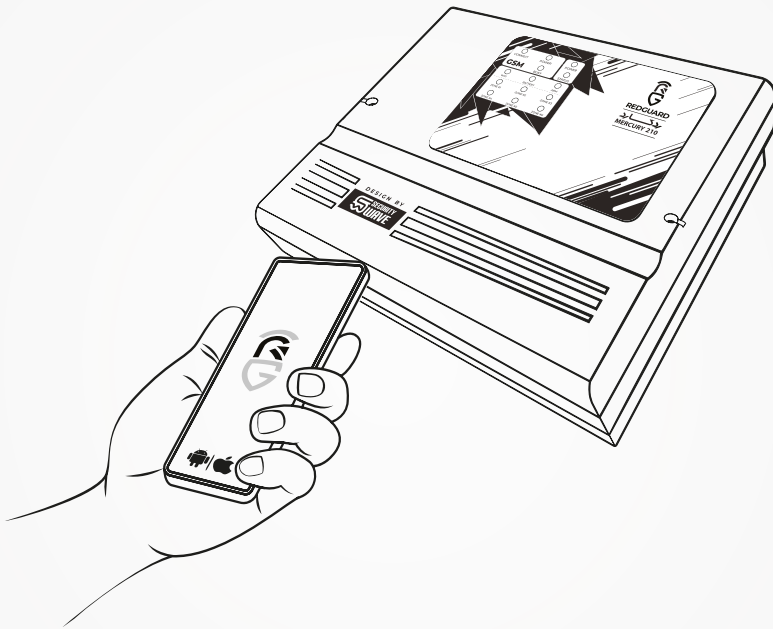


## راهنمای کاربری

# دیده بان هوشمند اماکن REDGUARD

مدل های M210 و M220



این راهنما را به دقت مطالعه کرده و سپس برای بهره‌برداری از دستگاه دزدگیر ردگارد اقدام نمایید.  
آشنایی و استفاده بهینه از این دستگاه متناسب با نیاز شما منوط به مطالعه دقیق این راهنما می‌باشد.  
پس از مطالعه این راهنما آن را برای بازبینی در مکانی قابل دسترس نگهداری کنید.

دیده بان مرکزی ردگارد (REDGUARD) نسل جدید سیستم‌های امنیتی بر پایه اینترنت اشیا (IOT) است که در کنار اپلیکیشن قدرتمند خود، به عنوان یک راهکار امنیتی مطمئن و همه‌جانبه به حفاظت و حراست از دارایی‌ها و سرمایه‌های ارزشمند شما پرداخته و آرامش خاطر را برای شما به ارمغان می‌آورد.

این دستگاه در کنار سنسورهای محیطی متصل به خودش به یک شبکه الکترونیکی یکپارچه تبدیل شده و مانند یک چشم همیشه بیدار، پیوسته و با دقت محیط را پایش کرده و هرگونه حرکت مشکوک را فوراً به اطلاع کاربران می‌رساند.

ردگارد با بهره‌گیری از فناوری‌های ارتباطی Wi-Fi، GSM و بستر اینترنت مبتنی بر فضای ابری (Cloud) امکان کنترل و مدیریت سیستم امنیتی را بدون محدودیت مکانی فراهم کرده است تا در هر زمان و از هر نقطه، از وضعیت محل مورد نظر خود آگاه باشید. در این ساختار، کاربرانی که در محدوده پوشش Wi-Fi قرار دارند می‌توانند به صورت محلی به دستگاه متصل شده و از طریق اپلیکیشن هوشمند REDGUARD کنترل کامل سیستم را در اختیار بگیرند. این اپلیکیشن که یکی از مهم‌ترین وجوه تمایز این محصول با نمونه‌های مشابه به شمار می‌رود، با محیطی ساده و کاربرپسند و امکانات مدیریتی پیشرفته، تجربه‌ای هوشمند و حرفه‌ای از مدیریت سیستم امنیتی ارائه می‌دهد.

همچنین در صورت اتصال دستگاه به اینترنت، ارتباط آن از طریق سرورهای امن ابری با اپلیکیشن برقرار می‌شود. این بستر ابری ارتباطی پایدار، سریع و ایمن میان کاربر و دستگاه ایجاد کرده و امکان مشاهده وضعیت لحظه‌ای، دریافت گزارش‌ها، ارسال فرمان‌ها و اعمال تنظیمات را در هر زمان فراهم می‌سازد.

علاوه بر این، بهره‌گیری از فناوری دوربین GSM در کنار بستر اینترنت، تضمین می‌کند که حتی هنگام ترک محل یا در زمان سفر نیز ارتباط شما با سیستم قطع نشود. کاربران می‌توانند از طریق اپلیکیشن، تماس تلفنی یا پیامک با دستگاه در ارتباط بوده و همواره از وضعیت امنیتی محل مطلع شوند.

از دیگر قابلیت‌های کاربردی این سیستم، پارتیشن‌بندی (تقسیم‌بندی محیط) است. با استفاده از این ویژگی می‌توان محیط تحت پوشش را به چند بخش مستقل تقسیم کرد و هر بخش را به صورت جداگانه فعال یا غیرفعال نمود. این امکان به کاربران اجازه می‌دهد تا متناسب با شرایط، تنها بخش‌های مورد نظر را تحت حفاظت قرار دهند؛ قابلیت‌هایی که به‌ویژه در فضاهای بزرگ، منازل چندطبقه یا محیط‌های کاری بسیار کاربردی خواهد بود.

## ویژگی‌های دستگاه دزدگیر REDGUARD

- حفاظت الکترونیکی بدون فیز و برگشت‌پذیر
- تامین حفاظت دستگاه با استفاده از سوییچ تمپر داخلی
- بهره‌گیری از تغذیه پایدار سوییچینگ به جای تغذیه ترانسی
- نصب و راه‌اندازی آسان و بدون نیاز به سیم‌کشی
- قابلیت شنود صدای محیط و ضبط پیام صوتی اعلان خطر
- امکان به‌روزرسانی دستگاه از طریق اپلیکیشن
- دارای باتری پشتیبان داخلی و ارائه سرویس پس از قطع برق
- امکان سفارشی‌سازی کلیدهای ریموت برای ارائه به هر کاربر
- امکان مدیریت کاربران و تعیین سطوح دسترسی ویژه هر کاربر
- اپلیکیشن هوشمند با قابلیت مدیریت پنج دستگاه دزدگیر ردگارد
- تشخیص خودکار تعویض سیم‌کارت دستگاه هنگام خرابکاری و اطلاع‌رسانی به کاربران
- امکان تعریف و تفکیک نواحی مختلف تحت حفاظت (پارتیشن‌بندی) و مدیریت امنیت آنها
- مدیریت پیامکی دستگاه از طریق اپلیکیشن بدون نیاز به وارد کردن کدهای دستوری خاص
- امکان ارسال درخواست کمک اضطراری به صورت پیامکی از طریق ریموت تنها با فشردن کلید SOS
- قابلیت انتخاب روش حفاظت ۲۴ ساعته به صورت مجزا برای هر زون و سنسور بی سیم از طریق اپلیکیشن
- نرم‌افزار هوشمند دو زبانه (فارسی و انگلیسی) با قابلیت پشتیبانی از سیستم عامل‌های Android و iOS
- پشتیبانی از دو بلندگو با قابلیت انتخاب صدا در کنار آژیر داخلی به منظور ایجاد صدای بیشتر در محوطه وسیع
- قابلیت برقراری ارتباط دوطرفه پیامکی و تماسی بین کاربر و دستگاه و اعلام گزارش وضعیت و هشدارهای پیامکی
- امکان ثبت اطلاعات ریموت تجهیزات جانبی نظیر روشنایی، درب، کرکره برقی و سایر دستگاه‌های عمومی از طریق اپلیکیشن
- اعلان هشدار در صورت بروز شرایط خطر به صورت صوتی، ارسال پیامک و برقراری تماس و اعلان اینترنتی (push notification)
- قابلیت انتخاب روش‌های اعلام خطر به صورت پیش‌فرض، دینگ‌دنگ یا بی‌صدا برای هر زون و سنسور بی سیم از طریق اپلیکیشن

## سخنی با مشتری

مشتری گرامی،

با سپاس از انتخاب هوشمندانه و اعتماد ارزشمند شما، حضور شما را در جمع خانواده بزرگ کاربران ردگارد مسمیمانه خوش‌آمد می‌گوییم.

امید است انتخاب این محصول، بهترین تجربه از امنیت را برای شما رقم بزند.

شرکت دانش‌بنیان «ایمن موج توس» با تکیه بر بیش از دو دهه تجربه در زمینه طراحی و تولید سیستم‌های حفاظت از سرقت و بهره‌مندی از دانش جوانان متخصص کشورمان، فعالیت خود را با طراحی و ساخت گیت‌های ضدسرقت فروشگاهی آغاز کرد و موفق شد عنوان ارزشمند «اولین و بزرگ‌ترین تولیدکننده گیت‌های ضدسرقت فروشگاهی» در کشور را از آن خود کند. امروزه شرکت ایمن موج مفتخر است در راستای گسترش فناوری‌های هوشمند امنیتی، از جدیدترین محصول امنیتی بومی خود با عنوان دزدگیر هوشمند اماکن ردگارد (REDGUARD) رونمایی کرده و پاسخی شایسته به نیاز کاربران خود دهد.

دستگاه دزدگیر ردگارد در سه مدل REDGUARD-M200 و REDGUARD-M220 و REDGUARD-M210 طراحی و عرضه شده است. هر دو مدل از نظر عملکرد یکسان‌اند و تنها در برخی تجهیزات جانبی تفاوت دارند.

دستگاه مدل M200 شامل دستگاه مرکزی و دو عدد ریموت کنترل است و کاربر باید پیش از راه‌اندازی، باتری پشتیبان و سیم‌کارت مناسب را تهیه کرده و بر اساس نیاز محل مورد حفاظت، سنسورها و هشداردهنده‌های صوتی (مانند آژیر یا بلندگو) را به دستگاه متصل کند.

در مقابل، دستگاه مدل M210 و M220 برای سهولت نصب و راه‌اندازی طراحی شده و افزون بر اجزای مدل M200، دارای سنسور(های) بی‌سیم، سیم‌کارت و باتری داخلی است و آژیر نیز به‌صورت توکار در دستگاه تعبیه شده است.

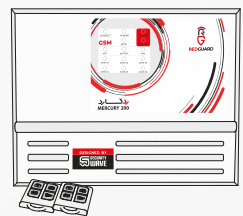
هر دو مدل از طریق اپلیکیشن اختصاصی REDGUARD، قابلیت مدیریت کامل و دسترسی به تنظیمات پیشرفته دستگاه را در اختیار کاربر قرار می‌دهند و تجربه‌ای مدرن، ساده و مطمئن از کنترل سیستم امنیتی را فراهم می‌سازند.



REDGUARD-M220



REDGUARD-M210



REDGUARD-M200

## فهرست مطالب

| ۷  | اطلاعات ایمنی و عمومی                                                    |
|----|--------------------------------------------------------------------------|
| ۷  | علائم ایمنی                                                              |
| ۷  | هشدارها و اقدامات احتیاطی                                                |
| ۹  | تعاریف و اصطلاحات                                                        |
| ۱۱ | معرفی شیوه‌های ارتباطی                                                   |
| ۱۲ | نظام مدیریت کاربران                                                      |
| ۱۳ | سایر قابلیت‌های مهم دستگاه                                               |
| ۱۵ | شرایط و الزامات نصب                                                      |
| ۱۶ | محتویات درون بسته‌بندی                                                   |
| ۱۷ | معرفی اجزا                                                               |
| ۱۹ | بخش منفرم: راه‌اندازی سریع                                               |
| ۲۶ | بخش اول: مدیریت دستگاه به روش ارتباطی WiFi                               |
| ۲۷ | مدیریت کاربران و شخصی‌سازی دستگاه                                        |
| ۲۷ | ورود به حساب کاربری                                                      |
| ۲۸ | ویرایش اطلاعات حساب برای کاربر جاری                                      |
| ۲۹ | افزودن عضو (کاربر) جدید به سامانه و تعیین سطوح دسترسی                    |
| ۳۰ | اولویت بندی کاربران برای اطلاع رسانی                                     |
| ۳۱ | مدیریت ریموت‌ها و افزودن ریموت جدید                                      |
| ۳۱ | ویرایش، حذف و مدیریت ریموت‌ها                                            |
| ۳۲ | فعال یا غیرفعال کلیدهای ریموت                                            |
| ۳۲ | کنترل عملکرد کلیدهای ریموت                                               |
| ۳۳ | افزودن ریموت جدید از نوع ریموت REDGUARD                                  |
| ۳۴ | افزودن ریموت جدید از سایر برندها                                         |
| ۳۶ | مدیریت سنسورهای بی سیم و سفارشی‌سازی آن‌ها                               |
| ۳۶ | ویرایش، حذف و مدیریت سنسورهای بی سیم                                     |
| ۳۷ | افزودن سنسورهای بی سیم جدید (از نوع چشمی‌های REDGUARD) و شخصی‌سازی آن‌ها |
| ۳۹ | افزودن سنسورهای بی سیم جدید (از نوع چشمی‌های متفرقه) و شخصی‌سازی آن‌ها   |
| ۴۱ | افزودن سنسورهای بی سیم جدید (از نوع مگنت‌های REDGUARD) و شخصی‌سازی آن‌ها |
| ۴۳ | افزودن سنسورهای بی سیم جدید (از نوع مگنت‌های متفرقه) و شخصی‌سازی آن‌ها   |
| ۴۵ | مدیریت زون‌ها و سفارشی‌سازی آن‌ها                                        |
| ۴۵ | مدیریت و ویرایش زون‌ها                                                   |
| ۴۶ | مدیریت رله‌ها و سفارشی‌سازی آن‌ها                                        |
| ۴۶ | مدیریت و ویرایش رله‌ها                                                   |
| ۴۷ | مدیریت دستگاه‌های جانبی                                                  |

|    |                                                                   |
|----|-------------------------------------------------------------------|
| ۵۰ | فعال سازی اعلان صوتی                                              |
| ۵۱ | تنظیمات عمومی دستگاه و اپلیکیشن                                   |
| ۵۱ | تنظیمات پیامک                                                     |
| ۵۲ | اولویت بندی تماس و پیامک                                          |
| ۵۳ | حالت مرفه جویی                                                    |
| ۵۳ | اطلاع رسانی وضعیت مسلح/غیرمسلح کردن                               |
| ۵۴ | تنظیمات بلندگوی اول                                               |
| ۵۴ | سیرین                                                             |
| ۵۵ | وضعیت دستگاه                                                      |
| ۵۵ | باتری                                                             |
| ۵۶ | تمپر دستگاه                                                       |
| ۵۷ | تنظیمات اینترنت دستگاه                                            |
| ۵۷ | فعال سازی و ثبت اطلاعات اینترنت                                   |
| ۵۸ | تعویض سیم کارت دستگاه                                             |
| ۶۰ | پشتیبان گیری و بازیابی اطلاعات                                    |
| ۶۰ | تهیه نسخه پشتیبان                                                 |
| ۶۱ | بازگشت به نسخه پشتیبان                                            |
| ۶۲ | بازگردانی به تنظیمات کارخانه                                      |
| ۶۳ | راه اندازی مجدد                                                   |
| ۶۴ | به روزرسانی دستگاه                                                |
| ۶۶ | ارسال گزارش                                                       |
| ۶۷ | <b>بخش دوم: ایجاد نواحی مستقل حفاظتی (پارتیشن) و مدیریت آن ها</b> |
| ۶۸ | مدیریت پارتیشن ها و سفارشی سازی آن ها                             |
| ۶۸ | مدیریت و ویرایش پارتیشن ها                                        |
| ۶۹ | افزودن پارتیشن های جدید و شخصی سازی آن ها                         |
| ۷۰ | قواعد مدیریت نواحی مستقل حفاظتی (پارتیشن ها)                      |
| ۷۱ | مسلح کردن و غیرمسلح کردن دستگاه دزدگیر در روش WiFi                |
| ۷۲ | <b>بخش سوم: مدیریت دستگاه به روش اینترنت</b>                      |
| ۷۳ | مسلح کردن و غیرمسلح کردن دستگاه دزدگیر در روش اینترنتی            |
| ۷۴ | <b>بخش چهارم: مدیریت دستگاه توسط ریموت کنترل</b>                  |
| ۷۵ | مسلح کردن و غیرمسلح کردن پارتیشن های دستگاه از طریق ریموت کنترل   |
| ۷۶ | <b>بخش پنجم: مدیریت دستگاه به روش ارتباطی پیامکی</b>              |
| ۷۸ | برقراری ارتباط پیامکی به روش غیرمستقیم                            |

|     |                                                                                          |
|-----|------------------------------------------------------------------------------------------|
| ۷۸  | <b>برقراری ارتباط پیامکی به روش غیرمستقیم در سیستم عامل Android</b>                      |
| ۷۹  | مسلح یا غیرمسلح کردن تمام پارتیشن ها در ارتباط پیامکی غیرمستقیم در سیستم عامل Android    |
| ۸۰  | مسلح یا غیرمسلح کردن بخشی از پارتیشن ها در ارتباط پیامکی غیرمستقیم در سیستم عامل Android |
| ۸۱  | مدیریت رله ها در ارتباط پیامکی در سیستم عامل Android                                     |
| ۸۲  | <b>برقراری ارتباط پیامکی به روش غیرمستقیم در سیستم عامل iOS</b>                          |
| ۸۲  | مسلح یا غیرمسلح کردن تمام پارتیشن ها در ارتباط پیامکی غیرمستقیم در سیستم عامل iOS        |
| ۸۳  | مسلح یا غیرمسلح کردن بخشی از پارتیشن ها در ارتباط پیامکی غیرمستقیم در سیستم عامل iOS     |
| ۸۴  | مدیریت رله ها در ارتباط پیامکی در سیستم عامل iOS                                         |
| ۸۵  | <b>برقراری ارتباط پیامکی به روش مستقیم</b>                                               |
| ۸۵  | مسلح یا غیرمسلح کردن بخشی از پارتیشن ها در ارتباط پیامکی مستقیم                          |
| ۸۶  | مسلح یا غیرمسلح کردن تمام پارتیشن ها در ارتباط پیامکی مستقیم                             |
| ۸۷  | <b>بخش ششم: مدیریت دستگاه به روش ارتباطی تماس</b>                                        |
| ۸۸  | <b>برقراری ارتباط تلفنی با دستگاه دزدگیر</b>                                             |
| ۸۹  | مسلح کردن و غیرمسلح کردن دستگاه دزدگیر در روش تماس                                       |
| ۹۰  | <b>پرسش های پرتکرار</b>                                                                  |
| ۹۲  | <b>جداول</b>                                                                             |
| ۹۲  | جدول ۱- پتل نشانگرها                                                                     |
| ۹۲  | جدول ۲- کلیدهای ریموت                                                                    |
| ۹۳  | جدول ۳- پیام های کوتاه                                                                   |
| ۹۴  | جدول ۴- مشخصات فنی                                                                       |
| ۹۴  | جدول ۵- روش های فعالیت دستگاه                                                            |
| ۹۵  | <b>پیوست</b>                                                                             |
| ۹۵  | دستورالعمل باز کردن درب دستگاه                                                           |
| ۹۶  | تهیه و جای گذاری سیم کارت                                                                |
| ۹۷  | باتری پشتیبان                                                                            |
| ۹۹  | اتصال زون های سیمی                                                                       |
| ۱۰۳ | اتصال برد رله                                                                            |
| ۱۰۴ | سایر اتصالات خارجی                                                                       |

## اطلاعات ایمنی و عمومی

## علائم ایمنی

هشدارهایی که عدم رعایت آنها منجر به عملکرد نامناسب دستگاه دزدگیر شده و موجب ابطال گارانتی می‌گردند.



نکاتی که باید مورد توجه قرار دهید.



پیامک هایی که از سمت دستگاه دریافت خواهید کرد.



به ترتیب شماره‌ها انتخاب کنید و پیش بروید.



برای انتخاب به مدت طولانی لمس کنید و به ترتیب شماره‌ها پیش بروید.



با انتخاب لینک، به صفحه آن هدایت می‌شوید.



این قابلیت‌ها در ارتباط اینترنتی در دست توسعه هستند.



## هشدارها و اقدامات احتیاطی

- قوانین و مقررات گارانتی هنگام راه اندازی اپلیکیشن «REDGUARD» نمایش داده می‌شود و لازم است آنها را به دقت مطالعه نمایید. همچنین شرایط گارانتی، برای مطالعه بیشتر، پس از ایجاد حساب کاربری در بخش تنظیمات «شرایط گارانتی نیز در دسترس و قابل مطالعه خواهد بود.
- میزان جریان قابل تامین توسط دستگاه برای کلیه تجهیزات متصل، حداکثر ۵/۱ آمپر می‌باشد.



جهت بهره‌برداری صحیح از دستگاه، مراحل هر بخش را طبق راهنما دنبال کنید.



- برچسب اطلاعات پایه دستگاه روی چاره سمت راست پدنه درج شده است. شما می‌توانید با اسکن QR Code روی آن، اطلاعات دستگاه را به اپلیکیشن اضافه کنید.
- دستگاه دزدگیر شما دارای سیم‌کارت داخلی با اعتبار اولیه است.
- شماره سیم‌کارت دستگاه را جهت شناسایی بهتر هنگام برقراری ارتباط پیامکی یا تماس تلفنی با نامی مناسب در موبایل خود ذخیره کنید.

- هنگام کمبود اعتبار سیم‌کارت دستگاه، پیامکی با محتوای کمبود اعتبار برای شما ارسال می‌شود. همواره میزان اعتبار مناسب سیم‌کارت را برای ارتباط صحیح و پایدار با دستگاه فراهم آورید.

- گاهی به علت برخی مشکلات مثل عدم سرویس دهی مناسب از طرف اپراتورها یا موقعیت مکانی نامناسب دستگاه و ... اختلالاتی در ارسال پیامک‌ها و برقراری تماس‌ها به وجود می‌آید. در چنین شرایطی شاید با تعویض سیم‌کارت دستگاه و تعویض اپراتور خدمات‌رسان، مشکل برقراری ارتباط حل شود. در صورت نیاز به تغییر سیم‌کارت به بخش «تهیه و جای گذاری سیم‌کارت» مراجعه نمایید. کلیه حقوق مرتبط با سیم‌کارت دستگاه برای شرکت «ایمن موج» محفوظ است و هرگونه دخل، تصرف و استفاده غیرمجاز از آن به عهده مشتری است.

- اپراتور سیم‌کارت دستگاه، همراه اول است. جهت افزایش اعتبار سیم‌کارت، می‌توانید از روش های مستقیم افزایش اعتبار استفاده نمایید.

- دستگاه دزدگیر شما دارای باتری پشتیبان داخلی است و در صورت فعال بودن باتری (از طریق کلید آن در پشت جعبه دستگاه)، پس از قطع برق به صورت خودکار به فعالیت خود ادامه می‌دهد. توجه داشته باشید که باتری به تنهایی قادر به روشن کردن دستگاه نیست و دستگاه دزدگیر فقط بعد از اتصال به برق روشن می‌شود.
- مدت زمان پشتیبانی باتری از سیستم وابسته به سنسورهای سیمی، تجهیزات متصل به دستگاه و میزان تردد در محیط است. در صورتی که نیاز به پشتیبانی طولانی مدت از دستگاه را دارید، با مراجعه به بخش «باتری پشتیبان» در پیوست راهنما، باتری مناسب را انتخاب و به سیستم اضافه کنید.
- ارائه اطلاعات کاربری معتبر برای ثبت گارانتی الزامی بوده و عواقب درج اطلاعات نادرست به عهده مالک دستگاه است.
- مراحل راه اندازی اولیه باید دقیقاً مطابق دستورالعمل ارائه شده دنبال شود.
- این راهنما براساس نسخه نرم‌افزاری V3.12.0 از سیستم عامل Android و V1.6.0 از سیستم عامل iOS گردآوری شده است.
- بهره‌برداری صحیح از اپلیکیشن «REDGUARD» وابسته به قابلیت‌های تلفن همراه شماست. جهت بهره‌گیری از امکانات اپلیکیشن، بهتر است تلفن همراه شما به نسخه بالاتر از 11 از سیستم عامل Android و بالاتر از 13 از سیستم عامل iOS مجهز باشد.
- قابلیت‌های اپلیکیشن «REDGUARD» در سیستم عامل‌های Android و iOS کاملاً مشابه بوده و تنها در روش «اتصال از طریق پیامک» تفاوتی جزئی وجود دارد.
- قبل از شروع به کار، اپلیکیشن «REDGUARD» را با اسکن QR Code زیر دریافت و روی موبایل خود نصب کنید.



- فرایند راه‌اندازی، نصب و بهره‌برداری از دستگاه دزدگیر به ساده‌ترین شکل ممکن (Plug and Play) طراحی شده است تا کاربران بتوانند بدون نیاز به انجام تنظیمات پیچیده، در کوتاه‌ترین زمان از دستگاه استفاده نمایند. همچنین مراحل نصب و بهره‌برداری دستگاه به‌صورت گام‌به‌گام در این راهنما و از طریق آموزش ویدئویی موجود در وبسایت رسمی محصول تشریح شده است. در صورت نیاز به راهنمایی برای نصب دستگاه، از طریق لینک زیر درخواست خود را ثبت کنید تا کارشناسان مرکز پشتیبانی با شما تماس بگیرند.



## تعاریف و اصطلاحات

### زون (Zone):

واژه زون به محوطه یا محلی اطلاق می‌شود که قصد مراقبت و حفاظت از آن را دارید. زون‌ها به وسیله مجموعه‌ای از سنسورها پایش می‌شوند و دستگاه دزدگیر بروز خطر سرقت را به اطلاع مخاطبان می‌رساند. هر زون می‌تواند شامل یک یا چند سنسور باشد.

### زون بندی یا پارتیشن (Zone Grouping or Partion)

به کمک قابلیت زون بندی، محیط مورد حفاظت به نواحی کوچکتر تقسیم می‌شود تا هر بخش از ساختمان مانند واحدهای اداری، انبار، پارکینگ یا طبقات مختلف به صورت دقیق و مستقل از سایر بخش‌ها مدیریت شود. این قابلیت ضمن افزایش دقت و انعطاف‌پذیری سیستم، موجب صرفه‌جویی در هزینه‌ها و سهولت در بهره‌برداری می‌شود؛ بدین ترتیب با یک دستگاه مرکزی می‌توان چندین ناحیه را به‌صورت مستقل و هم‌زمان مدیریت کرد. همچنین، در مواقع اضطراری، امکان تشخیص سریع محل بروز خطر از طریق پارتیشن مربوطه فراهم می‌گردد.



