# Watchguard™

# Wireless Keyfob
## User's Manual

V1.1.2

# Foreword

## General

This manual introduces the installation, functions and operations of the wireless keyfob (hereinafter referred to as the "keyfob"). Read carefully before using the device, and keep the manual safe for future reference.

## Safety Instructions

The following signal words might appear in the manual.

| Signal Words | Meaning |
|---|---|
| ⚠ DANGER | Indicates a high potential hazard which, if not avoided, will result in death or serious injury. |
| ⚠ WARNING | Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury. |
| ⚠ CAUTION | Indicates a potential risk which, if not avoided, could result in property damage, data loss, 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 |
|---|---|---|
| V1.1.2 | Added battery description. | August 2023 |
| V1.1.1 | Revised battery life. | June 2023 |
| V1.1.0 | • Added technical specifications and field of view.<br>• Updated descriptions of parameters.<br>• Updated images. | January 2022 |
| V1.0.0 | First release. | October 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 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 keyfob, hazard prevention, and prevention of property damage. Read carefully before using the keyfob, and comply with the guidelines when using it.

## Operation Requirements

⚠️

- 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.
- Only use the device within the rated power range.
- 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.

## Installation Requirements

⚠️ WARNING

- Connect the device to the adapter before power on.
- 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.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.

⚠️

- 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.
- Use the power adapter or case power supply provided by the device manufacturer.
- 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  Introduction

## 1.1  Overview

Wireless keyfob is a miniature remote that connects to the hub and controls the alarm system in your home. It works by sending wireless communication signals to the alarm system, which will recognize the signal and then perform the function that is assigned to the area.

## 1.2  Technical Specifications

This section contains technical specifications of the keyfob. Please refer to the ones that correspond with your model.

Table 1-1 Technical specifications

| Type | Parameter | Description |
|---|---|---|
| Port | Indicator Light | 1 × two-color status indicator (green: normal, red: abnormal) |
| | Button | 4 (Home, Away, Disarm, and SOS) |
| Function | Remote Update | Cloud update |
| | Low Battery Alarm | Yes |
| Wireless Parameters | Carrier Frequency | ALM-D1-RC: 433.1 MHz–434.6 MHz |
| | Communication Distance | ALM-D1-RC: Up to 500 m (1,640.42 ft) in an open space |
| | Communication Mechanism | Two-way |
| | Encryption Mode | AES128 |
| | Frequency Hopping | Yes |
| General | Power Supply | CR2032 battery |
| | Battery Voltage | 3 VDC |
| | Min. Voltage | 1.8 VDC |
| | Battery Low Threshold | 2.6 VDC |
| | Battery Restore Threshold | 2.65 VDC |
| | Consumption | Quiescent current 3 uA Max current 50 mA |
| | PS Type | Type C |
| | Battery Life | 3 years |

| Type | Parameter | Description |
|---|---|---|
| | Power Consumption | ALM-D1-RC:<br>Max. 85 mW |
| | Operating Environment | Indoor: –10 ℃ to +55 ℃ (+14 ℉ to +131 ℉)<br>Certified temperature: –10℃ to +40℃ (+14℉ to +104 ℉) |
| | Operating Humidity | 10%–90% (RH) |
| | Product Dimensions | 60.0 mm × 39.5 mm × 15.0 mm (2.36" × 1.56" × 0.59") (L × W × H) |
| | Packaging Dimensions | 135.0 mm × 98.5 mm × 27.8 mm (5.31" × 3.88" × 1.09") |
| | Net Weight | 20 g (0.04 lb) |
| | Gross Weight | 65 g (0.14 lb) |
| | Casing | PC + ABS |
| | ACE Type | Type B |
| Certifications | ALM-D1-RC:<br> CE<br>FCC | |

