1: Print. ● 0: Not Print.

Example

The admin user configures the system to print **Power Failure** events, but not to print other system events.

Step 1 The admin user enters 22210000000 under programming mode.

Step 2 Press **Enter**.

3.6.9.4 Printing Restored System Events

Description

When system events are restored, the printer output will be linked to print the events.

Command

Figure 3-35 Print restored events

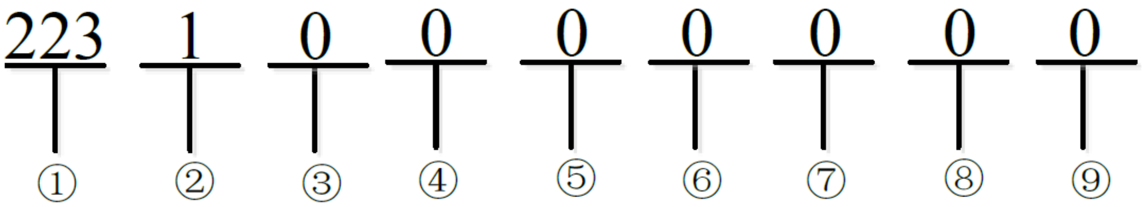


Table 3-38 Print restored events

Number	Description
1	The encoding address. The command operation means printing restored events.
2	**Power Restored**. ● 1: Print. ● 0: Not Print.
3	**Battery Voltage Restored**. ● 1: Print. ● 0: Not Print.
4	**PSTN Reconnected**. ● 1: Print. ● 0: Not Print.
5	**Controller Tamper Resolved**. ● 1: Print. ● 0: Not Print.
6	**Keypad Reconnected**. ● 1: Print. ● 0: Not Print.
7	**Wireless Network Reconnected**.

Number	Description
	● 1: Print. ● 0: Not Print.
8	**Wired Network Reconnected**. ● 1: Print. ● 0: Not Print.
9	**Expansion Module Reconnected**. ● 1: Print. ● 0: Not Print.

Example

The admin user configures the system to print **Power Restored** events, but not to print other restored system events.

Step 1 The admin user enters 22310000000 under programming mode.

Step 2 Press **Enter**.

3.6.9.5 Printing Operation Events

Description

When operation events occur, the printer will be linked to print the events.

Command

Figure 3-36 Print operation events

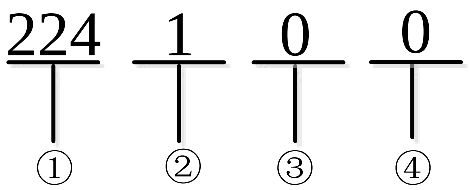


Table 3-39 Print operation events

Number	Description
1	The encoding address. The command operation means printing operation events.
2	**Arm Subsystem**. ● 1: Print. ● 0: Not Print.
3	**Bypass**. ● 1: Print.

Number	Description
	● 0: Not Print.
4	**Enter Programming**. ● 1: Print. ● 0: Not Print.

Example

The admin user configures the system to print **Arm Subsystem** event, but not to print other system events.

Step 1 The admin user enters 224100 under programming mode.

Step 2 Press **Enter**.

3.6.9.6 Printing Restored Operation Events

Description

When operation events are restored, the printer output will be linked to print the events.

Command

Figure 3-37 Print restored operation events

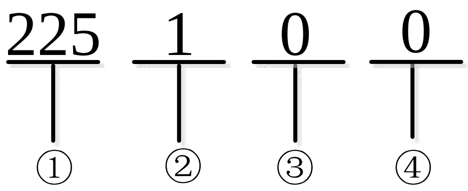


Table 3-40 Print restored operation events

Number	Description
1	The encoding address. The command operation means printing restored operation events.
2	**Disarm Subsystem**. ● 1: Print. ● 0: Not Print.
3	**Unbypass**. ● 1: Print. ● 0: Not Print.
4	**Exit Programming**.

Number	Description
	● 1: Print. ● 0: Not Print.

Example

The admin user configures the system to print **Disarm Subsystem** event, but not to print other restored system events.

Step 1 The admin user enters 225100 under programming mode.

Step 2 Press **Enter**.

3.6.9.7 Printing Panic Events

Description

When fire events, medical events, or duress events occur, the printer will be linked to print the events.

Command

Figure 3-38 Print panic events

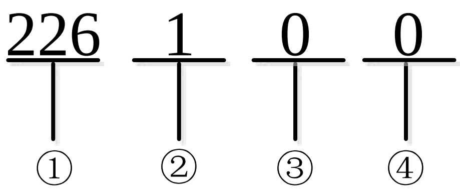


Table 3-41 Print panic events

Number	Description
1	The encoding address. The command operation means printing panic events.
2	**Fire**. ● 1: Print. ● 0: Not Print.
3	**Medical**. ● 1: Print. ● 0: Not Print.
4	**Duress**. ● 1: Print. ● 0: Not Print.

Example

The admin user configures the system to print **Fire** events, but not to print **Duress** or **Medical** events.

Step 1 The admin user enters 226100 under programming mode.

Step 2 Press **Enter**.

3.6.9.8 Printing Pulse Event

Description

When pulse events occur, such as PSTN scheduled test, and alarm controller resets, the printer output will be linked to print the events.

Command

Figure 3-39 Print pulse events

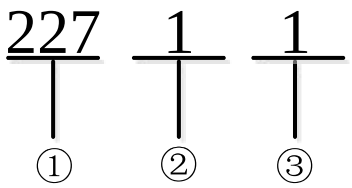


Table 3-42 Print pulse events

Number	Description
1	The encoding address. The command operation means printing pulse events.
2	**PSTN Scheduled Test**. ● 1: Print. ● 0: Not Print.
3	**Alarm Controller Reset**. ● 1: Print. ● 0: Not Print.