## مسلح بودن (Arm) و غیر مسلح بودن (Disarm):

ماهیت یک دستگاه دزدگیر با اعلان هشدار هنگام گذر از یک حریم حفاظت شده معنا می‌شود. این اعلان می‌تواند به صورت به صدا درآوردن آژیر، ارسال پیامک، برقراری تماس و... باشد.

**مسلح کردن (Arm)** دزدگیر REDGUARD، سیستم امنیتی را فعال و آن را به یک نگهبان هوشمند برای حفاظت از اموال و دارایی‌های شما مبدل می‌کند. در این حالت سیستم به طور مستمر محیط را پایش می‌کند و حضور افراد و بروز خطر سرقت را با به‌کاراندازی آژیر داخلی دستگاه، ارسال پیام کوتاه و برقراری تماس صوتی به مخاطبان اعلام می‌کند.

**غیر مسلح کردن (Disarm)** دزدگیر REDGUARD، سیستم امنیتی را در حالت غیرفعال قرار می‌دهد. در این وضعیت، تحریک سنسورها موجب فعال شدن هشدارهای صوتی، پیامکی یا تماسی نمی‌شود و تنها از طریق نشانگرهای پنل و اپلیکیشن اعلام می‌گردد.

## هشدار دهنده کامل (Default) در زون‌ها:

نوعی روش اعلام هشدار است که در آن بعد از تحریک زون‌ها، اطلاع‌رسانی با به‌کاراندازی آژیر داخلی دستگاه، بلندگوها (در صورت اتصال)، ارسال پیامک و برقراری تماس صورت می‌گیرد.

## هشدار دهنده دینگ‌دانگ (Chime) در زون‌ها:

نوعی روش اعلام هشدار است که در آن بعد از تحریک زون‌ها، اطلاع‌رسانی صرفاً با به صدا درآمدن آژیر داخلی دستگاه به مدت نیم ثانیه صورت می‌گیرد.

## هشدار دهنده بی‌صدا (Silent) در زون‌ها:

نوعی روش اعلام هشدار است که در آن بعد از تحریک زون‌ها، اطلاع‌رسانی صرفاً از طریق پیامک و تماس، بدون به صدا درآمدن آژیر صورت می‌گیرد.

## شیوه حفاظت تحریک ۲۴ ساعته (Always on) در زون‌ها:

نوعی روش حفاظت است که در آن فارغ از مسلح یا غیرمسلح بودن دستگاه، در صورت تحریک زون‌ها، اطلاع‌رسانی با توجه به شیوه هشدار دهنده انتخابی (پیش‌فرض، دینگ‌دانگ، بی‌صدا) صورت می‌گیرد.

## معرفی شیوه‌های ارتباطی

به طور کلی پنج روش برای مدیریت و کنترل دستگاه وجود دارد. انتخاب شیوه ارتباطی به عوامل مختلفی از جمله میزان فاصله با دستگاه، دسترسی به تجهیزات ارتباطی، شارژ سیم کارت دستگاه و ... بستگی دارد. کلیه روش های ارتباطی قابلیت مسلح یا غیر مسلح کردن پارتیشن های دستگاه دزدگیر را دارند و فقط در بعضی قابلیت های پیشرفته با هم تفاوت دارند.

در ادامه روش های ارتباط با دستگاه را تشریح و مقایسه خواهیم کرد. توجه کنید که استفاده از شیوه های کنترلی بعد از اجرای مراحل راه اندازی اولیه در دسترس خواهند بود.

## الف- اتصال از طریق شبکه محلی (WiFi)

کامل ترین شیوه مدیریت دستگاه و تنظیمات آن، در بستر WiFi انجام می شود. این روش هنگامی که در محدوده پوشش سیگنال های WiFi داخلی دستگاه قرار داشته باشید، به راحتی توانایی کنترل دستگاه را در اختیار شما قرار می دهد. دسترسی به تنظیمات و امکانات پیشرفته دستگاه مانند مدیریت پارتیشن ها، کاربران و زون ها، ایجاد اعلان صوتی، مدیریت سیم کارت، به روزرسانی سیستم عامل و ... از جمله امکاناتی است که در این روش ارتباطی در اختیار شما قرار می گیرد.

## ب- اتصال از طریق اینترنت (Cloud)

این روش در کنار مدیریت از طریق Wi-Fi، یکی از روش های پیشرفته کنترل دستگاه محسوب می شود که امکان مدیریت سیستم را از راه دور نیز فراهم می کند. در این حالت، کاربران می توانند به تمامی قابلیت ها و امکانات دستگاه از راه دور دسترسی داشته باشند (برخی قابلیت ها در حال توسعه هستند)، اعلان هشدار اینترنتی دریافت کنند و کنترل سیستم را به صورت کامل در اختیار بگیرند.

## ج- اتصال از طریق پیامک (SMS)

ارتباط از طریق پیامک، یکی از شیوه های ساده و دسترس پذیر برای ارتباط با دستگاه دزدگیر است که هم از طریق اپلیکیشن و هم از طریق پیام رسان تلفن همراه قابل دستیابی می باشد. در این روش، با توجه به پوشش گسترده شبکه های تلفن همراه، امکان برقراری ارتباط با کاربران بدون محدودیت فاصله فراهم می باشد. البته به علت ساختار ارتباطی این روش، امکانات و قابلیت های پیشرفته دستگاه محدود شده و کاربر در این روش تنها توانایی مسلح/غیرمسلح کردن دستگاه دزدگیر و کنترل رله های متصل شده را دارد. همچنین باید توجه داشت که ارتباط پیامکی در ماهیت خود، معمولاً از سرعت کمتری نسبت به سایر روش ها برخوردار است و بسته به کیفیت سرویس دهی اپراتور، احتمال تأخیر در ارسال یا دریافت اطلاعات وجود دارد.

## د- اتصال از طریق تماس (Call)

ارتباط از طریق تماس، یکی دیگر از روش های کنترلی از راه دور است. در این روش کاربر می تواند با برقراری ارتباط تلفنی با شماره سیم کارت دستگاه و وارد کردن کدهای دستوری خاص و کوتاه، اقدام به مسلح یا غیرمسلح کردن دستگاه دزدگیر نماید.

## ه- مدیریت از طریق ریموت کنترل

دستگاه دزدگیر شما به طور پیش فرض دارای دو ریموت چهار کلید می باشد. استفاده از ریموت برای کنترل دستگاه در مواقعی که به دستگاه نزدیک هستید، کاربرد دارد. استفاده از دو کلید با قابلیت ویژه، درخواست SOS و به صدا درآوردن آلارم، ریموت را به ابزاری کوچک، قابل حمل و کاربردی تبدیل کرده تا کاربران بتوانند آن را به همراه داشته و در مواقع اضطراری به سرعت از آن استفاده کنند.

| بستر ارتباطی                                 | سرعت دریافت پاسخ/میزان فاصله با دستگاه                                       | قابلیت های در دسترس                                                                                 |                           |
|----------------------------------------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|---------------------------|
| ارتباط از طریق اپلیکیشن                      | آنی و بلادرنگ<br>محدودیت فاصله با دستگاه                                     | مسلح یا غیرمسلح کردن دستگاه<br>دسترسی به کلیه تنظیمات و قابلیت های پیشرفته                          | اتصال محلی (WiFi)         |
| ارتباط از طریق اپلیکیشن یا پیام رسان موبایل  | وابسته به میزان آنتن دهی و سرعت پاسخگویی شبکه<br>عدم محدودیت فاصله با دستگاه | مسلح یا غیر مسلح کردن دستگاه<br>کنترل رله های متصل، وضعیت سیم کارت و انرژی                          | پیامک (SMS)               |
| ارتباط از طریق اپلیکیشن یا شماره گیری موبایل | وابسته به میزان آنتن دهی و سرعت پاسخگویی شبکه<br>عدم محدودیت فاصله با دستگاه | فقط مسلح یا غیرمسلح کردن دستگاه                                                                     | تماس (Call)               |
| ارتباط از طریق سخت افزار ریموت               | آنی و بلادرنگ<br>محدودیت فاصله با دستگاه                                     | مسلح یا غیرمسلح کردن دستگاه<br>امکان ارسال پیامک SOS<br>امکان به صدا درآوردن هشدار در مواقع اضطراری | کنترل از راه دور (Remote) |
| ارتباط از طریق اپلیکیشن                      | آنی و بلادرنگ<br>عدم محدودیت فاصله با دستگاه                                 | مسلح یا غیرمسلح کردن دستگاه<br>دسترسی به کلیه تنظیمات و قابلیت های پیشرفته                          | اینترنت (Cloud)           |

## نظام مدیریت کاربران

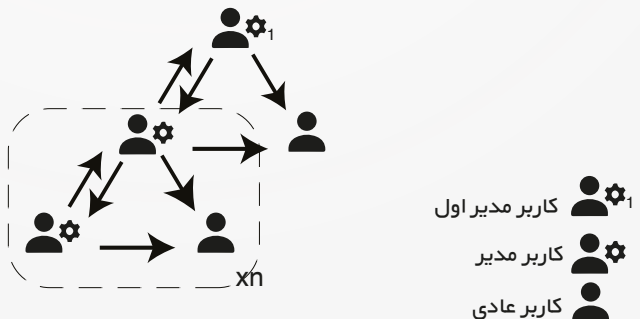
دستگاه دزدگیر شما مجهز به سامانه مدیریت کاربران و کنترل سطح دسترسی به تنظیمات است. به این ترتیب، هر کاربر بر اساس سطح دسترسی تعیین شده، در یکی از دو گروه زیر قرار می گیرد:

**مدیر:** کاربری که مدیریت کاربران (حذف، اضافه و ویرایش)، مدیریت زون ها و سنسورها (حذف، اضافه و ویرایش)، مدیریت رله ها (تغییر وضعیت و ویرایش) را برعهده داشته و به کلیه سطوح دسترسی (دریافت پیام و تماس، مسلح یا غیرمسلح کردن دستگاه، کنترل خروجی ها و کنترل تماس با دستگاه) دسترسی دارد.

**کاربر عادی:** کاربری که طبق نظر مدیر به بعضی از قابلیت های ارتباطی و کنترلی دستگاه دسترسی دارد.

## قوانین مدیریت کاربران

- ۱- کاربری که دستگاه را راه اندازی می کند، به عنوان مدیر اول تعیین می شود و می تواند مدیر یا کاربر عادی بعدی را اضافه کرده و سطح دسترسی آن ها را مشخص نماید.
- ۲- اطلاعات مربوط به سطح دسترسی هر کاربر در مسیر حساب کاربری << کاربران و دسترسی ها قابل مشاهده است.
- ۳- تغییر سطوح دسترسی کاربران تنها توسط نقش مدیر انجام می شود. هیچ کاربری (عادی یا مدیر) نمی تواند سطح دسترسی خود را تغییر داده یا حساب کاربری خود را حذف کند.
- ۴- محدودیتی در تعریف تعداد مدیران یا کاربران عادی وجود ندارد.
- ۵- دستگاه همواره حداقل یک مدیر دارد، اما ممکن است هیچ عضوی با نقش عادی تعریف نشده باشد.
- ۶- کاربر با نقش مدیر اول هیچ امتیاز برتری، نسبت به سایر مدیران ندارد و پس از راه اندازی دستگاه نقش مدیر را می گیرد.
- ۷- فقط کاربر با نقش مدیر می تواند پارتیشن، ریموت، سنسورهای بی سیم و زون ها را تعریف، ویرایش یا حذف کند.
- ۸- کاربر عادی می تواند فاقد هرگونه سطح دسترسی باشد.



## سایر قابلیت های مهم دستگاه

### اولویت بندی کاربران و شیوه های ارتباطی برای اطلاع رسانی شرایط خطر

یکی از قابلیت های دستگاه دزدگیر شما، امکان اولویت بندی کاربران برای اطلاع رسانی شرایط خطر است. مدیران دستگاه می توانند فهرست کاربران را به ترتیب اهمیت یا ضرورت مطلع شدن مرتب کنند تا در صورت وقوع شرایط خطر، دستگاه ابتدا با کاربرانی که در اولویت بالاتری باشند، ارتباط گرفته و با کاربران اولویت بعدی ادامه دهد. این ویژگی موجب می شود افراد کلیدی (به عنوان مثال نگهبان ساختمان) در کوتاه ترین زمان ممکن از شرایط خطر مطلع شوند. توجه کنید که اولویت در شیوه برقراری ارتباط (به صورت پیامکی یا تماس تلفنی) نیز از طریق تنظیمات دستگاه قابل تعیین است. به عنوان مثال با تعیین اولویت برقراری ارتباط به صورت پیامکی، دستگاه هنگام وقوع شرایط خطر، به ترتیب فهرست کاربران، ابتدا پیامک اعلان خطر ارسال کرده و سپس تماس تلفنی برقرار می کند.

### مدیریت تجهیزات جانبی از طریق اپلیکیشن

با استفاده از این قابلیت، می توانید ریموت کنترل تجهیزات جانبی مانند پمپ آب، کرکره برقی، سیستم روشنایی و سایر تجهیزات سازگار را در اپلیکیشن REDGUARD ثبت کنید. پس از ثبت ریموت، امکان کنترل تجهیز متصل به آن از طریق اپلیکیشن فراهم می شود و دیگر نیازی به استفاده مستقیم از ریموت فیزیکی نخواهید داشت. برای استفاده از این قابلیت، ریموت تجهیزات جانبی باید از نوع CodeLearn بوده و با فرکانس ۴۳۳ مگاهرتز کار کند. در حال حاضر، کنترل این تجهیزات از طریق شبکه محلی (Wi-Fi) امکان پذیر است و در اپدیت های بعدی، کنترل تجهیزات در بستر ارتباط پیامکی و اینترنتی نیز فراهم می شود.

### اعلان صوتی

به کمک این ویژگی، امکان پخش یک پیام صوتی از پیش ضبط شده هنگام برقراری ارتباط تلفنی فراهم شده تا کاربران را بسیار سریع از وقوع خطر مطلع کند.

### پشتیبان گیری و بازیابی اطلاعات

تهیه نسخه پشتیبان تضمین می کند که تمام اطلاعات و تنظیمات ذخیره شده در دستگاه و اپلیکیشن محفوظ بماند. بعد از تهیه نسخه پشتیبان، در صورت بروز مشکلاتی مانند ریست شدن دستگاه یا تغییرات ناخواسته در اپلیکیشن، می توانید تنظیمات را به سرعت بازیابی کنید.

### ارسال گزارش

در روند فعالیت یک سیستم امنیتی همواره ممکن است رویدادهای غیرمنتظره ای به دلایل غیر متعارف (خطاهای نرم افزاری، نوسانات برق، مشکل در اتصال به شبکه و ...) رخ دهد که سیستم را از چرخه عملکرد عادی خود خارج کند. در این شرایط، ارسال گزارش عملکرد دستگاه به مرکز پشتیبانی، امکان ارائه خدمات سریع تر و مؤثرتر را جهت رفع خطا به وجود آمده فراهم می سازد.

### به روزرسانی دستگاه و اپلیکیشن

تیم پشتیبانی ما همواره در حال ارتقاء سیستم است تا بالاترین سطح کارایی و کمترین میزان خطا را برای شما فراهم کند. به روزرسانی سیستم عامل دستگاه و اپلیکیشن، ضمن بهبود عملکرد و رفع مشکلات احتمالی، تجربه کاربری بهتری را در اختیار شما قرار می دهد.

برای اطلاع از انتشار نسخه های جدید، اتصال داده تلفن همراه یا اینترنت را فعال نگه دارید. اپلیکیشن REDGUARD به صورت خودکار، وجود نسخه های به روز شده را بررسی کرده و آن ها را در بخش «به روزرسانی» اپلیکیشن نمایش می دهد.

### راه اندازی مجدد و بازگشت به کارخانه

در صورت مواجهه با اختلالات جدی در عملکرد دستگاه، ابتدا از طریق گزینه «ارسال گزارش» در اپلیکیشن، تیم پشتیبانی را در جریان مشکل قرار دهید تا امکان بررسی فنی فراهم شود. سپس می‌توانید دستگاه را از طریق اپلیکیشن دوباره راه‌اندازی کنید. این عملیات معادل قطع و وصل کردن دستگاه از منبع تغذیه می‌باشد و با اجرای آن، دستگاه ارتباط خود با شبکه مخابراتی را بازیابی کرده و پس از شنیده شدن آژیر کوتاه، مجدداً آماده به کار می‌شود. این اقدام معمولاً زمانی کاربرد دارد که عملکرد دستگاه موقتاً دچار اختلال شده یا دستورات را به درستی اجرا نمی‌کند.

در شرایط خاص که دستگاه به طور کامل دچار مشکل شده و فرمان‌ها را دریافت یا اجرا نمی‌کند، می‌توان از قابلیت بازگشت به تنظیمات کارخانه استفاده کرد. توجه داشته باشید که اجرای این گزینه باید صرفاً در موارد ضروری و پس از تأیید واحد پشتیبانی انجام شود؛ زیرا با انجام این عملیات، تمامی اطلاعات و تنظیمات حذف شده و دستگاه به حالت اولیه کارخانه باز می‌گردد.

## شرایط و الزامات نصب دستگاه

یک سیستم حفاظت امنیت، از مجموعه‌ای از اجزا شامل پتل مرکزی، سنسورها و تجهیزات جانبی تشکیل شده که با هماهنگی در کنار هم امنیت محیط را تامین می‌کنند. یکی از عوامل مهم در تضمین عملکرد صحیح و پایدار سیستم امنیتی، انتخاب محل نصب مناسب و استاندارد می‌باشد. محل نصب دستگاه دزدگیر و تجهیزات جانبی باید براساس شرایط واقعی محیط و با در نظر گرفتن مواردی مانند نقشه فضا، نحوه سیم‌کشی، شرایط فیزیکی محیط، کیفیت آنتن‌دهی و سطح امنیت انتخاب شود و دارای ویژگی‌های زیر باشد:

### دستگاه دزدگیر:

- پتل مرکزی باید در محیطی سرپوشیده و مسقف (داخلی) نصب شود. از نصب دستگاه در فضای باز (بیرونی)، محیط‌های پرگردوغبار یا مکان‌هایی که احتمال نفوذ مستقیم آب و رطوبت وجود دارد، خودداری کنید. همچنین محل نصب باید دور از تابش مستقیم نور خورشید بوده و در معرض تنش‌های شدید دمایی (سرما یا گرما) بیش از حد قرار نگیرد.
- محل نصب دستگاه باید دارای پوشش‌دهی مناسب شبکه تلفن همراه باشد. قدرت آنتن‌دهی سیم‌کارت نقش مهمی در سرعت اتصال به شبکه، دریافت دستورات و ارسال پاسخ دارد. پیش از نصب نهایی، از کیفیت آنتن‌دهی در نقطه مورد نظر اطمینان حاصل کنید. درمورد آنتن‌دهی سیم‌کارت دستگاه در صفحه «خانه» اپلیکیشن بخش «وضعیت سیم‌کارت» قابل مشاهده است.
- از نصب دستگاه در مجاورت اجسام فلزی خودداری کنید. وجود تجهیزات و سطوح فلزی می‌تواند آنتن‌دهی دستگاه را به شدت تحت تأثیر قرار دهد. همچنین از نصب دستگاه داخل کمد، کابینت، کشو یا محیط‌های بسته کوچک پرهیز کنید.
- دستگاه را روی سطوح ناهموار یا نقاطی که احتمال سقوط دارد نصب نکنید.
- با توجه به ملاحظات امنیتی، محل نصب باید دور از دید مستقیم و دسترس افراد غیرمجاز باشد. بهتر است پتل دستگاه به گونه‌ای نصب شود که نشانگرهای پدنه دستگاه قابل مشاهده باشد.
- هنگام انتخاب محل نصب، فاصله مناسب از دیوارها و موانع اطراف را رعایت کنید تا امکان اسکن QR Code، مشاهده شماره سیم کارت، تغییر وضعیت کلید باتری، تعویض سیم کارت و باز و بسته کردن پیچ‌های بخش زیرین دستگاه فراهم باشد.
- تغذیه دستگاه از برق شهری 50Hz-220VAC تامین می‌شود. بهتر است در مسیر تغذیه دستگاه از چند راهی برق استفاده نشود. طول کابل برق دستگاه به طور تقریبی ۲ متر است.

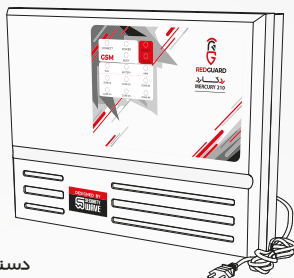
### تجهیزات جانبی:

- تعداد و محل نصب سنسورها و تجهیزات جانبی باید بعد از ارزیابی دقیق فضا و شناسایی نقاط حساس و پرخطر مانند ورودی اصلی، درب‌های فرعی، تراس و بالکن، پشت‌بام، زیرزمین و پنجره‌ها انجام شود تا کل محیط به شکل مؤثر پوشش داده شود و خطا در تشخیص به حداقل برسد.
  - میزان جریان قابل تامین توسط دستگاه برای کلیه تجهیزات متصل، حداکثر ۱/۵ آمپر می‌باشد.
  - اکیدا توصیه می‌شود برای پیشگیری از سرقت، کانال تمپر تجهیزات جانبی را به دستگاه دزدگیر وصل کنید تا از وقوع حادثه جلوگیری شود.
  - استفاده از برچسب‌های مخصوص نام‌گذاری کابل‌ها و تجهیزات متصل به دستگاه، علاوه بر تسهیل فرآیند نصب، در مراحل تعمیر و عیب‌یابی موجب صرفه‌جویی در زمان و جلوگیری از خطا می‌شود.
- ### چشمی‌ها
- برای افزایش ضریب اطمینان سیستم، اکیدا توصیه می‌شود شبکه چشمی‌های موجود در سیستم کاملاً بی‌سیم نباشد و حداقل یک چشمی سیمی در مجموعه چشمی‌ها به کار گرفته شود. وجود حداقل یک چشمی سیمی پایداری سیستم را تقویت کرده و در صورت بروز مشکل در ارتباطات بی‌سیم، مانع از کاهش سطح امنیت سیستم می‌شود.
  - توجه داشته باشید که مسیر مستقیم روبه‌روی چشمی‌ها نقطه کور محسوب می‌شود و چشمی‌ها در این محدوده هیچ‌گونه تشخیصی انجام نخواهند داد.

### هشدار دهنده‌ها

- استفاده از تجهیزات هشداردهنده عمومی مثل آذیرهای صوتی یا نورانی و بلندگوها، خود عاملی بازدارنده برای سرقت است. بکارگیری و نصب این تجهیزات در محل مناسب (قابل تشخیص و مشاهده) می‌تواند تا حد زیادی از وقوع سرقت جلوگیری نماید.
- سیم‌کشی تجهیزات سیمی باید توکار یا درون داکت محافظتی انجام شود تا از بریدن سیم‌ها یا دستکاری آن‌ها جلوگیری شود.
- هشداردهنده‌های صوتی باید در محلی نصب شوند که صدای آن‌ها واضح و قابل شنود برای همسایه‌ها، افراد نزدیک یا نگهبان باشد اما به سیستم شنوایی آسیب نزنند. از نصب هشداردهنده‌های صوتی در جای بسیار بسته خودداری کنید؛ این کار باعث خفه شدن صدا می‌شود.

## محتویات درون بسته بندی



دستگاه دزدگیر (REDGUARD M210 (PR2)



ریموت

x2



چشمی بیسیم همراه باتری

x1



پایه نصب



رول پلاک اتصال به دیوار

x3



پیچ اتصال به دیوار

x3



واشر تخت فلزی

x3



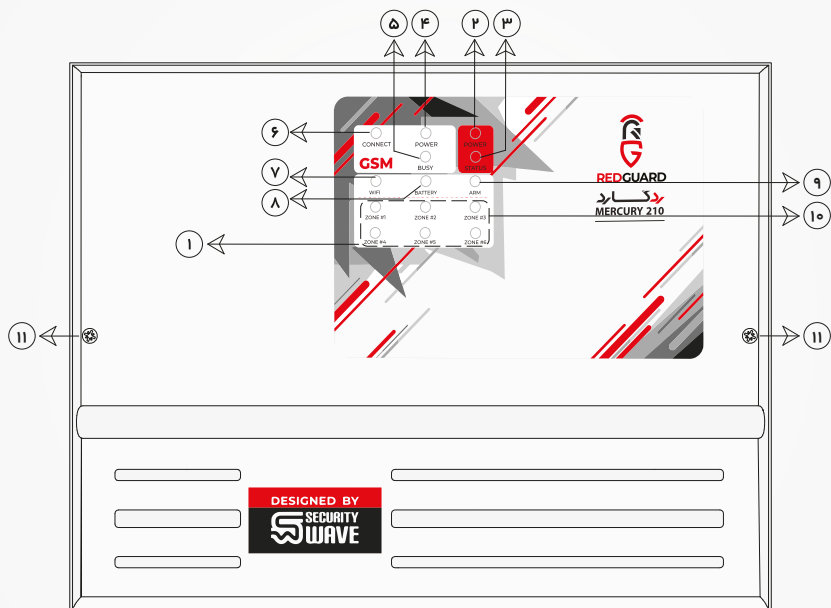
پیچ اتصال پایه

x2

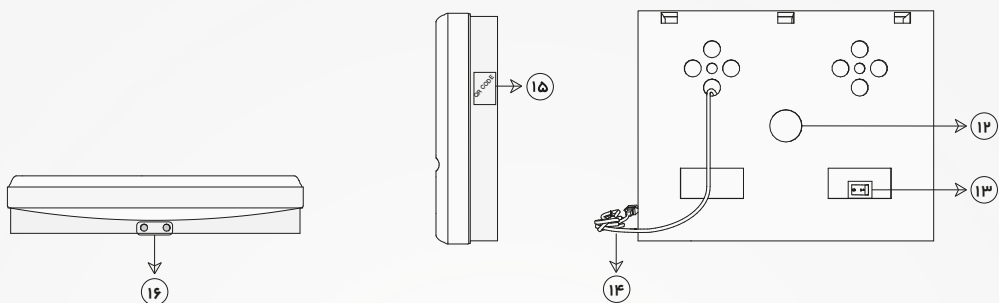
ممکن است در بسته بندی محصول شما، تعداد اقلام ذکر شده (وابسته به کد سفارش محصول) متفاوت باشد. 

