Wireless Siren

User's Manual



V1.0.0

Supplied by INFRONT TECHNOLOGIES

Phone 1300 736 970

sales@infronttech.com.au · infronttech.com.au

For more information call or email — Australia-wide sales, technical support and warranty service.

Foreword

General

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

Safety Instructions

The following categorized signal words with defined meaning 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.	January 2021

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

INFRONT TECHNOLOGIES
Supplied by INFRONT TECHNOLOGIES
Phone 1300 736 970
sales@infronttech.com.au · infronttech.com.au
For more information call or email — Australia-wide sales, technical support and warranty service.

Important Safeguards and Warnings

The following description is the correct application of the device. Please read the manual carefully before use to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.

Operating Requirements

- Do not place and install the device in an area exposed to direct sunlight or near heat generating device.
- Do not install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- Transport, use and store the device within allowed humidity and temperature range.
- Do not place the hub in the places close to radio interference sources, such as metal objects.

Power Requirement

- Use batteries according to requirements; otherwise, it might result in fire, explosion or burning of batteries.
- To replace batteries, use the same type of batteries.
- Use electric wires (power wires) recommended by this area, which shall be used within its rated specification.
- Use standard power adapter matched with this device. Otherwise, the user must undertake resulting personnel injuries or device damages.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, refer to device labels.
- Products with category I structure shall be connected to grid power output socket, which is equipped with protective grounding.
- Appliance coupler is a disconnecting device. During normal use, please keep an angle that facilitates operation.
- Use the accessories regulated by the manufacturer. The device must be installed and maintained by professionals.

INFRONT TECHNOLOGIES
Supplied by INFRONT TECHNOLOGIES
Phone 1300 736 970
sales@infronttech.com.au · infronttech.com.au
For more information call or email — Australia-wide sales, technical support and warranty service.

Table of Contents

Foreword I
Important Safeguards and Warnings II
1 Introduction 1
2 Checklist 2
3 Design 3
3.1 Appearance 3
3.2 Dimensions 4
4 Connecting to the Hub 5
5 Installation 6
6 Wireless Siren Configuration 7
6.1 Configuring the Siren 7
6.2 Viewing Status of the Siren 7
Appendix 1 Cybersecurity Recommendations 9

INFRONT TECHNOLOGIES
Supplied by INFRONT TECHNOLOGIES
Phone 1300 736 970
sales@infronttech.com.au · infronttech.com.au
For more information call or email — Australia-wide sales, technical support and warranty service.

1 Introduction

Wireless siren is an indoor siren that loudly alarms when an alarm event occurs. It features danger warning and intrusion determent.

INFRONT TECHNOLOGIES
Supplied by INFRONT TECHNOLOGIES
Phone 1300 736 970
sales@infronttech.com.au · infronttech.com.au
For more information call or email — Australia-wide sales, technical support and warranty service.

2 Checklist

Check the package according to the following checklist. If you find device damage or any loss, contact the after-sales service.

Figure 2-1 Checklist

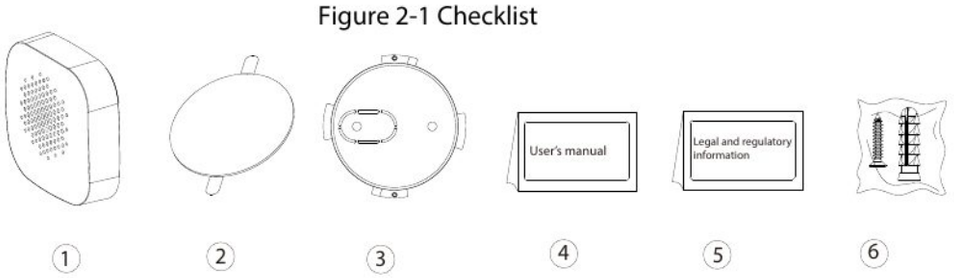


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Wireless siren	1	4	User' manual	1
2	Double-sided adhesive tape	1	5	Legal and regulatory information	1
3	Attachment panel	1	6	Screw package	1

INFRONT TECHNOLOGIES
Supplied by INFRONT TECHNOLOGIES
Phone 1300 736 970
sales@infronttech.com.au · infronttech.com.au
For more information call or email — Australia-wide sales, technical support and warranty service.

