



Alarm Expansion Module

Quick Start Guide








Foreword

This manual introduces the installation, functions, and configuration of the wireless expansion module. Read this manual before you use the product and keep this manual for future reference.

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	December 2022

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.

- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

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

Installation Requirements



WARNING

Safe and stable power supply is a prerequisite for proper operation of the device.

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.

Operation Requirements



A suitable operating environment is the foundation for the device to work properly. Confirm whether the following conditions have been met before use.

- Make sure that the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device.

Table of Contents

Foreword	I
Important Safeguards and Warnings.....	III
1 Overview	1
1.1 Introduction	1
1.2 Features.....	1
2 Structure	2
2.1 Dimensions	2
2.2 Front Panel.....	2
2.3 Rear Panel.....	4
3 Installation and Wiring	5
3.1 Installation Position	5
3.2 Installing the Module.....	5
3.3 Cable Connection.....	6
3.3.1 Local Alarm Input Cable Connection	7
3.3.2 Local Alarm Output Cable Connection	8
3.3.3 Power Port Wiring	9
4 ConfigTool Operations	11
4.1 Initializing the Device.....	11
4.2 Modifying IP Address.....	13
4.2.1 Modifying One IP	14
4.2.2 Modifying IP in Batches	14
4.3 Rebooting the device.....	15
4.4 Restoring the Device.....	16
4.4.1 Restoring to Default Configurations.....	16
4.4.2 Restoring to Factory Configurations	16
4.5 Modifying Device Password	17
5 Web Operations.....	19
5.1 Adding Expansion Module.....	19
5.1.1 Quick Adding	19
5.1.2 Manually Adding.....	20
5.2 Adding Wireless Device	20
5.2.1 Web Pairing	20
5.2.2 Manually Pairing	21
5.3 Testing Wireless Device Signal	21
5.4 Modifying Wireless Device Configuration	22

5.5 Alarm Configuration	23
5.6 Remote Upgrading of Expansion Module	23
5.6.1 WEB Upgrade	23
5.6.2 ConfigTool Upgrade	24
5.6.2.1 Upgrading One Device	24
5.6.2.2 Upgrading Devices in Batches	24
5.7 Wireless Device Remote Upgrade	25
6 FAQ	26
Appendix 1 Cybersecurity Recommendations	27

1 Overview

1.1 Introduction

This product is mainly used to connect wireless devices to a wired control panel, it communicates with wireless devices via 433 MHz or 868 MHz RF signal, and communicates with wired control panel via wired network signal, which makes the installation and deployment of the security system more convenient and lower cost, especially suitable for some projects that have been completed but need to increase zones later.

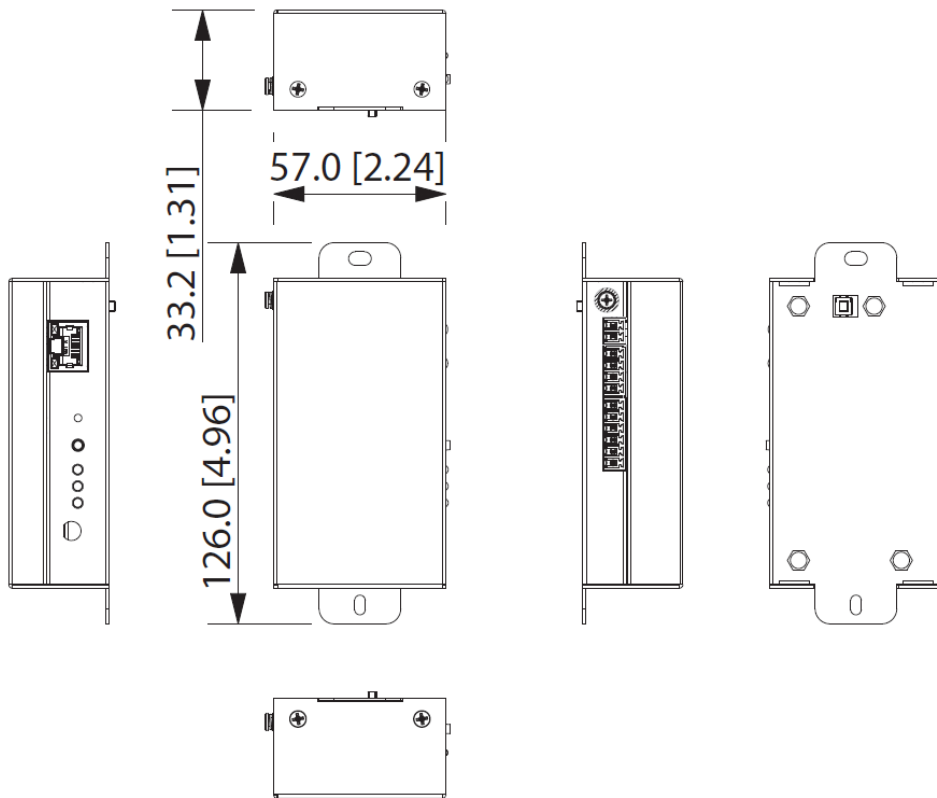
1.2 Features

- Supports 12 VDC power supply and standard PoE power supply.
- Supports local 2-channel alarm input, and 2-channel relay output.
- Supports multiple zone loop types (NO/NC, 1EOL, 2EOL, 3EOL).
- Supports EOLR values (2.7 K, 4.7 K, and 6.8 K)
- Supports converting wireless signal data into TCP/IP networking data and sending it to alarm control panel.
- Supports offline caching.
- Supports access and management of multiple wireless detectors and accessories.
- External wireless antenna with long wireless communication distance.
- Supports remote update.
- Supports connecting up to 16 wireless devices (up to 6 sirens).

2 Structure

2.1 Dimensions

Figure 2-1 Dimensions (unit: mm [inch])



2.2 Front Panel

The front panel includes antenna, indicator, button and network port.