Example

The admin user configures the system to print **PSTN Scheduled Test** and **Alarm Controller Reset** events.

Step 1 The admin user enters 22711 under programming mode.

Step 2 Press **Enter**.

3.6.10 Subsystem

3.6.10.1 Enabling Subsystem

Description

Enable or disable subsystem.

Command

Figure 3-40 Enable subsystem

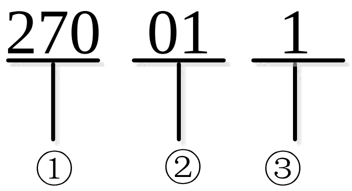


Table 3-43 Enable subsystem

Number	Description
1	The encoding address. The command operation means enabling or disabling the subsystem.
2	Subsystem number:01-08.
3	● 1: **Enable**. ● 0: **Disable**.

Example

The admin user enables subsystem 1.

Step 1 The admin user enters 270011 under programming mode.

Step 2 Press **Enter**.

3.6.10.2 Adding Zones to Subsystems

Description

Link a zone to a subsystem.

Command

Figure 3-41 Link a zone to a subsystem

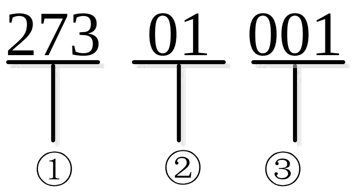


Table 3-44 Link a zone to a subsystem

Number	Description
1	The encoding address The command operation means linking a zone to a subsystem.
2	Subsystem number:01-08.
3	Zone number: 001-256.

Example

The admin user links zone 1 to subsystem 1.

Step 1 The admin user enters 27301001 under programming mode.

Step 2 Press **Enter**.

3.6.10.3 Deleting Zones from Subsystems

Description

Delete a zone from a subsystem.

Command

Figure 3-42 Delete a zone from a subsystem

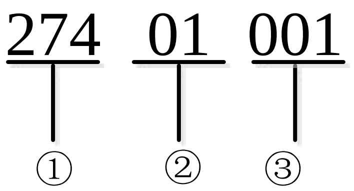


Table 3-45 Delete a zone from a subsystem

Number	Description
1	The encoding address. The command operation means deleting a zone from a subsystem.
2	Subsystem number:01-08.
3	Zone number: 001-256.

Example

The admin user deletes zone 1 from subsystem 1.

Step 1 The admin user enters 27401001 under programming mode.

Step 2 Press **Enter**.

3.6.11 Registering

3.6.11.1 Device ID

Description

Configure ID of a device that is registered to the server.

Command

Figure 3-43 Device ID

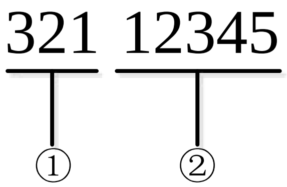


Table 3-46 Device ID

Number	Description
1	The encoding address. The command operation means configuring ID of a device that is registered to the server.
2	**Device ID**. Only letters and numbers are supported.

Example

The admin user configures the ID of a device that is registered to the server as 12345.

Step 1 The admin user enters 32112345 under programming mode.

Step 2 Press **Enter**.

3.6.11.2 Server IP Address

Description

Configure IP address of a server to register a device.

Command

Figure 3-44 Server IP address

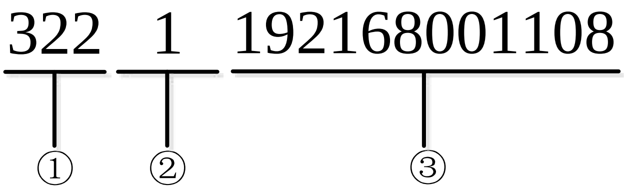


Table 3-47 Server IP address

Number	Descriptions
1	The encoding address. The command operation means configuring IP address of a server to register a device.
2	Server. ● 1: Server 1. ● 2: Server 2.
3	Address. 📖 The server IP address has 12 digits. 0 can be added for sections that have less than 3 digits. For example, if the server IP address is 192.168.1.108, then it will become 192168001108.

Example

The admin user configures the IP address of a server to register a device as 192.168.1.108.

Step 1 The admin user enters 3221192168001108 under programming mode.

Step 2 Press **Enter**.

3.6.11.3 Server Port Number

Description

. Configure port number of a server to register a device.

Command

Figure 3-45 Server port number

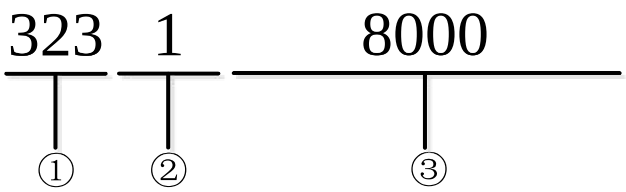


Table 3-48 Server port number

Number	Description
1	The encoding address. The command operation means configuring the server port mumber.
2	Server. ● 1: Server 1. ● 2: Server 2.
3	Port. 🕮 The ranger of the server port number is 1025 to 65535, and the number cannot be the same as the port number that already exited.

Example

The admin user configures the port number of server 1 as 8000.

Step 1 The admin user enters 32218000 under programming mode.

Step 2 Press **Enter**.

3.6.12 Alarm Center

3.6.12.1 Server IP Address

Description

Configure server IP address for the alarm center.

