Watchguard™

Wireless External Siren

User's Manual

V2.0.1

Foreword

General

This manual introduces the installation, functions and operations of the Wireless External Siren (hereinafter referred to as "the siren"). 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
V2.0.1	● Updated technical specifications. ● Updated installation function.	February 2023
V2.0.0	Updated technical specifications.	August 2022
V1.0.1	Updated siren name.	April 2022
V1.0.0	First release.	December 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 device, hazard protection, and protection of property damage. Read carefully before using the device, 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 external siren is a siren that alarms loudly when an alarm event occurs, attracting the attention of everyone within its vicinity. It features danger warning, intrusion determent, and is used in outdoor scenes such as in villas, homes, and on streets.

1.2 Technical Specifications

Please refer to the corresponding technical specifications according to the corresponding models.

Table 1-1 Technical specification

Type	Parameter	Description
Function	Remote Update	Cloud update
	Low Battery Alarm	Yes
	Battery Level Display	Yes
	Tamper	Yes
	Signal Strength	Signal strength detection
	Temperature Measurement	–30 °C to + 70°C (–22 °F to + 158 °F) (outdoor)
Wireless	Carrier Frequency	ALM-D1-SRX: 433.1 MHz–434.6 MHz
	Transmission Power	ALM-D1-SRX: Limit 10 mW
	Communication Distance	ALM-D1-SRX: Up to 1,200 m (3,937.01 ft) in an open space
	Communication Mechanism	Two-way
	Frequency Hopping	Yes
	Encryption Mode	AES128
General	Power Supply Mode	Battery (default), 12 VDC

Type	Parameter	Description
	Battery Model	4 × CR123A
	Battery Voltage	3 VDC
	Min. Voltage	2.6 VDC
	Battery Low Threshold	2.8 VDC
	Consumption	● Quiescent current: 92 uA ● Max. current: 1 A
	PS Type	Type B
	Battery Life	4 CR123A batteries can be used for 3.4 years (if triggered fortnightly and the alarm sounds for 120 s each time with a battery efficiency of 80%)
	Operating Temperature	−25 °C to +60 °C (−13 ℉ to +140 ℉)
	Operating Humidity	10%–90% (RH)
	Product Dimensions	200 mm× 200 mm× 52.5 mm (7.87" × 7.87" × 2.07") (L× W× H)
	Packaging Dimensions	255 mm× 239 mm× 64 mm (10.04" × 9.41" × 2.52") (L× W× H)
	Net Weight	610 g (1.34 lb)
	Gross Weight	920 g (2.03 lb)
	Installation	Wall mount
	Casing	PC + ABS
	Protection	IP65
Technical	Indicator Light	● 1 × green pairing indicator ● 12 × alarm LED group
	Button	1 × power switch
	Scenario	Outdoor/Indoor
	Sound and Light Alarm	Light alarm and multiple alarm sounds, including fire, medical, intrusion, panic, and more.
	Sound Pressure	LAFmax [dB(A)] @ 1m∈[95.2,104.9]