Figure 2-2 Front panel

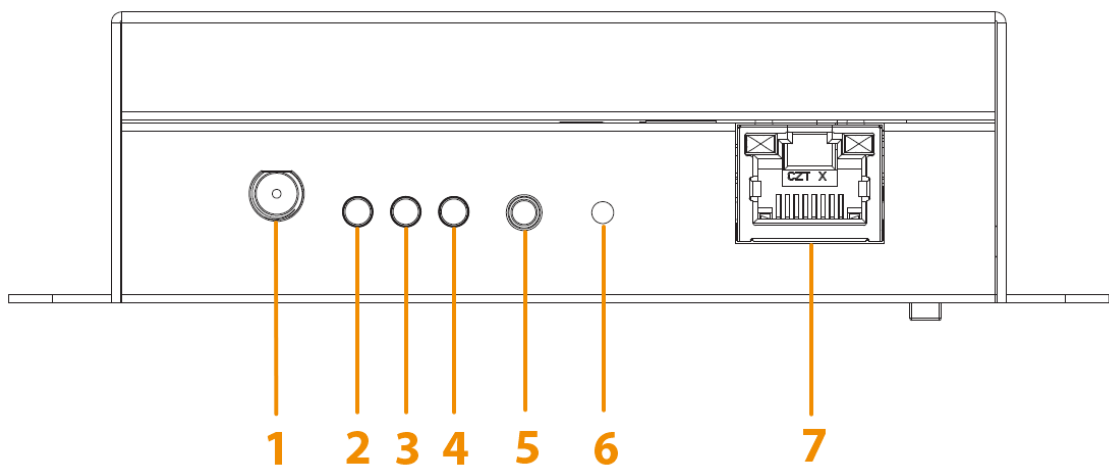






Table 2-1 Description of front panel ports

No.	Icon	Name	Description
1	-	Antenna	The antenna is used to receive wireless data.
2		Power indicator	After the device is powered on normally, the indicator light is solid red.
3		Wireless indicator	When the wireless communication status is normal, the green light is solid on; when the wireless device is offline, the green light flashes.
4		Pairing indicator	The light is off by default. When the module enters pairing mode, the green light flashes.
5	Pair	Pairing button	Button for wireless pairing. Double-click the button to enter the wireless pairing mode.
6	RST	Restore to factory configuration button	Press and hold the button for more than 5 s to restore the device to factory default settings.  After the factory configurations are restored, the pair indicator and wireless indicator flash 5 times at the same time.
7	-	Network port	10 Mbps/100 Mbps adaptive Ethernet port, supporting standard PoE power supply.

2.3 Rear Panel

The rear panel of the device includes power port, alarm input port and relay output port.

Figure 2-3 Rear panel

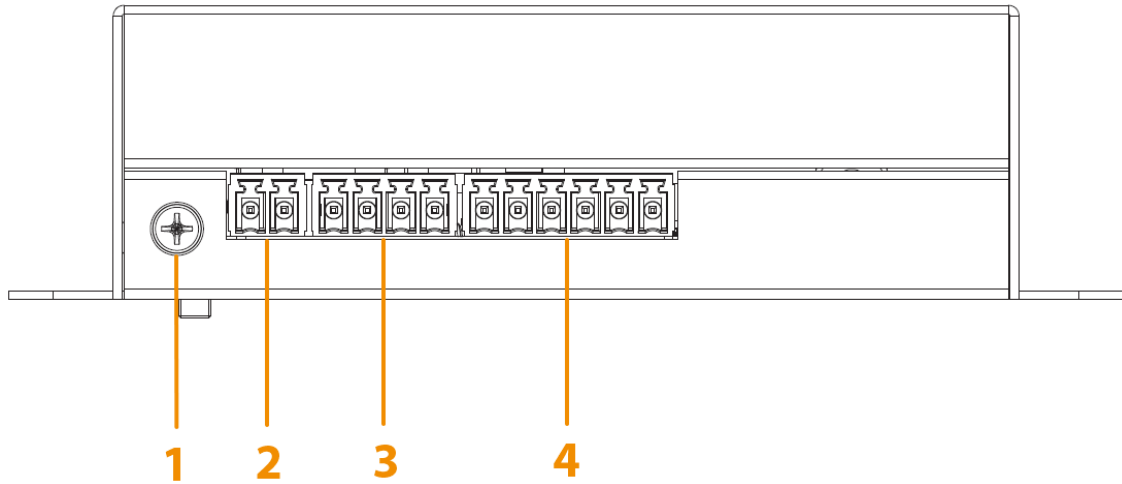



Table 2-2 Real panel ports description

No.	Name
1	Ground screw.  The installation of device must be grounded.
2	12 VDC power port.
3	Alarm input port.
4	Relay output port.

3 Installation and Wiring

3.1 Installation Position

- Do not affect the normal operation of the device, try to stay away from radiation sources such as heat sources or electromagnetic fields, locations that are prone to water leakage, and power inlets and outlets.
- Do not install the device in rooms with corrosive acid and alkaline gases.
- Do not affect the normal operation and maintenance of other devices, and do not occupy maintenance and exit corridors, and reserved places for devices.
- Do not install the device in a closed cabinet; otherwise, antenna signal receiving might be affected.
- The device should be installed far away from the interference sources that affect wireless receiving and transmission, such as steel plates and iron doors.
- The wiring of the device should be kept away from strong electricity.

3.2 Installing the Module

- Step 1 Open the package box, and then take out the plastic expansion tube and self-tapping screws.
- Step 2 Select the mounting location, and then dig 2 holes on the wall.
- Step 3 Insert the plastic expansion tube into the holes, and then fix the device with the self-tapping screws.
- Step 4 Screw in the device antenna, and then adjust the antenna direction.

Figure 3-1 Installing the module

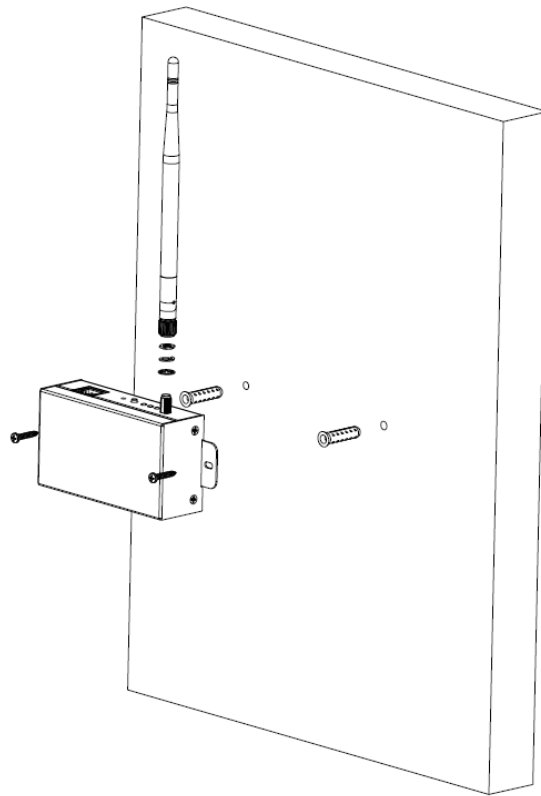
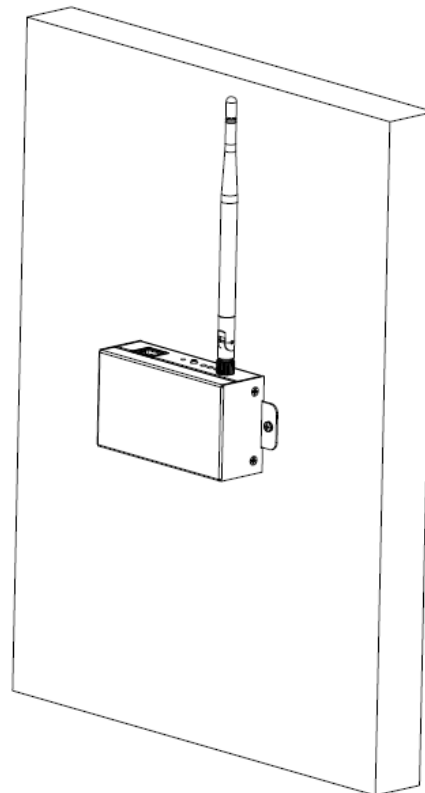


Figure 3-2 Installation complete



3.3 Cable Connection

3.3.1 Local Alarm Input Cable Connection

The device provides 2-channel alarm input port, supports normally open and normally closed access modes, and supports three resistance values of 2.7K, 4.7K and 6.8K. It also supports multiple pigtail cable resistance access methods (0EOL, 1EOL, 2EOL, 3EOL).