# 2 Checklist

Figure 2-1 Checklist
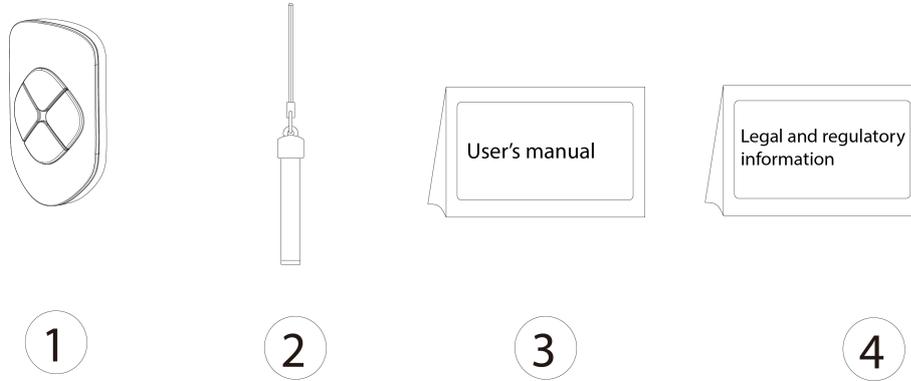


Table 2-1 Checklist

| No. | Item Name | Quantity |
|---|---|---|
| 1 | Wireless keyfob | 1 |
| 2 | String | 1 |
| 3 | User's manual | 1 |
| 4 | Legal and regulatory information | 1 |

# 3 Design

## 3.1 Appearance

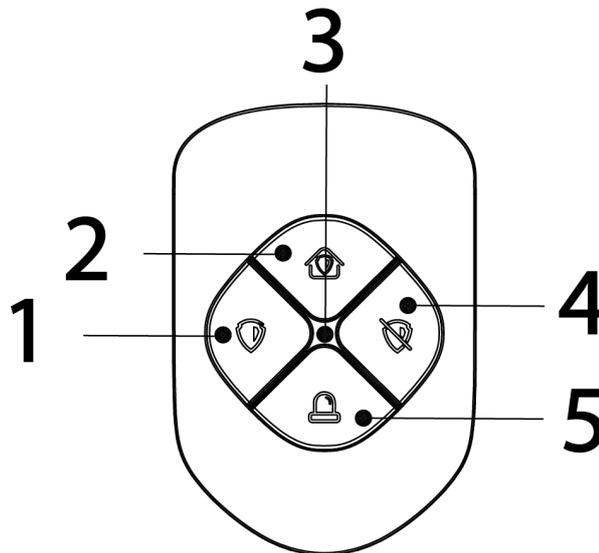Figure 3-1 Appearance
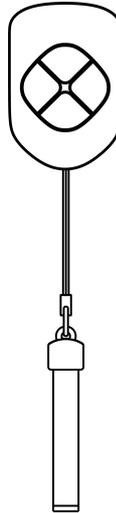


## 3.2 Function Key

Figure 3-2 Function key



Table 3-1 Description of function button

| No. | Name | Description |
|-----|------|-------------|
| 1 | Disarming button | Press the button once to disarm the system. |
| 2 | SOS | Press the panic button, and then the keyfob will send alarm signal to the alarm system. |

| No. | Name | Description |
|---|---|---|
| 3 | Arming button | Press the button once to arm the system. |
| 4 | Home mode | Press the home mode, and then the selected accessories will be armed. |
| 5 | Indicator | <ul><li>Flashes green quickly: Pairing mode.</li><li>Solid green: Normal.</li><li>Solid red: The keyfob is offline.</li><li>Flashes green first, and then turns to red: Connection with the hub failed.</li></ul> |

# 4  Adding the Keyfob to the Hub

## Prerequisites

Device configurations are performed on the DMSS app. Make sure that you have installed the DMSS app, created an account, and added the hub to the app. For details on adding the hub, see the user's manual of the corresponding hub.

- Make sure that the hub has a stable internet connection.
- Make sure that the hub is disarmed.

## Background Information

You can add the keyfob to the hub. This user's manual uses the operations on iOS as an example.

## Procedure

Step 1    Go to the hub screen, and then tap **Peripheral** to add the keyfob.

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

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

Step 4    Follow the on-screen instructions and press [icon] and [icon] once at the same time, and then tap **Next**.

Step 5    Wait for the pairing.

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

# 5 Keyfob Configuration

You can view and edit general information of the keyfob.

## 5.1 Viewing Status

On the hub screen, select a keyfob from the accessory list, and then you can view the status of the keyfob.