Type	Parameter	Description
Certifications	ALM-D1-SRX: ● FCC ● CE	

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

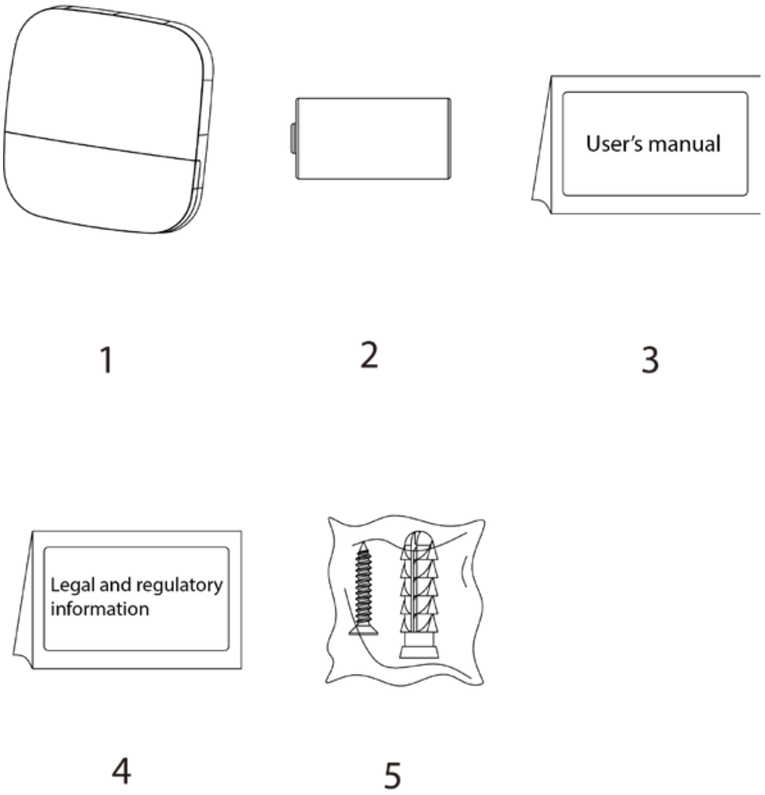


Table 2-1 Checklist

No.	Item	No.	Item
1	Wireless external siren	4	Legal and regulatory information
2	CR123A battery× 4	5	Screw package
3	User's manual	-	-

3 Design

3.1 Appearance

Figure 3-1 Appearance

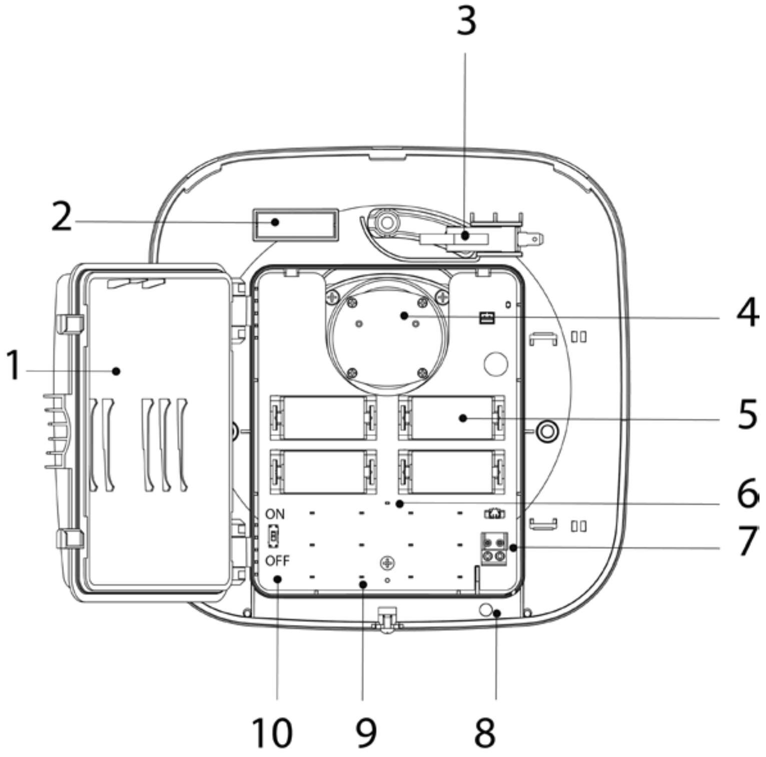
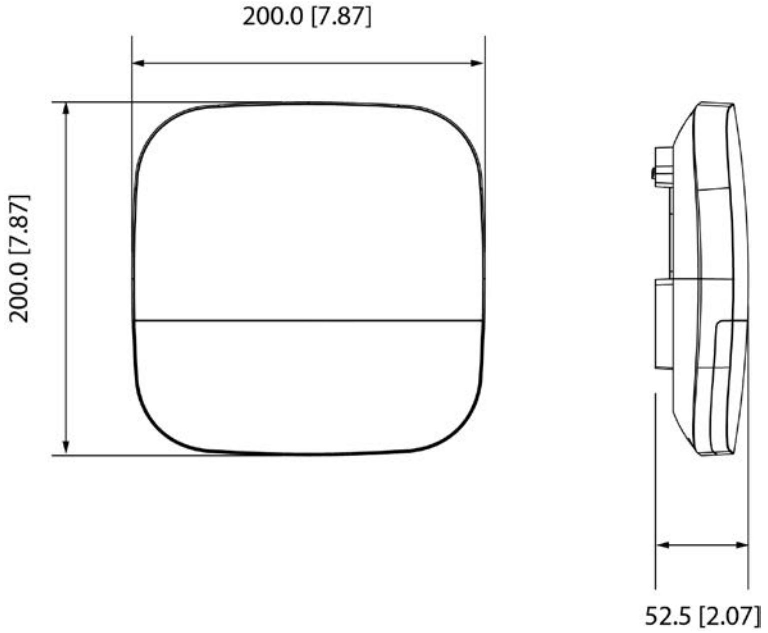


Table 3-1 Structure

No.	Name	Description
1	Waterproof cover	Protects the siren from water and dust.
2	Spirit level	Indicates whether the siren is horizontal and level.
3	Tamper switch	When the tamper switch is released, the tamper alarm will be triggered.
4	Buzzer	Alarms loudly when an alarm event occurs.
5	Battery	Install CR123A batteries according to the polarity mark.
6	Pairing indicator	● Flashes green quickly: Pairing. ● Solid green for 2 seconds: Pairing successful. ● Slowly flashes green for 3 seconds: Pairing failed.
7	12 VDC power terminal	Insert the 12 VDC power cable. 📖 The cable is not included in the package.
8	Power cable knockout	The entry for wiring the power cable.
9	Alarm indicator	Flashes quickly when an alarm event occurs.
10	On/Off switch	Turn on or turn off the siren.