## معرفی اجزا

## دستگاه دزدگیر ردگارد



- |                                  |                                          |
|----------------------------------|------------------------------------------|
| ۱ پل نشانگرها                    | ۷ نشانگر فعال بودن به شبکه داخلی WiFi    |
| ۲ نشانگر روشن/خاموش بودن دستگاه  | ۸ نشانگر وضعیت باتری                     |
| ۳ نشانگر وضعیت پردازش            | ۹ نشانگر وضعیت مسلح/غیر مسلح بودن دستگاه |
| ۴ نشانگر تغذیه ماژول GSM         | ۱۰ نشانگر وضعیت تحریک زون ها             |
| ۵ نشانگر وضعیت ارتباطی ماژول GSM | ۱۱ پیچ بزرگ اتصال قاب ها                 |
| ۶ نشانگر وضعیت اتصال به شبکه     |                                          |



۱۶ جای پیچ اتصال پایه

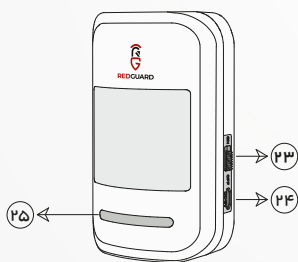
۱۵ برجسب اطلاعات دستگاه

۱۲ حلقه بزرگ نصب

۱۳ کلید قطع/وصل باتری

۱۴ دو شاخه برق

### چشمی بی سیم

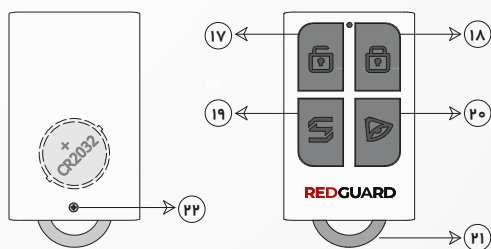


۲۳ سویچ کشویی ON/OFF

۲۴ درگاه MicroUSB

۲۵ نشانگر چشمی بی سیم

### ریموت کنترل



۱۷ کلید غیرمسلح کردن دستگاه

۱۸ کلید مسلح کردن دستگاه

۱۹ درخواست کمک (SOS)

۲۰ کلید اعلام خطر (به صدا درآمدن آژیر)

۲۱ حلقه آویز

۲۲ پیچ باز کردن قاب ریموت برای تعویض باتری

## ۱ آماده سازی دستگاه

دانلود و نصب اپلیکیشن REDGUARD

اتصال دستگاه به برق

انتظار برای برقراری اتصال به شبکه

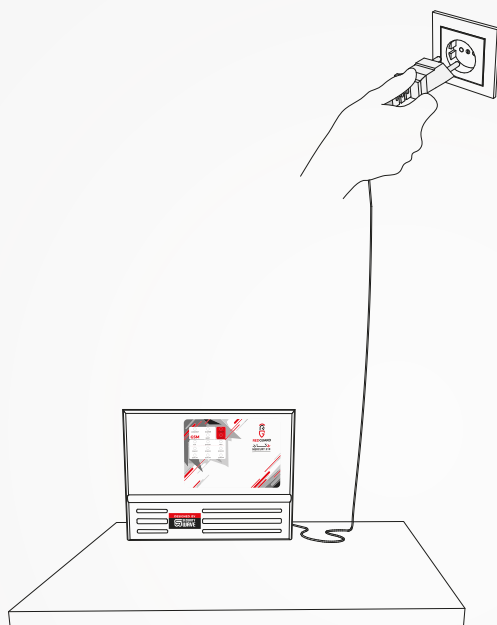
اجرای اپلیکیشن REDGUARD

## ۲ اتصال به دستگاه

## ۳ فعال سازی گارانتی

## ۴ ایجاد حساب کاربری

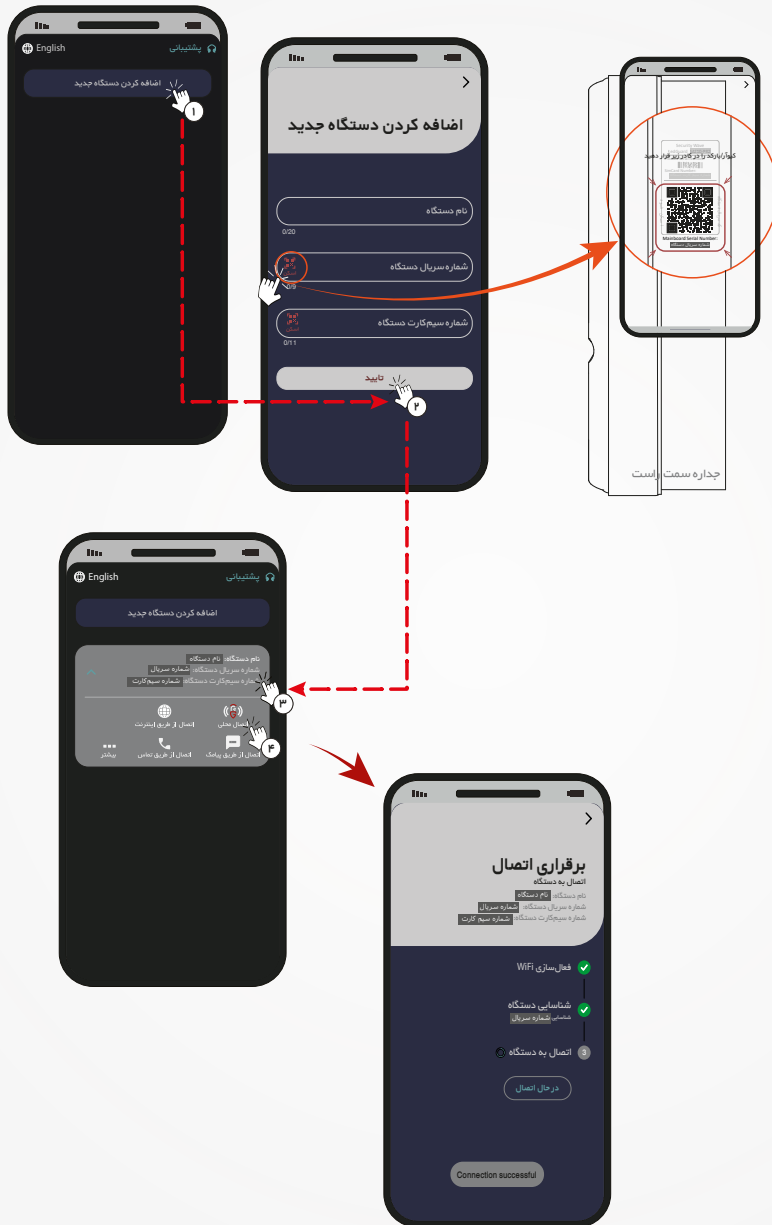
## ۵ فعال سازی اینترنت



توجه کنید که دستگاه پس از اتصال به منبع برق روشن می شود و باتری پشتیبان نمی تواند به تنهایی دستگاه را راه اندازی کند.

پس از اتصال دستگاه به برق، فرایند برقراری ارتباط با شبکه مخابراتی به صورت خودکار آغاز می شود. با پخش صدای آژیر کوتاه، فرآیند اتصال به شبکه پایان یافته و دستگاه برای راه اندازی اولیه آماده خواهد بود.

فرایند اتصال دستگاه به شبکه وابسته به میزان آنتن دهی سیم کارت دستگاه در محل نصب است. چنانچه ارتباط با شبکه برقرار نشد، ابتدا با توجه به الزامات محیط نصب، محل قرارگیری دستگاه را تغییر داده و مجدداً وضعیت اتصال را بررسی کنید. در صورت تداوم مشکل پس از جابجایی دستگاه، به بخش «تعویض سیم کارت» مراجعه کرده و سیم کارت دستگاه را تعویض نمایید.



آماده سازی دستگاه

اتصال به دستگاه

افزودن دستگاه جدید در صفحه مدیریت دستگاه ها

انتخاب نام مناسب برای دستگاه

اسکن یا وارد کردن شماره سریال

وارد کردن شماره سیم کارت

تایید و ذخیره کردن مشخصات دستگاه

انتخاب دستگاه افزوده شده

اتصال به دستگاه از طریق اتصال محلی

انتظار برای برقراری اتصال به دستگاه

فعال سازی گارانتی

ایجاد حساب کاربری

فعال سازی اینترنت



پس از درج اطلاعات در صفحه «فعال سازی گارانتی»، کارت گارانتی دستگاه به صورت دیجیتال در سامانه شرکت ثبت شده و زمان استفاده از گارانتی دستگاه آغاز می‌شود. ارائه اطلاعات کاربری معتبر برای ثبت گارانتی الزامی بوده و عواقب درج اطلاعات نادرست به عهده مالک دستگاه است.



نام کاربری برای ایجاد حساب کاربری باید متشکل از حداقل سه کاراکتر انگلیسی باشد.

کلمه عبور برای ایجاد حساب کاربری باید متشکل از حداقل شش کاراکتر انگلیسی باشد.

اطلاعات درج شده در صفحه ایجاد حساب کاربری به عنوان حساب مدیر اول در نظر گرفته می‌شود.

سیم‌کارتی که کاربر به دستگاه معرفی می‌کند باید فعال و همواره در دسترس باشد.

#### ۱ آماده سازی دستگاه

#### ۲ اتصال به دستگاه

#### ۳ فعال سازی گارانتی

وارد کردن مشخصات مالک

وارد کردن شماره موبایل مالک

مطالعه و موافقت با شرایط گارانتی

ثبت مشخصات مالک دستگاه و فعال شدن مدت زمان ضمانت

#### ۴ ایجاد حساب کاربری

انتخاب نام کاربری انگلیسی

انتخاب کلمه عبور انگلیسی

تکرار کلمه عبور انتخاب شده

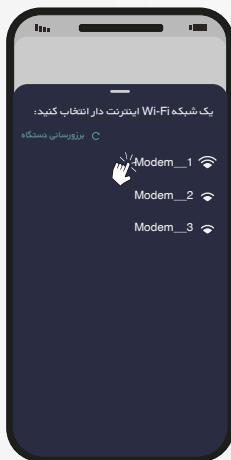
وارد کردن شماره تلفن همراه کاربر

وارد کردن آدرس ایمیل (اختیاری)

#### ۴ ایجاد حساب کاربری

#### ۵ فعال سازی اینترنت

اجرای این مرحله در فرآیند راه‌اندازی اولیه اختیاری می‌باشد. در صورت تمایل به فعال‌سازی اینترنت، می‌توانید پس از اجرای فرآیند راه‌اندازی اولیه، با اتصال به شبکه محلی دستگاه، از بخش تنظیمات اقدام نمایید.



۱ آماده‌سازی دستگاه

۲ اتصال به دستگاه

۳ فعال‌سازی گارانتی

۴ ایجاد حساب کاربری

۵ فعال‌سازی اینترنت

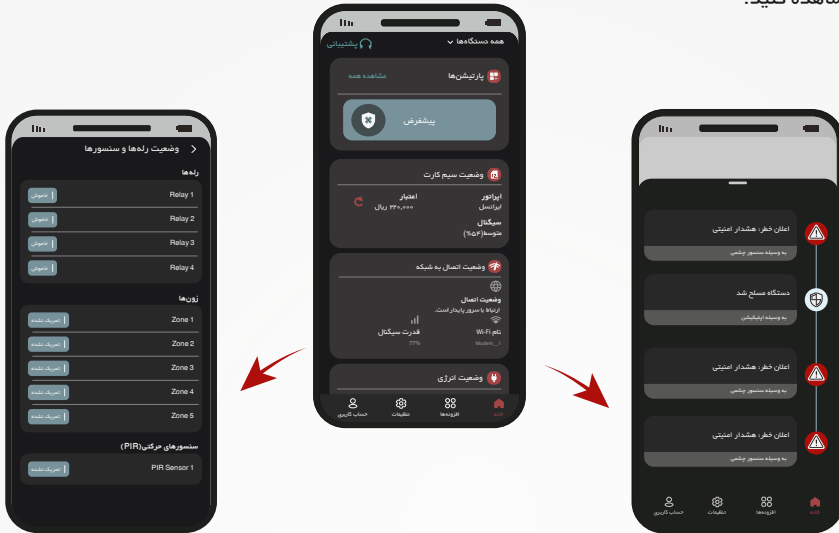
۶ فعال کردن گزینه شبکه محلی Wi-Fi

انتخاب شبکه Wi-Fi مجاور دستگاه و متصل به اینترنت

۶ افزودن ریموت

## معرفی صفحه خانه

در صفحه خانه اطلاعات کاملی از وضعیت فعالیت دستگاه، وضعیت سیم کارت و وضعیت انرژی قابل مشاهده است. همچنین با مراجعه به بخش «آخرین رویدادها» می توانید پیشینه رویدادهای سیستم و در بخش «وضعیت رله ها و سنسورها» وضعیت رله ها، زون ها و سنسورها را مشاهده کنید.



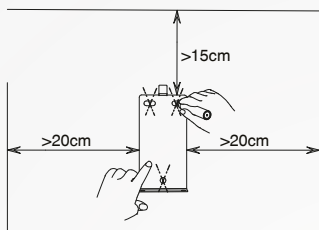
به طور کلی، امکان افزودن پنج دستگاه دزدگیر در اپلیکیشن وجود دارد که در صفحه «مدیریت دستگاه ها» یا بخش «همه دستگاه ها» قابل مشاهده هستند.

اطلاعات پیکربندی هر دستگاه به صورت QR Code در مسیر زیر قابل دستیابی است. شما می توانید این کد را در اختیار سایر کاربران قرار دهید تا به راحتی دستگاه مورد نظر را در اپلیکیشن اضافه کنند.

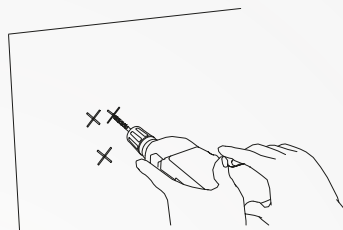


## نصب دستگاه در محل

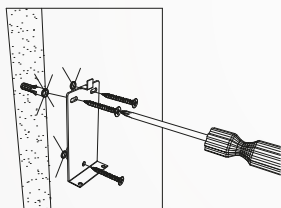
پیش از آغاز مراحل نصب، دستگاه را از منبع برق جدا کنید. 



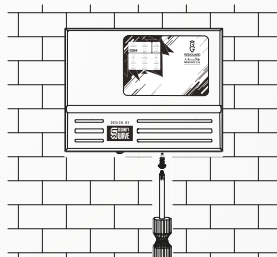
۱- پایه نصب را در محل نصب قرار داده و با توجه به فواصل مشخص شده، محل قرارگیری پیچ‌ها را علامت‌گذاری کنید. مقادیر تعیین شده در شکل حداقل ابعاد مورد نیاز فضای نصب را نشان می‌دهد. توجه داشته باشید که دستگاه باید به صورت قائم نصب گردد.



۲- محل علامت‌گذاری شده را کمی عمیق‌تر از اندازه رول پلاک با مته شماره ۳ و دریل سوراخ کنید.



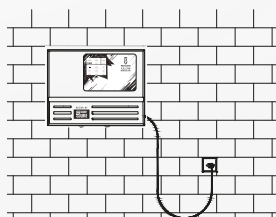
۳- رول پلاک را با چکش به محل سوراخ شده بکوبید تا هم سطح دیوار شود. سپس پایه نصب را با پیچ و واشر به رول پلاک متصل کنید.



۴- بررسی کنید که کلید باتری در وضعیت روشن باشد.

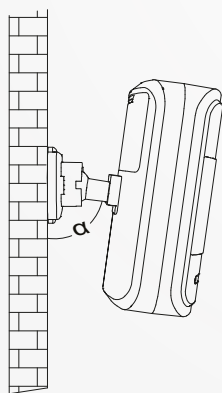
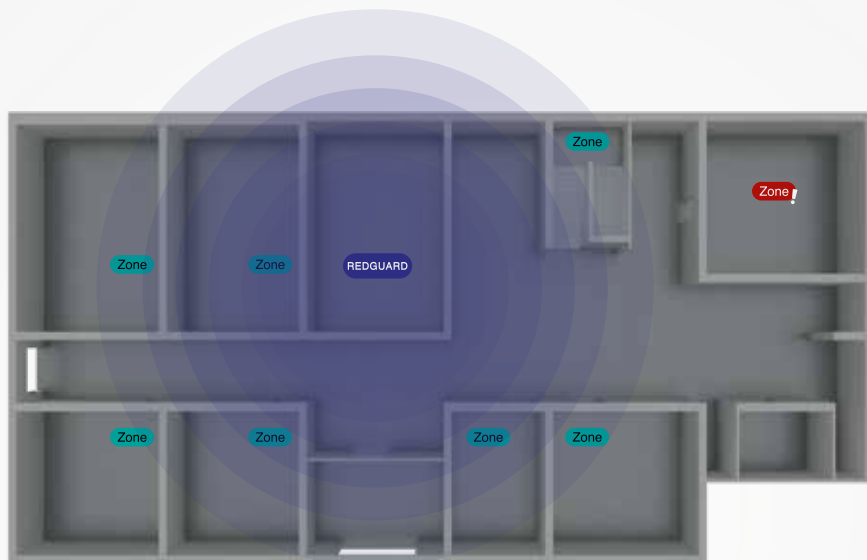
سپس دستگاه را از حلقه بزرگ پشت بدنه، روی قلاب پایه نصب قرار دهید.

۵- پیچ‌های اتصال به پایه نصب را در بخش زیرین بدنه دستگاه محکم نمایید.



۶- دستگاه دزدگیر را به برق متصل کنید.

ارتباط بی سیم چشمی ها و دستگاه به فاصله از دستگاه و همچنین موانع محیط به شدت وابسته است. لذا پیش از نصب چشمی ها، از ارتباط صحیح آن ها با دستگاه اطمینان حاصل نمایید.

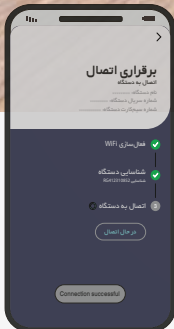


نحوه نصب و راه اندازی چشمی (های) موجود در بسته بندی به طور کامل در راهنمای کاربری اختصاصی آن ها شرح داده شده است. پس از نصب چشمی (ها)، لازم است زاویه سنجش چشمی (ها) را متناسب با محدوده پوشش دهی مورد نظر تنظیم کنید.

توجه داشته باشید که مسیر مستقیم روبه روی چشمی به عنوان نقطه کور محسوب می شود و چشمی در این محدوده هیچ گونه تشخیصی انجام نخواهد داد.

## بخش اول

### مدیریت دستگاه به روش ارتباطی Wi-Fi



شبکه محلی-داخلی Wi-Fi یک پروتکل ارتباطی بیسیم کوتاه‌برد است که امکان تبادل داده بین دستگاه دزدگیر و اپلیکیشن را بدون نیاز به اینترنت، مودم یا روتر فراهم می‌کند و یکی از روش‌های اصلی برای مدیریت و کنترل دستگاه به شمار می‌رود. در این شیوه مدیریت، پس از انتخاب «روش اتصال Wi-Fi»، دستگاه یک شبکه Wi-Fi اختصاصی ایجاد می‌کند و کاربر با اتصال تلفن همراه خود به این شبکه می‌تواند مراحل راه اندازی اولیه، پیکربندی، تغییر تنظیمات، مدیریت دستگاه و تجهیزات جانبی را انجام دهد.

## مدیریت کاربران و شخصی سازی دستگاه

## ورود به حساب کاربری

این صفحه درگاه ورود به حساب کاربری است.



برای ورود و دسترسی به تنظیمات و امکانات دستگاه، از نام کاربری و گذرواژه‌ای که توسط مدیر به شما اختصاص داده شده استفاده کنید. همچنین برای سهولت در فرآیند ورود، می‌توانید پس از نخستین ورود، قابلیت احراز هویت بیومتریک را در بخش «حساب کاربری» فعال نمایید.

در صورت فراموشی اطلاعات ورود، از گزینه «فراموشی نام کاربری یا رمز عبور» استفاده کرده و اطلاعات ورود به حساب را درخواست نمایید. سپس شماره موبایل کاربر موردنظر را وارد نمایید تا اطلاعات ورود به حساب برای آن پیامک شود.



توجه داشته باشید که شماره کاربر مورد نظر باید به عنوان کاربر دستگاه ثبت شده و سطح دسترسی «دریافت پیامک و تماس» برای آن فعال باشد.



RedGuard-Mercury210

شماره سریال دستگاه: SN:

نام کاربری: username:

کلمه عبور: password:

تاریخ و زمان اجرای دستور



## ویرایش اطلاعات حساب برای کاربر جاری



## گام دوم

در این صفحه می توانید شماره موبایل و ایمیل را ویرایش نمایید.



## گام اول

از بخش حساب کاربری، گزینه «تنظیمات حساب» را انتخاب کنید.

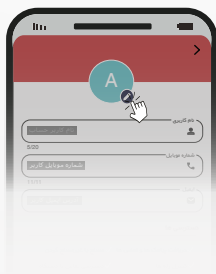


هر کاربر پس از ورود به حساب کاربری، تنها مجاز به ویرایش شماره موبایل حساب بوده و امکان حذف یا تغییر نام کاربری یا سطوح دسترسی حساب جاری را نخواهد داشت.

احراز اطلاعات کاربری برای ورود به حساب کاربری با وارد کردن نام کاربری و رمز عبور انجام می شود.

استفاده همزمان از یک حساب کاربری در دو یا چند تلفن همراه امکان پذیر نیست.

برای شناسایی راحت، می توانید تصویری مناسب برای پروفایل حساب کاربری انتخاب کنید.



## افزودن عضو (کاربر) جدید به سامانه و تعیین سطوح دسترسی

## گام اول

از بخش حساب کاربری، گزینه «کاربران و دسترسی ها» را انتخاب کنید.



## گام دوم

گزینه «افزودن کاربر جدید» را انتخاب کنید.



## گام سوم

در این صفحه، اطلاعات کاربر جدید، پارتیشن تحت کنترل سطح دسترسی آن را تعیین نمایید.  
دریافت پیامک و برقراری تماس

با فعال کردن این گزینه، به کاربر جدید اجازه می‌دهید توانایی دریافت گزارشات پیامکی و تماس اعلان هشدار از سوی دستگاه را داشته باشد.

مسلم کردن و غیرمسلم کردن

با فعال کردن این گزینه، به کاربر جدید اجازه می‌دهید توانایی مسلم یا غیرمسلم کردن پارتیشن های دستگاه را از طریق اپلیکیشن، پیامک و تماس داشته باشد.

مدیریت رله ها

با فعال کردن این گزینه، به کاربر جدید اجازه می‌دهید توانایی کنترل رله های متصل به دستگاه را از طریق اپلیکیشن و پیامک داشته باشد.

امکان برقراری تماس با دستگاه

با فعال کردن این گزینه، به کاربر جدید اجازه می‌دهید توانایی برقراری تماس با دستگاه را داشته باشد.

ارتباط از طریق سرور

با فعال کردن این گزینه، به کاربر جدید اجازه می‌دهید توانایی برقراری ارتباط با دستگاه را از طریق اینترنت داشته باشد.

دسترسی مدیر

با فعال کردن این گزینه، کاربر جدید را در نقش مدیر قرار می‌دهید.



## اولویت بندی کاربران برای اطلاع رسانی

هدف: مرتب کردن کاربران دستگاه به ترتیب اهمیت یا ضرورت مطلع شدن هنگام شرایط خطر.

### گام اول

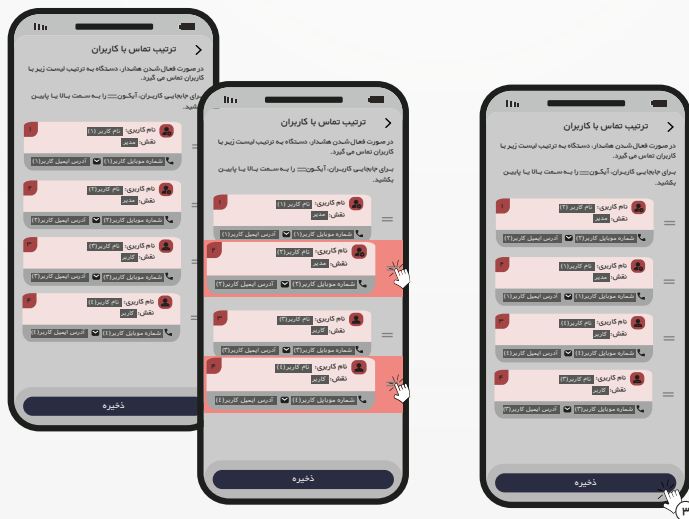
از بخش تنظیمات، گزینه «ترتیب تماس با کاربران» را انتخاب کنید.



### گام دوم

در این صفحه، با نگر داشتن و جابجایی نشان لغزان کنار نام کاربران، لیست اولویت بندی کاربران را مرتب کرده، سپس گزینه «ذخیره» را انتخاب کنید.

در این بخش، فهرست کاربرانی نمایش داده می شود که دارای نقش مدیر بوده یا به «دریافت پیامک و تماس» دسترسی دارند.



## مدیریت ریموت‌ها و افزودن ریموت جدید

## ویرایش، حذف و مدیریت ریموت‌ها



## گام اول

از بخش افزونه‌ها، گزینه «مدیریت ریموت‌ها» را انتخاب کنید.



## گام دوم

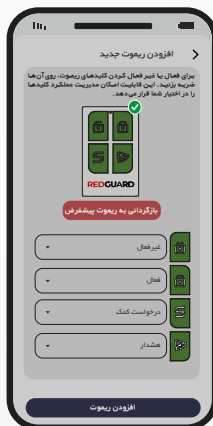
ریموت‌های دستگاه شما، به طور پیش فرض در کارخانه اضافه شده اند. جهت شخصی سازی، ریموت مورد نظر را انتخاب کنید.



## گام سوم

در این صفحه، می‌توانید نام ریموت و یا پارتیشن تحت کنترل با ریموت را ویرایش کنید.

شما می‌توانید با انتخاب گزینه «شخصی سازی ریموت» عملکرد کلیدهای ریموت را متناسب با نیاز کاربران شخصی سازی کنید.



## فعال یا غیرفعال کلیدهای ریموت

کلیدهای فعال ریموت با رنگ سبز مشخص می‌شوند. شما می‌توانید با انتخاب هر کلید، عملکرد آن را غیرفعال کنید تا با فشردن آن، هیچ عملیاتی انجام نشود. پس از غیرفعال سازی، رنگ کلید مربوطه از سبز به خاکستری تغییر می‌کند.



## کنترل عملکرد کلیدهای ریموت

کلیدهای ریموت از طریق اپلیکیشن قابل تنظیم هستند و می‌توان برای هر کلید یک عملکرد متفاوت تعریف کرد. کاربر می‌تواند عملکرد هر کلید را از میان گزینه‌های زیر انتخاب و ذخیره کند:  
فعال، غیرفعال، هشدار، کمک، خروجی رله ۱، خروجی رله ۲، خروجی رله ۳ و خروجی رله ۴.