Figure 3-3 Detector wiring (normally open)

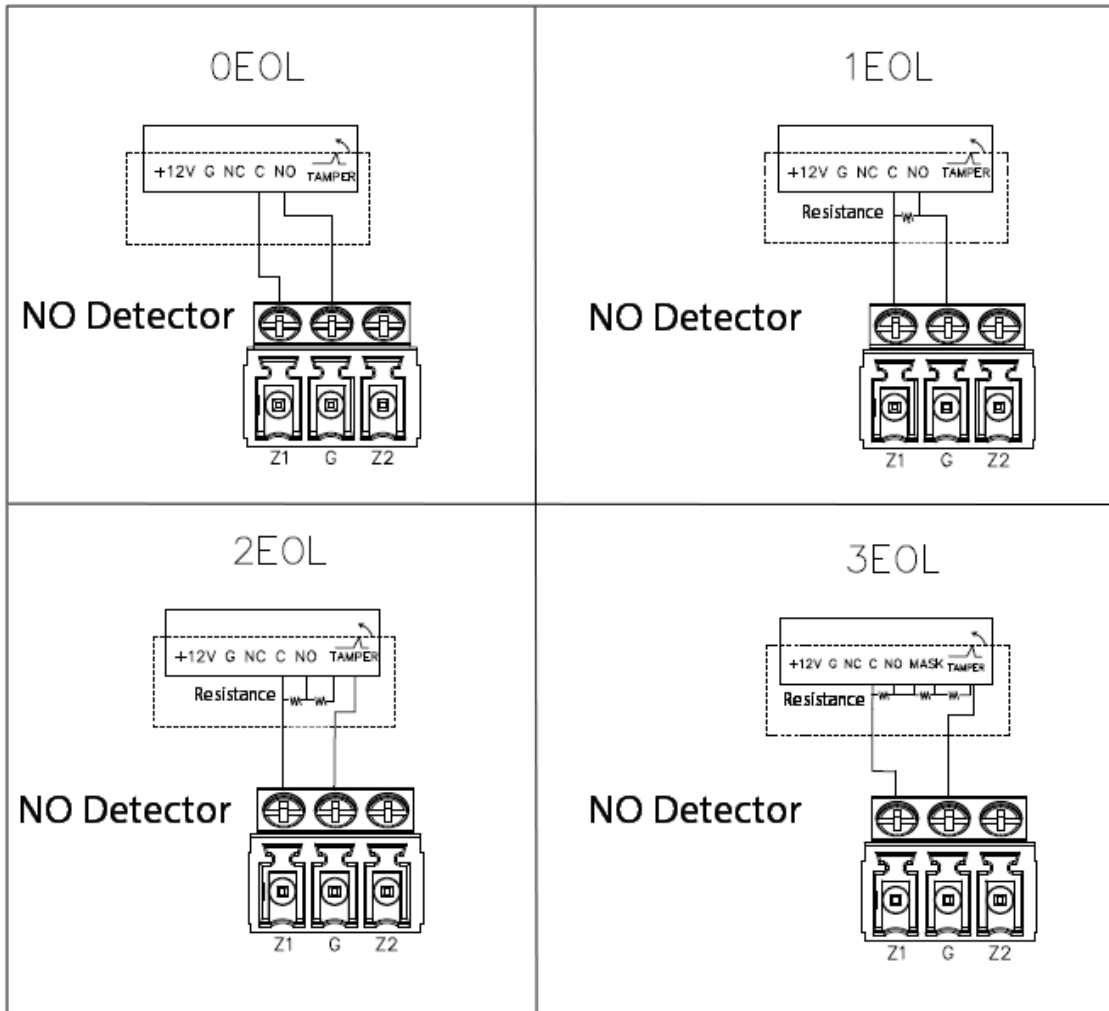
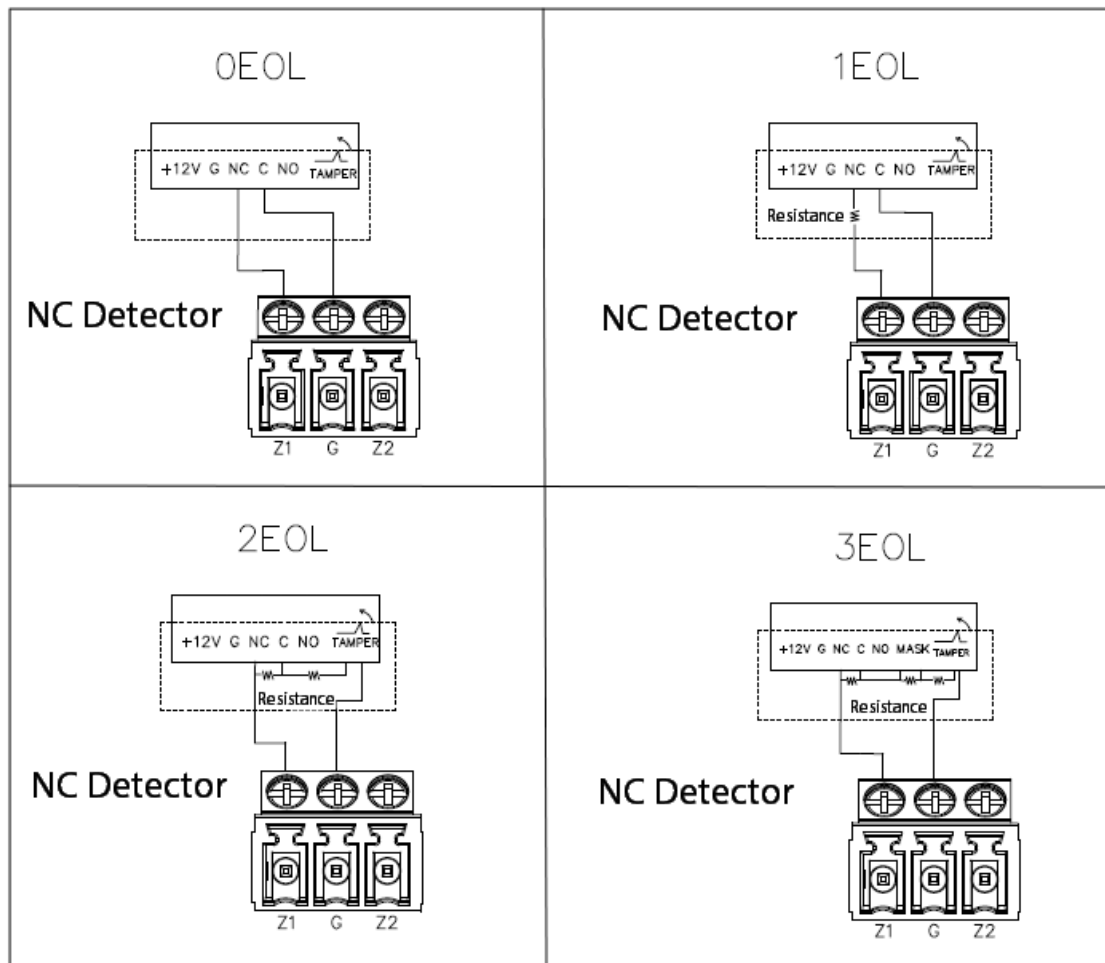


