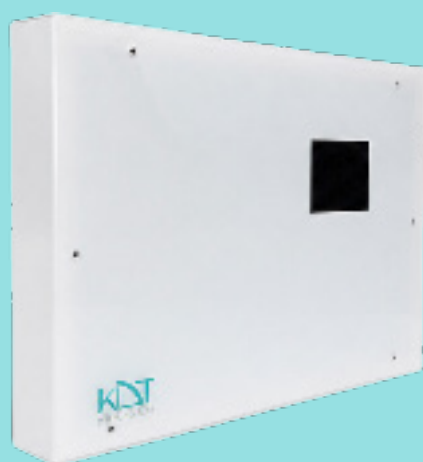


• راه اندازی سیستم اعلام سرقت •

• **KB-M2** •



از جعبه تا سیستم آماده کار، در دوازده گام ساده.

بدون نیاز به دانش فنی

زمان تقریبی: ۴۵ دقیقه

ویرایش ۱٫۰ راهنمای کاربری

مدل KB-M2

فهرست

- در یک نگاه
- پیش از شروع
- ورودی‌های کابل و سیم‌کشی جعبه دزدگیر
- ۱ اتصال و ورود
- ۲ آشنایی با صفحه اصلی
- ۳ اتصال به اینترنت
- ۴ تنظیم ساعت
- ۵ آماده‌سازی ناحیه (پارتیشن)
- ۶ افزودن سنسورها
- ۷ رمزها و دسترسی‌ها
- ۸ آژیر و خروجی‌ها
- ۹ اعلان و کنترل پیامکی
- ۱۰ مازول توسعه
- ۱۱ خودکارسازی
- ۱۲ کار روزمره
- نگهداری و به‌روزرسانی
- عیب‌یابی سریع
- راهنمای جامع آیکون‌ها و وضعیت صفحه‌نمایش
- راهنمای جامع تعریف فیزیکی تجهیزات (Learn / Pairing)
- چک‌لیست تحویل

در یک نگاه

تمامی مراحل در دوازده گام خلاصه می‌شود. گام‌های ۱ تا ۸ برای یک سیستم دزدگیر کاملاً کارآمد کافی است.

۱ اتصال و ورود با موبایل یا لپ‌تاپ وارد پنل شوید	۲ صفحه اصلی ببینید هر بخش چه کاری می‌کند	۳ اینترنت کابل شبکه، وای‌فای یا سیم‌کارت
۴ ساعت تا زمان رویدادها درست ثبت شود	۵ ناحیه نام و زمان تأخیر ورود و خروج	۶ سنسورها ثبت، نام‌گذاری و آزمون عملکرد
۷ رمزها رمز کاربر، کارت و ریموت کنترل	۸ آژیر انتخاب نوع آژیر و زمان پخش	۹ اعلان‌ها پیامک، تماس و کنترل از راه دور
۱۰ ماژول توسعه در صورت نیاز به زون‌های بیشتر	۱۱ خودکارسازی مثلاً روشن شدن چراغ با حرکت	۱۲ کار روزمره مسلح و غیرمسلح کردن سیستم

پیش از شروع

پیش از شروع پیکربندی و راه‌اندازی، موارد زیر را آماده و بررسی کنید:

- ☐ دستگاه به برق ۲۲۰ ولت شهری و باتری پشتیبان متصل شده باشد.
- ☐ یک دستگاه متصل به مرورگر وب (تلفن همراه، تبلت یا رایانه/لپ‌تاپ) در دسترس باشد.
- ☐ در صورت اتصال با کابل، از اتصال کابل شبکه (LAN) مطمئن شوید؛ و در صورت استفاده از شبکه بی‌سیم (Wi-Fi)، نام و رمز عبور شبکه را در دسترس داشته باشید.
- ☐ جهت فعال‌سازی قابلیت پیامک و تماس، یک سیم‌کارت فعال و دارای اعتبار را در شیار سیم‌کارت دستگاه قرار دهید.
- ☐ سنسورها، ریموت‌ها و صفحه‌کلیدهای بی‌سیم با باتری سالم در نزدیکی دستگاه قرار داده شوند.
- ☐ اطلاعات پیش‌فرض دستگاه (شامل آدرس آی‌پی، نام کاربری و رمز عبور اولیه) در دسترس باشد.

نکته

لازم نیست تمامی مراحل را یک‌باره انجام دهید. تمامی تنظیمات در حافظه دستگاه ذخیره می‌شوند و در هر زمان می‌توانید برای ویرایش یا تکمیل آن‌ها اقدام فرمایید.

راهنمای ورودی‌های کابل و مجاری عبور سیم جعبه دزدگیر

ورودی‌های پیش‌برش دایره‌ای جهت عبور منظم، ایمن و استاندارد کابل‌های تغذیه، شبکه و سنسورها

1 ورودی کابل از پشت (سیم‌کشی توکار)

Rear Entry - In-Wall Concealed Wiring

۱ ورودی پیش‌برش کفی



★ راهنمای فنی ترمینال‌ها و ماژول‌های سیستم (۱ تا ۱۱):

9 خروجی رله‌های فرمان (PGM 1-4) Relay Outputs (Normally Open)	5 درگاه شبکه اینترنت (PoE) Ethernet Port (PoE Supported)	1 باتری پشتیبان اضطراری Backup Battery Pack
10 شیار کارت حافظه (MicroSD) MicroSD Card Slot	6 خروجی آژیر (۱۲ ولت مستقیم) 12V DC Siren Output (BELL)	2 ورودی برق شهر ۲۲۰ ولت متناوب 220V AC Mains Input
11 شیار سیم‌کارت (ماژول 4G) SIM Card Slot (4G LTE)	7 خروجی تغذیه سنسورها (AUX) Aux Power Output (Max 0.5A)	3 کانکتور باتری پشتیبان Backup Battery Connector
	8 ورودی زون‌های باسیم (۱ تا ۶) Wired Zone Inputs (1 to 6)	4 ورودی تغذیه ۱۵ ولت مستقیم 15V DC Power Input

★ مشخصات و کاربرد سیم‌کشی توکار (Concealed Wiring):

این ورودی دایره‌ای روی کفی فلزی پشت جعبه تعبیه شده است. در پروژه‌هایی که لوله‌های برق و سیم‌های سنسورها داخل دیوار کار گذاشته شده‌اند، کابل‌ها مستقیماً از این بخش وارد محفظه می‌شوند تا هیچ سیمی از بیرون دستگاه در دسترس یا در معرض دید نباشد.

2 ورودی‌های کابل از زیر (سیم‌کشی روکار)

Bottom Entry - Surface & Trunking Wiring

۶ ورودی پیش‌برش دیواره زیرین



۶ ورودی دایره‌ای پیش‌برش روی لبه پایینی قاب فلزی

- ✓ امکان ورود مستقل و تفکیک‌شده کابل برق ۲۲۰V، کابل شبکه LAN و خطوط سنسورها
- ✓ تفکیک کابل‌ها جهت جلوگیری از تأثیر نویز الکترومغناطیسی برق بر زون‌ها و آژیر
- ✓ جداسازی آسان پولکی‌ها با وارد کردن ضربه آرام به لبه‌ی شیار پرسی

★ مشخصات و کاربرد سیم‌کشی روکار (Surface Wiring):

این ورودی در قسمت پایینی جعبه قرار دارند. برای اتصال کابل‌هایی که از طریق داکت پلاستیکی یا لوله فلکسی هدایت می‌شوند ایده‌آل است. نصاب می‌تواند متناسب با تعداد و حجم کابل‌ها، ورودی‌های مورد نیاز را باز کند.

دستورالعمل فنی باز کردن ورودی‌های پیش‌برش: جهت باز کردن هر ورودی، نوک یک پیچ‌گوشتی دوسو یا سنبه را روی لبه‌ی شیار دایره قرار داده و با یک ضربه آرام چکش به آن ضربه بزنید. پولکی فلزی به صورت کاملاً صاف، یکنواخت و تمیز جدا می‌شود.

۱ اتصال و ورود به پنل

تمامی تنظیمات از طریق مرورگر وب انجام می‌شود و نیازی به نصب هیچ نرم‌افزاری نیست. سه روش برای دسترسی به این صفحه وجود دارد:

راه اتصال	اقدام لازم	آدرس در مرورگر
وای‌فای داخلی دستگاه ساده‌ترین روش برای بار اول	در گوشی تلفن همراه یا رایانه خود، به شبکه وای‌فای Burglar متصل شده و رمز عبور alarm1234 را وارد کنید.	192.168.4.1
کابل شبکه	یک سر کابل شبکه را به پنل دستگاه و سر دیگر را به مودم یا سویچ متصل نمایید.	192.168.1.205
وای‌فای محل	پس از انجام گام ۳ و اتصال دستگاه به شبکه وای‌فای محل.	آدرسی که در گام ۳ نمایش داده می‌شود

صفحه ورود نمایش داده می‌شود. نام کاربری و رمز عبور پیش‌فرض کارخانه به شرح زیر است: نام کاربری **admin** و رمز عبور

123456

The screenshot shows a dark-themed login interface. At the top right, there is a label 'نام کاربری' (Username). Below it is a text input field. Further down, there is a label 'رمز عبور' (Password) and another text input field. At the bottom center, there is a prominent blue button labeled 'ورود' (Login).