خروجی رله - روشن: در این حالت با فشردن کلید تعریف‌شده بر روی ریموت، خروجی رله مربوطه بلافاصله فعال می‌شود.  
خروجی رله - خاموش: در این حالت با فشردن کلید تعریف‌شده بر روی ریموت، خروجی رله مربوطه بلافاصله غیرفعال می‌شود.  
خروجی رله - خاموش/روشن: در این حالت با هر بار فشردن کلید تعریف‌شده بر روی ریموت، خروجی رله مربوطه غیرفعال/فعال می‌شود.

## افزودن ریموت جدید از نوع ریموت REDGUARD



## گام اول

گزینه «افزودن ریموت جدید» را در صفحه «مدیریت ریموت ها» انتخاب کنید.



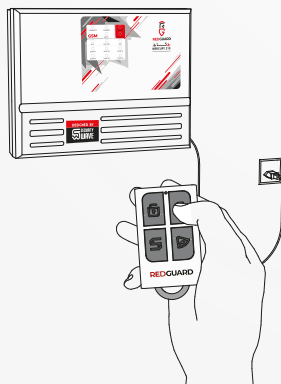
## گام دوم

نامی مناسب برای ریموت تعیین نموده و سپس پارتنش (های) تحت کنترل آن را مشخص کنید. در لیست کشویی مربوط به برند ریموت، گزینه «ردگارد» و سپس گزینه «شناسایی ریموت» را انتخاب نمایید.



## گام سوم

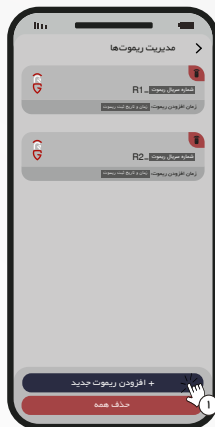
ریموت را نزدیک به دستگاه نگه داشته و یکی از کلیدهای آن را در حالت فشرده نگه دارید. بعد از ثبت موفق ریموت، با استفاده از گزینه «شخصی سازی ریموت» می‌توانید برای هر کلید یک عملکرد متفاوت تعریف کنید.



## افزودن ریموت جدید از سایر برندها

## گام اول

گزینه «افزودن ریموت جدید» را در صفحه «مدیریت ریموت ها» انتخاب کنید.



## گام دوم

نامی مناسب برای ریموت تعیین نموده و سپس پارتنش (های) تحت کنترل آن را مشخص کنید. سپس در لیست کشویی مربوط به برند ریموت، گزینه «متفرقه» را انتخاب نمایید.

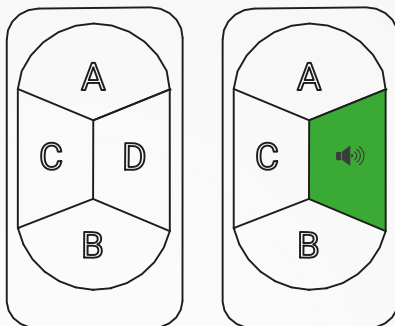


## گام سوم

ابتدا کلید مورد نظر خود را در اپلیکیشن انتخاب کرده و گزینه «شناسایی کلید» را انتخاب کنید. سپس دکمه مربوطه روی ریموت فیزیکی را تا لحظه پر شدن کامل نوار پیشرفت در حالت فشرده نگه دارید.



پس از شناسایی موفقیت‌آمیز، رنگ کلید در اپلیکیشن به سبز تغییر خواهد کرد.



نماد و عملکرد کلیدهای ریموت‌های متفرقه به صورت زیر می باشد:

فعال سازی صدای هشدار



غیر مسلح کردن دستگاه



مسلح کردن دستگاه



درخواست کمک



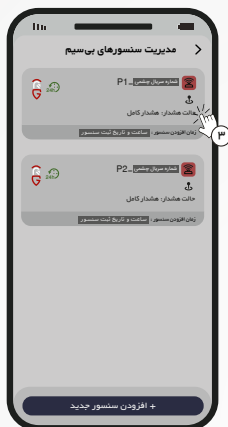
## مدیریت سنسورهای بی سیم و سفارشی سازی آن ها

## ویرایش، حذف و مدیریت سنسورهای بی سیم



## گام دوم

چشمی(های) دستگاه شما، به طور پیش فرض در کارخانه اضافه شده اند. جهت شخصی سازی، چشمی مورد نظر را انتخاب کنید.



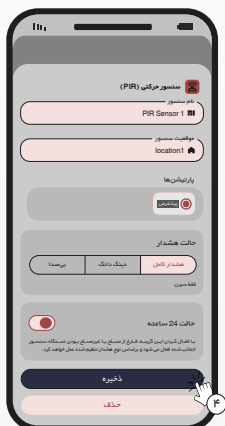
## گام اول

از بخش افزونه ها، گزینه «مدیریت سنسورهای بی سیم» را انتخاب کنید.



## گام سوم

در این صفحه می توانید عنوان، موقعیت، پارکیشن تحت حفاظت سنسور و سایر تنظیمات چشمی های ثبت شده در سیستم را تغییر داده یا آن را حذف کنید. همچنین در صورت نیاز می توانید سنسور را در شیوه حفاظت ۲۴ ساعته قرار دهید.



چشمی های موجود در بسته بندی در حالت «هشدار کامل» قرار دارند و شیوه حفاظتی ۲۴ ساعته برای آن(ها) فعال نیست. در صورت نیاز می توانید تنظیمات چشمی(ها) را ویرایش کنید.

## افزودن سنسورهای بی سیم جدید (از نوع چشمی های REDGUARD) و شخصی سازی آن ها

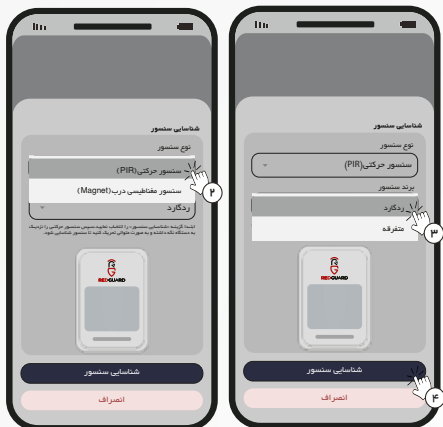
## گام اول

گزینه «افزودن سنسور جدید» را در صفحه «مدیریت سنسورهای بی سیم» انتخاب کنید.



## گام دوم

از لیست کشویی اول، نوع سنسور روی گزینه «سنسور حرکتی (PIR)» و از لیست کشویی دوم برند سنسور را «ردگارد» انتخاب کنید. سپس گزینه «شناسایی سنسور» را انتخاب کنید.



## گام سوم

چشمی Redguard را روشن کرده و نزدیک دستگاه قرار دهید. هنگام نمایش پیغام «درحال شناسایی سنسور» روی اپلیکیشن، چشمی را چند بار تحریک کنید تا پیغام ثبت موفق سنسور ظاهر شود. توجه کنید که سنسور حرکتی REDGUARD، با تشخیص حرکت از مقابل لنز فرنل تحریک شده و نشانگر آن به رنگ قرمز روشن می شود.



## گام چهارم

عنوان، موقعیت، پارتیشن و حالت هشدار سنسور جدید را تعیین کنید.  
در صورت نیاز می توانید سنسور را در شیوه حفاظت ۲۴ ساعته قرار دهید.  
در مرحله آخر برای ذخیره سازی سنسور، گزینه «افزودن سنسور» را انتخاب نمایید.



➡ فرایند افزودن چشمی را در فاصله نزدیک به دستگاه انجام دهید.

➡ هنگام ارسال پیامک اعلان سرقت، نام سنسور تحریک شده منعکس می گردد. از این رو انتخاب یک نام مناسب برای سنسورها جهت اقدام دقیق و به موقع مفید خواهد بود.

➡ در انتخاب شیوه اعلان هشدار سیستم دقت کافی را داشته باشید و مطمئن شوید بهترین شیوه را با توجه به اهمیت و محل نصب سنسور انتخاب کرده اید.

➡ محدودیتی در اضافه کردن چشمی های بی سیم به سیستم وجود ندارد.

➡ دستگاه دزدگیر هوشمند شما به طور کامل با سنسورها و چشمی های برند REDGUARD، تولیدشده توسط «شرکت ایمن موج» سازگار بوده و عملکرد آن به صورت کامل آزموده و تأیید شده است. استفاده از تجهیزات هم برند با سیستم، قابلیت اطمینان و عملکرد آن را فراهم می کند.

به منظور افزایش انعطاف پذیری سیستم و سهولت انتخاب برای کاربران، امکان افزودن سنسورهای سایر برندها (متفرقه) نیز در دستگاه پیش بینی شده که روش افزودن آن ها به سیستم در ادامه تشریح شده است. توصیه می شود پس از افزودن سنسورهای غیرهم برند، حتما از آن ها آزمون کنترل عملکرد به عمل آورید. توجه داشته باشید که تضمینی در خصوص عملکرد دائمی و بدون خطای این تجهیزات وجود ندارد و مسئولیت بکارگیری این نوع تجهیزات به عهده مشتری است.

جهت تهیه سنسورها و سایر تجهیزات جانبی معتبر تولید شده در شرکت ایمن موج و دریافت مشاوره تخصصی، می توانید به واحد فروش رسمی شرکت یا وبسایت ردگارد مراجعه فرمایید.



## افزودن سنسورهای بی سیم جدید (از نوع چشمی های متفرقه) و شخصی سازی آن ها

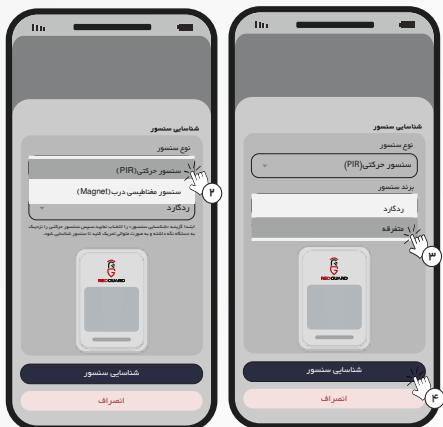
## گام اول

گزینه «افزودن سنسور جدید» را در صفحه «مدیریت سنسورهای بی سیم» انتخاب کنید.



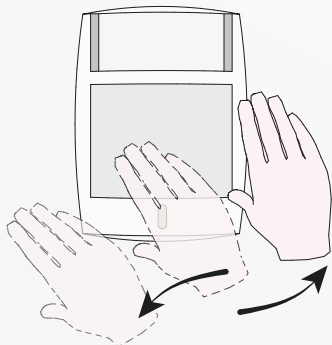
## گام دوم

از لیست کشویی اول، نوع سنسور روی گزینه «سنسور حرکتی (PIR)» و از لیست کشویی دوم برند سنسور را «متفرقه» انتخاب کنید. سپس گزینه «شناسایی سنسور» را انتخاب کنید.



## گام سوم

چشمی مورد نظر را در حالت آماده به کار، نزدیک دستگاه قرار دهید. هنگام نمایش پیام «در حال شناسایی سنسور» روی اپلیکیشن، چشمی را چند بار تحریک کنید تا خط اعتبار اطلاعات سنسور پر شده و پیام ثبت موفق سنسور ظاهر شود.



## گام چهارم

عنوان، موقعیت و حالت هشدار سنسور جدید را تعیین کنید.  
در صورت نیاز می توانید سنسور را در شیوه حفاظت ۲۴ ساعته قرار دهید.  
در مرحله آخر برای ذخیره سازی سنسور، گزینه «افزودن سنسور» را انتخاب نمایید.



➡ فرایند افزودن چشمی را در فاصله نزدیک به دستگاه انجام دهید.

➡ هنگام ارسال پیامک اعلان سرعت، نام سنسور تحریک شده منعکس می‌گردد. از این رو انتخاب یک نام مناسب برای سنسورها جهت اقدام دقیق و به موقع مفید خواهد بود.

➡ در انتخاب شیوه اعلان هشدار سیستم دقت کافی را داشته باشید و مطمئن شوید بهترین شیوه را با توجه به اهمیت و محل نصب سنسور انتخاب کرده‌اید.

➡ محدودیتی در اضافه کردن چشمی‌های بی سیم به سیستم وجود ندارد.

## افزودن سنسورهای بی سیم جدید (از نوع مگنت های REDGUARD) و شخصی سازی آن ها

## گام اول

گزینه «افزودن سنسور جدید» را در صفحه «مدیریت سنسورهای بی سیم» انتخاب کنید.



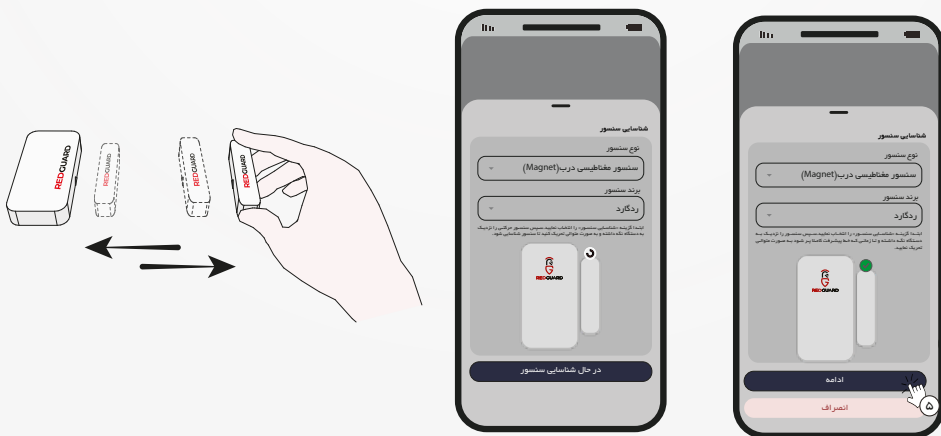
## گام دوم

از لیست کشویی اول، نوع سنسور روی گزینه «سنسور مغناطیسی درب (Magnet)» و از لیست کشویی دوم برند سنسور را «ردگارد» انتخاب کنید. سپس گزینه «شناسایی سنسور» را انتخاب کنید.



## گام سوم

مگنت Redguard را در حالت آماده به کار، نزدیک دستگاه قرار دهید. هنگام نمایش پیام «در حال شناسایی سنسور» روی اپلیکیشن، مگنت را چند بار تحریک کنید تا پیام ثبت موفق سنسور ظاهر شود. توجه کنید که سنسور مغناطیسی درب REDGUARD، با نزدیک شدن بخش آهنربایی به بخش حسگر تحریک شده و نشانگر آن به رنگ قرمز روشن می شود.



## گام چهارم

عنوان، موقعیت، پارتیشن فعالیت، نوع تحریک و حالت هشدار سنسور جدید را تعیین کنید.  
در صورت نیاز می توانید سنسور را در شیوه حفاظت ۲۴ ساعته قرار دهید.  
در مرحله آخر برای ذخیره سازی سنسور، گزینه «افزودن سنسور» را انتخاب نمایید.



- در صورت استفاده از مگنت های نوع ردگارد، می توانید نوع تحریک موردنظر مگنت را به صورت دقیق مشخص کنید تا دستگاه دزدگیر تنها نسبت به تغییر وضعیت دلاخواه شما واکنش نشان دهد.
- تحریک «باز شدن»: با انتخاب این گزینه، هر بار که درب یا پنجره باز شود، مگنت یک سیگنال به دستگاه دزدگیر ارسال می کند و نسبت به بسته شدن درب یا پنجره واکنشی نشان نمی دهد.
- تحریک «بسته شدن»: با انتخاب این گزینه، هر بار که درب یا پنجره بسته شود، مگنت یک سیگنال به دستگاه دزدگیر ارسال می کند و نسبت به باز شدن درب یا پنجره بی تفاوت خواهد بود.
- تحریک «باز و بسته شدن»: با انتخاب این گزینه، مگنت نسبت به هر دو تغییر وضعیت باز شدن و بسته شدن حساس بوده و در هر بار تغییر وضعیت درب یا پنجره، سیگنال مربوطه را به دستگاه دزدگیر ارسال می کند.
- فرایند افزودن مگنت را در فاصله نزدیک به دستگاه انجام دهید.
- هنگام ارسال پیامک اعلان سرعت، نام سنسور تحریک شده منعکس می گردد. از این رو انتخاب یک نام مناسب برای سنسورها جهت اقدام دقیق و به موقع مفید خواهد بود.
- در انتخاب شیوه اعلان هشدار سیستم دقت کافی را داشته باشید و مطمئن شوید بهترین شیوه را با توجه به اهمیت و محل نصب سنسور انتخاب کرده اید.
- محدودیتی در اضافه کردن مگنت های بی سیم به سیستم وجود ندارد.
- دستگاه دزدگیر هوشمند شما به طور کامل با سنسورها و مگنت های برند REDGUARD، تولیدشده توسط «شرکت ایمن موج» سازگار بوده و عملکرد آن به صورت کامل آزموده و تأیید شده است. استفاده از تجهیزات هم برند با سیستم، قابلیت اطمینان و عملکرد آن را فراهم می کند.
- به منظور افزایش انعطاف پذیری سیستم و سهولت انتخاب برای کاربران، امکان افزودن سنسورهای سایر برندها (متفرقه) نیز در دستگاه پیش بینی شده که روش افزودن آن ها به سیستم در ادامه تشریح شده است. توصیه می شود پس از افزودن سنسورهای غیرهم برند، حتما از آن ها آزمون کنترل عملکرد به عمل آورید. توجه داشته باشید که تضمینی در خصوص عملکرد دائمی و بدون خطای این تجهیزات وجود ندارد و مسئولیت بکارگیری این نوع تجهیزات به عهده مشتری است.
- جهت تهیه سنسورها و سایر تجهیزات جانبی معتبر تولید شده در شرکت ایمن موج و دریافت مشاوره تخصصی، می توانید به واحد فروش رسمی شرکت یا وبسایت ردگارد مراجعه فرمایید.



## افزودن سنسورهای بی سیم جدید (از نوع مگنت های متفرقه) و شخصی سازی آن ها

## گام اول

گزینه «افزودن سنسور جدید» را در صفحه «مدیریت سنسورهای بی سیم» انتخاب کنید.



## گام دوم

از لیست کشویی اول، نوع سنسور روی گزینه «سنسور مغناطیسی درب (Magnet)» و از لیست کشویی دوم برند سنسور را «متفرقه» انتخاب کنید. سپس گزینه «شناسایی سنسور» را انتخاب کنید.



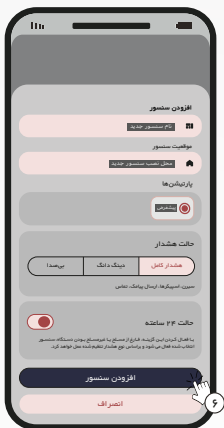
## گام سوم

مگنت مورد نظر را در حالت آماده به کار، نزدیک دستگاه قرار دهید. هنگام نمایش پیغام «در حال شناسایی سنسور» روی اپلیکیشن، سنسور را چند بار تحریک کنید تا خط اعتبار اطلاعات سنسور پر شود.



## گام چهارم

عنوان، موقعیت و حالت هشدار سنسور جدید را تعیین کنید.  
در صورت نیاز می توانید سنسور را در شیوه حفاظت ۲۴ ساعته قرار دهید.  
در مرحله آخر برای ذخیره سازی سنسور، گزینه «افزودن سنسور» را انتخاب نمایید.



➡ فرایند افزودن مگنت را در فاصله نزدیک به دستگاه انجام دهید.

➡ هنگام ارسال پیامک اعلان سرقت، نام سنسور تحریک شده منعکس می‌گردد. از این رو انتخاب یک نام مناسب برای سنسورها جهت اقدام دقیق و به موقع مفید خواهد بود.

➡ در انتخاب شیوه اعلان هشدار سیستم دقت کافی را داشته باشید و مطمئن شوید بهترین شیوه را با توجه به اهمیت و محل نصب سنسور انتخاب کرده‌اید.

➡ محدودیتی در اضافه کردن مگنت‌های بی سیم به سیستم وجود ندارد.

## مدیریت زون ها و سفارشی سازی آن ها

## مدیریت و ویرایش زون ها



## گام اول

از بخش افزوده ها، گزینه «مدیریت زون ها» را انتخاب کنید.



## گام دوم

زون مورد نظر را انتخاب کنید.



## گام سوم

در این صفحه می توانید عنوان، حالت هشدار و نوع عملکرد زون ها را تعیین کرده و در صورت نیاز زون مورد نظر را در شیوه حفاظت ۲۴ ساعته قرار دهید. توجه کنید که حالت عملکرد زون ها (NO یا NC) باید مطابق با عملکرد آنها و به درستی در اپلیکیشن تنظیم شوند.



دستگاه دزدگیر شما قابلیت اتصال پنج زون سیمی را دارد که بعد از برقراری اتصالات سخت افزاری قابل مدیریت هستند. برای اطلاع از نحوه برقراری

اتصالات سخت افزاری زون ها به بخش «اتصال زون های سیمی» در پیوست راهنما مراجعه نمایید.

## مدیریت رله‌ها و سفارشی‌سازی آن‌ها

## مدیریت و ویرایش رله‌ها

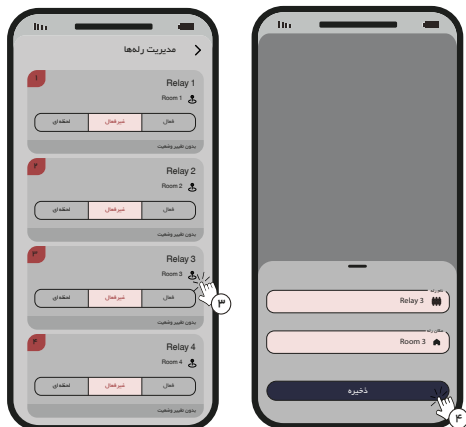
## گام اول

از بخش افزونه‌ها، گزینه «مدیریت رله‌ها» را انتخاب کنید.



## گام دوم

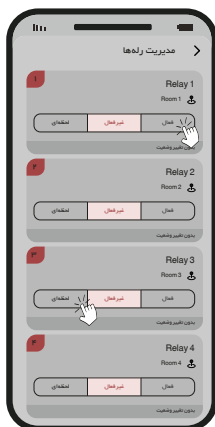
با انتخاب هر رله می‌توانید عنوان و موقعیت آن را ویرایش نمایید.  
پس از اعمال تغییرات گزینه «ذخیره» را انتخاب کنید.



## گام سوم

در این صفحه می‌توانید رله مورد نظر را فعال یا غیرفعال کنید.

همچنین با انتخاب حالت «لحظه‌ای» رله مورد نظر به مدت ۲ ثانیه فعال و سپس غیرفعال می‌گردد. استفاده از چنین قابلیت‌هایی برای فرامین لحظه‌ای مثل باز کردن درب خانه کاربرد دارد.



برای اطلاع از نحوه برقراری اتصالات سخت‌افزاری به بخش «اتصال برد رله» در پیوست راهنما مراجعه نمایید.

## مدیریت دستگاه های جانبی

## ویرایش، حذف و مدیریت ریموت دستگاه های جانبی



## گام دوم

گزینه «دستگاه های جانبی متفرقه» را انتخاب کنید.



## گام اول

از بخش افزوده ها، گزینه «مدیریت دستگاه های جانبی» را انتخاب کنید.



## گام سوم

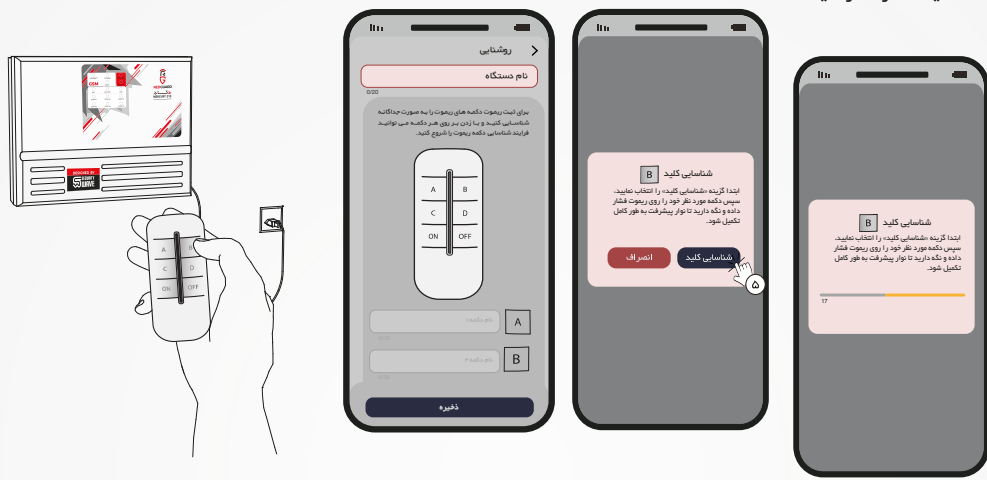
در این صفحه، تجهیزات جانبی در دسته بندی های مختلف قرار گرفته اند. برای افزودن ریموت کنترل دستگاه به اپلیکیشن، دسته بندی مربوط به تجهیز مورد نظر را انتخاب کنید. در صورتی که مدل دستگاه شما در دسته بندی های موجود قرار ندارد، دسته ای را انتخاب کنید که ریموت آن دارای تعداد کلید برابر یا بیشتر از ریموت دستگاه شما باشد. همچنین در صورت نیاز می توانید از دسته بندی «دیگر» برای ثبت ریموت استفاده کنید.

ریموت دستگاه های جانبی باید از نوع CodeLearn باشند و با فرکانس 433MHz کار کند.



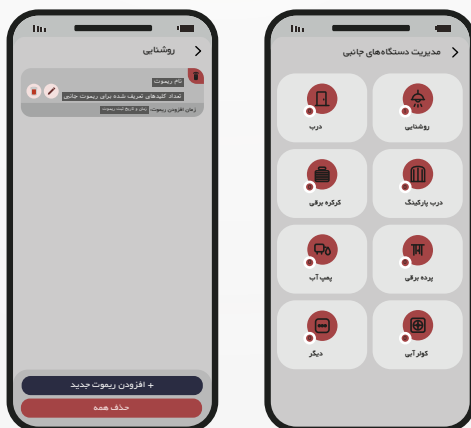
## گام سوم

برای ثبت کلید ریموت، ابتدا کلید موردنظر را در اپلیکیشن انتخاب کنید. سپس گزینه «شناسایی کلید» را انتخاب کرده و دکمه متناظر روی ریموت فیزیکی را فشار دهید و نگه دارید. ریموت را تا زمان تکمیل نوار پیشرفت، در نزدیکی دستگاه قرار دهید تا فرآیند شناسایی کلید انجام شود. ثبت تمامی کلیدهای ریموت در اپلیکیشن الزامی نیست. شما می‌توانید تنها کلیدهایی را که نیاز دارید در اپلیکیشن ثبت کرده و از ثبت سایر کلیدها صرف‌نظر کنید.