Figure 3-4 Detector wiring (normally closed)



3.3.2 Local Alarm Output Cable Connection

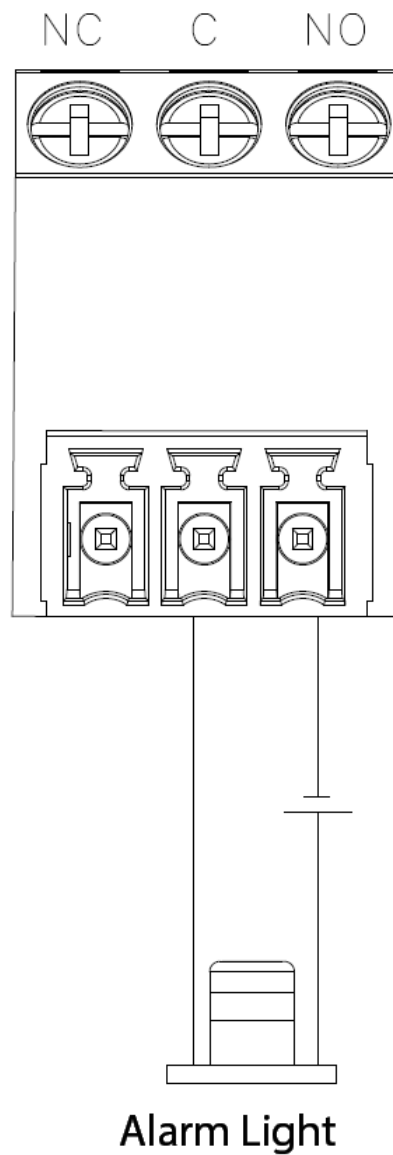


To avoid relay damage from overcurrent, do not connect the alarm output port of the control panel to large power load (no more than 30 VDC/1 A and limited to resistive load). If you need to use large power load or capacitive and inductive load, use a contactor.

Supports 2-channel relay outputs correspond to ports (NO1, C, NC1) - (NO2, C, NC2). The following uses the normally open type of alarm light as an example.

- NC: Normally closed port.
- C: Common port (COM).
- NO: Normally open port.

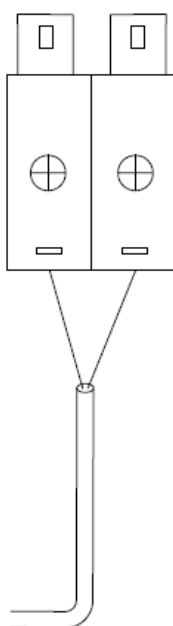
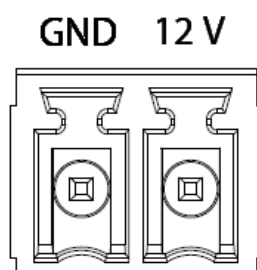
Figure 3-5 Local relay output cable connection



3.3.3 Power Port Wiring

The module supports PoE power supply and 12 VDC separate power supply.

Figure 3-6 Power port wiring



4 ConfigTool Operations

You can use the ConfigTool to initialize the device, modify the IP address and perform other basic operations.



- For the first-time use or after the device is restored to factory defaults, you need to initialize the device.
- Device initialization, modifying device IP address and other operations are available only when the IP address of the device (192.168.1.108 by default) and the computer stay on the same network segment.
- To ensure the device successfully access to network, plan the IP address reasonably based on actual network conditions.

4.1 Initializing the Device

You can initialize one or multiple devices.



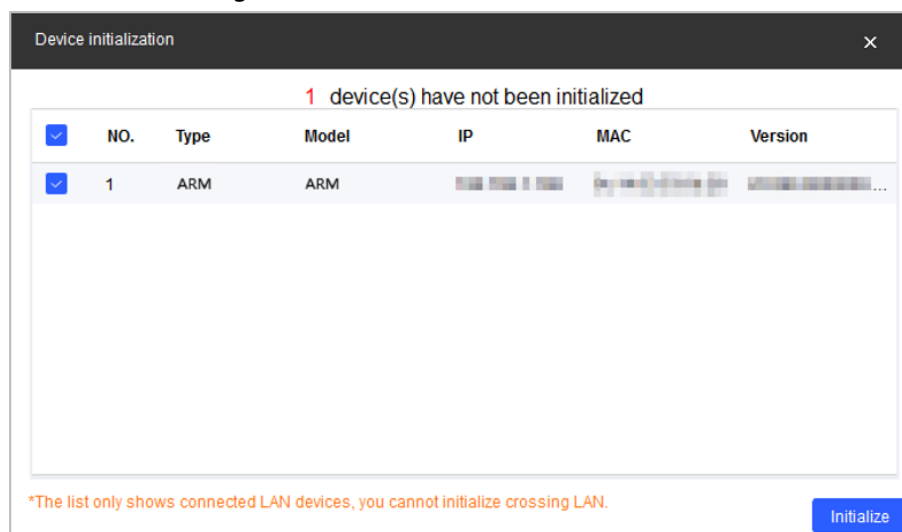
- The initializing operation can only be performed to the devices within the local area network.
- Operations cannot be performed on uninitialized devices, and they do not appear on other pages of the Tool. Please complete device initialization before performing operations on the device, such as upgrading the device.

Step 1 Double-click ConfigTool.exe to open the tool.

Step 2 Click **Modify IP**, select the uninitialized devices, and then click **Initialize**.

Step 3 Select the device to be initialized in the pop-up dialog box, and then click **Initialize**.

Figure 4-1 Device initialization (1)



Step 4 Configure initialization parameters, and then click **Next**.



When initializing devices in batches, initialization is performed in the way supported by the first device.