Command

Figure 3-46 Server IP address

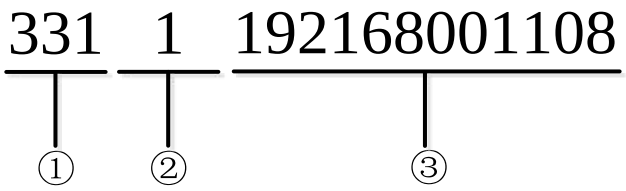


Table 3-49 Server IP address

Number	Description
1	The encoding address. The command operation means configuring IP address for the alarm center.
2	Server. ● 1: Server 1. ● 2: Server 2.
3	Address. 📖 The server IP address has 12 digits. 0 can be added for sections that have less than 3 digits. For example, if the server IP address is 192.168.1.108, then it will become 192168001108.

Example

The admin user configures IP address of server 1 as 192.168. 1.108 for the alarm center.

Step 1 The admin user enters 3311192168001108 under programming mode.

Step 2 Press **Enter**.

3.6.12.2 Port

Description

Configuring port number for the alarm center

Command

Figure 3-47 Port number

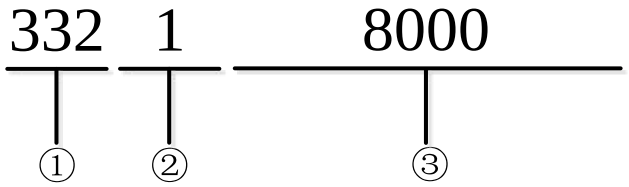


Table 3-50 Port number

Number	Description
1	The encoding address. The command operation means configuring port number for the alarm center.
2	Server. ● 1: Server 1. ● 2: Server 2.
3	Port. 📖 The ranger of the server port number is 1025 to 65535, and the number cannot be the

Number	Description
	same as the port number that already exists.

Example

The admin user configures the port number of server 1 as 8000.

Step 1 The admin user enters 33218000 under programming mode.

Step 2 Press **Enter**.

3.6.13 Network (2G/4G)

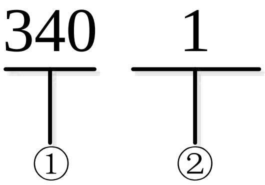
3.6.13.1 2G/4G

Description

Enable or disable 2G/4G.

Command

Figure 3-48 Enable 2G/4G



0: Disable; 1: Enable.

Example

The admin user enables **2G/4G**.

Step 1 The admin user enters 3401 under programming mode.

Step 2 Press **Enter**.

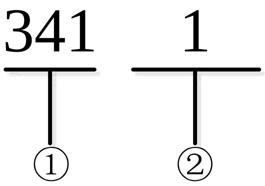
3.6.13.2 Dial

Description

Enable or disable dial.

Command

Figure 3-49 Enable dial



0: Disable; 1: Enable.

Example

The admin user enables **Dial**.

Step 1 The admin user enters 3411 under programming mode.

Step 2 Press **Enter**.

3.6.13.3 Configuring Network

Description

Configure network parameters.

Command

Figure 3-50 Network

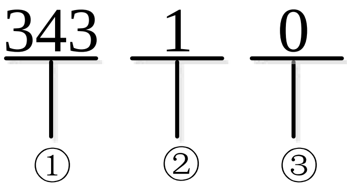


Table 3-51 Network

Number	Description
1	The encoding address. The command operation means configuring parameters for network.
2	● 1: Enable **2G/4G**. ● 0: Disable **2G/4G**.
3	● 1: Enable **Dial**. ● 0: Disable **Dial**.

Example

The admin user enables**2G/4G** and disables **Dial**.

Step 1 The admin user enters 34310 under programming mode.

Step 2 Press **Enter**.

3.6.14 Alarm Receiving Center

3.6.14.1 Enabling Alarm Receiving Center

Description

Enable or disable alarm receiving center.

Command

Figure 3-51 Enable alarm receiving center

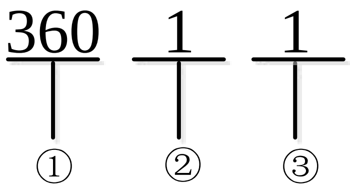


Table 3-52 Enable alarm receiving center

Number	Description
1	The encoding address. The command operation means enabling alarm receiving center.
2	Alarm receiving center No.: 1 - 6.
3	● 1: **Enable**. ● 0: **Disable**.

Example

The admin user enables alarm receiving center 1. The default passcode of the admin user is 1234.

Step 1 The admin user enters 36011 under programming mode.

Step 2 Press **Enter**.

3.6.14.2 Transmission Method

Description

Configure transmission methods for alarm receiving center.

Command

Figure 3-52 Transmission methods

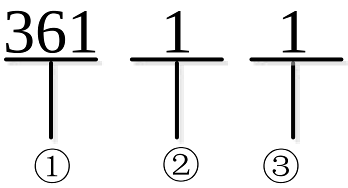


Table 3-53 Transmission methods

Number	Description
1	The encoding address. The command operation means configuring transmission methods for alarm receiving center.
2	Alarm receiving center No.: 1 - 6.
3	Transmission method. ● 1: **PSTN Network** (valid when protocol type is 1). ● 2: **NIC 1**. ● 3: **Cellular Data**. ● 4: **NIC 2**.

Example

The admin user configures the transmission method as **PSTN Network** for alarm receiving center 1.

Step 1 The admin user enters 36111 under programming mode.

Step 2 Press **Enter**.

3.6.14.3 Protocol Type

Description

Configure protocol type for alarm receiving center.

Command

Figure 3-53 Protocol type

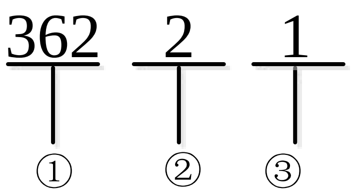


Table 3-54 Protocol type

Number	Description
1	The encoding address. The command operation means configuring protocol type for alarm receiving center.
2	Alarm receiving center No.: 1 - 6.
3	Protocol type. ● 1: **Call Alarm Receiving Center** (valid when transmission method is 1). ● 2: **Register**. ● 3: **Alarm Center**.