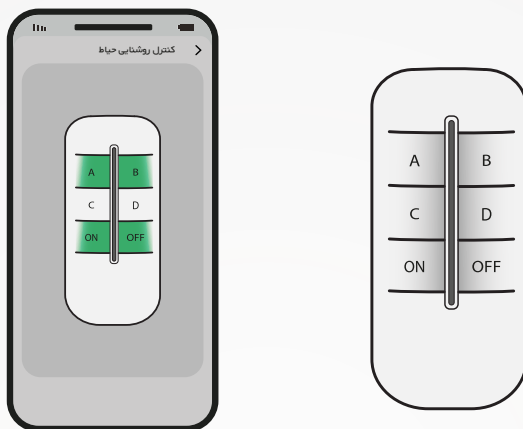


پس از ثبت و ذخیره ریموت، دستگاه ثبت‌شده در فهرست مربوط به دسته‌بندی خود نمایش داده می‌شود. عدد نمایش داده‌شده در کنار هر دسته بندی، تعداد ریموت‌های ثبت‌شده در آن دسته را نشان می‌دهد.

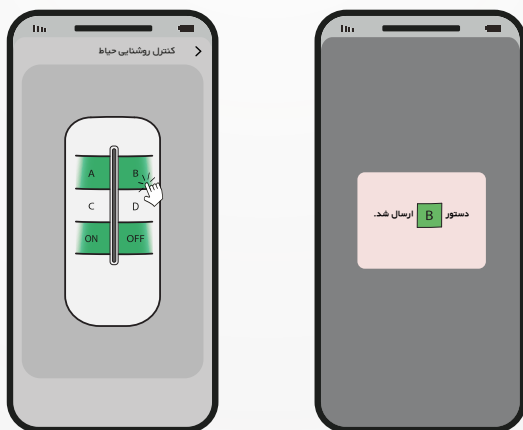
ریموت دستگاه‌های جانبی توسط کلیه کاربران قابل کنترل هستند.



پس از شناسایی موفقیت‌آمیز، رنگ کلیدهای فعال در اپلیکیشن به سبز تغییر خواهد کرد. (برای مثال در اینجا تنها کلیدهای A, B, ON, OFF تعریف شده اند.)



به‌منظور اطمینان از ثبت صحیح ریموت و عملکرد مناسب کلیدهای ریموت ذخیره شده، توصیه می‌شود پس از تکمیل فرآیند افزودن ریموت، یکبار عملکرد کلیدها را از طریق اپلیکیشن آزمایش کنید.



## فعال سازی اعلان موتی



## گام اول

از بخش تنظیمات، گزینه «ضبط پیام موتی» را انتخاب کنید.



## گام دوم

گزینه «ضبط پیام اعلان سرقت» را انتخاب کرده و بعد از برقراری ارتباط موفق، ظرف مدت ۳۰ ثانیه پیغام خود را با صدای رسا ضبط کنید. توجه کنید که تنها کاربران با نقش مدیر قادر به ضبط پیام اعلان سرقت خواهند بود.



## گام سوم

برای شنیدن محتوای اعلان ضبط شده، گزینه «پخش اعلان سرقت» را انتخاب کنید و منتظر تماس تلفنی از سوی دستگاه بمانید. پس از پاسخگویی تماس دستگاه، پیغام ضبط شده پخش خواهد شد.





## تنظیمات عمومی دستگاه و اپلیکیشن

### گام اول

از بخش تنظیمات، گزینه «تنظیمات دستگاه» را انتخاب کنید.



### گام دوم

برای دسترسی به تنظیمات قسمت‌های مختلف دستگاه، گزینه مربوط به آن را انتخاب کنید.  
در ادامه به تشریح نحوه اجرای تنظیمات دستگاه می‌پردازیم.



### گام سوم

## تنظیمات پیامک

با فعال کردن این گزینه، هنگام قطع یا وصل شدن باتری پیامکی به کاربران با سطح دسترسی مجاز ارسال می‌شود.

با فعال کردن این گزینه، هنگام قطع یا وصل شدن منبع برق پیامکی به کاربران با سطح دسترسی مجاز ارسال می‌شود.

با فعال کردن این گزینه، هنگام کاهش سطح شارژ باتری به کمتر از ۲۰ درصد، پیامکی به کاربران با سطح دسترسی مجاز ارسال می‌شود.

با فعال کردن این گزینه، هنگام روشن شدن دستگاه دزدگیر پیامکی به کاربران با سطح دسترسی مجاز ارسال می‌شود.

### اتصال/قطع باتری

پیش فرض: خاموش

### اتصال/قطع برق

پیش فرض: خاموش

### کمبود شارژ باتری

پیش فرض: روشن

### روشن شدن دستگاه

پیش فرض: روشن



## تنظیمات پیامک

با فعال کردن این گزینه، هنگام اتصال کوتاه شدن تغذیه یا سنسورها پیامکی به کاربران با سطح دسترسی مجاز ارسال می شود.

با فعال کردن این گزینه، می توانید متن پیام های کوتاه بین دو ساختار کوتاه شده و فشرده انتخاب کنید.

حالت اول (ساختار کوتاه شده): حذف مدل و شماره سریال دستگاه از متن پیامک ها و ارسال متن اصلی پیام به همراه تاریخ و ساعت وقوع رویداد.

حالت دوم (ساختار فشرده): حذف مدل دستگاه، شماره سریال دستگاه، تاریخ و ساعت وقوع رویداد از متن پیامک ها و ارسال متن اصلی پیام.

در این قسمت، میتوانید زبان متن پیام های کوتاه را انتخاب کنید.

### اتصال کوتاه تغذیه

پیش فرض: روشن

### فرمت پیام کوتاه

پیش فرض: خاموش

### زبان پیامک دستگاه

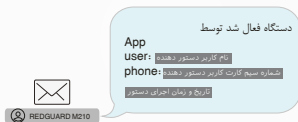
پیش فرض: فارسی



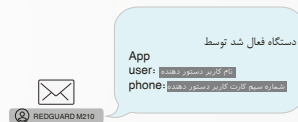
ساختار نمایش متن پیام های کوتاه در حالت های مختلف به صورت زیر است:



ساختار اصلی



ساختار حالت اول (کوتاه شده)



ساختار حالت دوم (فشرده)

## اولویت بندی تماس و پیامک

با فعال کردن این گزینه، در صورت وقوع شرایط سرقت، دستگاه دزدگیر بر اساس فهرست کاربران، ابتدا به تمامی کاربران تماس گرفته و سپس پیامک ارسال می نماید.

با فعال کردن این گزینه، در صورت وقوع شرایط سرقت، دستگاه دزدگیر بر اساس فهرست کاربران، ابتدا به تمامی کاربران پیامک ارسال کرده و سپس تماس برقرار می کند.

### تماس

پیش فرض: خاموش

### پیامک

پیش فرض: روشن



## حالت صرفه جویی

با فعال کردن این گزینه، هنگام کاهش سطح شارژ باتری به کمتر از ۲۰ درصد، بلندگوهای متصل به دستگاه، به طور خودکار غیرفعال می شوند.

با فعال کردن این گزینه، هنگام کاهش اعتبار سیم کارت به کمتر از ۱۰۰۰ تومان، برقراری ارتباط از طریق تماس غیرفعال می شود و در صورت بروز شرایط خطر، اطلاع رسانی فقط با ارسال پیامک به کاربران انجام می شود.

با فعال کردن این گزینه، هنگام کاهش اعتبار سیم کارت به کمتر از ۱۰۰۰ تومان، فقط پیامک های اعلان سرقت به کاربران با سطح دسترسی مجاز ارسال شده و دستگاه از ارسال سایر پیامک ها (به جز پیامک SOS) صرف نظر می کند.

### حالت صرفه جویی باتری

پیش فرض: خاموش

### غیر فعال کردن تماس ها

پیش فرض: خاموش

### فقط ارسال پیامک سرقت

پیش فرض: خاموش



## اطلاع رسانی وضعیت مسلح/غیرمسلح کردن

با فعال کردن این گزینه، هنگام مسلح یا غیرمسلح شدن دزدگیر، آژیر داخلی دستگاه به مدت کوتاهی به صدا در می آید.

با فعال کردن این گزینه، هنگام مسلح یا غیرمسلح شدن دزدگیر، بلندگوی اول به مدت کوتاهی به صدا در می آید.

با فعال کردن این گزینه، هنگام مسلح یا غیرمسلح شدن دزدگیر، بلندگوی دوم به مدت کوتاهی به صدا در می آید.

با فعال کردن این گزینه، هنگام مسلح یا غیرمسلح شدن دزدگیر، پیامکی به کاربران با سطح دسترسی مجاز ارسال می شود.

با فعال کردن این گزینه، هنگام مسلح یا غیرمسلح شدن دزدگیر، بازر داخلی دستگاه به مدت کوتاهی به صدا در می آید.

### سیرین

پیش فرض: روشن

### بلندگوی اول

پیش فرض: روشن

### بلندگوی دوم

پیش فرض: روشن

### ارسال پیامک

پیش فرض: روشن

### بازر

پیش فرض: روشن



## تنظیمات بلندگوی اول

با فعال کردن این گزینه، هنگام وصل شدن بلندگوی اول، پیامکی به کاربران با سطح دسترسی مجاز ارسال می‌شود.

با فعال کردن این گزینه، هنگام قطع شدن بلندگوی اول، پیامکی به کاربران با سطح دسترسی مجاز ارسال می‌شود.

سه مدل آوای هشداردهنده به انتخاب شما از بلندگوها قابل پخش است. برای شنیدن آواهای هشداردهنده، علامت پخش صدا را لمس کنید.

مدت زمان پخش آژیر هشدار به صورت پله‌های ۱، ۵ و ۱۰ دقیقه‌ای قابل تنظیم است.

پیامک ہنگام  
اتصال بلندگو

بیش فرض: خاموش

پیامک ہنگام قطع  
اتصال بلندگو

بیش فرض: خاموش

صدای هشدار

بیش فرض: هشدار ۱

مدت زمان پخش هشدار

پیش فرض: ۱۰ دقیقه



تنظیمات بلندگوی اول و دوم مشابه است.

دستگاه دزدگیر قابلیت اتصال دو بلندگو با مقاومت داخلی ۸ اهم و حداقل توان ۱۵ وات را دارد.

## تنظیمات سپرن

با فعال کردن این گزینه، در صورتی که هنگام به صدا درآمدن آژیر هشدار، سیرین دستگاه اتصال کوتاه شده باشد، پیامکی به کاربران با سطح دسترسی مجاز ارسال می شود.

مدت زمان پخش آثیر هشدار به صورت یله‌های ۱، ۵ و ۱۰ دقیقه‌ای قابل تنظیم است.

پیامک اتصال کوتاه

پیش فرض: خاموش

مدت زمان یخش

بیش فرض: ۱ دقیقه



## وضعیت دستگاه

با فعال کردن این گزینه، سیستم پس از هر بار روشن شدن، وضعیت (فعال یا غیرفعال بودن) پارتیشن‌ها را دقیقاً مطابق با آخرین تنظیمات پیش از خاموشی بازیابی می‌کند.

### روشن شدن در آخرین وضعیت

پیش فرض: خاموش



## باتری

نوع باتری پشتیبان داخلی دستگاه، به دو صورت اسیدی و لیتیومی قابل تنظیم است.

### نوع باتری

پیش فرض: اسیدی

انتخاب نادرست نوع باتری ممکن است باعث اختلال در فرآیند شارژ، عملکرد نامناسب سیستم، نمایش نادرست سطح شارژ باتری و در نهایت کاهش عمر مفید باتری شود.



## تمپر دستگاه

با فعال کردن این گزینه، هنگام باز شدن درب پنل مرکزی، پیامکی به کاربران با سطح دسترسی مجاز ارسال می‌شود.

با فعال کردن این گزینه، هنگام باز شدن درب پنل مرکزی، آژیر هشدار از طریق سیرین و بلندگوها پخش می‌شود.

### پیامک

پیش فرض: خاموش

### آلارم

پیش فرض: روشن



## تنظیمات اینترنت دستگاه

## فعال سازی و ثبت اطلاعات اینترنت

## گام اول

از بخش افزوده ها، گزینه «تنظیمات اینترنت دستگاه» را انتخاب کنید.



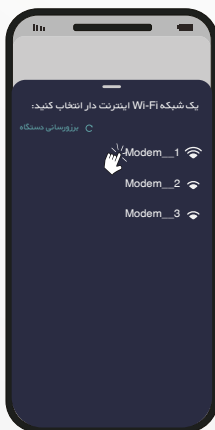
## گام دوم

گزینه شبکه Wi-Fi متصل به اینترنت را فعال کنید.



## گام سوم

پس از روشن کردن Wi-Fi، با استفاده از اطلاعات شبکه (نام شبکه و رمز عبور)، به مودم Wi-Fi متصل به اینترنت وصل شوید.



## تعویض سیم کارت دستگاه

## گام دوم

گزینه تغییر سیم کارت را انتخاب کنید.  
منتظر بمانید تا عملیات غیرفعال سازی طی شود.



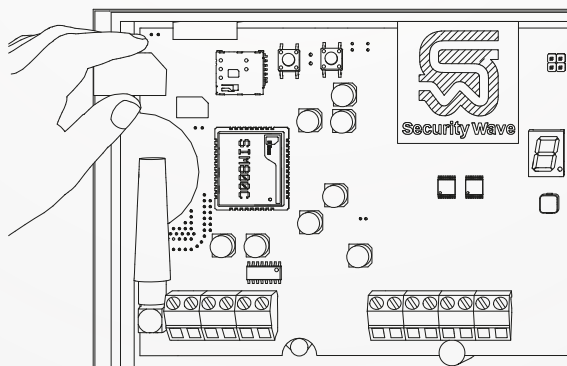
## گام اول

از بخش تنظیمات، گزینه «مدیریت سیم کارت» را انتخاب کنید.



## گام سوم

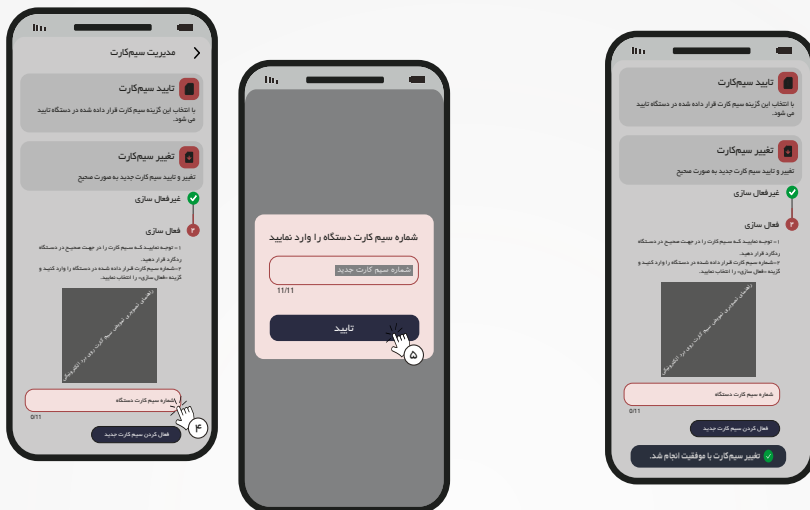
به پیوست راهنما مراجعه کرده و مطابق دستورالعمل، درب دستگاه را باز کنید.  
با توجه به راهنمای تصویری در بخش «تهیه و جای گذاری سیم کارت» در پیوست راهنما، اقدام به تعویض سیم کارت نمایید.



سایز سیم کارت مورد استفاده باید مطابق با جایگاه قرارگیری آن بر روی برد باشد. همچنین از غیرفعال بودن قفل PUK و کافی بودن میزان اعتبار سیم کارت جدید قبل از تعویض آن اطمینان حاصل نمایید.

## گام چهارم

شماره سیم کارت جدید را در قسمت «شماره سیم کارت دستگاه» وارد کنید. سپس گزینه «فعال کردن سیم کارت جدید» را انتخاب کنید.



در صورت دریافت پیامکی با محتوای «تغییر یافتن سیم کارت داخلی دستگاه»، به بخش «تایید سیم کارت» مراجعه کرده و شماره سیم کارت جدید را وارد و تایید نمایید.



RedGuard-Mercury210  
SN: [شماره سریال دستگاه]

سیم کارت دستگاه تغییر کرده است لطفاً از طریق نرم افزار REDGUARD تایید نمایید.



REDGUARD M210

## پشتیبان گیری و بازیابی اطلاعات

## تپیه نسخه پشتیبان

## گام اول

از بخش تنظیمات، گزینه «پشتیبان گیری و بازیابی» را انتخاب کنید.



## گام دوم

گزینه «ایجاد نسخه پشتیبان» را انتخاب کنید.



## گام سوم

پس از پایان فرایند پشتیبان گیری پیغام موفقیت در ایجاد نسخه پشتیبان ظاهر شده و نسخه پشتیبان در بخش «بازیابی به نسخه پشتیبان» قرار می گیرد.



برای جلوگیری از مشکلات ناگهانی، بعد از ایجاد تغییرات، از تنظیمات اپلیکیشن خود نسخه پشتیبان تهیه نمایید.

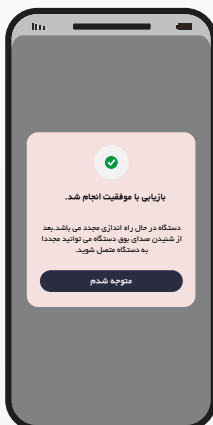
## بازگشت به نسخه پشتیبان

### گام اول

گزینه «بازیابی به نسخه پشتیبان» را انتخاب کرده و تا زمان بازنشانی اطلاعات منتظر بمانید.



پس از اتمام فرآیند بازیابی اطلاعات، دستگاه به‌طور خودکار دوباره راه‌اندازی شده و پس از پخش آذیر، آماده استفاده خواهد بود. 





## بازگردانی به تنظیمات کارخانه

### گام اول

از بخش تنظیمات، گزینه «پشتیبان گیری و بازیابی» را انتخاب کنید.



### گام دوم

گزینه «تنظیمات کارخانه» را انتخاب کنید.



### گام سوم

با استفاده از گزینه «تنظیمات کارخانه»، اطلاعات کاربران، پارتیشن ها، سنسورها، ریموت ها، اعلان های صوتی و نسخه پشتیبان حذف شده و تنظیمات دستگاه، رله ها و زون ها به حالت اولیه بازخواهد گشت. توجه کنید که استفاده از این قابلیت فقط در موارد خاص و پس از کسب تایید از مرکز پشتیبان مجاز به اجراست.





## راه اندازی مجدد

در برخی شرایط ممکن است عملکرد دستگاه به دلایل مختلفی مانند نوسانات برق، خطاهای موقت در حافظه داخلی، تغییرات نرم‌افزاری یا اختلالات گذرای شبکه با مشکل مواجه شود. بروز این اختلالات ممکن است به شکل‌هایی مانند عدم پاسخ‌دهی دستگاه به تحریک سنسورها، ذخیره نشدن تنظیمات جدید، تأخیر در اجرای دستورات یا رفتارهای غیرعادی برخی بخش‌های سیستم مشاهده شود.

در صورت مواجهه با چنین اختلالاتی، ابتدا از طریق گزینه «ارسال گزارش» در اپلیکیشن، تیم پشتیبانی را در جریان مشکل قرار دهید. سپس دستگاه را از طریق اپلیکیشن و با استفاده از قابلیت «راه‌اندازی مجدد» ریست کنید. قابلیت راه‌اندازی مجدد عملیات قطع و وصل دستگاه از منبع تغذیه را به صورت نرم افزاری اجرا می‌کند و می‌تواند باعث رفع خطاهای موقتی و بازگشت دستگاه به عملکرد عادی شود.



👉 برای راه‌اندازی مجدد دستگاه باید حتماً به برق متصل شده باشد و امکان استفاده از این قابلیت زمانی که تغذیه دستگاه تنها از طریق باتری پشتیبان تامین می‌شود، وجود ندارد.

👉 پس از راه‌اندازی مجدد، دستگاه به شبکه مخابراتی متصل شده و پس‌آزیر داخلی، دستگاه آماده استفاده می‌باشد.

## به روزرسانی دستگاه



## گام اول

پس از روشن کردن اتصال اینترنت (داده) تلفن همراه، از بخش تنظیمات، گزینه «به روز رسانی دستگاه» را انتخاب کنید.



## گام دوم

با ورود به این صفحه، اپلیکیشن انتشار نسخه های به روز شده را بررسی کرده و نمایش می دهد. در صورتی که این صفحه تازه سازی نشد، با انتخاب گزینه «بررسی به روز رسانی» صفحه را به روز کنید.



در صورت انتشار نسخه های جدید، صفحه به روزرسانی برای نصب آخرین نسخه فریمور نمایش داده خواهد شد.



بعد از اجرای عملیات به روزرسانی، دستگاه دزدگیر دوباره راه اندازی شده و پس از پخش صدای آژیر، قابل استفاده خواهد بود.

اگرچه توصیه می شود جهت کسب تجربه کاربری بهتر و بهره مندی از امکانات جدیدتر از محصول، انتشار نسخه های جدید از سیستم عامل را با تازه سازی این صفحه بررسی نموده و همواره محصول خود را به روز نگه دارید.

در برخی موارد، اپلیکیشن ممکن است نیاز به به‌روزرسانی اجباری سیستم‌عامل را تشخیص دهد. در این وضعیت، پیغام هشدار مبنی بر الزامی بودن به‌روزرسانی سیستم‌عامل نمایش داده می‌شود. در این حالت، برای استفاده از اپلیکیشن، لازم است سیستم‌عامل دستگاه خود را به آخرین نسخه موجود ارتقا دهید و سپس از آن استفاده نمایید.





## ارسال گزارش

## گام اول

پس از روشن کردن اتصال اینترنت (داده) تلفن همراه، از بخش تنظیمات، گزینه «ارسال گزارش» را انتخاب کنید.



## گام دوم

گزینه «ارسال گزارش» را انتخاب کنید.



## گام سوم

پس از ارسال گزارش، به مرکز پشتیبانی، پیام موفقیت در ارسال گزارش ظاهر شده و کارشناسان ما پس از بررسی اطلاعات دستگاه، در صورت نیاز با شما ارتباط می‌گیرند.



## بخش دوم

### ایجاد نواحی مستقل حفاظتی (پارتیشن) و مدیریت آن‌ها



پارتیشن به ناحیه‌ای گفته می‌شود که بتوان آن را به صورت مستقل از سایر نواحی، مسلح یا غیرمسلح کرد. این قابلیت به کاربر امکان می‌دهد تا بخش‌های مختلف ساختمان را به صورت جداگانه مدیریت کند؛ برای مثال، در خانه‌ای با چهار پارتیشن راهرو، اتاق خواب، پذیرایی و انباری تنها پارتیشن راهرو را مسلح کرده و بقیه پارتیشن‌ها را در حالت غیرمسلح نگه داشت. هر پارتیشن از زون‌ها و سنسورهای اختصاص یافته به همان ناحیه محافظت می‌کند و توسط کاربرانی که در آن پارتیشن عضو هستند، کنترل و مدیریت می‌شود. به کمک این ویژگی می‌توان دسترسی‌ها، هشدارها و عملکرد سیستم را برای هر بخش، به شکل دقیق و مستقل تنظیم نمود.

## مدیریت پارتیشن ها و سفارشی سازی آن ها

## مدیریت و ویرایش پارتیشن ها



## گام اول

از بخش افزونه ها، گزینه «مدیریت پارتیشن ها» را انتخاب کنید.



## گام دوم

با انتخاب هر پارتیشن (ناحیه مستقل حفاظتی) می توانید به تنظیمات آن وارد شده و آنها را ویرایش نمایید.



## گام سوم

دستگاه دزدگیر بعد از اجرای فرایند راه اندازی سریع، به صورت خودکار، پارتیشنی با عنوان «پیشفرض» را با مدیر اول، ریموت ها، زون های دستگاه، سنسورهای بی سیم (در صورت وجود) تشکیل می دهد. در این مرحله، شما می توانید کاربران، زون ها، سنسور (ها) یا ریموت حاضر در این پارتیشن را حذف یا اضافه نمایید.



## افزودن پارتیشن های جدید و شخصی سازی آن ها

## گام اول

گزینه «افزودن پارتیشن جدید» را انتخاب کنید.



## گام دوم

در این صفحه، اطلاعات پارتیشن جدید را وارد کرده و کاربران، زون (ها)، سنسور(ها) و ریموت آن را تعیین نمایید.

## نام پارتیشن

نام مناسبی برای پارتیشن انتخاب نمایید.

## کاربران

کاربرانی را که تمایل به مدیریت پارتیشن دارند، انتخاب نمایید.

## زون ها

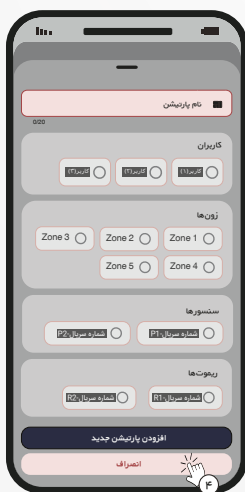
زون یا زون های موجود در ناحیه حفاظتی (پارتیشن) مربوطه را انتخاب نمایید.

## سنسورها

سنسور یا سنسورهای موجود در ناحیه حفاظتی (پارتیشن) مربوطه را انتخاب نمایید.

## ریموت ها

ریموت مورد نظر را برای کنترل ناحیه حفاظتی (پارتیشن) مربوطه، انتخاب کنید.



## قواعد مدیریت نواحی مستقل حفاظتی (پارتیشن ها)

بنا به تعریف، هر پارتیشن از حداقل یک عضو (کاربر) و یک زون یا سنسور تشکیل می شود. در مورد نواحی مستقل حفاظتی نکات زیر را مدنظر قرار دهید.

- ۱- پارتیشن های تعریف شده برای دستگاه، به راحتی در صفحه «خانه» روی اپلیکیشن در دسترس هستند.
- ۲- کاربران دستگاه تنها پارتیشن هایی را که در آنها عضو هستند، می بینند و در صورتی که به قابلیت «مسئول یا غیرمسئول کردن» دستگاه دسترسی داشته باشند، می توانند وضعیت حفاظتی پارتیشن مربوطه را تغییر دهند.
- ۳- طبق قاعده، هر زون تنها میتواند در یک پارتیشن حضور داشته باشد.
- ۴- محدودیتی در تعریف پارتیشن برای دستگاه دزدگیر وجود ندارد.