Figure 4-2 Device initialization (2)

Table 4-1 Device parameters

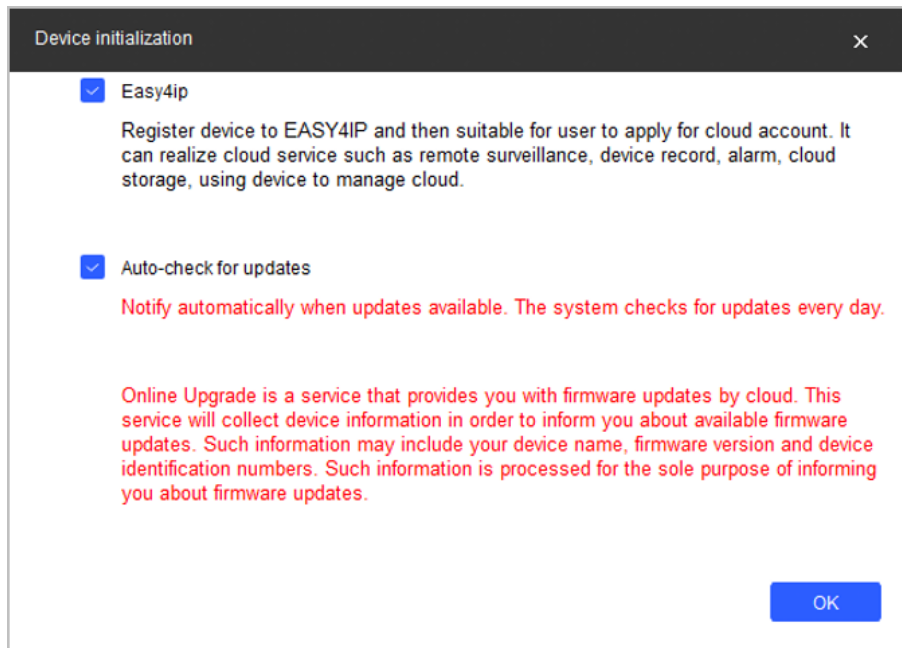
Parameter	Description
Username	The user name is admin by default.
New Password	Enter your new password. A prompt appears to inform you the strength of your new password. <p>The password strength might vary depending on the devices.</p>
Confirm Password	Confirm the new password you have entered.

Step 5 Cancel selecting **Easy4ip** and **Auto-check for updates**, and then click **OK**.



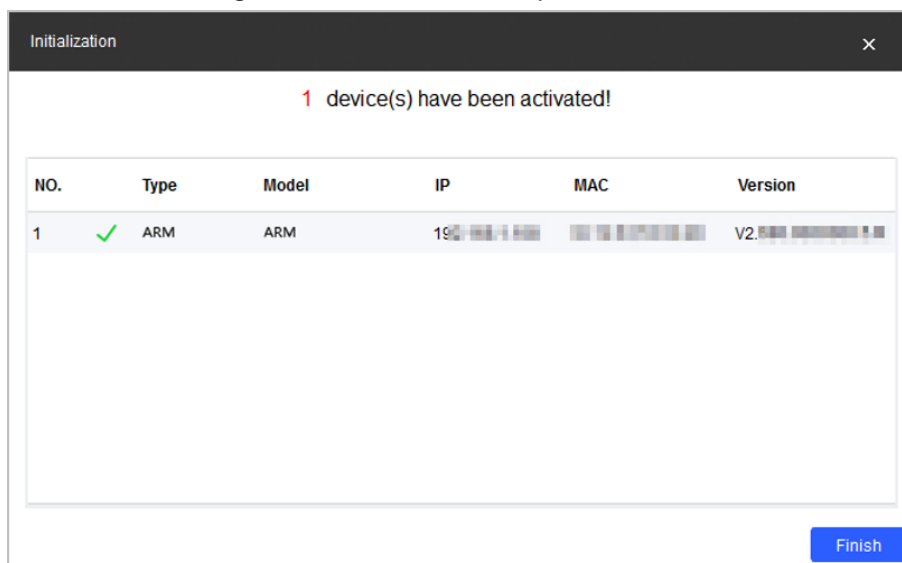
The device does not support automatic detection and Easy4ip at present.

Figure 4-3 Device initialization (3)



Step 6 Click the success icon (✓) or click the failure icon (⚠) for details.

Figure 4-4 Initialization complete



Step 7 Click **Finish**.

After initialization is completed, the status of the devices shows as **Initialized** on the main page of the Tool. The devices also appear on other pages of the Tool.

4.2 Modifying IP Address

You can modify IP for one or more devices at a time.

- When there are only a few devices or the device login passwords are different, you can modify one IP address at one time.
- When there are multiple devices and the device login passwords are the same, you can modify IP addresses in batches.

4.2.1 Modifying One IP

- Step 1 Double-click ConfigTool.exe to open the tool.
- Step 2 Click **Modify IP**, select the device for which you want to modify IP, and then click **Edit**.
- Step 3 Set the **Mode** to **Static**, and then enter the **Target IP**, **Subnet Mask**, and **Gateway**. The IP address of the device will be changed to the one you set.
- Step 4 Click **OK**.

Figure 4-5 Modify IP address

4.2.2 Modifying IP in Batches

- Step 1 Double-click ConfigTool.exe to open the tool.
- Step 2 Click **Modify IP**, select multiple devices, and then click **Batch Modify IP**.



If you need to modify the IP addresses of multiple devices with the same password, you need to enter the correct username and password of the device in **Search Setting** in advance.

- Step 3 Set the **Mode** to **Static**, and then enter the **Target IP**, **Subnet Mask**, and **Gateway**. The IP address of the device will be changed to the one you set.



If you select the **Same IP** checkbox, the IP address of the devices will be set to the same one. We recommend you use the default IP address.

- Step 4 Click **OK**.

Figure 4-6 Modify IP address in batches

4.3 Rebooting the device



Reboot will interrupt operations, reboot the device when it is idle.

- Step 1 Double-click ConfigTool.exe to open the tool.
- Step 2 Click **System Settings**, and then click the **Reboot** tab.
- Step 3 Click ► next to the device type, and then select one or more devices.
- Step 4 Click **Reboot** under the **Manual Reboot** type, and then the device is rebooted immediately.



The device does not support auto reboot.

Figure 4-7 Reboot the device

4.4 Restoring the Device

4.4.1 Restoring to Default Configurations

After the configuration is restored to the default, all information will be restored to the default configuration except:

- Network settings such as IP address.
- All user information, including admin passwords, added users and more.

Step 1 Double-click ConfigTool.exe to open the tool.

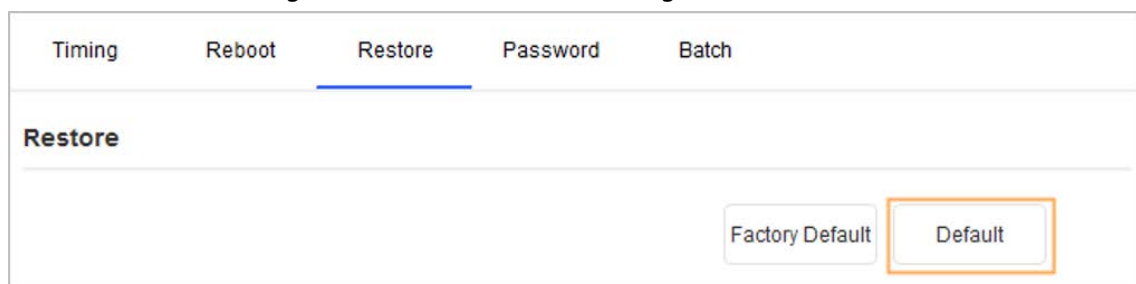
Step 2 Click **System Settings**, click ► next to the device type, and then select one or multiple devices.