Example

The admin user configures protocol type as **Call Alarm Receiving Center** for alarm receiving center 2.

Step 1 The admin user enters 36221 under programming mode.

Step 2 Press **Enter**.

3.6.14.4 Channel Servers

Description

Configure channel servers for the alarm receiving center.

Command

Figure 3-54 Channel server

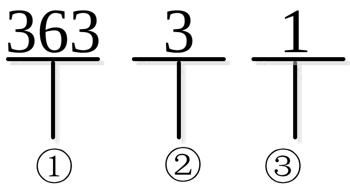


Table 3-55 Channel server

Number	Descriptions
1	The encoding address. The command operation means configuring channel server for alarm receiving center.
2	Alarm receiving center No.: 1 - 6.
3	Server. 1: Server 1. 2: Server 2.

Example

The admin user configures the alarm receiving center 3 to report the alarm messages to server 1.

Step 1 The admin user enters 36331 under programming mode.

Step 2 Press **Enter**.

3.6.14.5 Transmission Methods (Backup Channels)

Description

Configure transmission methods for backup channels of the alarm receiving center.

Command

Figure 3-55 Transmission methods (backup channel)

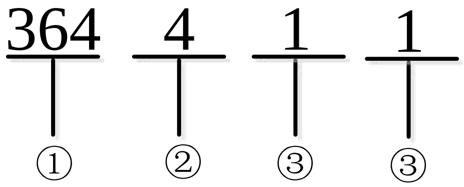


Table 3-56 Transmission methods (backup channel)

Number	Description
1	The encoding address. The command operation means configuring transmission methods for backup channel of alarm receiving center 1.
2	Alarm receiving center No.: 1 - 6.
3	Backup channel. ● 1: Backup channel 1. ● 2: Backup channel 2.
4	Transmission method. ● 1: **PSTN Network** (valid when protocol type is 1). ● 2: **NIC 1**. ● 3: **Cellular Data**. ● 4: **NIC 2**.

Example

The admin user configures the transmission method as **PSTN Network** for the backup channel 1 of alarm receiving center 4.

Step 1 The admin user enters 364411 under programming mode.

Step 2 Press **Enter**.

3.6.14.6 Protocol Type (Backup Channels)

Description

Configure protocol types for backup channels of alarm receiving center.

Command

Figure 3-56 Protocol type (backup channel)

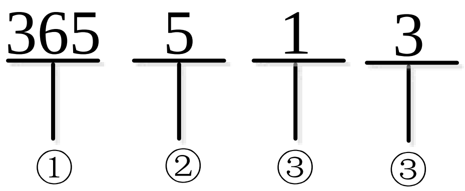


Table 3-57 Protocol type (backup channel)

Number	Description
1	The encoding address. he command operation means configuring transmission protocol for alarm receiving center groups.
2	Alarm receiving center No.: 1 - 6.
3	Backup channel. ● 1: Backup channel 1. ● 2: Backup channel 2.
4	Protocol type. ● 1: **Call Alarm Receiving Center** (valid when transmission method is 1). ● 2: **Register**. ● 3: **Alarm Center**.

Example

The admin user configures protocol type as **Alarm Center** for backup channel 1 of alarm receiving center 5.

Step 1 The admin user enters 365513 under programming mode.

Step 2 Press **Enter**.

3.6.14.7 Servers (Backup Channel)

Description

Configure servers for the backup channel of the alarm receiving center groups.

Command

Figure 3-57 Server (backup channel)

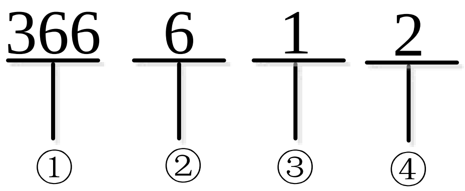


Table 3-58 Server (backup channel)

Number	Description
1	The encoding address. The command operation means configuring server for backup channel of the alarm receiving center groups.
2	Alarm receiving center No.: 1 - 6.
3	Backup channel.

Number	Description
	● 1: Backup channel 1. ● 2: Backup channel 2.
4	Server. 1: Server 1. 2: Server 2.

Example

The admin user configures the alarm receiving center 6 to report the alarm messages to server 2 of the backup channel 1.

Step 1 The admin user enters 366612 under programming mode.

Step 2 Press **Enter**.

3.6.15 Network (TCP/IP)

3.6.15.1 IP Address

Description

Configure IP address for alarm controller.

Command

Figure 3-58 IP address

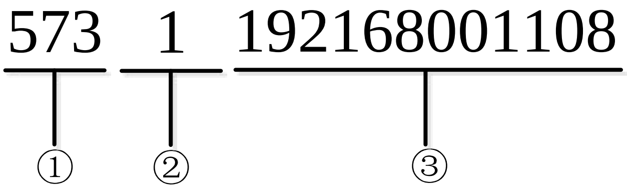


Table 3-59 IP address

Number	Description
1	The encoding address. The command operation means configuring IP address for the alarm controller.
2	**NIC**. ● 1: **NIC 1**. ● 2: **NIC 2**.
3	IP address. The IP address consists of 4 sections, each of which has 3 digits. 0 can be added for sections that have less than 3 digits. For example, if the server IP address is 192.168.1.108, then it will become 192168001108.

Example

The admin user configures IP address of **NIC 1** as 192.168 .1.108.

Step 1 The admin user enters 5731192168001108 under programming mode.

Step 2 Press **Enter**.

3.6.15.2 Port

Description

Configure TCP port for the alarm controller.