روی صفحه خانه حداکثر ۴ پارتیشن نمایش داده می شود. کاربران با انتخاب گزینه «مشاهده همه» در این بخش می توانند کلیه پارتیشن هایی را که به آن ها دسترسی دارند، مشاهده نمایند.



با لمس طولانی هر پارتیشن، می توانید پارتیشن ها را به صورت گروهی انتخاب کرده و وضعیت آنها را تغییر دهید.



## مسلح کردن و غیرمسلح کردن دستگاه دزدگیر در روش WiFi

در روش WiFi، پارتیشن‌ها (های) مورد نظر با استفاده از گزینه دو وضعیت مسلح / غیر مسلح تغییر حالت می‌دهد. با هر بار تغییر وضعیت (مسلح/غیرمسلح کردن) پیامک اعمال تغییرات برای کاربران با دسترسی مجاز به «دریافت پیامک و تماس» ارسال شده و آذیر کوتاهی از سمت دستگاه به صدا در می‌آید.

### مسلح کردن (Arm)



### غیرمسلح کردن (Disarm)



پس از اجرای فرامین، پیامکی با محتوای مرتبط برای کلیه کاربران با دسترسی مجاز ارسال می‌شود.

RedGuard-Mercury210

SN: شماره سریال دستگاه

وضعیت دستگاه تغییر کرده است:

پارتیشن: عنوان پارتیشن فعال

App

user: نام کاربر دستور دهنده

phone: شماره سیم کارت کاربر دستور دهنده

تاریخ و زمان اجرای دستور



REDGUARD M210

RedGuard-Mercury210

SN: شماره سریال دستگاه

وضعیت دستگاه تغییر کرده است:

پارتیشن: عنوان پارتیشن غیرفعال

App

user: نام کاربر دستور دهنده

phone: شماره سیم کارت کاربر دستور دهنده

تاریخ و زمان اجرای دستور



REDGUARD M210

## بخش سوم

### مدیریت دستگاه به روش اینترنت



ارتباط از طریق سرورهای امن ابری (Cloud) یکی از روش‌های پایدار و ایمن برای برقراری ارتباط میان دستگاه و اپلیکیشن هوشمند REDGUARD است. در این روش، دستگاه از طریق یک مودم Wi-Fi متصل به اینترنت به سرورهای ابری امن متصل می‌شود و از این طریق ارتباطی مطمئن با اپلیکیشن کاربر برقرار می‌گردد.

پس از فعال‌سازی این قابلیت، کاربر می‌تواند از هر مکان و در هر زمان که به اینترنت دسترسی داشته باشد، وضعیت لحظه‌ای سیستم را مشاهده کند، گزارش‌ها و رویدادهای دستگاه را دریافت نماید، فرمان‌های لازم را ارسال کرده و تنظیمات مورد نظر را اعمال کند. این شیوه ارتباطی امکان نظارت و مدیریت کامل سیستم امنیتی را حتی در زمانی که کاربر خارج از محل قرار دارد، فراهم می‌سازد. برای فعال‌سازی این روش، ابتدا لازم است از طریق ارتباط محلی، تنظیمات اینترنت دستگاه انجام شود؛ به این صورت که دستگاه با وارد کردن نام شبکه بی‌سیم (SSID) و رمز عبور آن به مودم Wi-Fi مجاور متصل می‌شود. پس از برقراری این اتصال، وضعیت اتصال در صفحه خانه به صورت «آنلاین» درآمده و امکان دسترسی و مدیریت دستگاه از راه دور فراهم خواهد شد.

## مسلح کردن و غیرمسلح کردن دستگاه دزدگیر در روش اینترنتی

در روش اینترنتی، در صورتی که دستگاه در وضعیت آنلاین قرار داشته باشد، پارتیشن (های) مورد نظر با استفاده از گزینه دو وضعیتی مسلح / غیر مسلح تغییر حالت می دهد. با هر بار تغییر وضعیت (مسلح/غیرمسلح کردن) پیامک اعمال تغییرات برای کاربران با دسترسی مجاز به «دریافت پیامک و تماس» ارسال شده و آذیر کوتاهی از سمت دستگاه به صدا در می آید.

### مسلح کردن (Arm)



### غیرمسلح کردن (Disarm)



پس از اجرای فرامین، پیامکی با محتوای مرتبط برای کلیه کاربران با دسترسی مجاز ارسال می شود.

RedGuard-Mercury210

شماره سریال دستگاه: SN: [REDACTED]

وضعیت دستگاه تغییر کرده است:

پارتیشن: عنوان پارتیشن فعال

Internet

user: نام کاربر دستور دهنده

phone: شماره سیم کارت کاربر دستور دهنده

تاریخ و زمان اجرای دستور



REDGUARD M210

RedGuard-Mercury210

شماره سریال دستگاه: SN: [REDACTED]

وضعیت دستگاه تغییر کرده است:

پارتیشن: عنوان پارتیشن غیرفعال

Internet

user: نام کاربر دستور دهنده

phone: شماره سیم کارت کاربر دستور دهنده

تاریخ و زمان اجرای دستور



REDGUARD M210

کنترل دستگاه در بستر اینترنت تنها در حالت آنلاین (اتصال به مودم اینترنت دار) امکان پذیر است. جهت مدیریت وضعیت شبکه و تغییر وضعیت آنلاین بودن، به بخش تنظیمات > تنظیمات اینترنت دستگاه مراجعه کنید.



## بخش چهارم

### مدیریت دستگاه توسط ریموت کنترل



کنترل محلی از طریق ریموت، یکی از ساده‌ترین و سریع‌ترین روش‌های مدیریت دستگاه دزدگیر است که امکان اجرای فوری فرمان‌ها را بدون نیاز به اپلیکیشن فراهم می‌کند. ریموت کنترل از طریق امواج رادیویی کوتاه‌برد (RF) با دستگاه ارتباط برقرار می‌کند و به کاربر اجازه می‌دهد زمانی که در نزدیکی دستگاه قرار دارد، عملیات مسلح یا غیرمسلح کردن پارتیشن‌ها و یا فعال کردن حالت‌های ویژه امنیتی را تنها با فشردن یک کلید انجام دهد. همچنین می‌توان سطح دسترسی هر ریموت را بنا بر نیاز کاربران شخصی‌سازی کرد. این قابلیت باعث می‌شود ریموت برای افراد متفاوت، تنها عملکردهای مجاز را در اختیار قرار دهد. به عنوان مثال، ریموت نگهبان یک واحد می‌تواند فقط قابلیت مسلح یا غیرمسلح کردن دستگاه را داشته باشد و یا برای سالمندان یک خانه، می‌توان فقط هشدارهای امنیتی را فعال نگه داشت.

## مسلح کردن و غیرمسلح کردن پارتیشن های دستگاه از طریق ریموت کنترل

با استفاده از ریموت کنترل، می‌توان پارتیشن‌های دستگاه را از طریق کلیدهای مسلح و غیرمسلح کنترل کرد. توجه داشته باشید ریموت تنها قادر به تغییر وضعیت پارتیشن‌هایی است که در آن‌ها عضو باشد و عملکرد آن برای سایر پارتیشن‌ها بی‌اثر است.

### مسلح کردن (Arm)



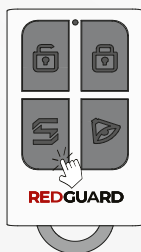
### غیرمسلح کردن (Disarm)



پس از اجرای فرامین، پیامکی با محتوای مرتبط برای تمامی کاربرانی که در پارتیشن مرتبط با ریموت عضو بوده و دسترسی «دریافت پیامک و تماس» دارند، ارسال می‌شود.

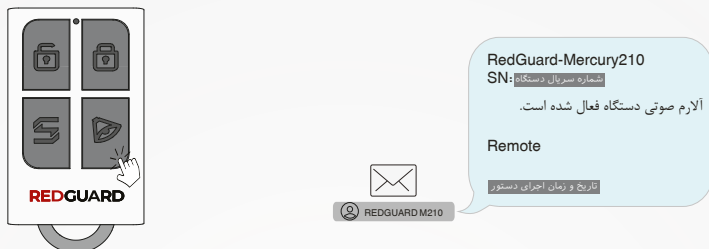


با فشردن کلید SOS، پیامکی با محتوای درخواست کمک برای تمامی کاربرانی که در پارتیشن مرتبط با ریموت عضو بوده و دسترسی دریافت پیامک و تماس دارند، ارسال می‌شود.



با فشردن کلید اعلام خطر صوتی، آژیر داخلی دستگاه و همچنین بلندگوهای متصل به آن فعال شده و پیامکی با محتوای مرتبط برای تمامی کاربرانی که در پارکیشن مرتبط با ریموت عضو بوده و دسترسی دریافت پیامک و تماس دارند، ارسال می‌شود.

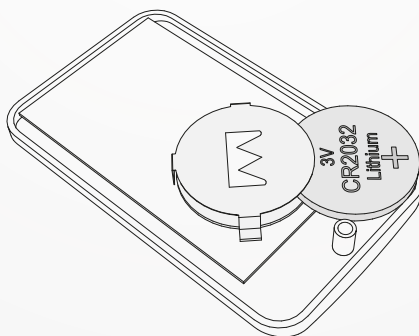
مدت زمان پخش صدای هشدار بر اساس تنظیمات تعریف‌شده برای سیرن و بلندگو در دستگاه تعیین می‌گردد.



نحوه افزودن انواع ریموت‌های استاندارد با فرکانس کاری 433MHz در بخش «افزودن ریموت جدید و شخصی‌سازی آن» شرح شده است. محدودیتی در اضافه کردن ریموت با مشخصات ذکر شده به سیستم وجود ندارد.

قدرت آنتن‌دهی ریموت به میزان شارژ باتری آن بستگی دارد. در صورتی که ریموت دستگاه به درستی کار نمی‌کند، از سلامت باتری آن مطمئن شوید.

باتری ریموت REDGUARD از نوع سکه‌ای و مدل CR2032 می‌باشد. برای تعویض باتری ریموت، پیچ آن در پشت قاب را باز کرده و با توجه به جهت قرارگیری باتری درون پلیت آن مطابق شکل زیر، اقدام به تعویض باتری قدیمی نمایید.



## بخش پنجم

### مدیریت دستگاه به روش ارتباطی پیامکی



ارتباط از طریق پیامک یکی از روش‌های ساده و کاربردی برای کنترل پارکینگ‌ها، مدیریت رله‌های متصل و دریافت گزارش از دستگاه می‌باشد که به دو شیوه مستقیم (Direct SMS) و غیرمستقیم (Application) قابل اجراست.

در روش مستقیم، کاربر با ارسال متون دستوری مشخص به شماره سیم‌کارت دستگاه از طریق پیام‌رسان تلفن همراه، فعالیت سیستم را کنترل می‌کند. در روش غیرمستقیم نیز، دستورات از طریق اپلیکیشن انتخاب شده و پیامک مرتبط به‌صورت خودکار آماده و ارسال می‌شود.

در هر دو روش، کاربر می‌تواند تمام پارکینگ‌هایی که در آن عضو است یا تنها بخشی از آن‌ها (حداکثر دو پارکینگ در هر پیامک) را مطابق نیاز خود مسلح یا غیرمسلح نماید. همچنین، امکان مدیریت رله‌های متصل و دریافت گزارش وضعیت دستگاه نیز در هر دو روش وجود دارد. این قابلیت، ابزاری مؤثر برای اطلاع از وضعیت و کنترل دستگاه از راه دور به‌شمار می‌رود.

توجه داشته باشید که شماره سیم‌کارتی که قصد برقراری ارتباط پیامکی با آن را دارید، باید به‌عنوان کاربر دستگاه تعریف شده و برای دریافت گزارش‌های پیامکی، سطح دسترسی «دریافت پیامک و تماس» را داشته باشد. همچنین سیم‌کارت نصب‌شده در دستگاه باید فعال بوده و دارای اعتبار کافی برای ارسال و دریافت پیامک باشد. روش برقراری ارتباط پیامکی در سیستم‌عامل‌های Android و iOS مشابه است و تنها در نحوه ارسال دستورات، تفاوتی جزئی به‌دلیل ساختارهای زیرساختی وجود دارد. در ادامه، شیوه برقراری ارتباط برای کاربران این دو سیستم‌عامل توضیح داده شده است.

## برقراری ارتباط پیامکی به روش غیرمستقیم

## Android برقراری ارتباط پیامکی به روش غیرمستقیم در سیستم عامل

## گام دوم

اسلات سیم کارتی که قصد برقراری ارتباط با آن را دارید، انتخاب کنید. شماره این سیم کارت باید به عنوان کاربر دستگاه ثبت شده باشد.



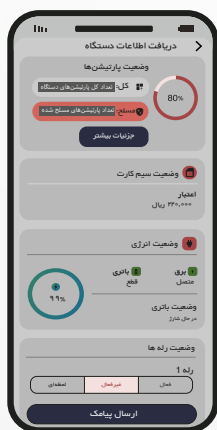
## گام اول

در صفحه «مدیریت دستگاه‌ها» دزدگیر موردنظر را انتخاب کرده و شیوه «اتصال از طریق پیامک» را برای برقراری ارتباط برگزینید.



## گام سوم

در صفحه «اتصال از طریق پیامک» می‌توانید دستگاه را مسلح یا غیرمسلح کرده و یا با انتخاب گزینه «دریافت اطلاعات دستگاه و مدیریت رله‌ها»، وضعیت پارتیشن‌ها، سیم کارت و انرژی دستگاه را مشاهده کرده و رله‌های دستگاه را کنترل نمایید.



با انتخاب گزینه «جزئیات بیشتر» لیست پارتیشن‌های دستگاه به صورت پیامکی ارسال می‌شود.

لیست پارتیشن‌ها:

لیست پارتیشن‌های دستگاه،  
مانند: اتاق خواب  
راهرو  
آشپزخانه  
سالن پذیرایی



## مسلح یا غیرمسلح کردن تمام پارتیشن‌ها در ارتباط پیامکی غیرمستقیم در سیستم عامل Android

### گام دوم

از لیست کشویی، گزینه «تمام پارتیشن‌ها» را انتخاب کنید.



### گام اول

اسلات سیم‌کارتی را انتخاب کنید که قصد دارید از طریق آن با دستگاه ارتباط برقرار کنید. سپس یکی از گزینه‌های «ارسال دستور مسلح» یا «ارسال دستور غیرمسلح» را انتخاب کنید.



### گام سوم

گزینه «ارسال پیامک» را انتخاب کنید.



RedGuard-Mercury210

SN: شماره سریال دستگاه

پارتیشن: لیست پارتیشن‌های دستگاه

دستگاه: مسلح/غیرمسلح شد توسط

SMS

user: نام کاربر دستور دهنده

phone: شماره سیم کارت کاربر دستور دهنده

تاریخ و زمان اجرای دستور

## مسلح یا غیرمسلح کردن بخشی از پارتیشن‌ها در ارتباط پیامکی غیرمستقیم در سیستم عامل Android

### گام دوم

از لیست کشویی، گزینه «بخشی از پارتیشن‌ها» را انتخاب کنید.



### گام اول

اسلات سیم‌کارتی را انتخاب کنید که قصد دارید از طریق آن با دستگاه ارتباط برقرار کنید. سپس یکی از گزینه‌های «ارسال دستور مسلح» یا «ارسال دستور غیرمسلح» را انتخاب کنید.



### گام سوم

نام دقیق پارتیشن مورد نظر را وارد کنید و سپس گزینه «ارسال پیامک» را انتخاب کنید. همچنین در صورت نیاز می‌توانید با انتخاب گزینه + وضعیت فعالیت یک پارتیشن دیگر را نیز تحت کنترل قرار دهید.



RedGuard-Mercury210

SN: [شماره سریال دستگاه]

وضعیت دستگاه تغییر کرده است:

پارتیشن: عنوان پارتیشن اول مسلح/غیرمسلح

SMS

user: نام کاربر دستور دهنده

phone: شماره سیم‌کارت کاربر دستور دهنده

تاریخ و زمان اجرای دستور



REGUARD M210

## مدیریت رله‌ها در ارتباط پیامکی در سیستم عامل Android

## گام اول

وضعیت نهایی رله‌های متصل به دستگاه را تعیین کرده و گزینه «ارسال پیامک» را انتخاب کنید. پس از اجرای فرامین، وضعیت رله‌ها در این صفحه به روز می‌شود.



با انتخاب حالت «لحظه‌ای»، رله مورد نظر به مدت ۲ ثانیه فعال و سپس غیرفعال می‌گردد. استفاده از چنین قابلیت‌هایی برای فرامین لحظه‌ای مثل باز کردن درب خانه کاربرد دارد.

## برقراری ارتباط پیامکی به روش غیرمستقیم در سیستم عامل iOS

## مسئله یا غیرمسئله کردن تمام پارتیشن‌ها در ارتباط پیامکی غیرمستقیم در سیستم عامل iOS

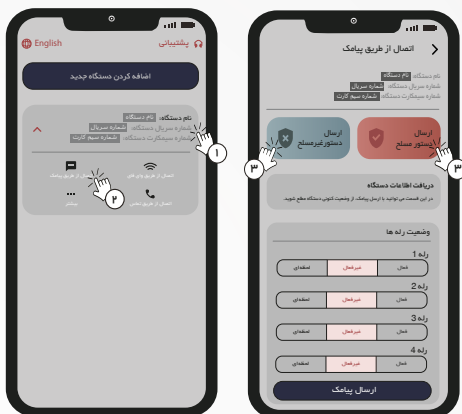
## گام دوم

از لیست کشویی، گزینه «تمام پارتیشن‌ها» را انتخاب کنید.



## گام اول

در صفحه «مدیریت دستگاه‌ها» دزدگیر مورد نظر را انتخاب کرده و شیوه «اتصال از طریق پیامک» را برای برقراری ارتباط برگزینید. سپس یکی از گزینه‌های «ارسال دستور مسلح» یا «ارسال دستور غیرمسلح» را انتخاب کنید.



## گام سوم

گزینه «ارسال پیامک» را انتخاب کنید.

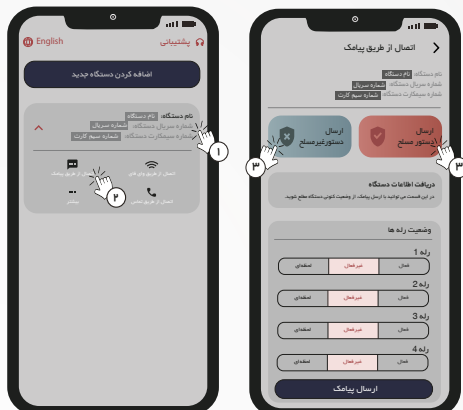


توجه داشته باشید شماره سیم‌کارتی که قصد برقراری ارتباط پیامکی با آن را دارید، باید به عنوان کاربر دستگاه ثبت شده و برای دریافت گزارشات پیامکی، سطح دسترسی «دریافت پیامک و تماس» برای آن فعال باشد.

## مسئله یا غیرمسئله کردن بخشی از پارتیشن‌ها در ارتباط پیامکی غیرمستقیم در سیستم عامل iOS

### گام اول

در صفحه «مدیریت دستگاه‌ها» دزدگیر موردنظر را انتخاب کرده و شیوه «اتصال از طریق پیامک» را برای برقراری ارتباط برگزینید. سپس یکی از گزینه‌های «ارسال دستور مسلح» یا «ارسال دستور غیرمسلح» را انتخاب کنید.



### گام دوم

از لیست کشویی، گزینه «بخشی از پارتیشن‌ها» را انتخاب کنید.



### گام سوم

نام دقیق پارتیشن مورد نظر را وارد کنید و سپس گزینه «ارسال پیامک» را انتخاب کنید.

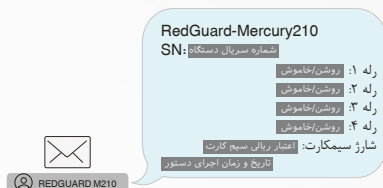


در صورت نیاز می‌توانید با انتخاب گزینه + وضعیت فعالیت یک پارتیشن دیگر را نیز تحت کنترل قرار دهید.

## مدیریت رله ها در ارتباط پیامکی در سیستم عامل iOS

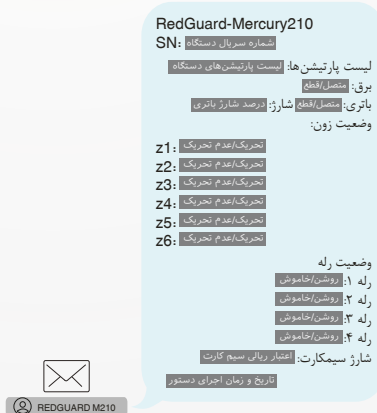
## گام اول

وضعیت نهایی رله های متصل به دستگاه را تعیین کرده و گزینه «ارسال پیامک» را انتخاب کنید. پس از اجرای فرامین، وضعیت رله ها در این صفحه به روز شده و پیامک وضعیت نهایی رله ها برای کلیه کاربران با دسترسی مجاز ارسال می شود.



با انتخاب حالت «لحظه‌ای»، رله مورد نظر به مدت ۲ ثانیه فعال و سپس غیرفعال می گردد. استفاده از چنین قابلیت برای فرامین لحظه‌ای مثل باز کردن درب خانه کاربرد دارد.

با انتخاب گزینه «دریافت اطلاعات دستگاه» گزارش کاملی از وضعیت فعالیت دستگاه، وضعیت انرژی، وضعیت زون ها و رله‌های دستگاه به صورت پیام کوتاه اعلام می شود.



## برقراری ارتباط پیامکی به روش مستقیم

### مسلح یا غیرمسلح کردن بخشی از پارتیشن‌ها در ارتباط پیامکی مستقیم

برای ارسال دستور «فعال/مسلح» یا «غیرفعال/غیرمسلح» از طریق پیامک به سیم‌کارت دستگاه، از ساختار دستوری زیر استفاده کنید:

<دستور> [فاصله] <نام\_پارتیشن\_اول>  
<دستور> [فاصله] <نام\_پارتیشن\_اول> [فاصله] <نام\_پارتیشن\_دوم>

واژه جایگزین <دستور> را می‌توانید از جدول زیر پیدا کنید:

|          |        |
|----------|--------|
| غیرمسلح  | مسلح   |
| غیرفعال  | فعال   |
| خاموش    | روشن   |
| disarm   | arm    |
| off      | on     |
| deactive | active |

به عنوان مثال، دستور زیر، پارتیشن **انبار** را به حالت مسلح در می‌آورد:

#### فعال انبار

و یا با ارسال دستور زیر، پارتیشن‌های **اتاق خواب** و **انبار** به طور همزمان غیرمسلح خواهند شد.

#### off اتاق خواب انبار

دستگاه پس از دریافت پیامک، پاسخ تأیید مبنی بر اجرای عملیات را ارسال خواهد کرد.



REDGUARD M210

در صورت عدم دریافت پاسخ پیامکی از سمت دستگاه، موارد زیر را بررسی کنید:

- شماره فرستنده پیام به عنوان کاربر دستگاه تعریف شده است،
- کاربر فرستنده پیام نقش مدیر را دارد یا به «دریافت پیامک و تماس» دسترسی دارد،
- نام پارتیشن دقیق پارتیشن(ها) به درستی وارد می‌شود،
- سیم‌کارت دستگاه فعال و دارای اعتبار است و آنتن‌دهی در محل نصب دستگاه مطلوب می‌باشد.

در هر پیام کوتاه، وضعیت حداکثر دو پارتیشن را می‌توان تغییر داد.

## مسلح یا غیرمسلح کردن تمام پارتیشن‌ها در ارتباط پیامکی مستقیم

چنانچه دستور بدون ذکر نام پارتیشن ارسال شود، دستگاه به‌طور خودکار همه پارتیشن‌هایی را که کاربر در آن‌ها عضو است، بر اساس دستور ارسالی، مسلح یا غیرمسلح می‌کند. ساختار دستوری، برای تغییر وضعیت تمام پارتیشن‌ها به صورت زیر است:

<دستور>

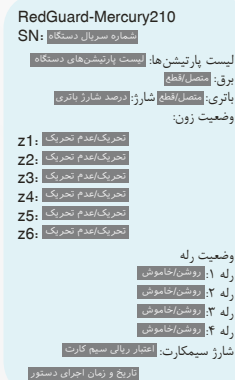
واژه جایگزین <دستور> را می‌توانید از جدول زیر پیدا کنید:

| غیرمسلح  | مسلح   |
|----------|--------|
| غیرفعال  | فعال   |
| خاموش    | روشن   |
| disarm   | arm    |
| off      | on     |
| deactive | active |

دستگاه پس از دریافت پیامک، پاسخ تأیید مبنی بر اجرای عملیات را ارسال خواهد کرد.

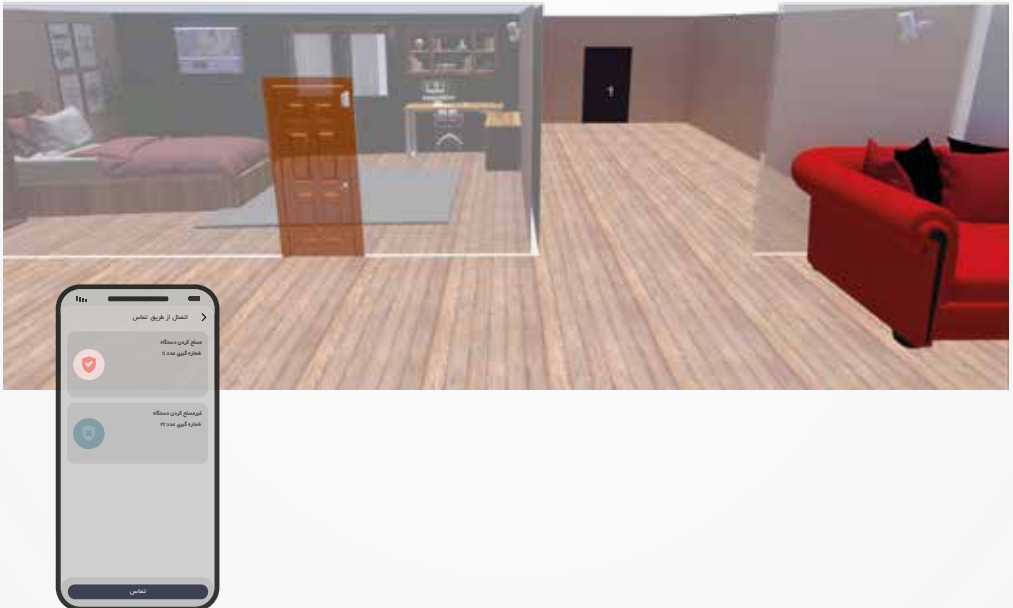


با ارسال واژه‌های **وضعیت** و **info** در قالب پیامک به شماره سیم کارت دستگاه، گزارش پیامکی کاملی از نحوه فعالیت تمام پارتیشن‌های دستگاه برای کاربر ارسال می‌شود.