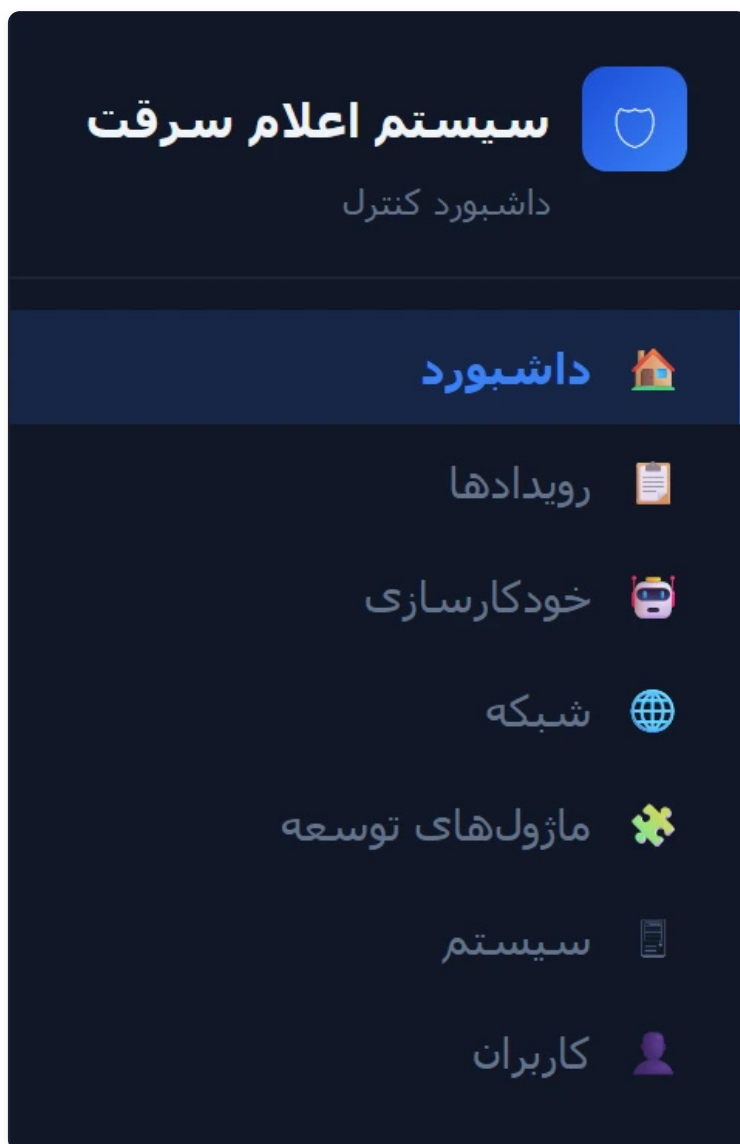
تصویر ۱ - صفحه ورود به سامانه. در صورت نمایش زبان انگلیسی، از منوی پایین صفحه گزینه «فارسی» را انتخاب کنید؛ این تنظیم در مرورگر شما ذخیره خواهد شد.

مهم

جهت حفظ امنیت سیستم، رمز عبور پیش‌فرض کارخانه را در نخستین راه‌اندازی تغییر دهید. دستورالعمل تغییر رمز در بخش **نگهداری و به‌روزرسانی** شرح داده شده است.

۲ آشنایی با صفحه اصلی

پس از ورود، صفحه داشبورد نمایش داده می‌شود. از طریق منوی کناری به تمامی بخش‌های سیستم دسترسی خواهید داشت:



تصویر ۲ - منوی کناری پنل کاربری. تمامی بخش‌ها از این منو باز می‌شوند؛ در انتهای منو، خلاصه وضعیت سیستم و نسخه میان‌افزار جاری نیز درج شده است.

در بالای صفحه داشبورد، پنج کارت وضعیت قرار دارد که وضعیت‌های مختلف سیستم دزدگیر را نمایش می‌دهد:

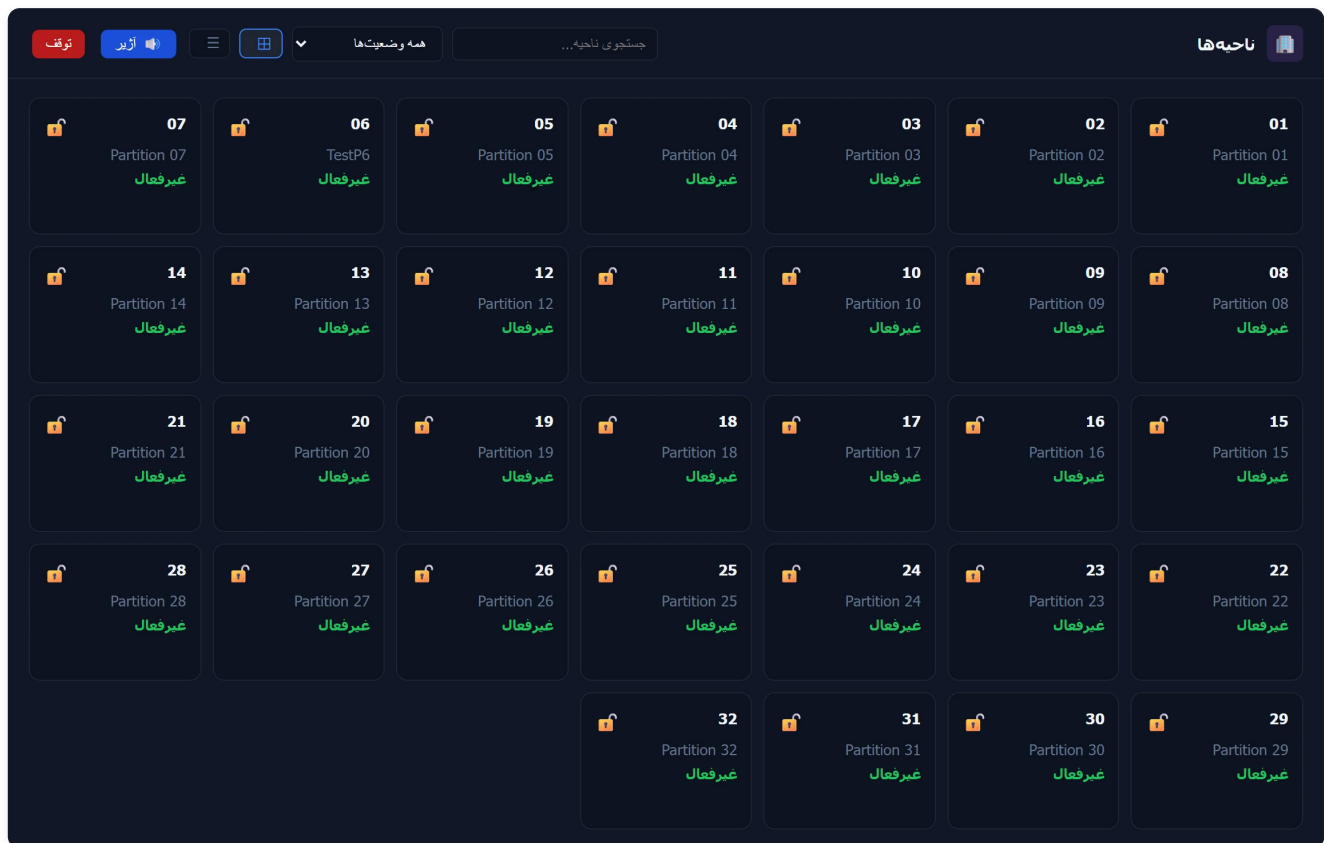


تصویر ۳ - کارت‌های وضعیت کلی: وضعیت مسلح/غیرمسلح، تعداد ناحیه‌های فعال، هشدارهای فعال، خرابی‌ها و زون‌های حذف‌شده موقت.

اصطلاحات پرکاربرد سیستم

اصطلاح	شرح و کاربرد
ناحیه (Partition)	یک بخش مستقل از ساختمان (مانند طبقه اول، واحد اداری یا انبار). هر ناحیه را می‌توان به طور جداگانه مسلح یا غیرمسلح کرد (این دستگاه تا ۳۲ ناحیه مجزا را پشتیبانی می‌کند).
زون (Zone)	یک نقطه تشخیص امنیتی؛ یعنی یک حسگر مشخص یا یک ورودی باسیم (مانند «سنسور درب ورودی»).
فعال‌سازی (Arm)	مسلح کردن سیستم؛ قرار گرفتن دزدگیر در وضعیت آماده‌باش و حساس به تحریک حسگرها.
حالت حضور (Stay)	حالت ماندن در منزل؛ در این حالت تنها سنسورهای پیرامونی (مانند درب و پنجره) فعال بوده و حسگرهای حرکتی داخلی برای تردد ساکنان غیرفعال هستند.
حذف موقت (Bypass)	نادیده گرفتن موقت یک زون مشخص در زمان مسلح‌سازی (مانند پنجره‌ای که باز مانده یا سنسوری که نیاز به سرویس دارد).
خرابی (Trouble)	گزارش اشکال فنی در سیستم؛ نظیر قطع برق شهر، افت ولتاژ باتری سنسور یا قطع ارتباط بی‌سیم.
دستکاری (Tamper)	هشدار امنیتی فیزیکی؛ ناشی از باز شدن درپوش، جدا شدن دستگاه یا سنسور از روی دیوار، یا تلاش برای تخریب فیزیکی.

در بخش پایین‌تر، فهرست پارتیشن‌ها (ناحیه‌ها) قرار دارد. هر کارت نشان‌دهنده یک ناحیه است و با کلیک بر روی آن وارد تنظیمات اختصاصی همان ناحیه می‌شوید:



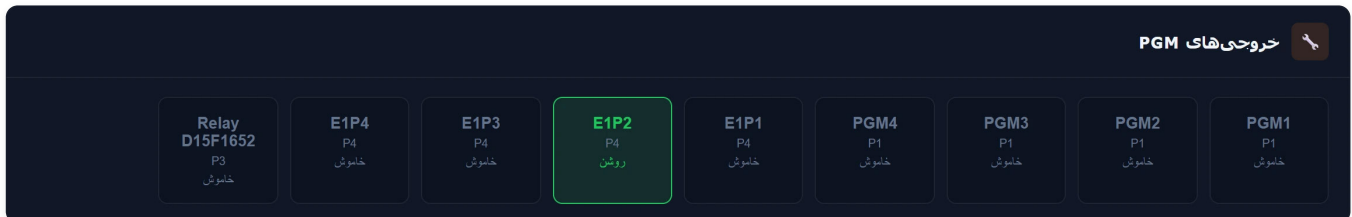
تصویر ۴ - نمای کلی پارتیشن‌ها (ناحیه‌ها). دکمه‌های «آزیر» و «توقف» در بالای این بخش، امکان فعال‌سازی یا توقف دستی آزیر را فراهم می‌کنند.



تصویر ۵ - کارت هر ناحیه: نمایشگر شماره ناحیه، نام اختصاصی و وضعیت لحظه‌ای آن (مسلح / غیرمسلح / هشدار).

اطلاعات سیستم 	
KDT Burglar System	نام پنل
KB-M2	مدل پنل
v3.0.1	میان‌افزار
Aug 15 2026 16:39:56	نسخه ساخت
قطع	MQTT ابری
متصل	MQTT محلی
فعال	اکسس‌پوینت WiFi
15h 57m 2s	مدت روشن بودن
12.92 V (100%)	باتری
موجود	برق شهر
فارسی کامل	وضعیت شارژ

تصویر ۶ - پنجره اطلاعات سیستم. هنگام بروز اختلال، نخستین مرجع بررسی است: وضعیت ولتاژ باتری، برق شهر و وضعیت اتصالات ابری و شبکه.



تصویر ۷ - خروجی‌های قابل برنامه‌ریزی (PGM): رله‌ها و کنتاکت‌هایی برای روشن کردن روشنایی، دربازکن یا سایر تجهیزات جانبی. با کلیک بر روی هر گزینه می‌توان آن‌ها را به صورت دستی فعال یا غیرفعال نمود.