Command

Figure 3-59 TCP port

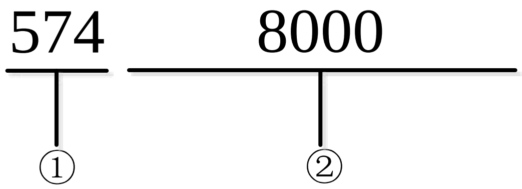


Table 3-60 TCP port

Number	Description
1	The encoding address. The command operation means configuring TCP port number for the alarm controller.
2	TCP port. The range of the port number is 1025 to 65535 and the default is 37777.

Example

The admin user configures **TCP Port** of alarm controller as 8000.

Step 1 The admin user enters 5748000 under programming mode.

Step 2 Press **Enter**.

3.6.15.3 Subnet Mask, Gateway and DNS

Description

Configure subnet mask, gateway and DNS for the alarm controller.

Command

Figure 3-60 Subnet mask, gateway and DNS

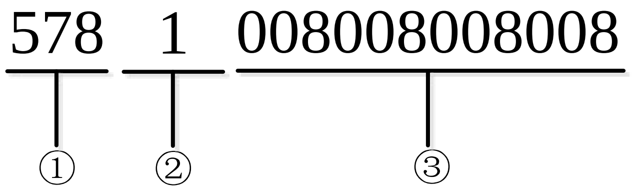


Table 3-61 Subnet mask, gateway and DNS

Number	Descriptions
1	The encoding address. The command operation means configuring subnet mask, gateway and DNS for the alarm controller. ● 575: **Subnet Mask**. ● 576: **Gateway**. ● 578: **Preferred DNS**. ● 579: **Alternate DNS**.
2	**NIC**. ● 1: **NIC 1**. ● 2: **NIC 2**.
3	IP address. The IP address consists of 4 sections, each of which has 3 digits. 0 can be added to sections that have less than 3 digits. For example, if the server IP address is 192.168.1.108, then it will become 192168001108.

Example

The admin user configures **Alternate DNS** of **NIC 1** as 008008008008 for the alarm controller.

Step 1 The admin user enters 5781008008008008 under programming mode.

Step 2 Press **Enter**.

3.6.15.4 DHCP

Description

Enable or disable **DHCP**.

Command

Figure 3-61 DHCP

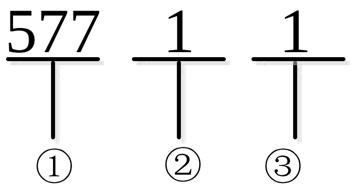


Table 3-62 DHCP

Number	Description
1	The encoding address. The command operation means enabling or disabling **DHCP**.
2	**NIC**. ● 1: **NIC 1**. ● 2: **NIC 2**.
3	● 1: Enable. ● 0: Disable.

Example

The admin user enables or disables **DHCP** for **NIC 1**.

Step 1 The admin user enters 57711 under programming mode.

Step 2 Press **Enter**.

3.6.16 Keyfob Key Bindings

Description

Enable or disable key bindings for the keyfob.

Command

661: Enable. 662: Disable.

Example

The admin user enables key bindings for the alarm keyfob.

Step 1 The admin user enters 661 under programming mode.

Step 2 Press **Enter**.

3.6.17 Keypad

Description

Link or cancel to link subsystem of the keypad.

Command

Figure 3-62 Keypad

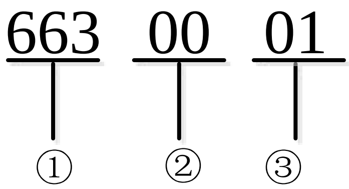


Table 3-63 Keypad

Number	Description
1	The encoding address. The command operation means linking or cancelling to link subsystem of the alarm keypad. ● 663: Link. ● 664: Cancel to link.
2	Keypad address: 00-31.
3	Subsystem number:01-08.

Example

The admin user links the keypad address 00 to the subsystem 1.

Step 1 The admin user enters 6630001 under programming mode.

Step 2 Press **Enter**.

3.6.18 Card Key Bindings

Description

Enable or disable card key bindings.

Command

665: Enable. 666: Disable.

Example

The admin user enables card key bindings.

Step 1 The admin user enters 665 under programming mode.

Step 2 Press **Enter**.

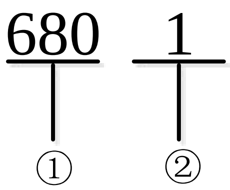
3.6.19 Web Access Control

Description

Enable or disable web access control.

Command

Figure 3-63 Enable web access control



0: Disable; 1: Enable.

Example

The admin user enables web access control.

Step 1 The admin user enters 6801 under programming mode.

Step 2 Press **Enter**.

3.6.20 NIC 2

Description

Configure NIC 2 events.

Command

Figure 3-64 NIC 2 events

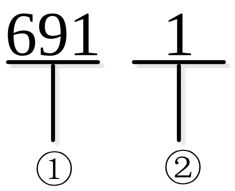


Table 3-64 NIC 2 events

Number	Description
1	The encoding address. The command operation means configuring NIC 2 events. ● 691: NIC 2 network disconnected. ● 692: NIC 2 IP conflict. ● 693: NIC 2 MAC conflict.
2	● 0: Disable. ● 1: Enable.

Example

The admin user enables NIC 2 network disconnected events.

Step 1 The admin user enters 6911 under programming mode.

Step 2 Press **Enter**.

3.6.21 Arming

Description

Enable of disable arming function for the keypad.

Command

Figure 3-65 Arm

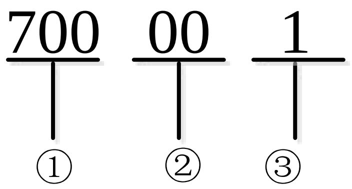


Table 3-65 Arm

Number	Description
1	The encoding address. The command operation means configuring arming function for the keypad.
2	Keypad address: 00-31.
3	● 0: Disable. ● 1: Enable.