3.2 Dimensions

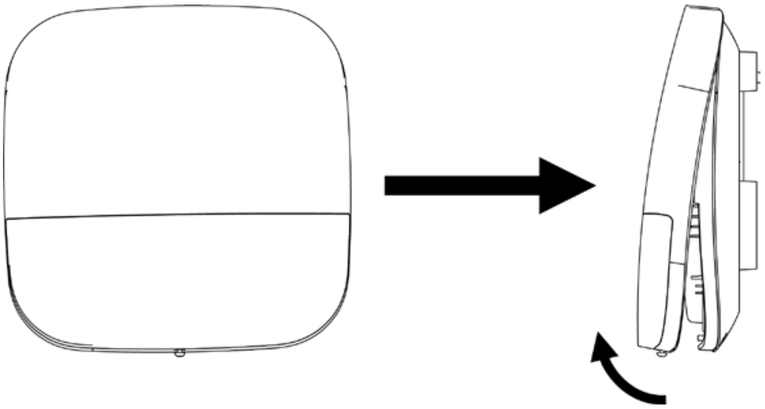
Figure 3-2 Dimensions (mm [inch])



4 Power On

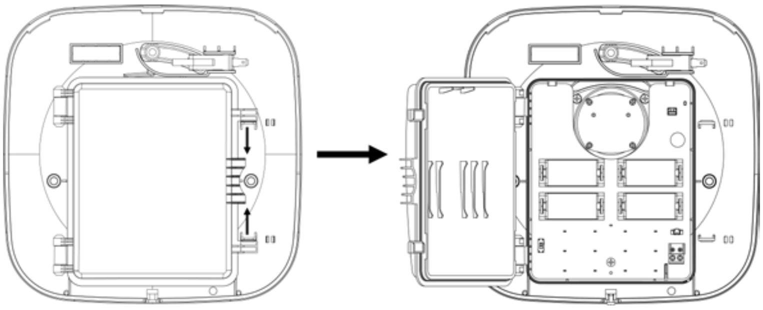
Step 1 Open the front panel of the siren.

Figure 4-1 Open the front panel



Step 2 Open the waterproof cover.

Figure 4-2 Open the waterproof cover



Step 3 Power on.

- Battery power: Install four CR123A batteries according to the polarity mark.
- 12 VDC power (Optional): Feed the 12 VDC power cable into the case through the power cable knockout.

Step 4 Push the power switch to ON.

5 Connecting to the Hub

Before you connect siren to the hub, install the DMSS app to your phone. This manual uses iOS as an example.

- Make sure that the version of the DMSS app is 1.96 or later, and the hub is V1.001.R.211209 or later.
- Make sure that you have already created an account, and added the hub to DMSS.
- Make sure that the hub has a stable internet connection.
- Make sure that the hub is disarmed.

Step 1 Go to the hub screen, and then tap **Peripheral** 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 the 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, and select the area, and then tap **Completed**.

6 Installation

Prior to installation, power on the siren, connect it to the hub, and then check the signal strength of the installation location. We recommend you install the siren in a place with a signal strength of at least 2 bars.