۳ اتصال به اینترنت

از منوی کناری وارد بخش «شبکه» شوید. دستگاه از سه بستر ارتباطی پشتیبانی می‌کند (الزامی به تنظیم هر سه نبوده و راه‌اندازی هر بستری که در دسترس است کفایت می‌کند). در صورت فعال بودن هم‌زمان هر سه بستر، دستگاه بهینه‌ترین مسیر را به صورت هوشمند انتخاب می‌نماید و در صورت قطعی یکی از آن‌ها، فوراً و به طور خودکار به بستر ارتباطی بعدی سوئیچ خواهد کرد.

الف) کابل شبکه

اینترنت (LAN)

استفاده از DHCP ☐ دریافت خودکار آدرس IP از روتر

آدرس IP: 192.168.115.207

ماسک زیرشبکه: 255.255.255.0

دروازه: 192.168.115.1

سرور DNS: 8.8.8.8

تصویر ۸ - اتصال با کابل شبکه: ساده‌ترین روش، فعال نگه داشتن گزینه «استفاده از DHCP» جهت دریافت خودکار آدرس آی‌پی است. تنها در صورتی که مدیر شبکه تنظیم IP ایستا (Static IP) را تعیین کرده باشد، این گزینه را خاموش کرده و مقادیر را به صورت دستی وارد نمایید.

ب) وای‌فای

جستجوی شبکه‌ها

WIFI (STA)

SSID: MyHome-WiFi

رمز عبور (برای حفظ مقدار فعلی خالی بگذارید):

برای حفظ مقدار فعلی خالی بگذارید

استفاده از DHCP ☐ دریافت خودکار آدرس IP از طریق WIFI

آدرس IP: 192.168.115.224

ماسک زیرشبکه: 255.255.255.0

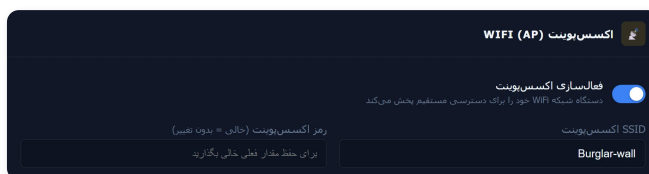
دروازه: 192.168.115.1

سرور DNS: 8.8.8.8

تصویر ۹ - اتصال به وای‌فای: پس از انتخاب نام شبکه (SSID) و درج رمز عبور، گزینه دریافت خودکار آدرس (DHCP) را فعال بگذارید. در صورت نیاز به تعیین آدرس ثابت، آن را غیرفعال کرده و اطلاعات IP را به صورت دستی تنظیم فرمایید.

توجه مهم

پس از اتصال دستگاه به شبکه وای‌فای محل، آدرس آی‌پی (IP) آن بر اساس محدوده مودم شما تغییر خواهد کرد. لطفاً آدرس جدید نمایش داده شده را یادداشت کرده و در دفعات بعد از آن برای باز کردن پنل استفاده نمایید. در غیر این صورت، برای ورود به پنل باید مجدداً به شبکه وای‌فای داخلی دستگاه (Burglar) متصل شده و آدرس 192.168.4.1 را در مرورگر وارد کنید.



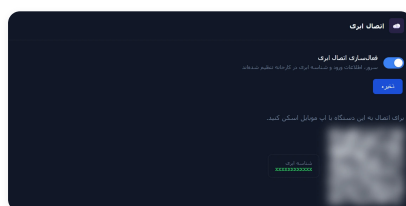
تصویر ۱۰ - اکسس پوینت داخلی (AP): جهت دسترسی پشتیبان، نام شبکه و رمز عبور پیش فرض قابل استفاده است.

ج) سیم کارت (4G)



تصویر ۱۱ - مازول سیم کارت: کارت وضعیت باید عبارات «آماده»، «ثبت شده» و «متصل» را به رنگ سبز نشان دهد.

د) اتصال به اپلیکیشن موبایل (Ramona Pro)



تصویر ۱۲ - اتصال ابری و بارکد اختصاصی سیستم جهت جفت سازی با اپلیکیشن موبایل Ramona Pro.

مرحله	اقدام	دستورالعمل اجرایی
۱	دانلود اپلیکیشن	دریافت و نصب برنامه Ramona Pro از بسترهای App Store یا Google Play.
۲	فعال سازی اتصال ابری	در زبانه Network، کلید «اتصال ابری (Cloud)» را روشن نمایید (تصویر ۱۲).
۳	اسکن کد تصویری (QR)	در اپلیکیشن گزینه «+ افزودن پنل» را انتخاب و بارکد روی نمایشگر را اسکن کنید.
۴	نظارت و مدیریت آنلاین	سامانه فوراً متصل شده و دریافت هشدارهای Push و کنترل از راه دور فعال می گردد.

راهکار جایگزین دانلود مستقیم: چنانچه برنامه «Ramona Pro» در فروشگاه Google Play در دسترس نبود یا یافت نشد، فایل نصبی (APK) را مستقیماً از نشانی رسمی کی دی تی دریافت نمایید:

<https://ftp.kdt.ir/KdtTechnical/05-Android/Ramona-Pro/>

ه) یکپارچه سازی با سامانه مدیریت ساختمان (اتصال محلی Local MQTT به کنسول KDT)

پروتکل Local MQTT برای اتصال مستقیم پنل دزدگیر به نرم افزار جامع مدیریت هوشمند ساختمان تحت عنوان «کنسول (KDT Console) KDT» به کار می رود. این بستر به صورت کاملاً محلی (Local) و بدون نیاز به اینترنت فعالیت می کند.

قانون اساسی و حیاتی شبکه (دید متقابل تجهیزات):

پنل دزدگیر، رایانه سرور کنسول KDT، تاج پنل های BMS و بلندگوهای تحت شبکه (IP Speaker) الزاماً باید همگی به یک شبکه محلی کاملاً یکسان (همان Subnet و محدوده IP) متصل باشند و بتوانند یکدیگر را در بستر شبکه بدون مانع یا فایروال مشاهده کنند؛ در غیر این صورت تبادل فرامین، دریافت وضعیت ها و پخش پیام های صوتی مختل خواهد شد.

مراحل فعال سازی در زبانه Network ← بخش Local MQTT:

۱. کلید Local MQTT را فعال کنید. ۲. در فیلد Broker Host آدرس آی پی سیستم سرور KDT Console (مانند 192.168.1.80) را وارد کنید. ۳. پورت پیش فرض (1883) و مشخصات ورود را ثبت و روی «ذخیره» کلیک فرمایید.

۴ تنظیم ساعت

تنظیم دقیق تاریخ و ساعت برای ثبت صحیح وقایع و اجرای منظم زمان‌بندی‌ها ضروری است. از منوی کناری وارد بخش «سیستم» شده و به کارت «ساعت (RTC)» مراجعه کنید.

تصویر ۱۳ - همگام‌سازی ساعت: ساده‌ترین روش، کلیک بر روی دکمه «تنظیم روی اکنون» جهت یکسان‌سازی ساعت پنل با زمان رایانه یا گوشی، و سپس کلیک بر روی دکمه «ذخیره در ساعت دستگاه» است.

نکته

در صورت اتصال به اینترنت، دستگاه به صورت خودکار ساعت خود را همگام می‌سازد؛ با این حال انجام این تنظیم در نخستین راه‌اندازی جهت اطمینان از صحت عملکرد آفلاین توصیه می‌شود.

۵ آماده‌سازی ناحیه

از صفحه داشبورد بر روی ناحیه مورد نظر کلیک کنید. صفحه مدیریت ناحیه با هفت زبانه (تب) تخصصی باز شده و بخش عمده فرآیند راه‌اندازی در این بخش انجام می‌پذیرد:



تصویر ۱۴ - زبانه‌های تنظیمات ناحیه: نمای کلی، دستگاه‌ها، دسترسی، خروجی‌ها، گزارش‌ها، اعلان‌ها و تنظیمات.

ابتدا وارد زبانه «تنظیمات» شوید:

تصویر ۱۵ - فرم تنظیمات ناحیه. پس از اعمال هرگونه تغییر، حتماً بر روی دکمه «ذخیره» در پایین فرم کلیک فرمایید.

- **نام ناحیه:** عنوان مشخص و واضحی (مانند «طبقه همکف» یا «انبار») تعیین کنید؛ همین نام در پیامکها و هشدارهای ارسالی درج خواهد شد.
- **تأخیر خروج (Exit Delay):** مدت زمانی (معمولاً ۳۰ ثانیه) که پس از فعالسازی دزدگیر فرصت دارید از محیط تحت پوشش خارج شوید بدون آنکه آژیر به صدا درآید.
- **تأخیر ورود (Entry Delay):** مدت زمانی (معمولاً ۳۰ ثانیه) که پس از باز شدن درب اصلی مهلت دارید تا با ورود رمز عبور یا کارت، سیستم را پیش از به صدا درآمدن آژیر غیرفعال نمایید.
- **پخش آژیر هنگام دستکاری (Tamper):** در صورت فعال بودن، باز شدن درب پنل یا درپوش هر یک از سنسورها و آژیرهای این ناحیه موجب اعلام هشدار فوری دستکاری فیزیکی خواهد شد.
- **مسلح سازی و خلع سلاح خودکار زمان بندی شده:** در صورت تمایل به فعال یا غیرفعال شدن خودکار سیستم در ساعات مشخصی از شبانه روز (مثلاً مسلح شدن در ساعت ۲۳:۰۰ و غیرفعال شدن در ساعت ۰۷:۰۰)، برنامه زمانی و روزهای هفته را در این بخش تعیین فرمایید.

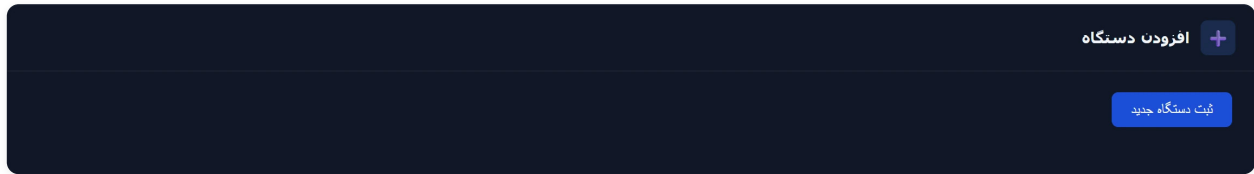
نکته

توجه فرمایید که زمان تأخیر ورود تنها برای زونهایی اعمال می شود که در گام ۶ گزینه «مسیر تأخیر ورود» برای آنها فعال شده باشد (این گزینه معمولاً منحصرأً برای حسگر درب ورودی اصلی فعال می شود).