Example

The admin user enables the arming function for the keypad (address: 00).

Step 1 The admin user enters 700001 under programming mode.

Step 2 Press **Enter**.

3.6.22 Keypad RS-485 Address

Description

Modify keypad RS-485 address.

Command

Figure 3-66 Modify keypad RS-485 address

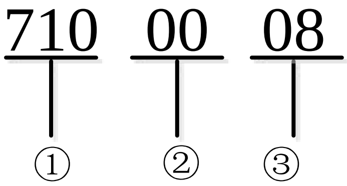


Table 3-66 Modify alarm keypad RS-485 address

Number	Description
1	The encoding address. The command operation means modifying keypad RS-485 address.
2	Keypad address before modifying: 00-31.
3	Keypad address after modifying: 00-31.

Example

The admin user modifies the keypad address from 00 to 08.

Step 1 The admin user enters 7100008 under programming mode.

Step 2 Press **Enter**.

3.6.23 Keypad Display Time

Description

Modify the keypad display time. When you first press a key after not operating the keypad for a while, the keypad will take a set period of time to wake. During this time, it will not dim its display.

Command

Figure 3-67 Keypad display time

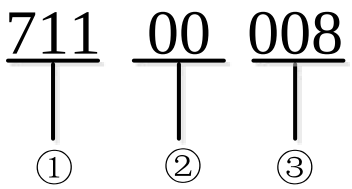


Table 3-67 Keypad display time

Number	Description
1	The encoding address. The command operation means configuring keypad display time.
2	Keypad address: 00-31.
3	Keypad display time: 0 to 999 seconds.

Example

The admin user modifies display time of the keypad (address: 00) to 8.

Step 1 The admin user enters 71100008 under programming mode.

Step 2 Press **Enter**.

3.6.24 Wired Network

Description

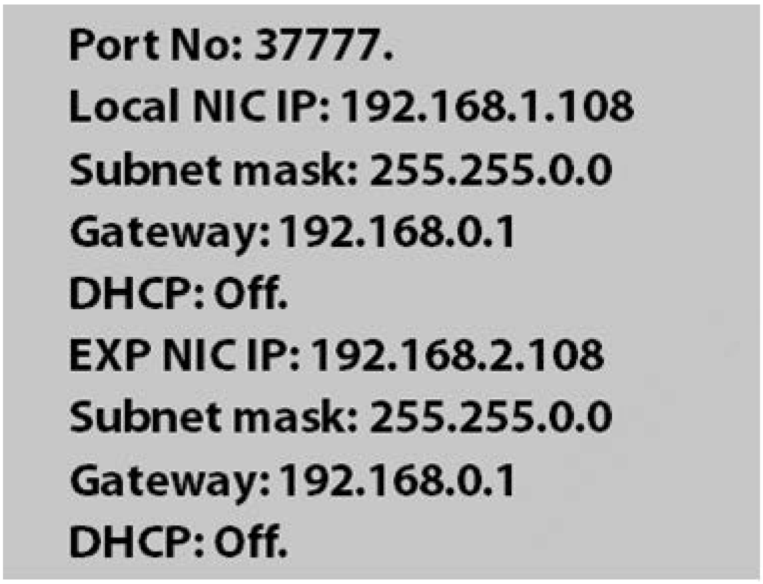
Search for information on wired network.

Command

*02

Keypad Information

Figure 3-68 Keypad information



```
Port No: 37777.
Local NIC IP: 192.168.1.108
Subnet mask: 255.255.0.0
Gateway: 192.168.0.1
DHCP: Off.
EXP NIC IP: 192.168.2.108
Subnet mask: 255.255.0.0
Gateway: 192.168.0.1
DHCP: Off.
```

3.6.25 Alarm Controller

Description

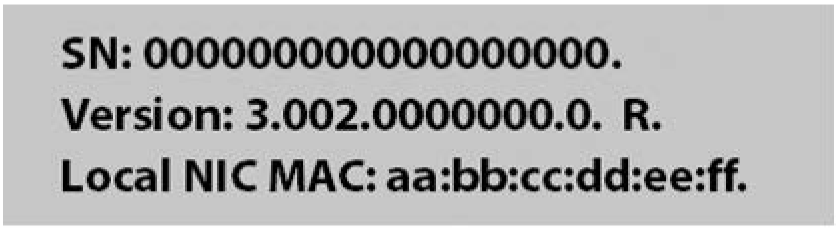
Search for information on the alarm controller.

Command

Enter *04.

Alarm Controller Information

Figure 3-69 Alarm controller information



```
SN: 000000000000000000.
Version: 3.002.0000000.0. R.
Local NIC MAC: aa:bb:cc:dd:ee:ff.
```

3.6.26 2G/4G Modules

Description

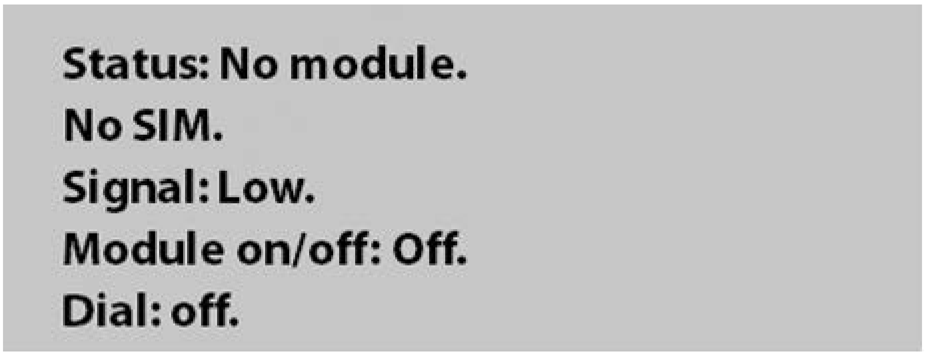
Search for information on 2G/4G modules.