## بخش ششم:

### مدیریت دستگاه به روش ارتباطی تماس



یکی از روش‌های سریع و مطمئن برای کنترل دستگاه دزدگیر، استفاده از تماس مستقیم تلفنی با دستگاه است. در این حالت، کاربر با برقراری تماس با شماره سیم‌کارت دستگاه می‌تواند با وارد کردن کد دسترسی خاصی، پارتیشن‌هایی را که در آنها عضو باشد، مسلح یا غیرمسلح کند. در این روش کاربران باید به سطح دسترسی «امکان برقراری تماس با دستگاه» مجهز بوده و برای دریافت گزارش پیامکی دسترسی «دریافت پیامک و برقراری تماس» را داشته باشد. با فرض آنتن دهی مطلوب در محل نصب دستگاه، سرعت اجرای فرمان در این روش بیشتر از روش ارتباطی پیامکی می‌باشد.

## برقراری ارتباط تلفنی با دستگاه دزدگیر

### گام اول

در صفحه «مدیریت دستگاه ها» دزدگیر مورد نظر را انتخاب کرده و شیوه «اتصال از طریق تماس» را برای برقراری ارتباط برگزینید.



### گام دوم

گزینه «تماس» را انتخاب کنید تا به صفحه شماره‌گیری هدایت شوید. پس از برقراری ارتباط موفق، می‌توانید با شماره گیری کدهای دستوری خاص، دستگاه دزدگیر را مسلح یا غیر مسلح کنید.

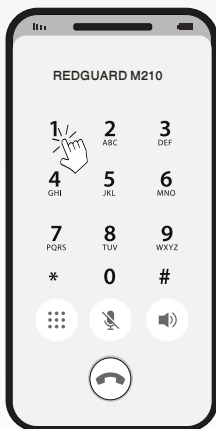


توجه داشته باشید شماره سیم‌کارتی که قصد برقراری ارتباط تلفنی با آن را دارید، باید به عنوان کاربر دستگاه ثبت شده و سطح دسترسی «امکان برقراری تماس با دستگاه» برای آن فعال باشد.

## مسلح کردن و غیرمسلح کردن دستگاه دزدگیر در روش تماس

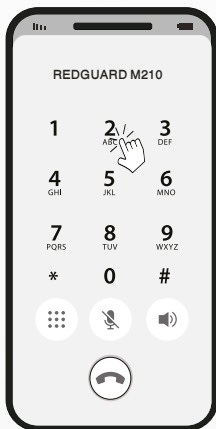
مسلح کردن (Arm):

شماره گیری کد «۱۱»



غیرمسلح کردن (Disarm):

شماره گیری کد «۲۲»



پس از دریافت فرمان، دستگاه بلافاصله عملیات مربوطه را روی تمام پارتیشن هایی که کاربر در آنها عضو بوده، اجرا کرده و صدای تأیید آن از طریق آژیر داخلی پخش خواهد شد. تماس برقرارشده تا زمان پخش صدای آژیر ادامه می‌یابد و سپس به‌طور خودکار قطع می‌شود. پس از اجرای عملیات، پیامکی با محتوای مرتبط برای تمامی کاربرانی که در پارتیشن های مرتبط عضو بوده و دسترسی «دریافت پیامک و تماس» دارند، ارسال می‌شود.

RedGuard-Mercury210

SN: شماره سریال دستگاه

دستگاه فعال شد توسط

Call

user: نام کاربر دستور دهند:

phone: شماره سیم کارت کاربر دستور دهند:

تاریخ و زمان اجرای دستور



REDGUARD M210

RedGuard-Mercury210

SN: شماره سریال دستگاه

دستگاه غیرفعال شد توسط

Call

user: نام کاربر دستور دهند:

phone: شماره سیم کارت کاربر دستور دهند:

تاریخ و زمان اجرای دستور



REDGUARD M210

## پرسش های پرتکرار

آیا می توانم دو دستگاه دزدگیر ردگارد را در اپلیکیشن مدیریت کنم؟! 

بله. شما می توانید حداکثر پنج دستگاه ردگارد را در اپلیکیشن REDGUARD مدیریت نمایید. برای انجام این کار در هنگام ورود به اپلیکیشن در صفحه "مدیریت دستگاه ها" از گزینه «افزودن دستگاه» اقدام به تعریف دستگاه جدید نمایید. 

در صورتی که ریموت یکی از کاربران سرقت و یا مفقود شود، چه اقدامی باید انجام دهم؟! 

در کمال حفظ خونسردی، با مراجعه به بخش «مدیریت ریموت ها» از قسمت افزونه ها، ریموت مفقود شده را انتخاب و حذف نمایید. با این کار ریموت مفقود شده قادر به مسلح/غیرمسلح کردن دستگاه دزدگیر نخواهد بود. 

من مدیر یک مجتمع هستم و نیاز دارم که واحد نگهبانی در صورت وقوع خطر سرقت مطلع گردد. آیا این امکان در اپلیکیشن REDGUARD قابل انجام است؟! 

بله. برای این منظور یک کاربر جدید با شماره همراه واحد نگهبانی ایجاد کرده و سطح دسترسی مناسب این کاربر را در همان قسمت مشخص نمایید. به عنوان مثال می توانید واحد نگهبانی را به عنوان یک کاربر فقط با سطح دسترسی «دریافت پیامک و تماس» معرفی کرده تا قابلیت مسلح/غیرمسلح کردن دزدگیر شما را نداشته باشد. 

در هنگام قطعی برق، دستگاه از کار می افتد؟! 

خیر. دستگاه دزدگیر اماکن ردگارد مدل M210 دارای یک باتری پشتیبان داخلی است که در مواقع قطعی برق، انرژی لازم برای ادامه فعالیت دزدگیر را کاملاً فراهم می کند. این باتری به صورت خودکار در زمان اتصال برق شهری به صورت استاندارد شارژ می شود تا علاوه بر حفظ سلامت باتری، نگرانی شما را هنگام قطعی برق رفع نماید. 

در محل مورد نظر برای نصب ردگارد قطعی برق به صورت چندین ساعت رخ می دهد، آیا باتری ردگارد مدل M210 و M220 می توانند چندین ساعت در زمان قطعی برق به ادامه حفاظت بپردازد؟! 

میزان شارژدهی باتری داخلی دزدگیر ردگارد مدل M210 و M220 به میزان تردد و اعلان خطر در محل مورد نظر وابسته است. اما برای استفاده در مکان هایی با قطعی برق طولانی دو راهکار زیر پیشنهاد می گردد: 

**راهکار اول:** گزینه کمبود شارژ باتری و حالت ذخیره نیرو در بخش «تنظیمات دستگاه» را فعال نمایید. در این حالت در صورتی که میزان شارژ باتری داخلی ردگارد به ۲۰٪ کاهش یابد، دستگاه علاوه بر ارسال پیامک کمبود شارژ باتری، اعلان هشدار با بلندگوها را غیرفعال نموده و وقوع خطر سرقت را از طریق پیامک، تماس و آژیر داخلی اطلاع رسانی می کند. با این قابلیت، دستگاه می تواند زمان بیشتری در هنگام قطعی برق به ادامه فعالیت خود بپردازد.

**راهکار دوم:** می توانید باتری داخلی دستگاه را تعویض کرده و از باتری های 12V از نوع لیتیومی یا اسیدی با ظرفیت بالاتر استفاده نمایید و سپس نوع باتری را در تنظیمات دستگاه انتخاب کنید. جهت کسب اطلاعات بیشتر، به پیوست راهنما مراجعه فرمایید.

در خانواده ما سالمندی زندگی می کند که ممکن است در مواقعی که در منزل تنها است، نیازمند کمک باشد. برای این هدف، قابلیتی در دزدگیر ردگارد گنجانده شده است؟! 

بله. طراحی و تولید ردگارد نه تنها به منظور رفع نیازهای امنیتی کاربران بوده، بلکه به منظور رفع نگرانی نگهداری از سالمندان نیز به این امر پرداخته شده است. بدین منظور با فشردن کلید SOS بر روی ریموت، یک پیامک درخواست کمک به اعضا، پارتیشن که مجوز دریافت پیامک دارند ارسال می گردد که می توان برای این امر از آن بهره برد. 

منظور از به روزرسانی سیستم عامل دزدگیر ردگارد چیست؟

✓ عملکرد و قابلیت های دزدگیر به سیستم عامل آن بستگی دارد. از آنجایی که قابلیت های مورد نیاز کاربران در گذر زمان تغییر می یابد، قابلیت به روزرسانی سیستم عامل در بخش تنظیمات اپلیکیشن با عنوان «به روزرسانی دستگاه» تعریف شده تا به صورت پیوسته ویژگی های جدید در جهت آرامش خاطر کاربران به سیستم امنیتی ردگارد افزوده شود.

همچنین به روزرسانی اپلیکیشن «REDGUARD» نیز امکانات تازه ای در اختیار شما قرار داده و تجربه کاربری بهتری را به همراه خواهد داشت. برای اجرای این عملیات، از قسمت «به روزرسانی اپلیکیشن» در بخش تنظیمات اقدام نمایید.

؟ اگر سیستم امنیتی ردگارد در اثر قطعی برق و همچنین اتمام شارژ باتری آن خاموش شود، تمامی اطلاعات کاربران و تنظیمات آن حذف می شوند؟

✓ خیر. نه تنها اطلاعات کاربران و تنظیمات حذف نشده، بلکه به محض اتصال مجدد برق، دستگاه به کار خود ادامه می دهد.

؟ اگر نیازمند شدت صدای بیشتری نسبت به آژیر داخلی در هنگام فعال شدن اعلان خطر باشیم، می توان شدت صدای آژیر دستگاه را تغییر داد؟

✓ شدت صدای آژیر داخلی دستگاه ثابت و مناسب مکان های داخلی است. برای افزایش شدت صدای آژیر می توانید دو عدد بلندگو ۸ اهم با حداقل توان ۱۵ وات را به دستگاه دزدگیر متصل نمایید. همچنین برای تنظیم مدت زمان و نوع آژیر این دو بلندگو از قسمت «تنظیمات دستگاه» و تنظیمات بلندگوها، تغییرات لازم را اعمال کنید. جهت کسب اطلاعات بیشتر در خصوص نحوه اتصال بلندگوها به بخش پیوست مراجعه کنید.

؟ اعتبار سیم کارت دستگاه را چگونه مشاهده نمایم؟

✓ با ورود به صفحه "خانه" در اپلیکیشن REDGUARD می توانید اطلاعات وضعیت دستگاه را از جمله اعتبار سیم کارت مشاهده نمایید. همچنین در صورت کاهش اعتبار سیم کارت به مبلغ ۱۰۰۰۰ ریال، پیامکی مبنی بر کمبود اعتبار سیم کارت دزدگیر ردگارد به کاربران ارسال خواهد شد.

؟ سوال من در هیچ کدام از موارد فوق نبود، چگونه پاسخ خود را بیابم؟

✓ چنانچه پاسخ سوال شما در بخش سوالات متداول موجود نبود، می توانید با انتخاب گزینه «پشتیبانی» در صفحه «خانه» اپلیکیشن یا از طریق لینک زیر، با کارشناسان ما در ارتباط باشید.



ارتباط با پشتیبانی

## جداول

جدول (۱)

## پنل نشانگرها

| خاموش                                          | چشمک زن                                                                                                     | روشن                    |                   |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-------------------------|-------------------|
| دستگاه خاموش است.                              | -                                                                                                           | دستگاه روشن است.        | POWER             |
| -                                              | دستگاه در حال پردازش است.                                                                                   | دستگاه بیکار است.       | STATUS            |
| تغذیه واحد GSM قطع است.                        | -                                                                                                           | تغذیه واحد GSM وصل است. | POWER-GSM         |
| -                                              | چشمک زن آهسته:<br>دستگاه در حال جستجو شبکه است.<br>چشمک زدن کوتاه:<br>دستگاه به شبکه متصل شده است.          | -                       | CONNECT           |
| -                                              | دستگاه مشغول ارسال پیامک به کاربران است.                                                                    | -                       | BUSY              |
| -                                              | شبکه WiFi داخلی دستگاه روشن است.                                                                            | -                       | WiFi              |
| باتری متصل نیست یا<br>توسط کلید باتری قطع است. | چشمک زن آهسته:<br>باتری دستگاه در حال شارژ است.<br>چشمک زن سریع:<br>برق دستگاه قطع است و باتری در مدار است. | شارژر باتری کامل است.   | BATTERY           |
| دستگاه دزدگیر غیرمسلح است.                     | -                                                                                                           | دستگاه دزدگیر مسلح است. | ARM               |
| زون بدون تحریک است.                            | -                                                                                                           | زون تحریک شده است.      | ZONE#1~<br>ZONE#6 |

جدول (۲)

## کلیدهای ریموت

|                            |  |
|----------------------------|--|
| مسلح کردن دستگاه           |  |
| غیرمسلح کردن دستگاه        |  |
| درخواست کمک (اعلان پیامکی) |  |
| اعلام خطر صوتی             |  |

جدول (۳)

## پیام های کوتاه

| متن پیام کوتاه                                                                                              | رخداد                                             |    |
|-------------------------------------------------------------------------------------------------------------|---------------------------------------------------|----|
| دزدگیر روشن شد. وضعیت پارتیشن (ها): <b>فعال/غیرفعال</b>                                                     | روشن شدن دستگاه بعد از اتصال برق یا باتری         | ۱  |
| – برق دستگاه قطع شد.                                                                                        | قطع شدن برق دستگاه                                | ۲  |
| – برق دستگاه وصل شد.                                                                                        | وصل شدن برق دستگاه                                | ۳  |
| – باتری دستگاه وصل شد.                                                                                      | اتصال باتری به دستگاه                             | ۴  |
| – باتری دستگاه قطع شد.                                                                                      | قطع شدن باتری دستگاه                              | ۵  |
| – میزان شارژ باتری دستگاه کم است.                                                                           | کاهش یافتن شارژ باتری                             | ۶  |
| پارتیشن: <b>عنوان پارتیشن ها</b><br>دستگاه <b>فعال/غیرفعال</b> شد توسط (CALL, SMS, D-SMS, Remote)           | مسلم/غیرمسلم نمودن تمامی پارتیشن های دستگاه       | ۷  |
| وضعیت دستگاه تغییر کرده است.                                                                                | مسلم/غیرمسلم نمودن بخشی از پارتیشن های دستگاه     | ۸  |
| آلارم دستگاه فعال شده است.<br>پارتیشن: <b>عنوان پارتیشن (ها)</b><br>نام سنسور: <b>عنوان سنسور تحریک شده</b> | تحریک سنسورها و وقوع خطر                          | ۹  |
| هشدار: بلندگو شماره یک وصل شد.                                                                              | متصل شدن بلندگو به ترمینال SP1                    | ۱۰ |
| هشدار: بلندگو یک قطع شد.                                                                                    | قطع شدن بلندگوی متصل به ترمینال SP1               | ۱۱ |
| هشدار: بلندگو شماره دو وصل شد.                                                                              | متصل شدن بلندگو به ترمینال SP2                    | ۱۲ |
| هشدار: بلندگو شماره دو قطع شد.                                                                              | قطع شدن بلندگوی متصل به ترمینال SP2               | ۱۳ |
| خروجی تغذیه دستگاه اتصال کوتاه شده است.                                                                     | وقوع اتصال کوتاه در خط تغذیه (EXT, ZONE و RELAY)  | ۱۴ |
| هشدار: سیرین خارجی اتصال کوتاه شده است.                                                                     | وقوع اتصال کوتاه در سیرین متصل به ترمینال SIR     | ۱۵ |
| درخواست SOS                                                                                                 | فشردن دکمه SOS ریموت                              | ۱۶ |
| سیم کارت دستگاه تغییر کرده است لطفا از طریق نرم افزار REDGUARD تایید نمایید.                                | تغییر یافتن سیم کارت داخلی دستگاه بدون تایید کردن | ۱۷ |
| هشدار: سیم کارت جدید دستگاه توسط کاربر زیر تایید گردید.                                                     | تایید کردن سیم کارت جدید در دستگاه                | ۱۸ |
| سیم کارت دستگاه فعال شد.                                                                                    | فعال شدن سیم کارت                                 | ۱۹ |
| شارژ سیم کارت دستگاه کم است.<br>شارژ کنونی: ۷۵۶ ریال                                                        | کاهش یافتن اعتبار سیم کارت دستگاه                 | ۲۰ |

جدول (۴)

## مشخصات فنی

|                                   |                        |
|-----------------------------------|------------------------|
| 433MHz                            | فرکانس کاری تجهیزات RF |
| 220VAC                            | ولتاژ تغذیه            |
| Wi-Fi, GSM, RF 433MHz             | بستر ارتباطی بیسیم     |
| 12.6V 2200mAH-Lithium ion         | مشخصات باتری پشتیبان   |
| 280x225x80 mm                     | ابعاد بدنه دستگاه      |
| 58x35x12 mm                       | ابعاد ریموت کنترل      |
| تقریباً 95-110dB در فاصله یک متری | سطح صدا آزر داخلی      |

جدول (۵)

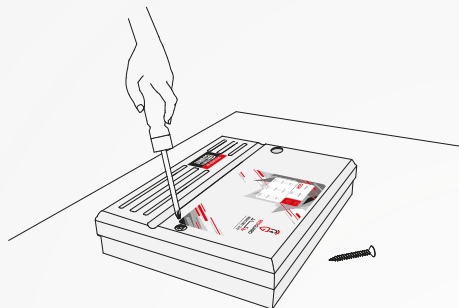
## روش های فعالیت دستگاه

| غیرمسلح کردن دستگاه                                                                                                 | مسلح کردن دستگاه                                                                                          |                  |
|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|------------------|
| انتخاب گزینه                       | انتخاب گزینه             | اپلیکیشن         |
| فشاردن کلید  روی ریموت           | فشاردن کلید  روی ریموت | ریموت            |
| وارد کردن عبارت '۲۲' بعد از برقراری تماس                                                                            | وارد کردن عبارت '۱۱' بعد از برقراری تماس                                                                  | تماس تلفنی       |
| ارسال یکی از واژه های "غیرمسلح" یا "غیرفعال" یا "خاموش" یا "disarm" یا "off" یا "deactive" به شماره سیم کارت دستگاه | ارسال یکی از واژه های "مسلح" یا "فعال" یا "روشن" یا "arm" یا "on" یا "active" به شماره سیم کارت دستگاه    | ارسال پیام کوتاه |

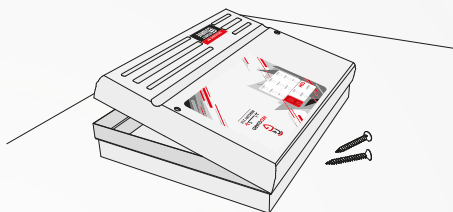
## پیوست

اجرا و نصب تجهیزات جانبی دستگاه که در این بخش شرح داده شده‌اند، به منظور راهنمایی تکنسین مجاز نصب بوده و پیامدهای ناشی از نصب نامناسب تجهیزات جانبی به عهده مالک محصول خواهد بود.  
میزان جریان قابل تامین توسط دستگاه برای کلیه تجهیزات متصل حداکثر ۱/۵ آمپر می‌باشد.

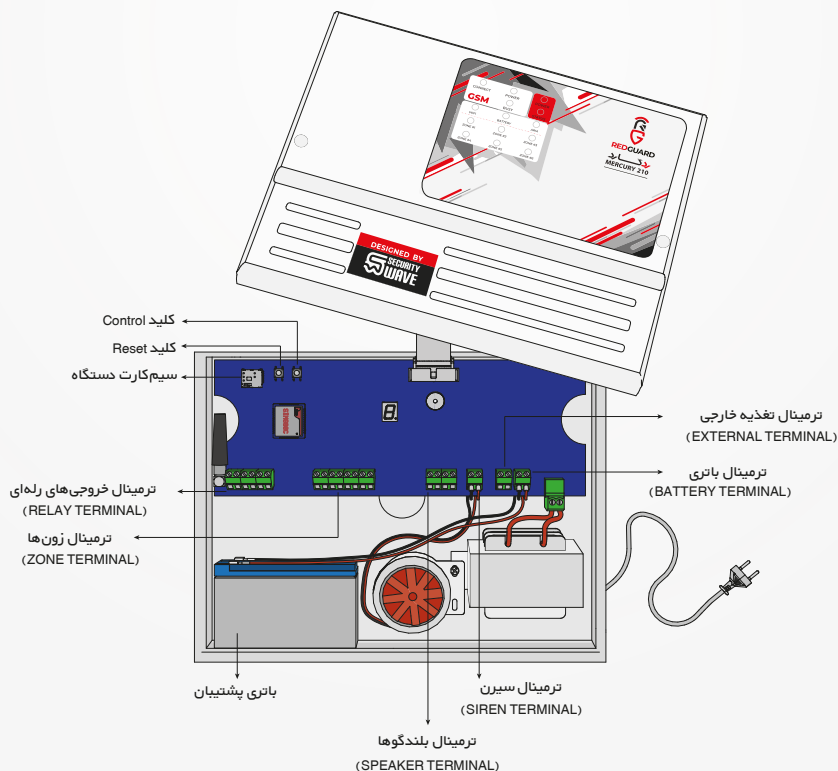
## دستورالعمل باز کردن درب دستگاه



گام اول- دستگاه را از محل نصب خارج کنید و پیچ‌های بزرگ اتصال قاب را باز کنید.



گام دوم- درب را به آهستگی باز کنید. مراقب باشید حین باز کردن درب، اتصالات داخلی دستگاه، دچار قطعی نگردند.



## تهیه و جای گذاری سیم کارت

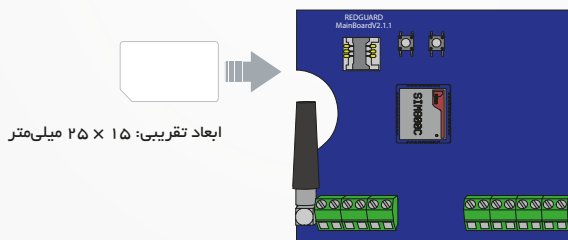
### انتخاب و تهیه سیم کارت

پیش از انتخاب سیم کارت، نکات زیر را مدنظر داشته باشید:

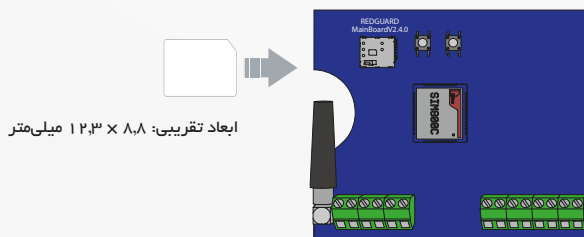
- از آنجا که دستگاه برای برقراری ارتباط از طریق پیامک و تماس تلفنی از بستر شبکه تلفن همراه استفاده می‌کند، کیفیت پوشش آنتن در محل نصب، نقشی تعیین‌کننده در برقراری اتصال پایدار، سرعت اطلاع‌رسانی و عملکرد کلی سیستم دارد.
- بنابراین توصیه می‌شود پیش از نصب سیم کارت، پوشش شبکه اپراتورهای مختلف را بررسی کرده و سیم‌کارتی را انتخاب کنید که از قدرت آنتن‌دهی و پایداری بالاتری برخوردار است.
- درصد آنتن‌دهی سیم‌کارت دستگاه در صفحه «خانه» اپلیکیشن و در بخش «وضعیت سیم‌کارت» قابل مشاهده است. در این قسمت میزان آنتن‌دهی به‌صورت درصدی بیان شده است. هرچه مقدار این عدد بیشتر از ۵۰٪ باشد، کیفیت پوشش شبکه در محل نصب، مناسب‌تر بوده و سرعت برقراری ارتباط، دریافت فرمان‌ها و ارسال پیام‌ها بیشتر خواهد بود.
- عملکرد صحیح دستگاه با سیم‌کارت‌های اپراتورهای همراه اول و ایرانسل بررسی و تأیید شده است. عملکرد دستگاه با سیم‌کارت‌های سایر اپراتورها تضمین نمی‌شود.
- سیم‌کارت دستگاه باید فاقد قفل PUK باشد.
- سیم‌کارت مورد استفاده باید از نوع اعتباری (غیر دائمی) بوده و همواره دارای شارژ کافی برای برقراری ارتباط و ارسال هشدارها باشد.
- اندازه سیم‌کارت باید متناسب با محل تعبیه‌شده روی برد الکترونیکی دستگاه باشد.

### جای گذاری سیم کارت درون دستگاه

خشب(اسلات) سیم کارت دستگاه دزدگیر شما ممکن است به یکی از دو شکل زیر باشد. با توجه به راهنمای تصویری زیر، سیم کارت با اندازه مناسب را در جهت درست درون خشاب آن قرار دهید.



نحوه قرار دادن سیم کارت Mini SIM در خشاب تخت



نحوه قرار دادن سیم کارت Nano SIM در خشاب فنی

## باتری پشتیبان

### تعویض باتری دستگاه

عواملی همچون دما، رطوبت و ... بر عمر باتری دستگاه تاثیرگذار می‌باشند و ممکن است با گذشت زمان کیفیت مطلوب باتری را کاهش دهند. با توجه به اهمیت وجود باتری جهت ادامه فعالیت سیستم امنیتی هنگام قطع برق، لازم است در چنین شرایطی، بعد از تهیه باتری جایگزین با مشخصات منطبق با باتری دستگاه، اقدام به تعویض آن نمایید.

➡ مشخصات نامی باتری پشتیبان (پیش فرض کارخانه): 12.6V 2200mAh-Lithium ion

➡ هنگام تعویض باتری به جهت صحیح اتصال باتری (قطب های + و -) دقت نمایید.

### انتخاب باتری پشتیبان با ظرفیت مناسب

با توجه به ضرورت فعال بودن بی وقفه سیستم حفاظتی، استفاده از باتری پشتیبان با ظرفیت مناسب، باعث می‌شود دستگاه برای مدت طولانی‌تری بدون اتصال به منبع برق فعال بماند. این موضوع به خصوص در زمان قطعی طولانی مدت برق اهمیت بیشتری پیدا می‌کند.