۶ افزودن سنسورها و دستگاهها

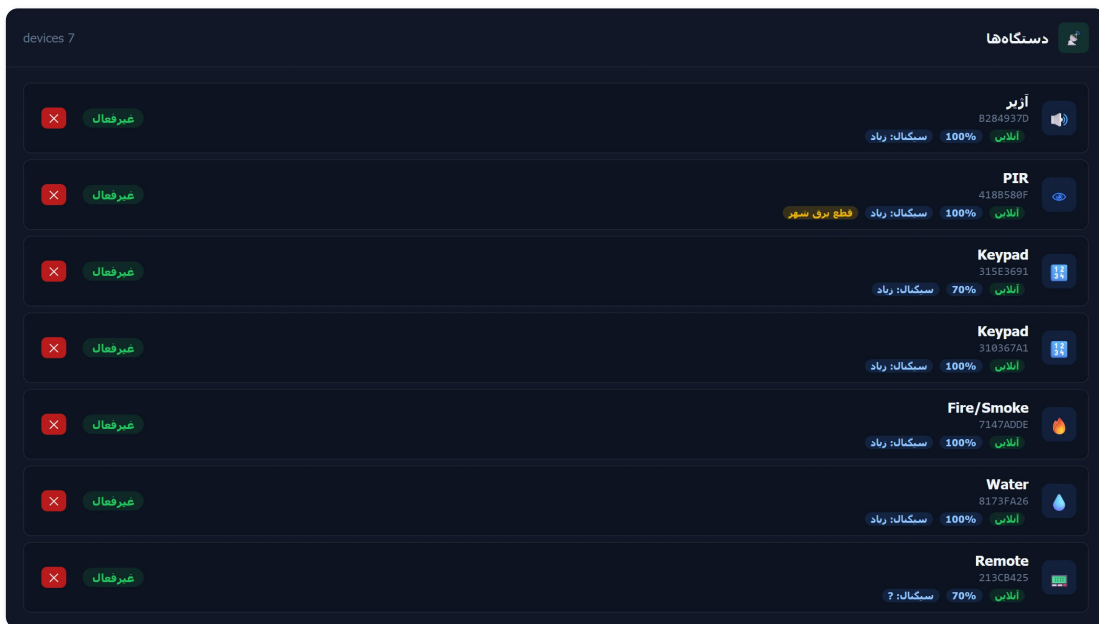
وارد زبانه «دستگاهها» در ناحیه مورد نظر شوید. تمامی تجهیزات بی‌سیم (حسگرها، ریموت‌ها، صفحه‌کلیدها، آژیرها و رله‌ها) طبق همین فرآیند به سیستم شناسانده می‌شوند.

ثبت یک دستگاه جدید



تصویر ۱۶ - کارت «افزودن دستگاه» در انتهای صفحه دستگاهها.

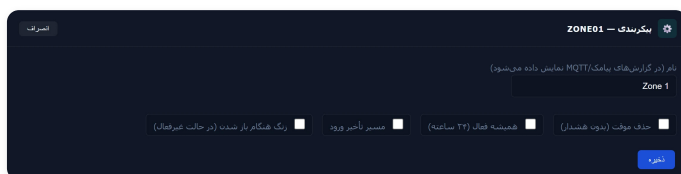
۱. بر روی دکمه «ثبت دستگاه جدید» کلیک کنید؛ پنل در حالت آماده‌باش برای دریافت سیگنال شناسایی قرار می‌گیرد.
۲. بلافاصله فرآیند جفت‌سازی (Learn) حسگر را طبق راهنمای تعریف فیزیکی انجام دهید (یا حسگر را با باز کردن مغنت درب یا حرکت در برابر چشمی تحریک کنید).
۳. حسگر شناسایی شده و به فهرست تجهیزات این ناحیه اضافه خواهد شد.
۴. در صورت عدم شناسایی، حسگر را به پنل نزدیک‌تر کرده، سلامت باتری آن را بررسی نموده و مجدداً تلاش کنید.



تصویر ۱۷ - فهرست تجهیزات ثبت‌شده در ناحیه: نمایش نوع دستگاه، شناسه سخت‌افزاری، وضعیت برخظ، درصد شارژ باتری و قدرت سیگنال بی‌سیم (دکمه قرمز جهت حذف دستگاه از سیستم است).

نام گذاری و رفتار هر زون

روی هر دستگاه در فهرست کلیک کنید تا فرم پیکربندی آن باز شود:



تصویر ۱۸ - فرم پیکربندی زون: نام گذاری معنادار (مانند «درب ورودی» به جای «Zone 1») جهت شناسایی دقیق در پیامک های هشدار.

رفتار سنسورها در حالت مسلح سازی «در محل» (Stay Mode) و سنسورهای ایمنی ۲۴ ساعته

- **قاعده حالت «در محل» (Stay):** هنگام مسلح کردن سیستم در وضعیت Stay، حسگرهای حرکتی (PIR) در حالت پیرامونی (Perimeter) قرار گرفته و مگنت های درب و پنجره در حالت داخلی (Interior) عمل می کنند تا ساکنان بتوانند با آزادی عمل در فضاهای تعریف شده تردد نمایند.
- **حسگرهای حفاظت از جان و ایمنی محیطی:** حسگرهای نشت گاز (Gas)، تشخیص دود (Smoke) و نشت آب (Water Leakage) به صورت پیش فرض کارخانه ای همواره در وضعیت ۲۴ ساعته (Hour Active-24) قرار دارند و حتی در زمان غیرمسلح بودن دزدگیر، پیوسته فعال بوده و به محض وقوع حادثه آژیر خطر را فعال می سازند.

چک لیست بررسی و انطباق سنسورها ویژه کاربران (Double-Check Checklist)

نوع حسگر / گزینه	تنظیم پیش فرض کارخانه	اقدام الزامی کاربر بر حسب موقعیت فیزیکی
درب ورودی اصلی ساختمان	فوری (بدون تأخیر)	دستی فعال شود: تیک «مسیر تأخیر ورود» فعال شود تا فرصت ورود کد باشد.
حسگرهای دود، گاز و نشت آب	۲۴ ساعته فعال (همیشه بیدار)	دست نزنید: به صورت پیش فرض فعال است و باید همواره فعال بماند.
زنگ اعلام ورود (Chime)	غیرفعال	اختیاری: در صورت تمایل به پخش بوق هنگام ورود مراجعین، تیک آن را بزنید.
حذف موقت (Bypass)	غیرفعال	موقت: فقط در صورت خرابی فیزیکی یا اتمام باتری حسگر فعال گردد.

تست و راستی آزمایی عملکرد سنسورها (Walk Test)

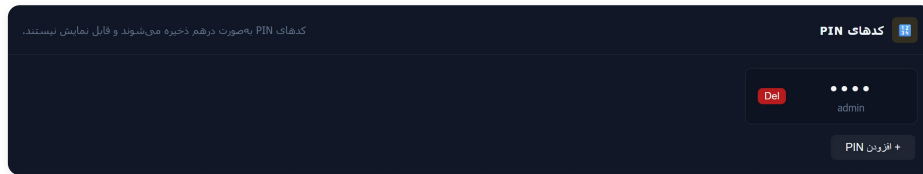


تصویر ۱۹ - آزمون قدم زنی: روی «شروع آزمایش قدم زنی» کلیک کرده، در برابر حسگرها راه بروید و درب ها را باز کنید تا دریافت سیگنال توسط پنل با تیک سبز تأیید گردد (آزمون پس از ۳۰ دقیقه پایان می یابد).

۷ رمزها و دسترسی‌ها

به زبانه دسترسی در ناحیه مورد نظر بروید. در این بخش مشخص می‌نمایید چه کسانی و با چه ابزارهایی مجاز به مسلح یا غیرمسلح کردن سیستم هستند.

رمز عددی فراگیر (PIN Code)



تصویر ۲۰ - تعریف رمزهای کاربری: کدی که در این بخش وارد می‌کنید، رمز فراگیر (Universal PIN) برای صفحه‌کلید، پیامک، تاج‌پنل‌های BMS و نرم‌افزار کنسول KDT است.

نکته بسیار مهم امنیتی

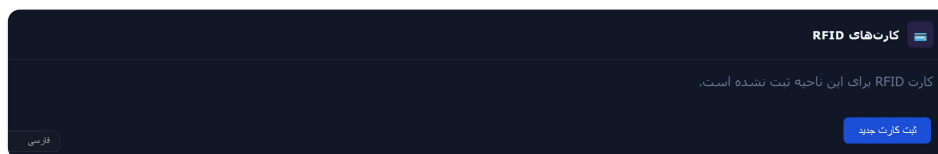
رمزها به صورت رمزنگاری‌شده در حافظه ثبت می‌شوند و قابل بازخوانی نیستند. در صورت فراموشی، باید رمز پیشین را حذف و یک کد جدید تعریف نمایید.

معماری یکپارچه کدهای عبور در زیست‌بوم KDT (کی‌پد، کنسول KDT و پنل‌های BMS)

رمز عبور ۴ رقمی ثبت‌شده در این زبانه، کلید مشترک مدیریت سیستم در تمام سامانه‌هاست. قواعد مسیریابی و نحوه ورود رمز به شرح زیر است:

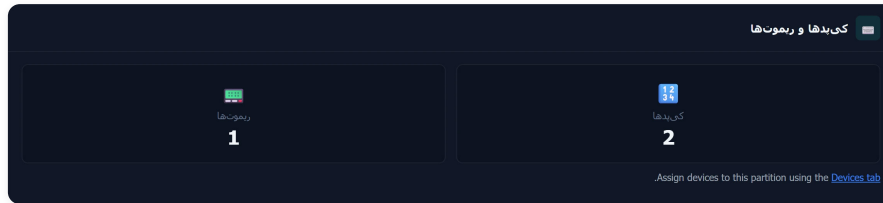
بستر کنترلی	قاعده ساختار رمز عبور و شیوه ورود
کنسول مانیتورینگ KDT (KDT Console)	جهت مسلح یا غیرمسلح کردن هر پارتیشن از طریق نرم‌افزار رایانه‌ای KDT Console، کاربر باید کد PIN همان پارتیشن را وارد نماید.
تاج‌پنل دیواری BMS (تک‌پارتیشن)	چنانچه پنل لمسی BMS صرفاً به یک پارتیشن مشخص منتسب شده باشد، کاربر مستقیماً کد PIN استاندارد ۴ رقمی را وارد می‌کند (مثال: 1234).
تاج‌پنل دیواری BMS (کلیه پارتیشن‌ها)	اگر پنل لمسی BMS به طور سراسری به تمام پارتیشن‌ها دسترسی داشته باشد، کاربر باید شماره ۲ رقمی پارتیشن را به عنوان پیشوند قبل از رمز وارد کند (مثال: برای کنترل پارتیشن ۱ با رمز ۱۲۳۴، کد 011234 و برای پارتیشن ۲، کد 021234 وارد می‌شود).