Command

Enter *05.

2G/4G Module Information

Figure 3-70 2G/4G module information



Status: No module.
No SIM.
Signal: Low.
Module on/off: Off.
Dial: off.

3.6.27 Exiting Programming Mode

Description

Exit programming mode.

- If you do not operate the keypad for 3 seconds, it will automatically exit programming mode and then enter global mode.
- Exit programming mode first before switching to other modes.

Command

Enter *.

Example

The admin user exits programming mode. The default passcode of the admin user is 1234.

Step 1 The admin user enters * under programming mode.

Step 2 Press **Enter**.

3.7 Walk Test Mode

3.7.1 Entering Walk Test Mode

Description

Under global mode, walk test your system in walk test mode.

- The security system will only report alarm events to the keypad under walk test mode.
- The security system will not report alarm events to the keypad in isolated zones.
- Exit programming mode first by switching to other modes.

Command

Enter default passcode + * + 18.

Example

The admin user enters programming mode. The default passcode of the admin user is 9090.

Step 1 The installer enters 9090*18 on global mode.

Step 2 Press **Enter**.

Walk Test Mode is displayed.

3.7.2 Exiting Walk Test Mode

Description

Exit walk test mode.

- If you do not operate the keypad for 3 seconds, it will automatically exit programming mode and enter global mode.
- Exit programming mode first by switching to other modes.

Command

Enter installer default passcode + * + 19.

Example

The admin user enters walk test mode. The default passcode of the admin user is 9090*19.

Step 1 The installer enters 9090*19 in global mode.

Step 2 Press **Enter**.

Appendix 1 Keypad Command Table

Appendix Table 1-1 Keypad command

Type		Operation
Global mode	Disarm the subsystem	Enter passcode + * + 2 + * + subsystem number.
	Away arm the subsystem	Enter passcode + * + 3 + * + subsystem number.
	Forced arm the subsystem	Enter passcode + * + 4 + * + subsystem number.
	Home arm the subsystem	Enter passcode + * + 5 + * + subsystem number.
	Forced home arm the subsystem	Enter passcode + * + 6 + * + subsystem number.
	Switch system status	Enter passcode.
	Arm a single zone:	Enter passcode + * + 10 + * + zone number.
	Disarm a single zone	Enter passcode + * + 11 + * + zone number.
	Cancel alarm	● Cancel all: Enter passcode + * + 1. ● Cancel zone alarm: Enter passcode + * + 1 + * + subsystem number. ● Cancel subsystem: Enter passcode + * + 23 + * + zone number.
	Bypass and isolate	● Unbypass: Enter passcode + * + 7 + * + zone number. ● Bypass: Enter passcode + * + 8 + * + zone number. ● Isolate: Enter passcode + * + 9 + * + zone number.
	Relay	● Manually turn on the relay output: Enter passcode + * + 13 + * + relay number. ● Manually turn off the relay output: Enter passcode + * + 14 + * + relay number.
	PSTN test	● PSTN manual test: Enter passcode + * + 15. ● SMS manual test: Enter passcode + * + 16 + * + phone number. ● Call manual test: Enter passcode + * + 17 + * + phone number.
	Restart the alarm controller	Enter passcode + * + 20.
	Initialize the alarm controller	Enter user passcode + * + 21 + * + passcode you configured.
	Restore to the default settings	Enter passcode + * + 22.
Programming mode	Enter programming mode.	Enter admin default passcode or installer default passcode or manufacturer passcode or operator passcode + * + 12.
	Manage users	● Add a user: Enter 000 + passcode. ● Delete a user: Enter 001 + passcode. ● Configure Permissions

Type		Operation
		◇ Add permissions to a user: Enter 002 + user passcode + * + permission passcode. ◇ Delete permissions from a user: Enter 003 + user passcode + * + permission passcode. ● Chang user passcode: Enter 004 + user old passcode + * + user new password. ● Link users to subsystems: Enter 005 + user passcode + * + subsystem number. ● Cancel to link users to the subsystems: Enter 006 + user passcode + * + subsystem number ● Enable arming: Enter 007 + user passcode + * + 0 or 1. ● Configure arming and disarming: Enter 008 + user passcode + * + 1 or 2 or 3. ● Configure arming mode: Enter 009 + user passcode + * + 0 or 1. ● Enable forced arming: Enter 010 + user passcode + * + 0 or 1.
		● Configure sensor type: Enter 101 + zone + NO/NC. ● Configure zone type: Enter 102 + zone + zone type. ● Configure sensing type: Enter 103 + zone + sensing type. ● Configure entry delay time: Enter 104 + zone + entry delay time. ● Configure exit delay time: Enter 105 + zone + exit delay time. ● Configure module type: Enter 106 +zone + 0 or 1 or 2 or 3. ● Configure module address: Enter 107 +zone + module address. ● Configure module channel number: Enter 108 +zone + channel number. ● Configure resistance: Enter 109 + zone + resistance.
	Relay	● Configure relay output time: Enter 002 + zone + output ti,e. ● Configure module type: Enter 021 + zone + 0 or 1 or 2 or 3. ● Configure module address: Enter 022 +