Step 3 Click the **Restore** tab.

Step 4 Click **Default**, and then click **OK** to restore to default configurations.

The results are displayed next to the device after restoring is completed. Icon (✓) means success; icon (⚠) means failure and you can click the icon to view the details.

Figure 4-8 Restore to default configurations



4.4.2 Restoring to Factory Configurations

After restoring to factory configurations, all device parameters (including network parameters such as the device IP address) are restored to default factory settings.

Step 1 Double-click ConfigTool.exe to open the tool.

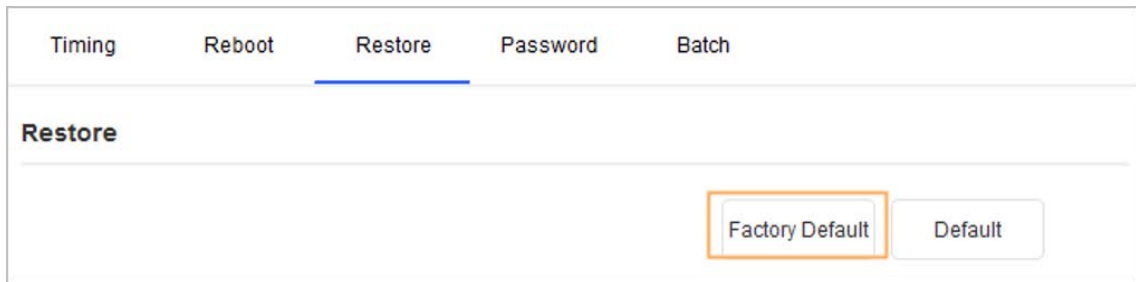
Step 2 Click **System Settings**, click ► next to the device type, and then select one or multiple devices.

Step 3 Click the **Restore** tab.

Step 4 Click **Factory Default**, and then click **OK** to restore to default factory configurations.

The results are displayed next to the device after restoring is completed. Icon (✓) means success; icon (⚠) means failure and you can click the icon to view the details.

Figure 4-9 Restore to factory configurations



4.5 Modifying Device Password

Step 1 Double-click ConfigTool.exe to open the tool.

Step 2 Click **System Settings**, and then click the **Device Password** tab. Click ► next to the device type, and then select one or multiple devices.



If you select multiple devices, the login passwords must be the same.

Step 3 Set the password.

Table 4-2 Password parameters

Parameter	Description
Old Password	Enter the device old password. To make sure that the old password is entered correctly, you can click Check to verify.
New Password	Enter the new password for the device. Follow the password security notice to set a high security level password. <p>The password might vary depending on the devices.</p>
Confirm Password	Confirm the new password.

Step 4 Click **OK** to complete modification.

Figure 4-10 Modifying device password

Modify Password

Old Password	<input type="text"/>	<input type="button" value="Check"/>
New Password	<input type="password"/>	
	<input type="checkbox"/> Weak <input type="checkbox"/> Medium <input type="checkbox"/> Strong	
Confirm Password	<input type="password"/>	<input type="button" value="OK"/>

*After you have set new password, please set password again in "Search setting".

5 Web Operations



This guide only introduces the configuration related to webpage of alarm control panel and the network expansion module. For details on the other configurations on the alarm control panel, see Dahua Alarm Controller User's Manual.

5.1 Adding Expansion Module

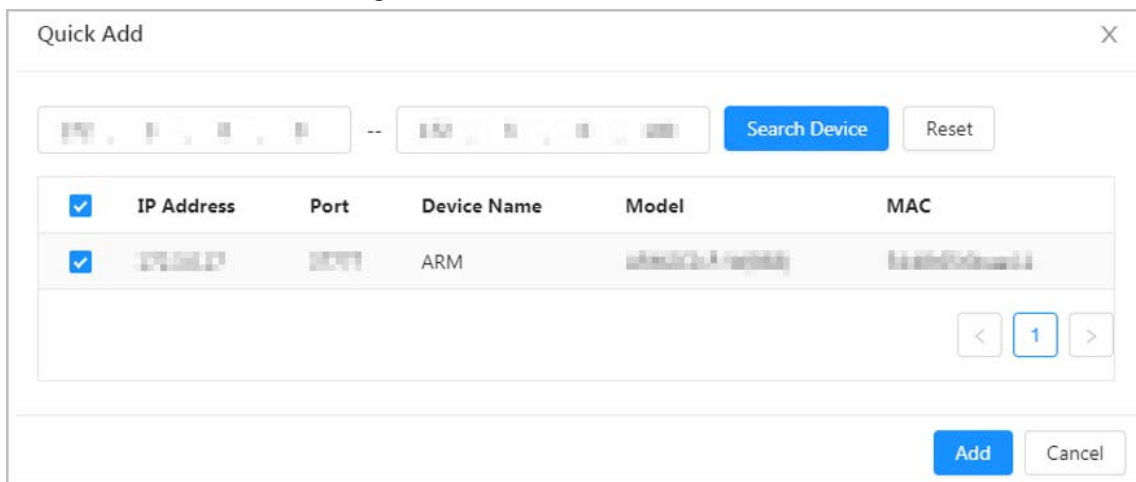
Network expansion module supports quick adding and manually adding.

5.1.1 Quick Adding

Step 1 Log in to the webpage, and then select **System > Peripheral > Network Module**.

Step 2 Click **Quick Add**, enter the IP address of the network segment, and then click **Search Device**.

Figure 5-1 Search the device



<input checked="" type="checkbox"/>	IP Address	Port	Device Name	Model	MAC
<input checked="" type="checkbox"/>	192.168.1.100	8077	ARM	ARM-2012-01-01	88:88:88:88:88:88

Step 3 Select the device, and then click **Add**.

Step 4 Enter the username and password of the device, and then click **OK**.

Figure 5-2 Enter the password

Dialog box titled "Password" with a close button (X). It contains two input fields: "Username" (value: admin) and "Password" (masked with dots). At the bottom right are "OK" and "Cancel" buttons.

5.1.2 Manually Adding

- Step 1 Log in to the webpage, and then select **System > Peripheral > Network Module**.
- Step 2 Click **Manual Add**, enter the device name, IP address, port, username and password, and then click **OK**.

Figure 5-3 Manually adding


Dialog box titled "Manual Add" with a close button (X). It contains five input fields: "Name", "IP Address" (with dots), "Port" (value: 37777), "Username" (value: admin), and "Password" (masked with dots). At the bottom right are "OK" and "Cancel" buttons.