کارت و تگ RFID



تصویر ۲۱ - کارت‌ها و تگ‌های مجاز جهت خلع سلاح سریع از طریق نزدیک کردن به صفحه‌کلید بدون نیاز به فشردن کلیدها.

صفحه‌کلید و ریموت



تصویر ۲۲ – تجهیزات کنترل اختصاص‌یافته به ناحیه: نمایش کی‌پدها و ریموت‌های مجاز.

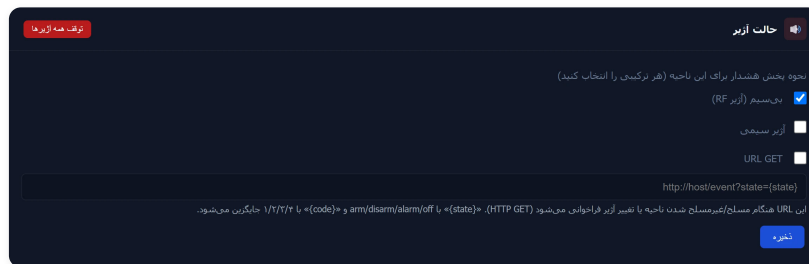
کاربران



تصویر ۲۳ – کاربران دارای مجوز دسترسی به این ناحیه از طریق پنل کاربری وب.

آژیر و خروجی‌ها

وارد زبانه «خروجی‌ها (Outputs)» در ناحیه مورد نظر شوید. در این بخش رفتار تجهیزات هشداردهنده تعیین می‌شود:

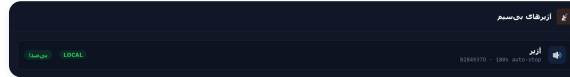


تصویر ۲۴ – انتخاب نوع آژیر و خروجی‌ها: امکان فعال‌سازی ترکیبی آژیر بی‌سیم، آژیر باسیم و فرمان شبکه URL GET.

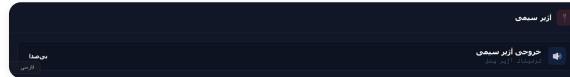
- **آژیر بی‌سیم و باسیم:** آژیرهای محیطی رادیویی یا پیژوی متصل به ترمینال بورد پنل مرکزی جهت ایجاد صدای هشدار در محل.
- **خروجی شبکه URL GET (دکمه نامرئی دیجیتال):** برای درک آسان، این قابلیت را مانند یک «دکمه نامرئی دیجیتال» تصور کنید؛ با وقوع حادثه یا مسلح شدن دزدگیر، پنل به صورت خودکار و نامحسوس یک آدرس وب تحت شبکه را باز می‌کند تا به سایر تجهیزات هوشمند ساختمان فرمان دهد (مانند ارسال دستور به بلندگوی تحت شبکه KDT (IP Speaker) جهت پخش هشدار صوتی ضبط‌شده، یا ارسال پیام به سرور خانه هوشمند برای روشن ساختن اضطراری تمام چراغ‌ها).



تصویر ۲۵ - تنظیم زمان قطع خودکار آژیر باسیم (مسیر سیستم ← دستگاه‌ها): مقدار پیش فرض ۱۸۰ ثانیه (۳ دقیقه) جهت جلوگیری از آلودگی صوتی ممتد است. مقدار ۰ به معنی تداوم پخش آژیر تا خلع سلاح دستی خواهد بود.



تصویر ۲۶ - فهرست آژیرهای بی سیم ثبت شده و فعال در این ناحیه.



تصویر ۲۷ - وضعیت لحظه‌ای خروجی آژیر باسیم روی برد پنل.



تصویر ۲۸ - خروجی‌های برنامه‌پذیر (PGM) جهت کنترل رله‌های فرمان روشنایی یا درب‌بازکن.

مدیریت و مسیریابی یکپارچه تجهیزات (System → Devices)

در منوی سیستم ← دستگاه‌ها (System → Devices)، مدیریت تجهیزات بر پایه منوهای کشویی (Dropdown) انجام شده و انتساب سخت‌افزارها به پارتیشن‌ها با سهولت کامل صورت می‌پذیرد:

نوع تجهیز / قابلیت	شرح عملکرد و شیوه تخصیص در منوی دستگاه‌ها
زون‌های باسیم و رله‌های PGM (Wired Zones & PGMs)	در این بخش دیگر از چک‌باکس استفاده نمی‌شود. در کنار هر زون باسیم و رله PGM یک منوی کشویی تعبیه شده تا کاربر به سادگی مشخص کند آن سخت‌افزار دقیقاً به کدام تک‌پارتیشن تعلق دارد.
خروجی آژیر باسیم (Wired Alarm Outputs)	امکان درج تایمر دقیق (بر حسب ثانیه) برای خروجی آژیر باسیم فراهم است تا پس از زمان تعیین شده، آژیر جهت جلوگیری از آلودگی صوتی ممتد به صورت خودکار قطع گردد.
آژیرهای بی سیم (RF Sirens)	فرآیند دو مرحله‌ای: ابتدا آژیر در پارتیشن دلخواه شناسانده (Learn) می‌شود؛ سپس با مراجعه به این منو، کاربر می‌تواند آژیر را جهت واکنش به پارتیشن‌های مختلف مسيردهی نماید.
صفحه کلیدها (Keypads)	هر صفحه کلید دارای یک منوی کشویی است که کاربر می‌تواند آن را جهت کنترل سراسری «همه ناحیه‌ها» یا کنترل انحصاری «یک ناحیه خاص» تخصیص دهد.
ریموت کنترل‌ها (Remote Controllers)	ریموت‌ها ابتدا در یک پارتیشن خاص تعریف می‌شوند، اما کاربر می‌تواند در این منو ریموت را انتخاب کرده و آن را هم‌زمان به چندین پارتیشن اختصاص دهد.
تاج پنل‌های BMS (BMS Panels)	پنل‌های BMS از طریق پروتکل Local MQTT خودکار شناسایی و اضافه می‌شوند. با انتخاب پنل، می‌توان آن را برای مدیریت «همه ناحیه‌ها» یا «یک ناحیه خاص» منتسب کرد.
مسیریابی هشدار اضطراری (SOS Routing)	تعیین پارتیشن مقصد برای شاسی خطر: مشخص کردن «ناحیه‌های که SOS دستگاه‌های اختصاص یافته به همه ناحیه‌ها را دریافت میکند» جهت هدایت دقیق آلارم‌های سراسری.

۹ اعلان و کنترل پیامکی

وارد زبانه «اعلان‌ها» در ناحیه مورد نظر شوید.

مخاطبان دریافت اعلان (پیامک / تماس)

مخاطبان پیامک / تماس

+ افزودن شماره

هنوز شماره‌ای اضافه نشده است.

تصویر ۲۹ - تعریف مخاطبان: بر روی «+ افزودن شماره» کلیک کرده و شماره همراه را وارد کنید. برای هر شماره می‌توانید نوع اطلاع‌رسانی (پیامک، تماس صوتی یا مجوز کنترل پیامکی) را تعیین نمایید.

انتخاب وقایع جهت ارسال گزارش

گزارش رویدادها به MQTT

نخیره

انتخاب کنید این ناحیه کدام رویدادها را به سرور ابری بفرستد.

هشدار

فعال‌سازی

غیرفعال‌سازی

خرابی

دستکاری

وضعیت PGM

تغییرات پیکربندی

رویدادهای سطح پیل

این‌ها زیرمجموعه دسته‌های خرابی و دستکاری بالا هستند. برداشتن تیک یک دسته، همه رویدادهای آن را خاموش می‌کند.

برق شهر

باتری پیل

شبکه همراه

ارتباط ورودی/خروجی

دستکاری پیل

توسعه‌دهنده

تصویر ۳۰ - فیلتر وقایع: جهت کاهش پیام‌های غیرضروری، تیک گزینه‌های کم‌اهمیت‌تر (مانند تغییرات پیکربندی) را بردارید. توصیه می‌شود تیک «هشدار» همواره فعال بماند.

کنترل سیستم با پیامک

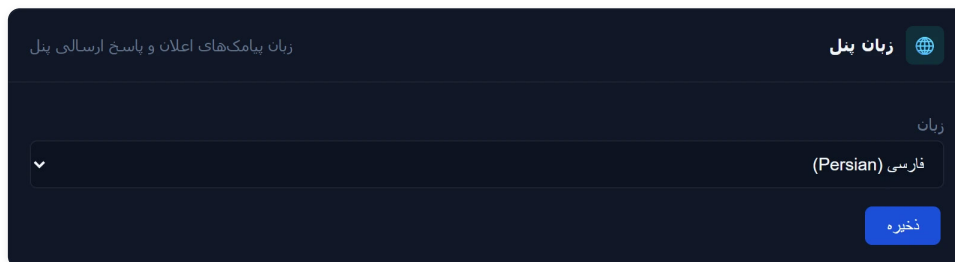
شماره‌هایی که دسترسی «اجازه کنترل» برای آن‌ها فعال شده است، می‌توانند با ارسال دستورات پیامکی سیستم را مدیریت کنند. تمامی فرامین با رمز عبور ناحیه (مانند 1234) آغاز می‌شوند:

عملکرد	دستور پیامکی
مسلح کردن کامل ناحیه ۱	1234 ARM 1
مسلح کردن در حالت حضور در منزل (ناحیه ۱)	1234 STAY 1
غیرمسلح کردن (خلع سلاح) ناحیه ۱	1234 DISARM 1
قطع فوری صدای آژیر	1234 STOP
استعلام و دریافت گزارش وضعیت سیستم	1234 STATUS
روشن کردن خروجی PGM شماره ۲ در ناحیه ۱	1234 PGM 1 2 ON
فعال‌سازی رله بی‌سیم شماره ۱ در ناحیه ۳	1234 RELAY 3 1 ON



تصویر ۳۱ – راهنمای دستورات پیامکی در زبانه «دسترسی». کد دستوری (PIN) ناحیه در همین بخش تعیین می‌گردد.

زبان پیامکها



تصویر ۳۲ – تعیین زبان پیامکها (مسیر سیستم ← دستگاهها): زبان متون ارسالی را مستقل از زبان رابط کاربری تعیین نمایید.