3 Design

3.1 Appearance

Figure 3-1 Appearance

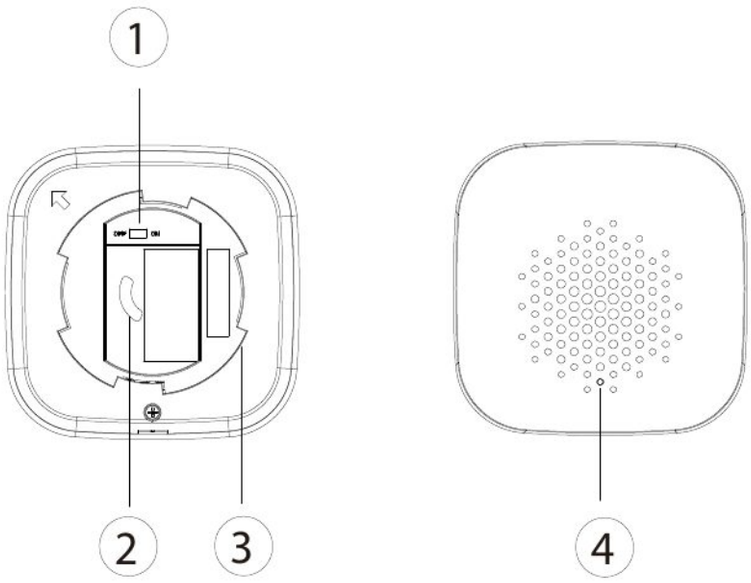


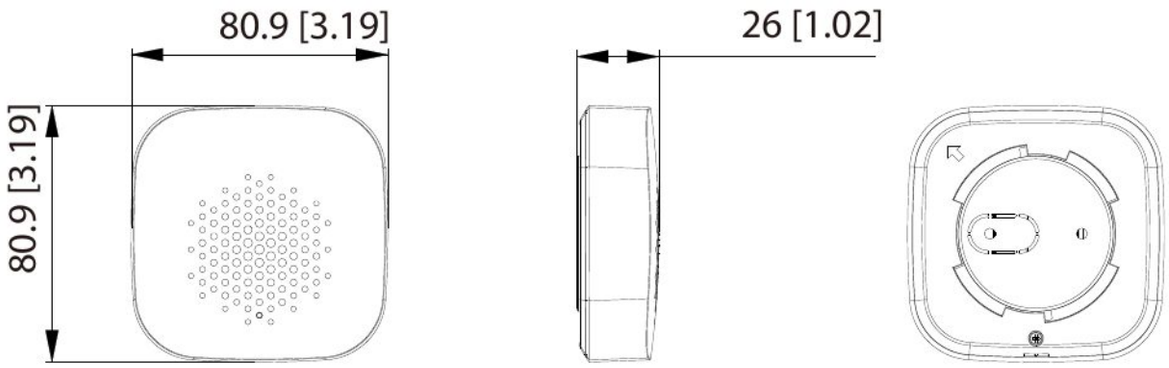
Table 3-1 Structure

No.	Name	Description
1	On/Off button	Turn on or turn off the siren.
2	Tamper button	The tamper mode of the accessory, which reacts to the detachment of the body.
3	Lid	• Normal status: Lid closed. • Abnormal status: Lid open.
4	Indicator	• Flashes green quickly: Pairing mode. • Solid green: Alarm event is triggered. • Shows green every 3 seconds: Arming mode.

INFRONT TECHNOLOGIES
Supplied by INFRONT TECHNOLOGIES
Phone 1300 736 970
sales@infronttech.com.au · infronttech.com.au
For more information call or email — Australia-wide sales, technical support and warranty service.

3.2 Dimensions

Figure 3-2 Dimensions (mm[inch])



INFRONT TECHNOLOGIES
Supplied by INFRONT TECHNOLOGIES
Phone 1300 736 970
sales@infronttech.com.au · infronttech.com.au
For more information call or email — Australia-wide sales, technical support and warranty service.

4 Connecting to the Hub

Prior to connection with the hub, install the DMSS App on your phone. Make sure that you have installed the latest version of the App. Interfaces and functions might vary with different added devices, and the actual interface shall prevail. This manual takes iOS as an example.

- Make sure that you have already created an account, and added hub to the application.
- Make sure that the hub has stable internet connection.
- Make sure that the hub is disarmed.

Step 1 Go to the hub interface, and then tap Sensor to add the siren.

Step 2 Tap + to scan the QR code at the bottom of the siren, and then tap **Next**.

Step 3 Tap **Next** after the siren has been found.

Step 4 Follow on-screen instructions and switch the siren to on, and then tap **Next**.

Step 5 Wait for the pairing.

Step 6 Customize the name of the siren, select an area, and then tap **Completed**.

INFRONT TECHNOLOGIES
Supplied by INFRONT TECHNOLOGIES
Phone 1300 736 970
sales@infronttech.com.au · infronttech.com.au
For more information call or email — Australia-wide sales, technical support and warranty service.

5 Installation

Prior to installation, connect the siren to the hub and check the signal level at the installation location. We recommend installing the siren in a place with the signal strength of at least 2 bars.

We recommend installing the siren with expansion screws.