5.2 Adding Wireless Device

Wireless device adding supports web pairing and manually pairing.

5.2.1 Web Pairing

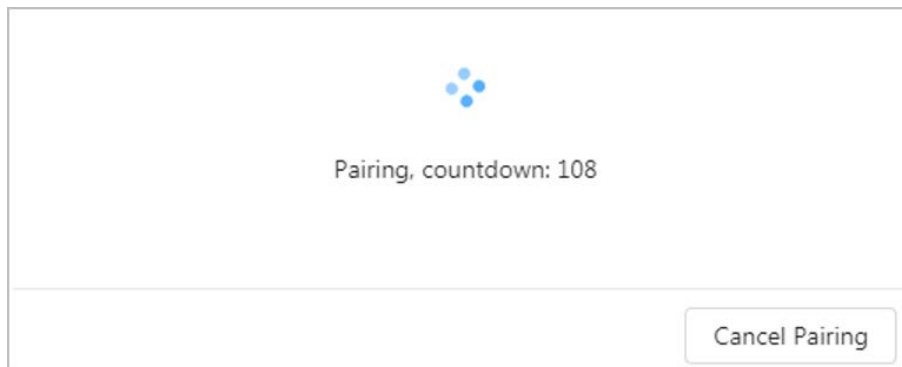
- Step 1 Log in to the webpage, and then select **System > Peripheral > Network Module**.

- Step 2 Select the module to be paired, and then click .
- Step 3 After the module starts pairing, the pair indicator flashes, and the wireless device enters pairing mode.



Each wireless device has a different mode to enter the pairing mode. For details, see the manual of each wireless device.

Figure 5-4 Web pairing



- Step 4 Click **OK** to complete pairing or click **Pair More** to continue pairing the next device.

5.2.2 Manually Pairing

- Step 1 Double-click the pairing button on the expansion module device.



If the control panel is armed, the module is offline, or other network modules on the control panel are pairing, you cannot enter the pairing mode by pressing the button.

- Step 2 Configure the wireless device to the pairing mode.



Each wireless device has a different mode to enter the pairing mode. For details, see the manual of each wireless device.

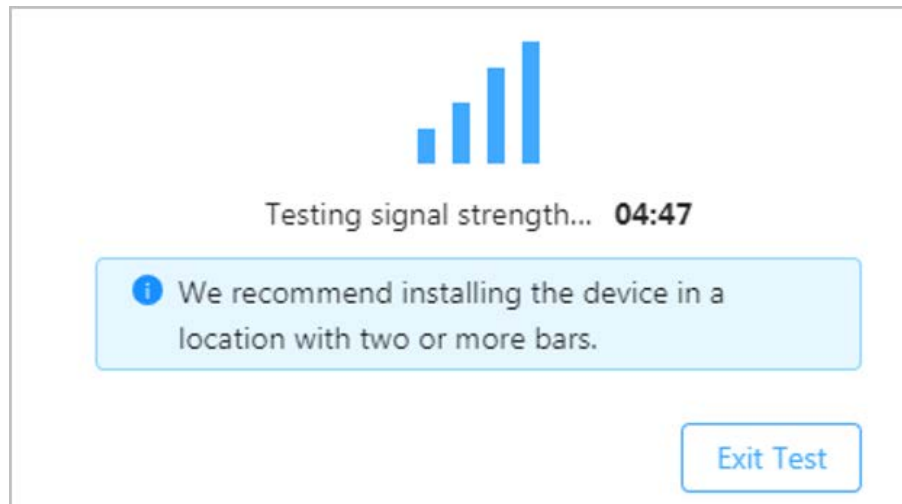
- Step 3 Log in to the webpage, and then select **System > Peripheral > Wireless Device** to check whether the device has been added successfully.

5.3 Testing Wireless Device Signal

Before installing the device, perform wireless device signal test to find the best installation location.

- Step 1 Log in to the webpage, and then select **System > Peripheral > Wireless Device**.
- Step 2 Select the added device, and then click **Check**.

Figure 5-5 Wireless device signal testing



- Step 3** Move the wireless device to the target installation position, and then log in to the webpage to check the signal strength.

5.4 Modifying Wireless Device Configuration

Each wireless device supports modifying some wireless parameters through webpage, including LED enablement, PIR sensitivity, alarm volume, and more. The following uses alarm light as an example to describe how to modify the configuration of wireless devices.


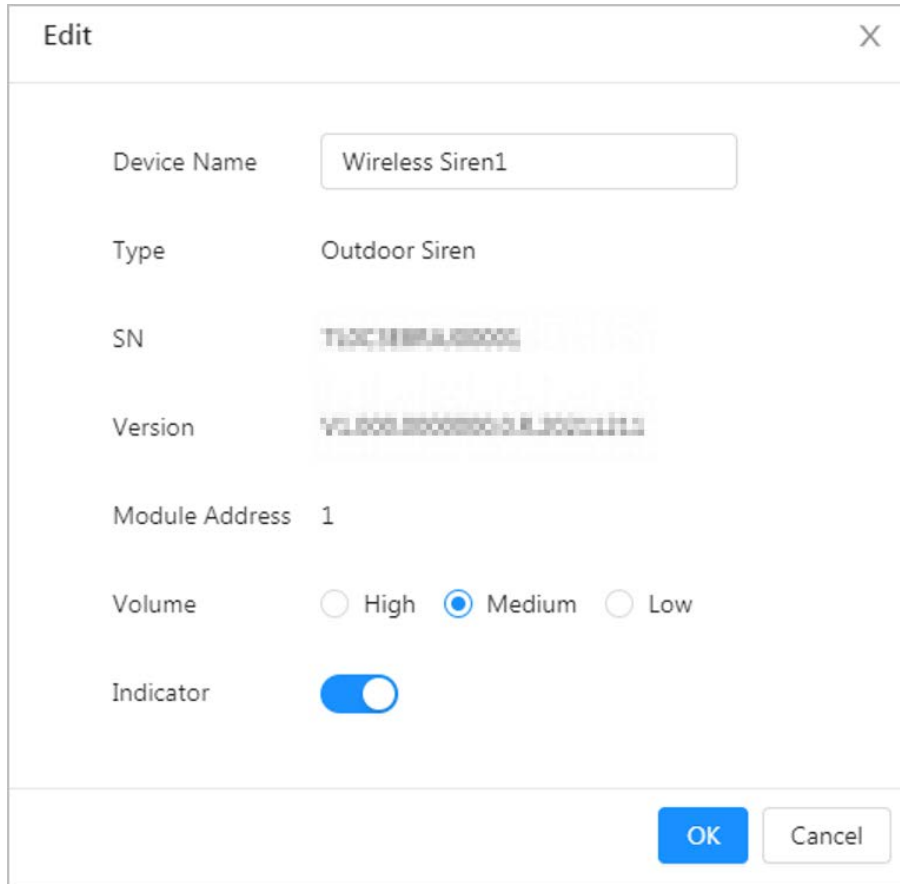
- Step 1** Log in to the webpage, and then select **System > Peripheral > Wireless Device**.
- Step 2** Select the added device, and then click .
- Step 3** Modify device configurations, and then click **OK**.