پیام صوتی اضطراری و تماس خودکار (Voice Message Alerts)

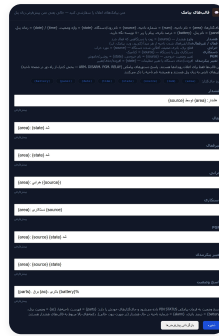
در هنگام بروز خطر، پتل می‌تواند بلافاصله با شماره‌های تعیین‌شده تماس تلفنی برقرار کرده و پیام صوتی هشدار را پخش کند. ثبت این پیام به دو روش امکان‌پذیر است:

روش اول – تماس و ضبط مستقیم (Call Me & Record - ساده‌ترین روش):

۱. در کارت Voice Message، شماره همراه خود را وارد کنید. ۲. دکمه سبز **Call Me & Record** را بزنید. ۳. ظرف چند ثانیه تلفن همراه شما زنگ می‌خورد؛ پاسخ دهید. ۴. پس از شنیدن بوق، پیام هشدار را شفاف بیان فرمایید (مانند: «توجه! هشدار امنیتی از دزدگیر کی‌دی‌تی... نفوذ غیرمجاز!»). ۵. تماس را قطع کنید؛ پیام بلافاصله در حافظه دستگاه ذخیره می‌شود.

روش دوم – بارگذاری فایل صوتی (Audio File Upload):

در صورت داشتن فایل ضبط‌شده حرفه‌ای، می‌توانید فایل صوتی را با فرمت **.wav** از طریق رایانه مستقیماً در پتل بارگذاری (Upload) نمایید.



تصویر ۳۳ - ویرایش قالب پیامک‌ها (مسیر سیستم ← پیام‌رسانی): الگوهای پیش‌فرض پیامک برای اغلب کاربری‌ها مناسب هستند؛ در صورت تمایل می‌توانید متون را با برچسب‌های هوشمند شخصی‌سازی فرمایید.

برچسب‌های هوشمند الگوهای پیامک (Smart Tags)

در هنگام تنظیم متن قالب‌ها، برچسب‌های هوشمند زیر به صورت خودکار با اطلاعات واقعی جایگزین می‌شوند:

برچسب هوشمند	داده واقعی جایگزین‌شده
{area}	نام پارتیشن رخداد (مانند «دفتر مدیریت» یا «انبار»)
{source}	نام سنسور تحریک‌شده (مانند «چشمی راهرو» یا «مگنت پنجره»)
{state}	نوع وضعیت امنیتی (ALARM، TAMPER یا RESTORED)
{time} / {date}	ساعت و تاریخ دقیق وقوع رویداد
{battery}	میزان ولتاژ لحظه‌ای باتری دستگاه

نمونه الگو: {time} در ساعت {source} توسط {area} در {state}: هشدار
پیامک دریافتی: «هشدار: ALARM در دفتر مدیریت توسط چشمی راهرو در ساعت 14:35»

۱۰ مازول توسعه

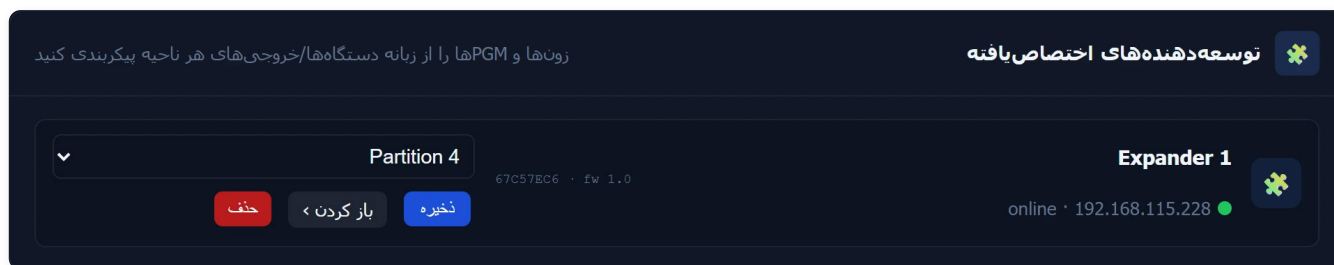
جهت افزایش زون‌های باسیم یا خروجی‌های رله، مازول توسعه را به شبکه متصل کرده و از منوی اصلی وارد «ماژول‌های توسعه» شوید.



تصویر ۳۴ - مازول‌های توسعه شناسایی‌شده در شبکه که آماده تخصیص به ناحیه هستند.

قواعد اتصال و پیکربندی شبکه مازول‌های توسعه (Expander):

- اتصال فیزیکی شبکه (کابل LAN): مازول توسعه حتماً باید از طریق یک کابل شبکه فیزیکی (LAN) به سوئیچ یا روتر متصل شود.
- الزام حضور در شبکه محلی یکسان: مازول توسعه و پنل اصلی دزدگیر کی‌دی‌تی حتماً و موقتاً باید به یک شبکه محلی کاملاً یکسان متصل باشند تا بتوانند با یکدیگر تبادل اطلاعات کنند.
- مسیریابی و ثبت آی‌پی پنل اصلی (Pairing): برای جفت‌سازی، وارد صفحه تنظیمات اختصاصی مازول توسعه شوید، آدرس آی‌پی (IP) پنل اصلی دزدگیر را در صفحه پیکربندی مازول وارد نموده و دکمه ذخیره را بزنید. با این اقدام، مازول دقیقاً می‌داند داده‌های سنسورها را به کدام پنل ارسال نماید و بلادرنگ در فهرست فوق پدیدار می‌گردد.



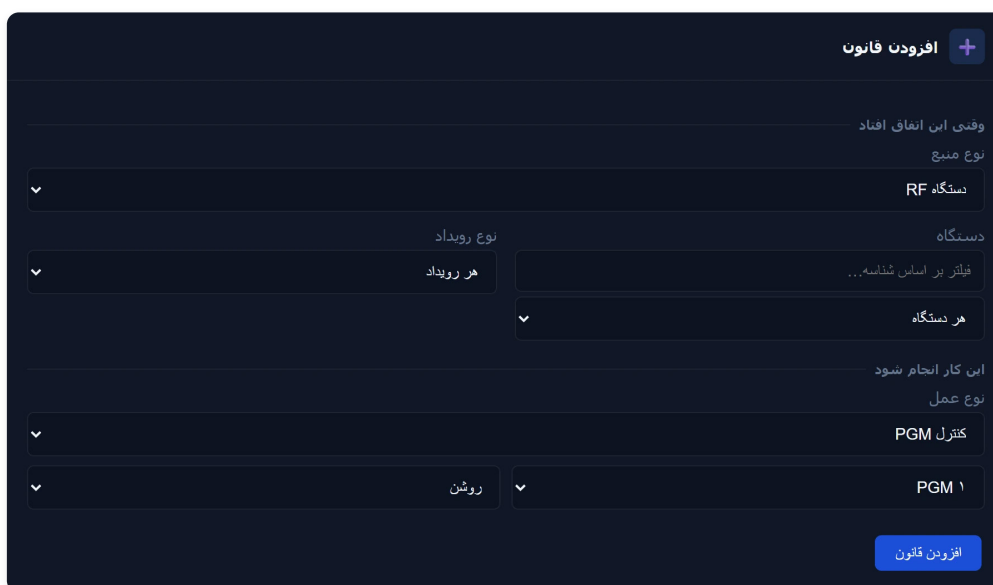
تصویر ۳۵ - تخصیص ماژول توسعه: ناحیه مربوطه را انتخاب کرده و کلید «ذخیره» را بزنید. پس از آن، زون‌ها و خروجی‌های این ماژول در زبانه‌های همان ناحیه فعال و قابل تنظیم خواهند بود.

نکته

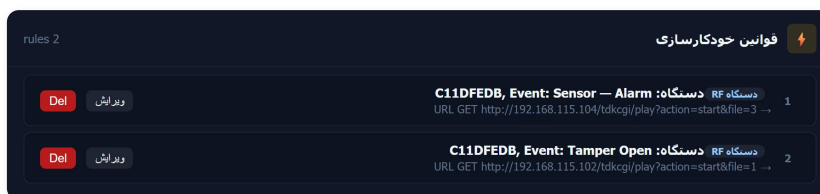
تا زمانی که ماژول به یک ناحیه اختصاص داده نشود، هیچ‌گونه فعالیتی نخواهد داشت؛ این سازوکار امنیتی مانع از اتصال ناخواسته ماژول‌های مجاور بر روی شبکه می‌گردد.

۱۱ خودکارسازی

این بخش اختیاری است و برای ایجاد سناریوهای هوشمند «شرط و عمل» (مانند روشن شدن خودکار چراغ در صورت تشخیص حرکت در حیاط) کاربرد دارد. جهت تعریف سناریوها، از منوی اصلی وارد بخش «خودکارسازی» شوید.



تصویر ۳۶ - فرم ایجاد قانون خودکارسازی: در بخش شرط، رویداد و دستگاه محرک را انتخاب کنید و در بخش عمل، وضعیت خروجی PGM را مشخص کرده و بر روی «افزودن قانون» کلیک نمایید.



تصویر ۳۷ - فهرست سناریوهای خودکارسازی فعال: امکان مشاهده، ویرایش یا حذف قوانین تعریف شده.

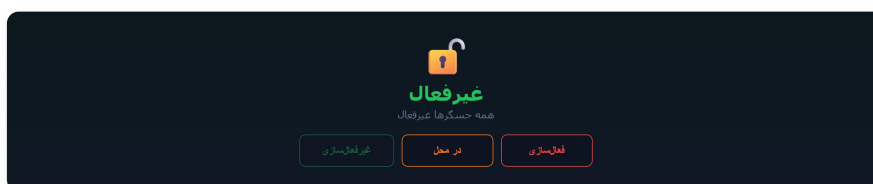
سناریوهای کاربردی خودکارسازی برای کاربران روزمره (Practical Automation Scenarios)

بخش قوانین خودکارسازی (Automation Rules) به شما اجازه می‌دهد واکنش‌های هوشمندی بر پایه فرمول «اگر [شرط رخ دهد]، آنگاه [عمل اجرا شود]» بسازید. در جدول زیر چهار سناریوی پرکاربرد آورده شده است:

عنوان سناریو	شرط رویداد (Trigger)	اقدام اجرایی خودکار (Action) و کاربرد واقعی
روشنایی هوشمند محوطه (کنترل رله PGM)	تحریک چشمی حرکتی محوطه در ساعات شب	فعال‌سازی رله PGM: رله فوراً چراغ‌های ورودی یا حیاط را روشن می‌کند تا علاوه بر تأمین دید، موجب فرار متجاوز احتمالی گردد.
پیام صوتی خوش‌آمد/ مسلح‌سازی (فرمان URL GET)	مسلح شدن دزدگیر توسط کاربر	فراخوانی آدرس بلندگوی تحت شبکه (IP Speaker): پخش فایل صوتی از بلندگوی KDT با صدای رسا: «سامانه امنیتی با موفقیت فعال گردید».
هشدار تردد پس از ساعت اداری (ارسال پیامک اختصاصی)	باز شدن درب انبار یا مدیریت در ساعات غیرکاری	ارسال پیامک فوری به مدیر: سیستم پیامکی اختصاصی برای شماره مدیریت می‌فرستد: «هشدار: درب انبار در ساعت غیرمجاز باز شد».
صدای تک‌بوق تأیید آژیر (Chime / Beep)	تغییر وضعیت پارتیشن (مسلح / خلع‌سلاح)	تحریک آژیر به مدت ۱ ثانیه: آژیر یک تک‌بوق کوتاه (Chirp) پخش می‌کند تا کاربر بدون نگاه به پنل، از اجرای درست فرمان مطمئن شود.