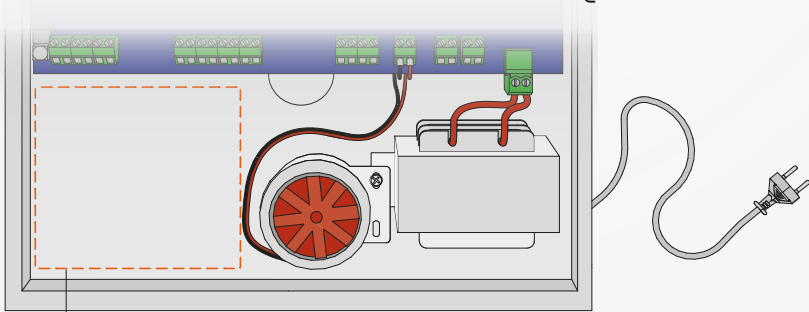
دستگاه دزدگیر شما امکان نصب دو نوع باتری پشتیبان 12 ولت اسیدی مدل SLA و باتری‌های لیتیومی را دارد. محل نصب باتری در شکل اجزای داخلی دستگاه نشان داده شده است. با توجه به تفاوت ابعاد باتری در برندهای مختلف، پیش از خرید، حتماً اندازه آن را با فضای داخلی قاب دستگاه تطبیق دهید.

ظرفیت باتری انتخابی باید با مشخصات فنی دستگاه مطابقت داشته باشد. استفاده از باتری‌های نامرغوب، فاقد استاندارد یا خارج از محدوده ظرفیت اعلام شده می‌تواند موجب آسیب به برد الکترونیکی دستگاه شده و گارانتی را از اعتبار خارج کند.

باتری‌های SLA از رایج‌ترین انواع باتری پشتیبان در سیستم‌های امنیتی هستند. این باتری‌ها قیمت مناسب‌تری دارند، به راحتی در دسترس هستند و برای کاربردهای عمومی گزینه‌ای مطمئن و اقتصادی به شمار می‌روند. در مقابل، باتری‌های لیتیومی وزن کمتر، طول عمر بیشتر، سرعت شارژ بهتر و بازدهی بالاتری دارند و معمولاً برای کاربرانی مناسب هستند که به عملکرد بهتر، دوام بیشتر و ابعاد یا وزن کمتر اهمیت می‌دهند.

به طور کلی، باتری SLA انتخابی اقتصادی و متداول برای استفاده‌های معمول است، در حالی که باتری لیتیومی گزینه‌ای پیشرفته‌تر با طول عمر و کارایی بالاتر محسوب می‌شود. با این حال، برای استفاده صحیح و ایمن، لازم است نوع باتری متصل شده در تنظیمات دستگاه به درستی انتخاب شود.

➡ پس از اتصال باتری، لازم است نوع باتری مورد استفاده را در بخش تنظیمات < تنظیمات دستگاه > باتری مطابق با باتری نصب شده تنظیم نمایید. انتخاب نادرست نوع باتری در تنظیمات دستگاه ممکن است باعث اختلال در فرآیند شارژ، عملکرد نامناسب سیستم، نمایش نادرست سطح شارژ باتری و در نهایت کاهش عمر مفید باتری شود.



فضای قرارگیری باتری پشتیبان

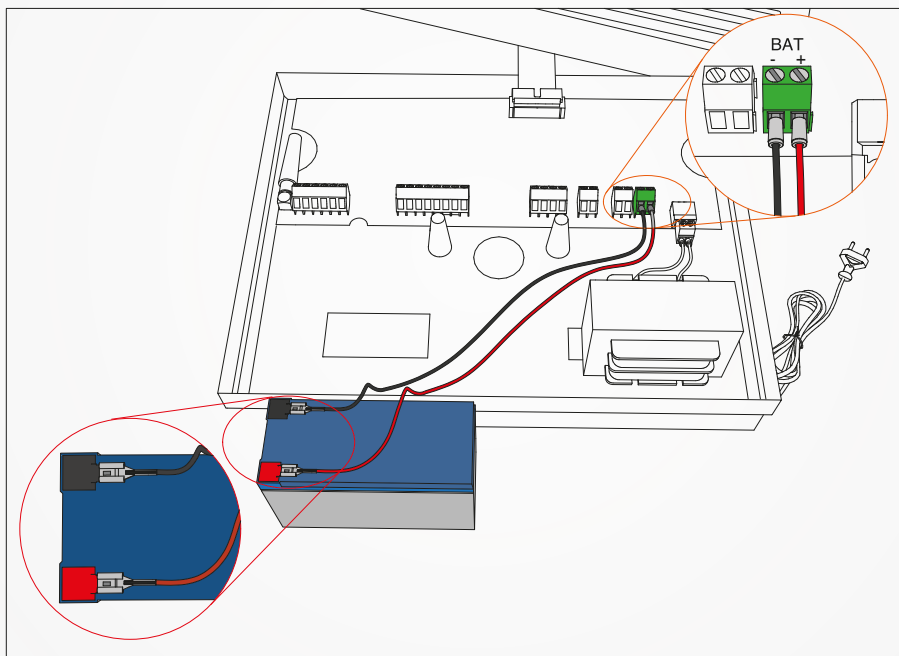
## نصب باتری پشتیبان

سیم های باتری را مطابق جدول و نقشه زیر به ترمینال BAT روی برد الکترونیکی و پایه های مثبت و منفی باتری متصل کنید.

باتری 12V-SLA      سیم اتصال به ترمینال      ترمینال BAT روی برد دستگاه

ترمینال BAT+      سیم قرمز رنگ      قطب + (قرمز)

ترمینال BAT-      سیم مشکی رنگ      قطب - (مشکی)



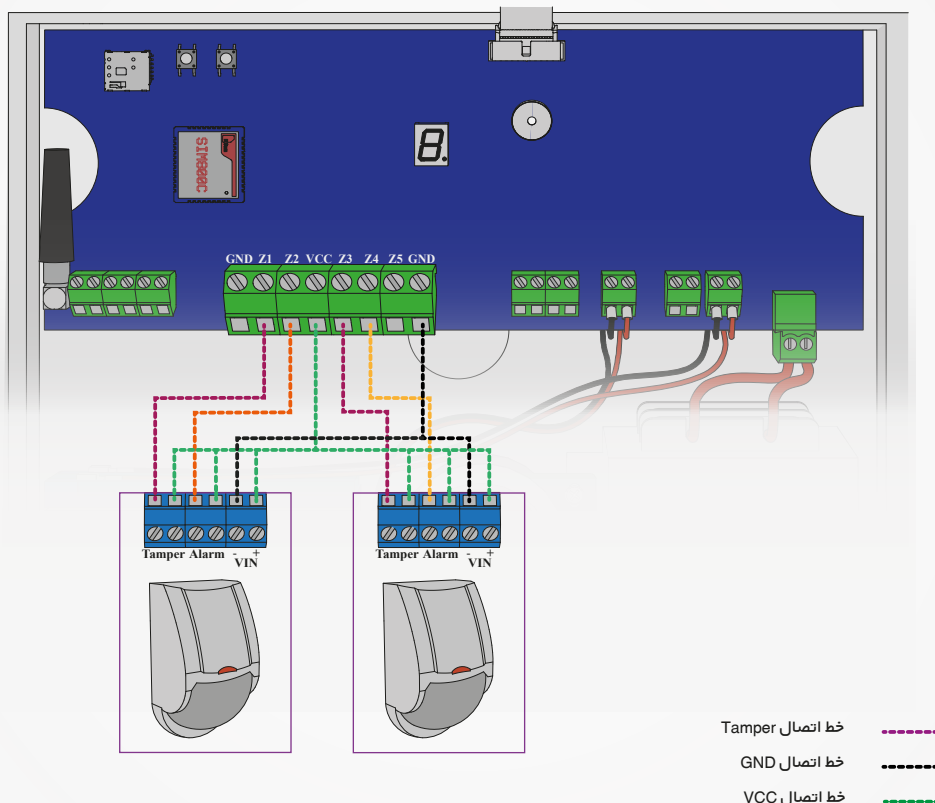
## اتصال زون‌های سیمی

در مواقعی که شرایط محل نصب دستگاه استفاده از سنسورهای سیمی را ایجاب می‌نماید، می‌توان از زون‌های سیمی دستگاه استفاده نمود.

پیش از آغاز نصب، با مراجعه به راهنمای چشمی، از نوع عملکرد چشمی به صورت NC(Normally Close) و یا NO(Normally Open) کسب اطلاع کنید.

### اتصال چشمی‌ها به صورت مجزا

نحوه سیم‌بندی سنسورها به صورت مجزا و اتصال به ترمینال زون‌ها طبق نقشه زیر می باشد:



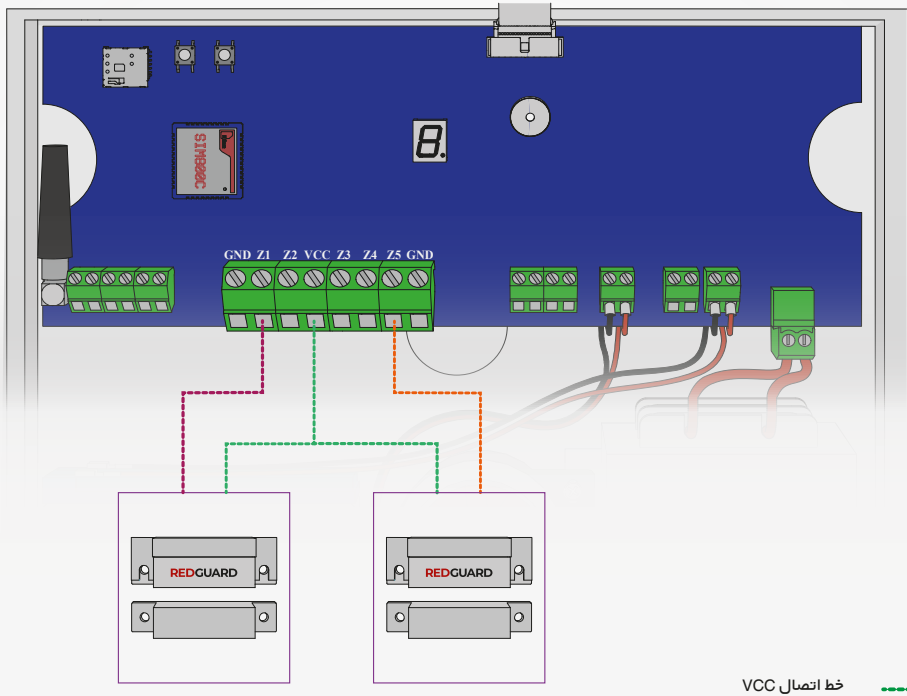
حالت عملکرد چشمی‌ها (NC یا NO) باید مطابق با عملکرد آنها و به درستی در اپلیکیشن تنظیم شوند.

دستگاه دزدگیر ردگارد قابلیت اتصال پنج زون سیمی را دارد. در صورت نیاز، می‌توانید مطابق نقشه بالا، خروجی Tamper چشمی‌ها را بعد از سری کردن به یک زون مجزا متصل کرده و زون مربوطه را در حالت عملکردی NC و شیوه حفاظت ۲۴ ساعته در اپلیکیشن قرار دهید.

پایه‌هایی از کانکتور Zone Terminal که هیچ تجهیز به آن‌ها متصل نیست، باید در بخش «افزونه‌ها» مدیریت زون‌ها در اپلیکیشن، در حالت NO (حالت باز) تنظیم شوند. این عملیات از اعلام هشدار نادرست توسط دستگاه جلوگیری می‌کند. جهت کسب اطلاعات بیشتر به بخش «مدیریت زون‌ها و سفارشی سازی آن‌ها» مراجعه نمایید.

## اتصال مگنت ها به صورت مجزا

نحوه سیم بندی مگنت ها به صورت مجزا و اتصال به ترمینال زون ها طبق نقشه زیر می باشد:



👉 حالت عملکرد مگنت ها (NO یا NC) باید مطابق با عملکرد آنها و به درستی در اپلیکیشن تنظیم شوند.

در حالت NC، مدار مگنت در شرایط عادی (درب یا پنجره بسته) بسته است. با باز شدن درب یا پنجره، مدار قطع شده و دستگاه دزدگیر اعلان هشدار صادر می کند.

قرار دادن مگنت در وضعیت عملکرد NC، حالت استاندارد سیستم امنیتی محسوب می شود زیرا در این حالت در صورت قطع سیم یا خرابی مگنت نیز هشدار صادر می شود.

در حالت NO، مدار مگنت در شرایط عادی (درب یا پنجره بسته) باز است. با بسته شدن درب یا پنجره، مدار وصل شده و دستگاه دزدگیر اعلان هشدار صادر می کند.

این حالت برای کاربردهای خاص طراحی شده و در صورت استفاده نادرست، امنیت سیستم کاهش می یابد.

👉 پس از تنظیم حالت مگنت در اپلیکیشن، از صحت عملکرد با باز و بسته کردن درب/پنجره اطمینان حاصل کنید.

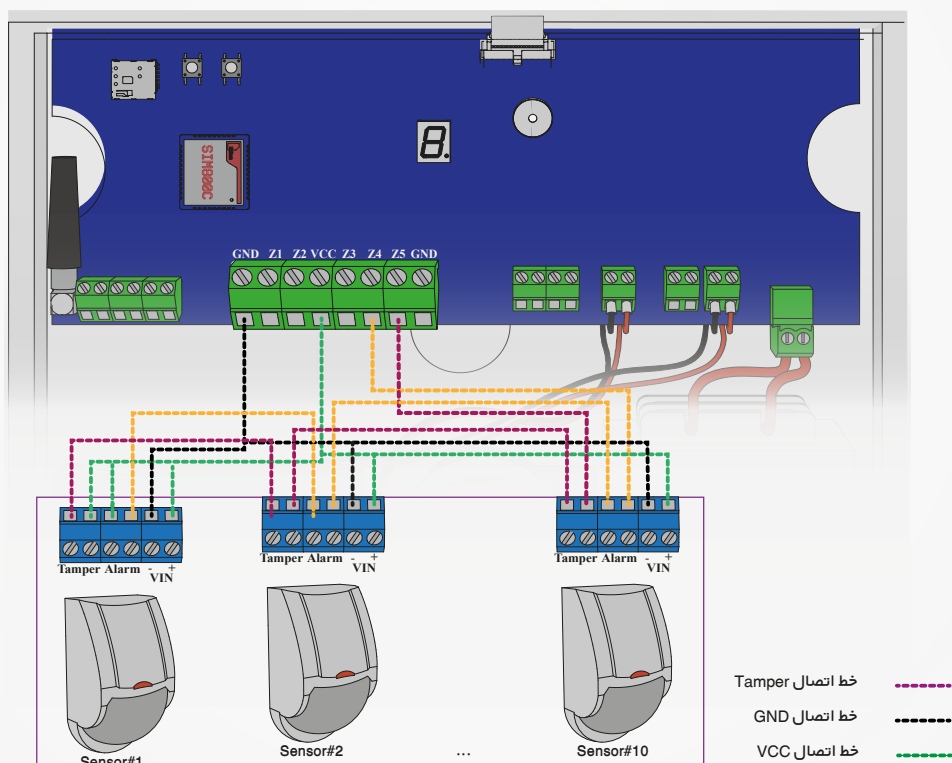
## اتصال سری چشمی‌ها

در صورتی که تعداد مگنت‌های مورد نیاز بیشتر از تعداد زون‌های دستگاه باشد، می‌توانید با سری کردن مگنت‌ها مطابق نقشه زیر، این محدودیت را برطرف کنید.

توجه داشته باشید که نقشه‌های سیم‌کشی ارائه‌شده بر اساس سیم مسی با مقطع ۰.۶ میلی‌متر و حداکثر طول ۱۰۰ متر طراحی و تست شده‌اند و در صورت استفاده از سیم با مشخصات نامنطبق، عملکرد صحیح و سلامت دستگاه تضمین نمی‌شود. همچنین با توجه به تأمین تغذیه سنسورها از خود دستگاه، مجموع جریان کشیده‌شده از دستگاه نباید از ۱/۵ آمپر بیشتر شود.

در دزدگیر ردگارد، هر زون سیمی قابلیت اتصال ۱۰ عدد چشمی به صورت سری تا طول سیم ۱۰۰ متر را دارد.

نحوه سیم‌بندی سنسورها به صورت سری شده و اتصال به ترمینال زون‌ها طبق نقشه زیر می‌باشد:



سنسورهای موجود در شاخه‌های سری باید از نوع عملکردی NC (کنتاکت بسته) باشند و به همین صورت در اپلیکیشن تنظیم شوند.

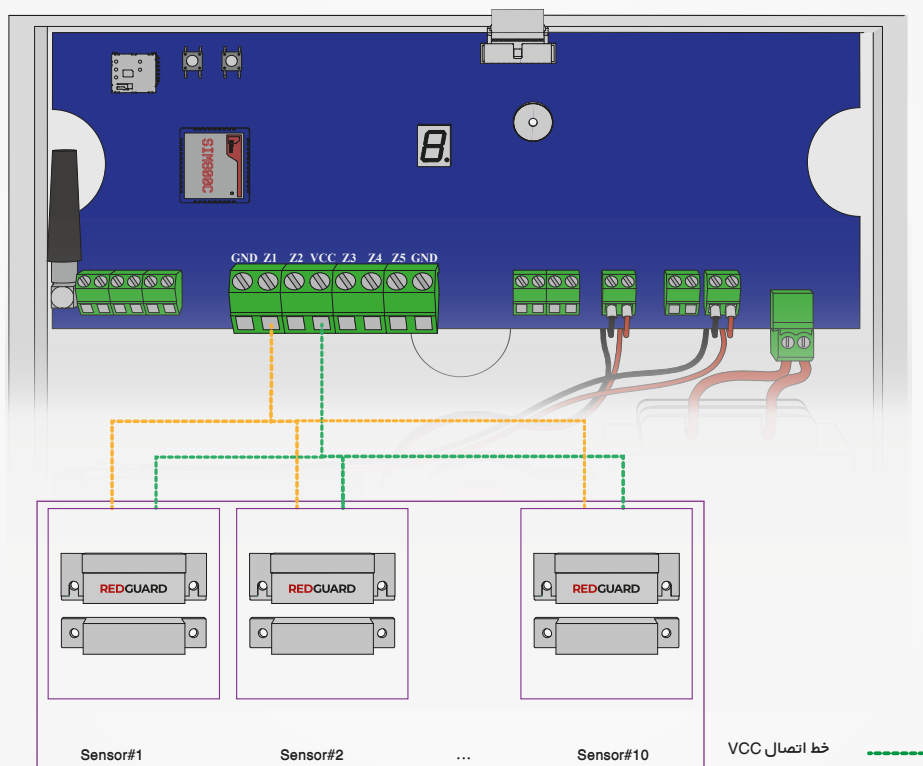
در صورت نیاز، خروجی Tamper چشمی‌ها را بعد از سری کردن به یک زون مجزا متصل کرده و زون مربوطه را در حالت عملکردی NC و شیوه حفاظت ۲۴ ساعته در اپلیکیشن قرار دهید.

## اتصال سری مگنت‌ها

در صورتی که تعداد مگنت‌های مورد نیاز بیشتر از تعداد زون‌های دستگاه باشد، می‌توانید با سری کردن مگنت‌ها مطابق نقشه زیر، این محدودیت را برطرف کنید.

توجه داشته باشید که نقشه‌های سیم‌کشی ارائه‌شده بر اساس سیم مسی با مقطع ۰٫۶ میلی‌متر و حداکثر طول ۱۰۰ متر طراحی و تست شده‌اند و در صورت استفاده از سیم با مشخصات نامنتطبق، عملکرد صحیح و سلامت دستگاه تضمین نمی‌شود.

نحوه سیم‌بندی سنسورها به صورت سری شده و اتصال به ترمینال زون‌ها طبق نقشه زیر می‌باشد:



سنسورهای موجود در شاخه‌های سری باید از نوع عملکردی NC (کنتاکت بسته) باشند و به همین صورت در اپلیکیشن تنظیم شوند.

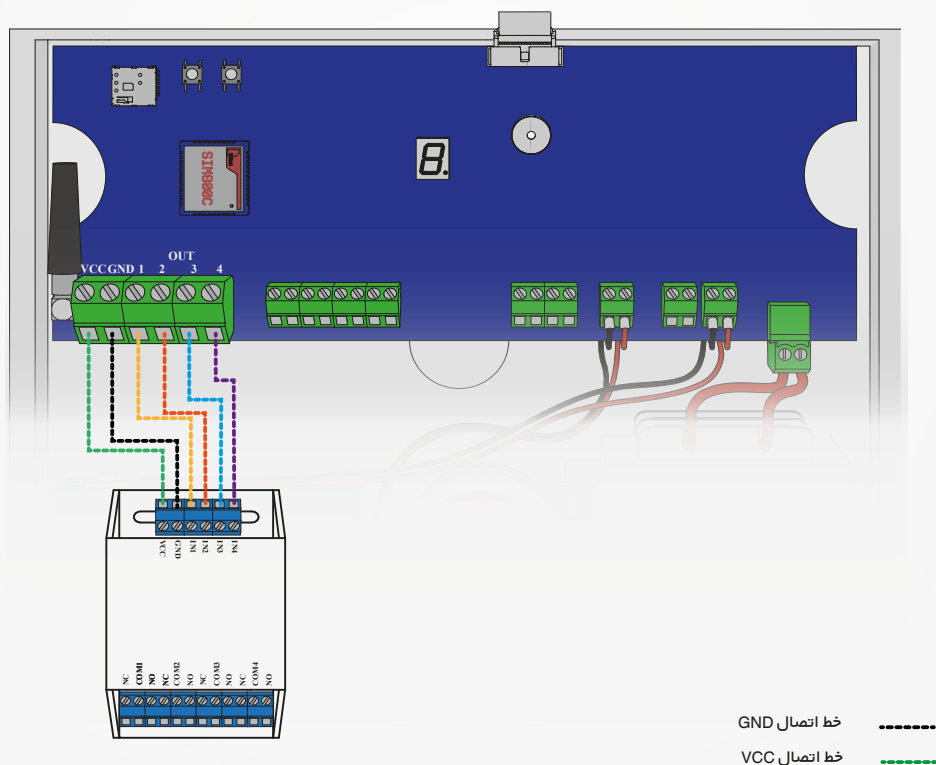
## اتصال برد رله

به طور کلی رله یک کلید الکتریکی است که با فرمان‌پذیری از واحد پردازش مرکزی قابلیت فعال/غیرفعال‌سازی مصرف‌کننده‌های متصل به خود را دارد. دستگاه دزدگیر هوشمند ردگارد با ارائه چهار خروجی رله‌ای می‌تواند قابلیت کنترل انواع تجهیزات الکتریکی را برای شما فراهم آورد.

استفاده از ماژول رله در زمینه‌های متنوعی کاربرد دارد و محدود به استفاده برای حفظ و کنترل امنیت اماکن نیست و می‌توان به وسیله آن تجهیزات برقی مختلفی (سیستم روشنایی، گرمایش و سرمایش، درب‌های برقی و...) را از طریق اپلیکیشن REDGUARD از راه دور کنترل نمود.

دستگاه دزدگیر ردگارد قابلیت اتصال چهار عدد رله ۱۲ ولت را داراست. 

نحوه سیم‌بندی برد رله و اتصال به ترمینال رله‌ها طبق نقشه زیر می‌باشد:



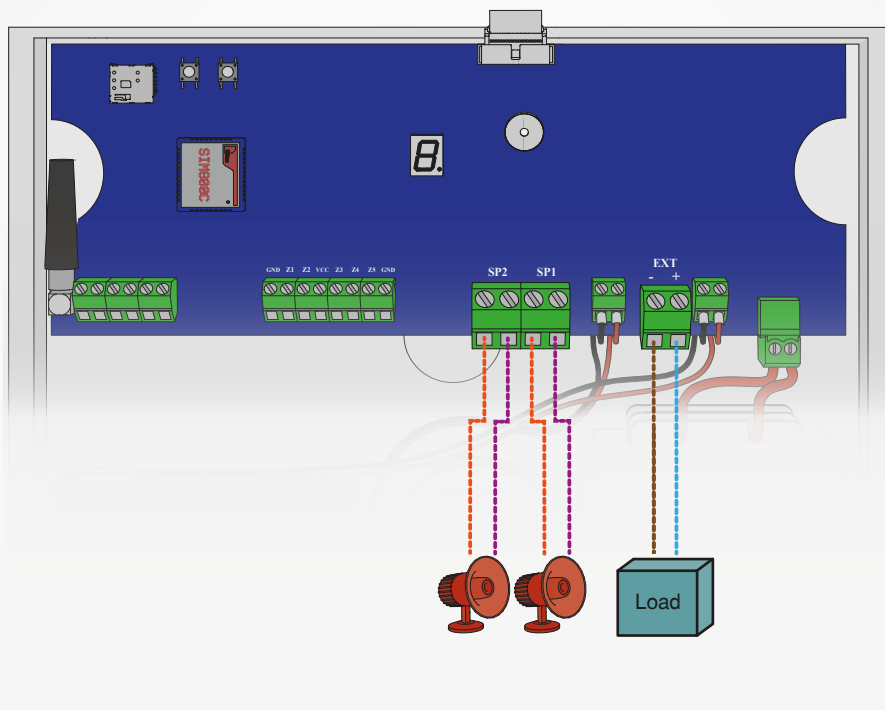
در صورتی که تمایل دارید وسیله موردنظر برای کنترل، در وضعیت اولیه فعال باشد و غیرفعال سازی آن را کنترل کنید، از ترمینال (کنتاکت بسته) NC روی رله و در صورتی که می‌خواهید وسیله مورد نظر در وضعیت اولیه غیرفعال باشد و فعال‌سازی آن را کنترل کنید، از ترمینال (کنتاکت باز) NO روی رله استفاده کنید. 

## سایر اتصالات خارجی

## اتصال بلندگوها و تغذیه خارجی

دستگاه دزدگیر شما قابلیت پشتیبانی از دو بلندگو با مقاومت ۸ اهم و توان خروجی حداقل ۱۵ وات و یک خروجی 12V-DC را دارا می‌باشد.

نحوه سیم‌بندی بلندگوها و تغذیه ۱۲ ولت خارجی و اتصال به ترمینال‌های SP و EXT طبق نقشه زیر می‌باشد:





با سپاس از همراهی شما، جهت اطلاعات بیشتر و راهنمایی در خصوص محصولات کد زیر را اسکن نمایید:



۰۲۱-۴۱۶۳۵۰۰۰

شماره تماس (خط ویژه)



Info@Securitywave.net

رایانامه



redguardalarm.com

تارنما



@RedGuard\_Alarm

شبکه‌های اجتماعی