Table 5-1 Status

| Parameter | Value |
|---|---|
| Temporary Deactivate | The status for whether the functions of the keyfobs are enabled or disabled.<br><br>●     : Enable.<br><br>●     : Only disable tamper alarm.<br><br>●     : Disable.<br><br>📖<br><br>The function is only available when the version of the DMSS app is 1.96 or later, the hub is V1.001.0000000.6.R.211215 or later, and the PIR is V1.000.0000001.0.R.20211203 or later. |
| Battery Level | The battery level of the keyfob.<br><br>●     : Fully charged.<br><br>●     : Sufficient.<br><br>●     : Moderate.<br><br>●     : Insufficient.<br><br>●     : Low. |
| SOS Status | The status of the SOS alarm. |
| Relay Status | The status of whether the keyfob forwards accessory messages to the hub through the repeater.<br>📖<br><br>The function is only available when the version of the DMSS app is 1.96 or later, the hub is V1.001.0000000.6.R.211215 or later, and the keyfob is V1.000.0000001.0.R.20211203 or later. |
| Program Version | The program version of the keyfob. |

# 5.2 Configuring the Keyfob

On the hub screen, select a keyfob from the peripheral list, and then tap  ☑  to configure the parameters of the keyfob.

Table 5-2 Keyfob parameter description

| Parameter | Description |
|---|---|
| Device Configuration | • View device name, type, SN and device model.<br>• Edit device name, and then tap **Save** to save configuration. |
| Area | • View the existing area.<br>• Add the area that you want to arm, and then tap **Save** to save configuration. |
| Temporary Deactivate | • Tap **Enable** , and then the keyfob will send alarm messages to the hub**Enable** is set by default.<br>• Tap **Only Disable Tamper Alarm**, and then the system will only ignore tamper alarm messages.<br>• Tap **Disable**, and then the keyfob will not send alarm messages to the hub. |
| LED Indicator | **LED Indicator**  is enabled by default on the app. You also need to press any button on the keyfob to enable the function.<br>📖<br>• If **LED Indicator**  is disabled, the LED indicator will remain off regardless of whether the keyfob is functioning normally or not.<br>• The function is only available when the version of the DMSS app is 1.96 or later, the hub is V1.001.0000000.4.R. 211014 or later, and the keyfob is V1.000.0000001.0.R. 20210818 or later. |
| Control Permissions | Select the area over which the keyfob has control permissions. |
| SOS Alarm | If enabled, the SOS alarm messages will be pushed when an alarm event is detected. |
| Siren Linkage | When an alarm is triggered, the accessories will report the alarm events to the hub and alert with siren. |
| Alarm-video Linkage | When an alarm is triggered, the accessories will report the alarm events to the hub and then will be linked with videos. |
| Video Channel | Select the video channel as needed. |
| Cloud Update | Update online.<br>If the latest version is detected, you need to tap **Update** on the app, and then press any button on the keyfob to update the keyfob. |

| Parameter | Description |
|-----------|-------------|
| Delete | Delete the online peripheral. <br> 📖 <br> Go to the hub screen, select the peripheral from the list, and then swipe left to delete it. |

# 6 Using the Keyfob

Maximum connection distance between the keyfob and the hub is 1,500 meters. This distance is reduced by walls, inserted floors and any objects hindering the signal transmission.

After the accessories have been added on the hub, you can operate on the keyfob.

- Press ⬜ and ⬜ once at the same time to connect with the hub.
- Press ⬜ once to enable the away mode, and then all the accessories in the area will be armed.

    Press ⬜ twice if the **System Integrity Check** is enabled in the hub.

- Press ⬜ once to enable the home mode, and then the selected accessories in the area will be armed.
- Press ⬜ once to enable the disarm mode, and then all the accessories in the area will be disarmed.
- Press ⬜ once to enable SOS.

- If the battery is dead, you need to replace the battery.
- Please manually use downward and outward force to open the shell at the buckle position to avoid using tools to open and cause damage to the shell.
- Before you insert the new battery, make sure to press the buttons first, or wait 30 seconds after you take out the old one.

# 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 Watchguard 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 Watchguard's official website (www.watchguardsystems.com.au) for security announcements and the latest security recommendations.

You deserve to feel safe, secure & protected