۱۲ کار روزمره

بهره‌برداری روزانه از سیستم شامل عملیات مسلح‌سازی، حالت در محل و خلع‌سلاح به شرح زیر است:



تصویر ۳۸ - زبانه «نمای کلی»: کلید «فعال‌سازی» برای خروج، «در محل» برای شب‌هنگام و «غیرفعال‌سازی» هنگام بازگشت.

حسگرها idle 3	فعال شده 0 فعال در حال حاضر	دستکاری 0 دستکاری گزارش شد	آزیرهای پوشش‌دهنده 1 محلی + سراسری
------------------	-----------------------------------	----------------------------------	--

تصویر ۳۹ - بررسی پیش از مسلح‌سازی: غیرصفر بودن «تحریک‌شده» نشانه باز بودن درب یا پنجره است.

log.txt

تازه سازی

۱۰۰ مورد آخر

همه ناحیه ها

تاریخچه رویدادها

زمان	نوع	ناحیه	کاربر	پیام
AM 8:44:14 , 8/16/2026	trouble	#4	-	expander 1 offline
AM 8:31:11 , 8/16/2026	trouble	#4	-	expander 1 offline
AM 3:14:09 , 8/16/2026	trouble	#4	-	expander 1 offline
PM 4:50:26 , 8/15/2026	trouble	#4	-	expander 1 offline
PM 4:32:43 , 8/15/2026	alarm	#1	-	alarm cleared on disarm
PM 4:31:08 , 8/15/2026	alarm	#1	-	ALARM RAISED via REMOTE_SOS
PM 4:30:53 , 8/15/2026	alarm	#1	-	alarm cleared on disarm
PM 4:30:51 , 8/15/2026	alarm	#1	-	ALARM RAISED via REMOTE_SOS
PM 4:29:53 , 8/15/2026	alarm	#1	-	alarm cleared on disarm
PM 4:29:49 , 8/15/2026	alarm	#1	-	ALARM RAISED via REMOTE_SOS
PM 4:23:43 , 8/15/2026	alarm	#1	-	alarm cleared on disarm
PM 4:23:40 , 8/15/2026	alarm	#1	-	ALARM RAISED via REMOTE_SOS
PM 4:18:19 , 8/15/2026	alarm	#1	-	alarm cleared on disarm
PM 4:18:16 , 8/15/2026	alarm	#1	-	ALARM RAISED via REMOTE_SOS
PM 4:17:51 , 8/15/2026	alarm	#1	-	alarm cleared on disarm
PM 4:17:47 , 8/15/2026	alarm	#1	-	ALARM RAISED via REMOTE_SOS
PM 4:09:00 , 8/15/2026	alarm	#1	-	alarm cleared on disarm
PM 4:08:34 , 8/15/2026	alarm	#1	-	ALARM RAISED via REMOTE_SOS
PM 3:59:09 , 8/15/2026	alarm	#1	-	alarm cleared on disarm
PM 3:58:58 , 8/15/2026	alarm	#1	-	ALARM RAISED via REMOTE_SOS
PM 3:49:54 , 8/15/2026	alarm	#1	-	alarm cleared on disarm

تصویر ۴۰ - بخش رویدادها (لاگ سیستم): گزارش زمانی دقیق تمامی وقایع ثبت شده در سیستم شامل هویت کاربر خلع سلاح کننده، زمان دقیق وقوع هشدارها، تحریک حسگرها و رخداد های فنی نظیر قطعی برق.

نگهداری و به روزرسانی

مشخصات دستگاه

زمان ساخت

Aug 15 2026 16:39:56

نسخه میان افزار

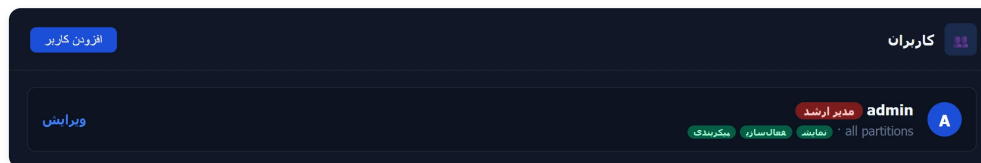
Burglar Alarm System v3.0.1

شناسه دستگاه MQTT

tdks5auvafmr

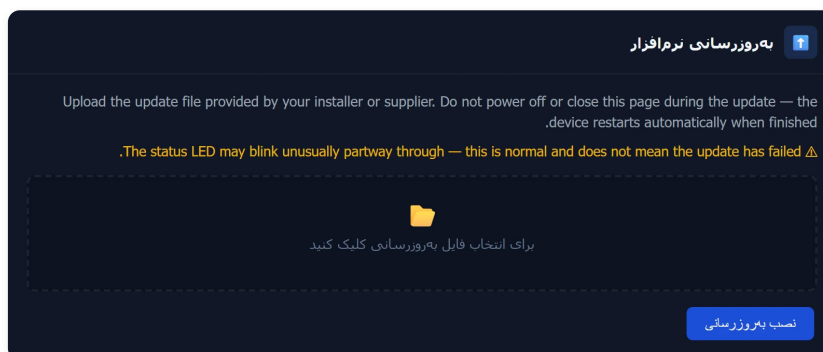
تصویر ۴۱ - مشخصات و اطلاعات فنی دستگاه (مسیر سیستم ← سیستم): هنگام تماس با مرکز پشتیبانی فنی، این اطلاعات (شامل نسخهٔ میان افزار و شناسهٔ دستگاه) را آماده داشته باشید.

ساخت کاربر و تغییر رمز ورود



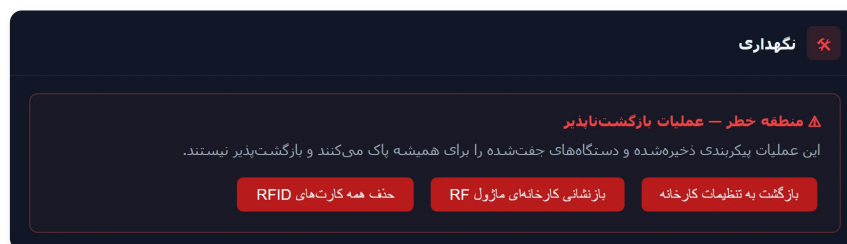
تصویر ۴۲ - از منوی اصلی وارد بخش **کاربران** شوید. جهت تغییر رمز عبور پیش فرض، بر روی گزینه «ویرایش» در سطر کاربر **admin** کلیک نمایید. توصیه می شود برای هر یک از کاربران حسابی مجزا با سطوح دسترسی مشخص به نواحی مورد نیاز تعریف فرمایید.

به روز رسانی نرم افزار



تصویر ۴۳ - ارتقای میان افزار: صرفاً از فایل های تأیید شده توسط شرکت کی دی تی یا نمایندگی مجاز استفاده فرمایید. در طول فرآیند به روز رسانی، جریان برق را قطع نکرده و پنجره مرورگر را نبندید؛ پس از پایان موفقیت آمیز عملیات، دستگاه به صورت خودکار راه اندازی مجدد خواهد شد.

بازگشت به تنظیمات کارخانه



تصویر ۴۴ - گزینه های بازنشانی سیستم: استفاده از این بخش موجب پاک شدن کامل تمامی تنظیمات، پارتیشن ها و تجهیزات ثبت شده خواهد گردید.

خطر

عملیات بازگشت به تنظیمات کارخانه **غیر قابل بازگشت است**. پس از اجرای آن، تمامی حسگرها و تجهیزات جانبی باید مجدداً در سیستم تعریف و جفت سازی شوند. اکیداً توصیه می شود این فرآیند را صرفاً با هماهنگی و راهنمایی کارشناسان پشتیبانی فنی اجرا نمایید.

عیب یابی سریع

در صورت بروز هرگونه اختلال یا خطا در سیستم، ابتدا راهکارهای جدول زیر را بررسی کنید:

مشکل	چه کار کنید
صفحه پنل باز نمی شود	از اتصال به همان شبکه محلی دستگاه اطمینان حاصل فرمایید. در صورت عدم اطمینان، به شبکه وای فای داخلی Burglar متصل شده و نشانی 192.168.4.1 را در مرورگر باز نمایید.
رمز ورود را فراموش کرده ام	رمز ورود از طریق پنل وب قابل بازیابی نیست؛ لطفاً با نصاب مجاز یا واحد پشتیبانی فنی شرکت کی دی تی تماس حاصل فرمایید.
سنسور ثبت نمی شود	میزان شارژ باتری حسگر را بررسی کرده، فاصله آن را تا پنل کاهش دهید و مجدداً گزینه «ثبت دستگاه جدید» را انتخاب نمایید.
سنسور در فهرست هست ولی آفلاین است	غالباً به دلیل اتمام شارژ باتری یا فاصله ارتباطی زیاد رخ می دهد. باتری حسگر را تعویض کرده یا محل نصب را نزدیک تر بیاورید.
سیستم مسلح نمی شود	در زبانه «نمای کلی»، شمارنده «تحریک شده» را بررسی کنید؛ احتمال باز ماندن درب یا پنجره وجود دارد. در صورت نیاز، زون مربوطه را به صورت موقت غیرفعال (Bypass) نمایید.
آژیر بی دلیل می زند	در بخش رویدادها، زون فعال کننده هشدار را مشخص کرده و شرایط محیطی محل نصب حسگر (مانند تابش مستقیم آفتاب، جریان باد کولر یا تردد حیوان خانگی) را بررسی فرمایید.
پیامک نمی آید	اعتبار ریالی سیم کارت را بررسی کرده، از سبز بودن نشانگر وضعیت 4G در صفحه شبکه مطمئن شوید و ثبت بودن شماره را در بخش «مخاطبان پیامک/تماس» تأیید نمایید.
خرابی «قطع برق شهر» می آید	در صورت وصل بودن برق ساختمان، سلامت آداپتور و کابل تغذیه را بازبینی فرمایید. سیستم تا زمان اتصال مجدد برق شهری، با باتری پشتیبان به کار خود ادامه می دهد.
ساعت رویدادها اشتباه است	مراحل گام ۴ (تنظیم تاریخ و ساعت سیستم) را مجدداً تکرار فرمایید.