Figure 5-6 Modify wireless device configuration



Device Name	Wireless Siren1
Type	Outdoor Siren
SN	T10C1E1B1A100000
Version	V1.000.00000000.0.R.00001111
Module Address	1
Volume	<input type="radio"/> High <input checked="" type="radio"/> Medium <input type="radio"/> Low
Indicator	<input checked="" type="checkbox"/>

5.5 Alarm Configuration

The extended protection zones, wireless devices and wireless accessories of the alarm control panel accessed through the network module can be configured as protection zones, relays and sirens and more. For details on the specific configuration, see *Dahua Alarm Control Panel User's Manual*.

5.6 Remote Upgrading of Expansion Module

The network module can be remotely upgraded through the alarm control panel webpage or ConfigTool.

5.6.1 WEB Upgrade

- Step 1 Log in to the webpage, select **System > Update**.
- Step 2 Select the **Type** as **Network Module Update**, and then select the module address.
- Step 3 Click **Browse** to select the update file, and then click **Update**.

Figure 5-7 WEB upgrade

5.6.2 ConfigTool Upgrade

You can upgrade device individually or in batches.



- If the device disconnects during update, the device might restart and automatically tries to update again.
 - ◇ If the system notices **Upgraded successfully**, search the devices again and the devices with upgraded versions show up.
 - ◇ If the system notices **Wait for retry**, wait for 1 - 2 minutes and then retry.
 - ◇ If the system notices **Upgrade overtime** or **Failed to upgrade**, search the device and upgrade again.
- When the network module is added to the alarm control panel and the control panel system is in the defense state, the module cannot be upgraded by the ConfigTool.

5.6.2.1 Upgrading One Device

Step 1 Double-click ConfigTool.exe to open the tool.






Step 2 Click **Device Upgrade**, click  next to the device that you want to upgrade. Select the specific file that needs to be upgraded, and then click **Open**.

Figure 5-8 Upgrade one device

<input type="checkbox"/>	NO.	Model	IP	Version	Upgrade File Path	Operate
<input type="checkbox"/>	1	VT-XXXXXX	192.168.1.100	V1.0.0.0		
<input type="checkbox"/>	2	VT-XXXXXX	192.168.1.101	V1.0.0.0		

Step 3 Click  to start upgrading.

After upgrade is complete, a **Prompt** dialog box will be displayed indicating the device will be restarted, and then the device restarts automatically.

5.6.2.2 Upgrading Devices in Batches

You can upgrade multiple devices in the same software version.

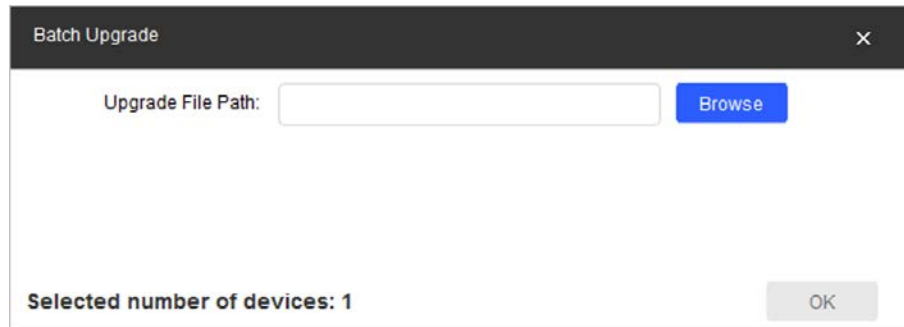
Step 1 Double-click ConfigTool.exe to open the tool.

Step 2 Click **Device Upgrade**, select the devices that need to be upgraded, and then click **Batch**

Upgrade.

The device selected must be upgraded to the same software version.

Figure 5-9 Batch upgrade



Step 3 Click **Browse** to select the files that need to be upgraded.

Step 4 Click **OK**.

5.7 Wireless Device Remote Upgrade

The wireless device connected to the alarm control panel through the network module can remotely upgrade the wireless device through the webpage of alarm control panel.

Step 1 Log in to webpage, select **System > Update**.

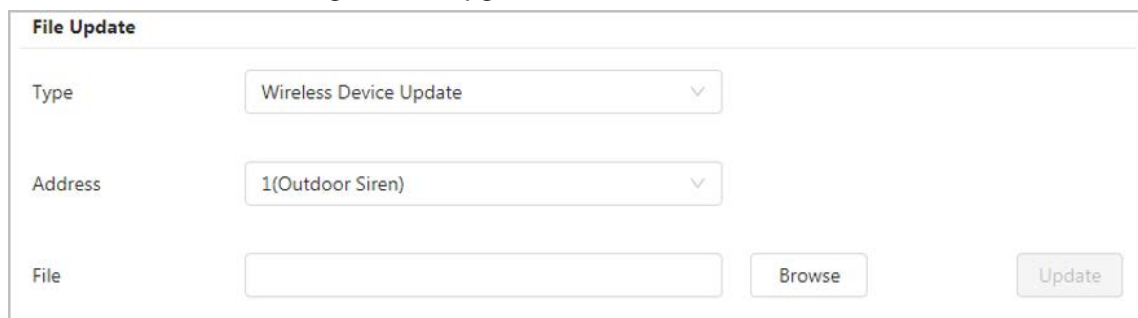
Step 2 Select the **Type** as **Wireless Device Update**, and then select the module address.

Step 3 Click **Browse** to select the update file, and then click **Update**.



For keyfobs and emergency button devices, you need to manually press the button to upgrade the device.

Figure 5-10 Upgrade wireless device



6 FAQ

1. **The module cannot be paired manually.**
 - The control panel system is armed.
 - The network of the module is offline.
 - Other modules in the control panel are in pairing mode.
 - This module cannot enter pairing mode when the detector under this module is in the upgrade process.
2. **The module cannot pair with the wireless device.**
 - The module is too far away from the wireless device.
 - The wireless device has been paired with other devices in this environment.
 - The battery of the wireless device is low.
3. **The alarm control panel cannot receive wireless device alarms normally.**
 - The network is abnormal, and the module is offline on the control panel.
 - The installation location of the alarm control panel is too far away and exceeds the wireless transmission range.
 - There are wireless interference sources in the environment.
 - The wireless device is not added to the protection zone.
4. **The wireless devices are frequently online and offline.**
 - There are wireless interference sources in the environment, resulting in shorter communication distances.
 - The battery of the wireless device is low.
 - The module antenna is obscured by interference.
5. **Forget the login password of the module.**

Restore to the factory settings, initialize the device, and then reset the password.
6. **Forget the IP address of the module.**

Restore to the factory settings, initialize the device, and then modify IP address.

Appendix 1 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 from Dahua 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.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

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