Figure 6-1 Installation

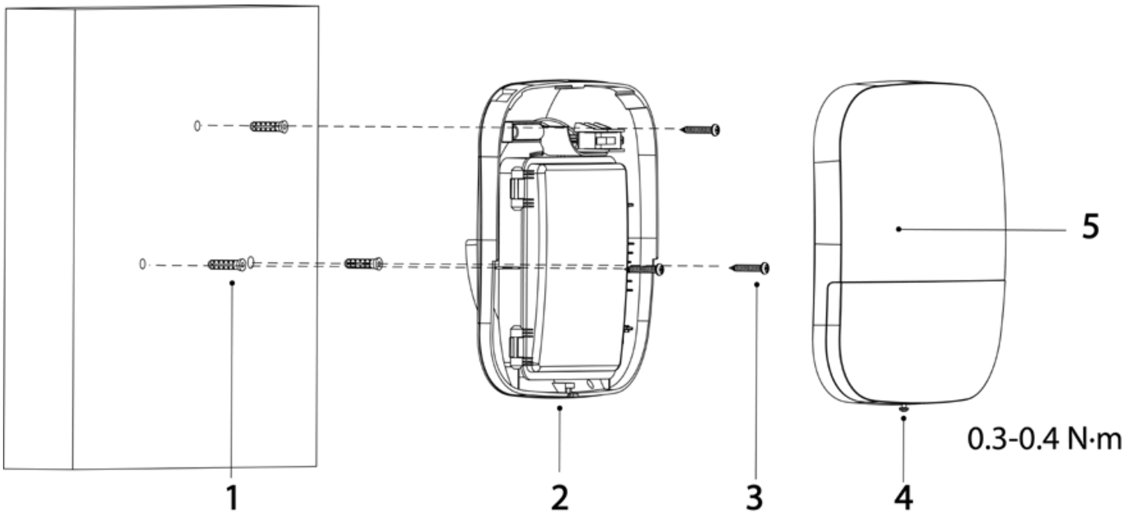


Table 6-1 Installation items

No.	Item Name	No.	Item Name
1	Expansion bolt	4	Screw
2	Rear panel	5	Front panel
3	ST4 × 25 mm self-tapping screw	-	-

Step 1 Loosen the screw at the bottom of the siren to remove the front panel.

Step 2 Set the siren into a horizontal position. Use the spirit level to make sure the siren is horizontal and level.

Step 3 Put the expansion bolts into the holes.

Step 4 Align the screw holes on the rear panel with the expansion bolts.

Step 5 Secure the rear panel with three ST4 × 25 mm self-tapping screws.

Step 6 Tighten the screw at the bottom of the front panel to secure the siren.

7 Configuration

You can view and edit general information of the siren.

7.1 Viewing Status

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

Table 7-1 Status

Parameter	Description
Temporary Deactivate	The status for whether the functions of the siren are enabled or disabled. ● ⓘ : Enable. ● ⓘ : Only disable tamper alarm. ● ⊘ : Disable.
Temperature	The temperature of the environment.
Signal Strength	The signal strength between the hub and the siren. ● 📶 : Low. ● 📶 : Weak. ● 📶 : Good. ● 📶: Excellent. ● 📶: No.
External Power Status	Whether there is a 12 VDC power failure alarm. ● ⊂⊃: Connected. ● ⊂|⊃: Disconnected.
Battery Level	The battery level of the siren. ● 🟦: Fully charged. ● 🟩: Sufficient. ● 🟨: Moderate. ● 🟧: Insufficient. ● 🟥: Low.
Anti-tampering Status	The tamper status of the siren, 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.
Enter/Exit Arming and Disarming Ringtone	The ringtone when entering or exiting arming mode.

Parameter	Description
Beep Volume	High, medium and low.
Transmit through Repeater	The status of whether the siren forwards accessory messages to the hub through the repeater.
Program Version	The program version of the siren.

7.2 Configuring the Siren

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

Table 7-2 Siren parameter description

Parameter	Description
Device Configuration	● View siren name, type, SN and device model. ● Edit siren name, and then tap **Save** to save your configurations.
Area	Select the area to which the siren is assigned.
Temporary Deactivate	● Tap **Enable**, and then the function of the siren will be enabled. **Enable** is set by default. ● Tap **Only Disable Tamper Alarm**, and then the system will only ignore tamper alarm messages. ● Tap **Disable**, and then the function of the siren will be disabled.
Control Permissions	Select areas to which the siren will be linked when an alarm is triggered.
External Power Detection	If **External Power Detection** is enabled, power failure alarm messages will be pushed to the DMSS.
LED Indicator	**LED Indicator** is enabled by default. For details on indicator behavior, see "3.1 Appearance". If **LED Indicator** is disabled, the LED indicator will remain off regardless of whether the siren is functioning normally or not.
Sound Settings	● Configure volume level of the alarm sound. Select from low, medium, and high. ● Enable or disable the function of beep during arming and disarming, and enter and exit delay.
Alarm Duration	● Configure the duration of the alarm sound. ● Select from 3 s through 80 s.
Alarm Status Indication	If **Alarm Status Indication** is enabled, the LED indicator will turn on when an alarm is triggered in an armed area. The LED indicator will flash twice every minute if an area has not been disarmed, and an alarm event ended 30 seconds before.

Parameter	Description
Beep Volume	Set beep volume during arming and disarming, and enter and exit delay. Select from **High**, **Medium** and **Low**.
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 transmission power levels are, the further transmissions can travel, but power consumption increases.
Cloud Update	Update online.

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