Figure 5-1 Installation

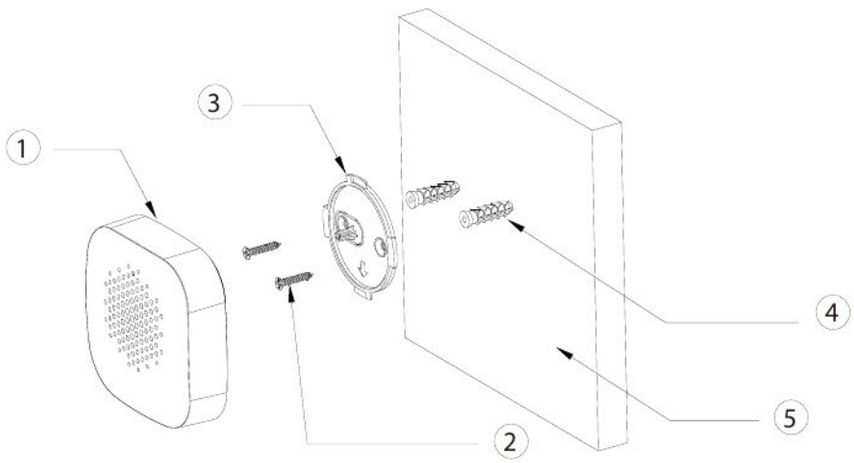


Table 5-1 Installation items

No.	Item name	No.	Item name
1	Wireless siren	4	Expansion bolt
2	ST3 × 18 mm self-tapping screw	5	Wall
3	Attachment panel	—	—

Step 1 Drill 2 holes in wall according to the hole positions of the attachment panel.

Step 2 Put the expansion bolts into the holes.

Step 3 Align the screw holes on the plate with the expansion bolts.

Step 4 Fix the attachment panel with ST3 × 18 mm self-tapping screws.

Step 5 Align the arrow engraved on the rear shell of the siren with the arrow engraved on the attachment panel, and then fix the siren into the attachment panel in the clockwise direction.

INFRONT TECHNOLOGIES
Supplied by INFRONT TECHNOLOGIES
Phone 1300 736 970
sales@infronttech.com.au · infronttech.com.au
For more information call or email — Australia-wide sales, technical support and warranty service.

6 Wireless Siren Configuration

You can view and edit general information of the siren.

6.1 Configuring the Siren

On the **Hub** interface, select the siren as needed from the accessory list, and then you can configure the parameters of the siren.

Table 6-1 Siren parameter description

Parameter	Description
Device Configuration	• View device name, type, SN and device model. • Edit device name, and then tap **Save** to save configuration.
Area	Select the area to which the siren is assigned.
Control Permissions	Select the area over which the siren has control permissions.
Sound Settings	• Configure volume level. • Select from low, medium, and high.
Alarm Duration	• Configure the duration of the alarm sound. • Select from 3 s to 180 s.
Alarm Demand	If enabled, the siren flashes green every three seconds, indicating that the detector is armed now.
Signal Strength Detection	Check the current signal strength.
Speaker Test	Tap **Start Detection** to test the volume level of the alarm.
Transmit Power	• Select from high, low, and automatic. • The higher the transmission power, the farther the transmission and the higher power consuming.
Cloud Update	Update online.

6.2 Viewing Status of the Siren

On the **Hub** interface, select the siren as needed from the accessory list, and then tab ☑ to view the status of the siren.

Table 6-2 Status

Parameter	Description
Temperature	The temperature of the environment.

INFRONT TECHNOLOGIES
Supplied by INFRONT TECHNOLOGIES
Phone 1300 736 970
sales@infronttech.com.au · infronttech.com.au
For more information call or email — Australia-wide sales, technical support and warranty service.

Parameter	Description
Signal Strength	The signal strength between the hub and the siren. • : Ultra low. • : Low. • : Moderate. • : High. • : No.
Battery Level	The battery level of the siren. • : Fully charged. • : Sufficient. • : Moderate. • : Insufficient.
Anti-tampering Status	The tamper mode of the accessory, which reacts to the detachment of the body.
Online Status	Online and offline status of the siren. • : Online. • : Offline.
Volume	Alarm volume level.
Alarm Duration	Duration of the alarm sound.
Alarm Demand	If enabled, the siren warns about the alarm event by the indicator and sound signal.
Enter/Exit Arming and Disarming Ringtone	The ringtone when entering or exiting arming mode.
Program Version	The program version of the siren.

INFRONT TECHNOLOGIES
Supplied by INFRONT TECHNOLOGIES
Phone 1300 736 970
sales@infronttech.com.au · infronttech.com.au
For more information call or email — Australia-wide sales, technical support and warranty service.

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 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**

INFRONT TECHNOLOGIES
Supplied by INFRONT TECHNOLOGIES
Phone 1300 736 970
sales@infronttech.com.au · infronttech.com.au
For more information call or email — Australia-wide sales, technical support and warranty service.

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.

INFRONT TECHNOLOGIES
Supplied by INFRONT TECHNOLOGIES
Phone 1300 736 970
sales@infronttech.com.au · infronttech.com.au
For more information call or email — Australia-wide sales, technical support and warranty service.

You deserve to feel safe, secure & protected

Website: www.watchguardsystems.com.au | Email: sales@watchguardsystems.com.au | Tel: 02 4545 2598

INFRONT TECHNOLOGIES

Supplied by INFRONT TECHNOLOGIES

Phone 1300 736 970

sales@infronttech.com.au · infronttech.com.au

For more information call or email — Australia-wide sales, technical support and warranty service.