Type		Operation
		zone + address. ● Configure module channel number: Enter 023 +zone + module channel number.
	Siren	● Enable siren: Enter 050 + 0 or 1. ● Configure siren output duration: Enter 051 + duration.
	Alarm receiving center	● Configure sending strategy: Enter 151 + sending strategy. ● Configure dial attempts: Enter 153 + alarm receiving center No. + dial attempts. ● Configure dial delay: Enter 154 + alarm receiving center No. + dial delay. ● Configure alarm receiver number: Enter 155 + alarm receiving center No. + alarm receiver number. ● Configure user code: Enter 156 + alarm receiving center No. + user code. ● Configure call alarm receiving center: Enter 160 + alarm receiving center No.+ dial attempt+ dial delay +user code.
	Test report	● Enable test report: Enter 170 + 0 or 1. ● Configure report period: ◇ Enter 171 + periods (day). ◇ Enter 172 + periods (hour). ● Configure alarm receiving center function: ◇ Enable: Enter 173 + alarm receiving center. ◇ Disable: Enter 174 + alarm receiving center. ● Configure time for uploading first test report: Enter 175 + periods.
	CID Linkage	● Configure protocol type: Enter 200 + 1 or 2. ● Enable or disable report restored event: Enter 201 + 0 or 1. ● Enable linking events with the alarm receiving center: Enter 202 + event No. + alarm receiving center number. ● Disable linking events with call alarm receiving center: Enter 203 + event No. + alarm receiving center number. ● Modify event code: Enter 204 + event No. + alarm receiving center number.
	Printer	● Enable or disable printer: Enter 220 + 0 or 1.

Type		Operation
		- Configure to print zone alarm events: Enter 221 + 0 or 1 + 0 or 1. - Configure to print system events: Enter 222 + 0 or 1 + 0 or 1 + 0 or 1 + 0 or 1 + 0 or 1 + 0 or 1 + 0 or 1 + 0 or 1. - Configure to print restored system events: Enter 223 + 0 or 1 + 0 or 1 + 0 or 1 + 0 or 1 + 0 or 1 + 0 or 1 + 0 or 1 + 0 or 1. - Configure to print operation events: Enter 224 + 0 or 1 + 0 or 1 + 0 or 1 + 0 or 1. - Configure to print restored operation events: Enter 225 + 0 or 1 + 0 or 1 + 0 or 1 + 0 or 1. - Configure to print panic events: Enter 226 + 0 or 1 + 0 or 1. - Configure to print pulse events: Enter 227+ 0 or 1 + 0 or 1.
	Subsystem	- Enable or disable subsystem: Enter 270 + subsystem number + 0 or 1. - Add a zone to a subsystem: Enter 273 + subsystem number + zone number. - Delete a zone from a subsystem: Enter 274 + subsystem number + zone number.
	Register	- Configure device ID: Enter 321 + ID number. - Configure server IP address: Enter 322 + server + IP address. - Configure server port number: Enter 323 + server + port number.
	Alarm center	- Configure server IP address: Enter 331 + server + IP address. - Configure server port number: Enter 332 + server + port number
	Network (2G/4G)	- Enable or disable 2G/4G: Enter 340 + 0 or 1. - Enable or disable dial: Enter 341 + 0 or 1. - Configure network: Enter 343 + 0 or 1 + 0 or 1.
	Alarm receiving center	- Enable or disable alarm receiving center: Enter 360 + alarm receiving center No. + 0 or 1. - Configure transmission method for alarm receiving center: Enter 361 + alarm receiving center No. + transmission method.

Type		Operation
		● Configure protocol type for alarm receiving center: Enter 362 + alarm receiving center No. + protocol type. ● Configure channel servers for alarm receiving center: Enter 363 + alarm receiving center No. + server. ● Configure transmission modes for alarm receiving center groups' backup channels: Enter 364 + alarm receiving center groups + backup channels + transmission mode. ● Configure transmission methods for backup channels of the alarm receiving center: Enter 364 + alarm receiving center No. + backup channels + transmission method. ● Configure protocol types for backup channels of alarm receiving center: Enter 365 + alarm receiving center No. + backup channels + protocol type.
	Network (TCP/IP)	● Configure IP address: Enter 573 + NIC + IP address. ● Configure port: Enter 574 + TCP port number ● Configure subnet mask, gateway and DNS. ◇ Subnet mask: Enter 575 + NIC + IP address. ◇ Gateway: Enter 576 + NIC + IP address. ◇ Preferred DNS: Enter 578 + NIC + IP address. ◇ Alternate DNS: Enter 579 + NIC + IP address. ● Enable or disable DHCP: Enter 577 + 0 or 1.
	Card key bindings	Enable or disable card key bindings: Enter 661 or 662.
	Keypad	● Link subsystem to the keypad: Enter 663 + keypad address + subsystem number. ● Cancel to link subsystem to the keypad: Enter 664 + keypad address + subsystem number.
	Card key bindings	Enable or disable card key bindings: Enter 665 or 666.
	Web access control	Configure web access control: Enter 680 + 0 or 1.
	NIC 2 events	● Configure NIC 2 network disconnected events: Enter 691 + 0 or 1.

Type		Operation
		● Configure NIC 2 IP conflict events: Enter 692 + 0 or 1. ● Configure NIC 2 MAC conflict events: Enter 693 + 0 or 1.
	Arming	Enable of disable arming function for the keypad： Enter 700 + keypad address + 0 or 1.
	Keypad RS-485 address	Modify keypad RS-485 address: Enter 710 + keypad address before modifying + keypad address after modifying.
	Keypad display time	Modify keypad display time: Enter 711 + keypad address +keypad display time.
	Search for wired network information	Enter *02.
	Search for alarm controller information	Enter *04.
	Search for information of 2G/4G modules	Enter *05.
	Exit programming mode	Enter *.
Walk test	Enter walk test mode	Enter default passcode + * + 18.
	Exit walk test mode	Enter default passcode + * + 19.

Appendix 2 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong 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; character types include 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 overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883