راهنمای جامع آیکون‌ها و وضعیت صفحه نمایش

در این راهنما، معنی و مفهوم تمامی آیکون‌ها و رنگ‌های اختصاصی رابط کاربری دستگاه به زبان ساده و همراه با تصویر واقعی هر آیکون گردآوری شده است.

۱. نوار بالایی (ارتباطات، شبکه و باتری)

نوار بالای صفحه وضعیت اتصالات شبکه، سرورهای ابری، وضعیت آنتن و باتری را به صورت زنده نمایش می‌دهد:

اولویت اتصال فعال (Active Transport)



آیکون بستر فعلی متصل به سرور ابری (کابل شبکه LAN، وای‌فای WiFi یا سیم‌کارت SIM) به رنگ سبز روشن نمایش داده می‌شود. در صورتی که بستر شبکه متصل باشد اما هنوز به سرور ابری نرسیده باشد، همان آیکون به صورت تیره و کم‌رنگ دیده خواهد شد.

وضعیت سرورهای ابری و محلی (MQTT)



یک آیکون ابر بسته به وضعیت ارتباط رنگ عوض می‌کند: آبی (اتصال همزمان سرور ابری و محلی)، سبز (فقط سرور ابری وصل است)، زرد (فقط سرور محلی متصل است) و قرمز (قطعی کامل تمامی اتصالات).

وضعیت آنتن و دیتای سیم‌کارت (Cellular)



میزان آنتن از ۰ تا ۴ خط نشان داده می‌شود؛ با این حال، اگر اینترنت دیتای سیم‌کارت (GPRS) قطع باشد، حتی در صورت سیگنال کامل، آیکون به رنگ قرمز و به شکل قطع کامل درمی‌آید تا وضعیت اشتباه گزارش نشود.

چرخش آدرس‌های آی‌پی (IP Rolling)

چرخش IP (هر ۵ ثانیه)

در صورت اتصال همزمان دستگاه به چند شبکه (مانند کابل LAN، شبکه بی‌سیم STA و نقطه اتصال داخلی AP)، سیستم به صورت خودکار هر ۵ ثانیه آدرس آی‌پی مربوط به هر شبکه را روی صفحه می‌چرخاند.

وضعیت باتری و منبع تغذیه (Battery)



آیکون وضعیت‌های گوناگون توان دستگاه را گزارش می‌دهد: آیکون باتری متصل به برق در زمان شارژ کامل، آیکون رعدوبرق هنگام شارژ شدن، ۶ سطح پله‌ای درصد شارژ باقی‌مانده و آیکون قرمز ضربدر به نشانه نبود یا قطعی باتری.

۲. وضعیت پارتیشن‌ها (بخش‌های ۳۲ گانه سیستم)

صفحه نمایش تمامی ۳۲ پارتیشن را در یک جدول اختصاصی نمایش داده و وضعیت هر بخش را به صورت لحظه‌ای با آیکون‌های زیر مشخص می‌کند:

مسلح کامل (Armed)

آیکون قفل بسته قرمز رنگ؛ بخش مربوطه به طور کامل مسلح و فعال است.



آژیر خطر (Active Alarm)

آیکون آژیر قرمز رنگ؛ نشان‌دهنده وقوع هشدار و به صدا درآمدن دزدگیر در این بخش است.



حالت در منزل (Stay)

آیکون خانه نارنجی رنگ؛ نشان‌دهنده فعال بودن در حالت ماندن در منزل است.



تاخیر ورود (Entry Delay)

آیکون در نیمه‌باز به رنگ قرمز-کهربایی؛ مهلت غیرفعال کردن سیستم رو به اتمام است.



غیرفعال (Disarmed)

آیکون قفل باز سبز رنگ؛ این بخش از سیستم کاملاً غیرفعال و خاموش است.



تاخیر خروج (Exit Delay)

آیکون در نیمه‌باز به رنگ زرد؛ نشان می‌دهد سیستم در حال مسلح شدن است و کاربر باید خارج شود.

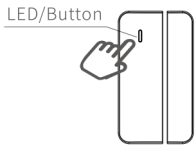
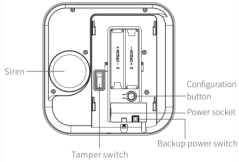
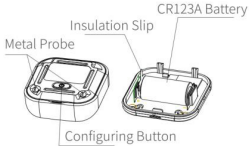
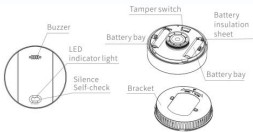


راهنمای جامع تعریف فیزیکی تجهیزات (Learn / Pairing)

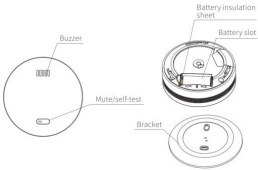
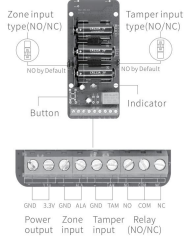
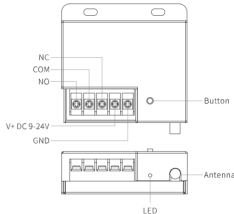
ابتدا در رابط وب دزدگیر وارد ناحیه (پارتیشن) مورد نظر شوید. سپس در زبانه تجهیزات (Devices) و در بخش ADD DEVICE بر روی گزینه ثبت دستگاه جدید (Learn New Device) کلیک نمایید؛ سپس مطابق با جدول زیر، دستورالعمل فیزیکی مربوط به هر حسگر را جهت جفت‌سازی اجرا فرمایید.

نکته بسیار مهم پیش از شروع جفت‌سازی:

قبل از اضافه کردن هر کدام از حسگرها باید عایق باتری حسگر را جدا فرمایید در غیر اینصورت به دستگاه اضافه نمی‌شود. برای جدا کردن عایق باتری هر حسگر باید درب محفظه پشت حسگر را باز نمایید.

ردیف	نام دستگاه	مدل	دستورالعمل فرآیند فیزیکی (Learn)	عکس دکمه Learn دستگاه
۱	مگنت درب و پنجره	KB-MG1-W	کلید Learn یا چراغ روی بدنه را به مدت ۳ ثانیه فشار داده و نگه دارید تا LED شروع به چشمک زدن سریع کند و به دزدگیر اضافه شود.	
۲	آژیر فضای باز	KB-SO1-W	کلید Learn تعبیه شده روی برد داخلی دستگاه را به مدت ۳ ثانیه نگه دارید تا سیگنال جفت‌سازی به پنل دزدگیر ارسال گردد.	
۳	حسگر نشستی آب	KB-WLS1-W	دکمه پشت حسگر را به مدت ۳ ثانیه نگه دارید تا نشانگر وضعیت فعال شده و کد شناسایی به دزدگیر منتقل شود.	
۴	حسگر دود	KB-SD1-W	کلید Learn روی بدنه حسگر را به مدت ۳ ثانیه فشار دهید و نگه دارید تا دستگاه وارد دزدگیر شود.	

ردیف	نام دستگاه	مدل	دستورالعمل فرآیند فیزیکی (Learn)	عکس دکمه Learn دستگاه
۵	صفحه کلید بیسیم	KB-K2-W	کلیدهای «Delete» و «Confirm» را به طور همزمان به مدت ۳ ثانیه فشار داده و نگه دارید تا چراغ سبز چشمک بزند و دستگاه وارد حالت شبکه و Pair شود.	
۶	ریموت کنترل	KB-R2	دکمه های «Arm» (قفل/فعال) و «Disarm» (باز/غیرفعال) را همزمان فشار داده و نگه دارید تا نشانگر LED سبز رنگ به سرعت چشمک بزند و ریموت روی پنل ثبت شود.	
۷	حسگر چشمی پرده ای	KB-PC1-W	کلید Pair پشت جعبه محفظه سنسور را به مدت ۳ ثانیه نگه دارید تا LED چشمک بزند و ارتباط برقرار شود.	
۸	حسگر چشمی حرکتی داخلی	KB-Pi2-W	دکمه Learn جلوی سنسور را ۳ ثانیه نگه دارید تا با فلاش زدن LED، کد شناسایی ارسال گردد.	
۹	حسگر چشمی حرکتی فضای باز	KB-PO1-W	کلید فیزیکی Learn روی برد اصلی کنار باتری دستگاه را به مدت ۳ ثانیه نگه دارید تا فرآیند جفت سازی با پنل مرکزی تکمیل گردد.	

ردیف	نام دستگاه	مدل	دستورالعمل فرآیند فیزیکی (Learn)	عکس دکمه Learn دستگاه
۱۰	حسگر مونوکسید کربن	KB-CMD1-W	کلید Learn روی بدنه را به مدت ۳ ثانیه فشار داده و نگه دارید تا سیگنال تعریف به سیستم ارسال شود.	
۱۱	فرستنده بیسیم	KB-WM1-TR	کلید فشاری لرن (Learn Button) تعبیه شده روی برد PCB (مجاور ترمینالها) را به مدت ۳ ثانیه نگه دارید تا چراغ LED شروع به چشمک زدن کند.	
۱۲	رله بیسیم	KB-WR1	دکمه Learn روی برد ماژول رله را به مدت ۳ ثانیه نگه دارید تا LED وضعیت سریع چشمک زده و ماژول در پنل ثبت شود.	

چک لیست تحویل

پیش از ترک محل نصب، چک لیست زیر را با دقت بررسی و تأیید نمایید:

☐ رمز عبور پیش فرض کارخانه ای ورود تغییر یافته و رمز جدید به مالک سیستم تحویل داده شده است.

☐ اتصال دستگاه به اینترنت (کابل شبکه، وای فای یا سیم کارت) برقرار بوده و وضعیت آن سبز است.

☐ تاریخ و ساعت سیستم به درستی تنظیم و همگام سازی شده است.

☐ نام گذاری تمامی ناحیه ها و زون ها به صورت معنادار و دقیق (نه به صورت پیش فرض مانند «Zone 1») انجام شده است.

☐ زمان های تأخیر ورود و خروج تنظیم شده و عملکرد آن بر روی درب ورودی اصلی آزمایش شده است.

☐ آزمون قدم زنی (Walk Test) با موفقیت اجرا شده و دریافت سیگنال از تمامی حسگرها تأیید گردیده است.

☐ عملکرد پخش آژیر به صورت واقعی تست شده و مدت زمان پخش صدای آن تنظیم گردیده است.

☐ حداقل یک شماره تلفن همراه جهت دریافت هشدارها ثبت شده و ارسال پیامک آزمایشی بررسی شده است.

☐ ارسال دستور پیامکی STATUS تست شده و پاسخ استعلام وضعیت از دستگاه دریافت گردیده است.

☐ مالک یا بهره بردار سیستم، فرآیند مسلح سازی و خلع سلاح را با نظارت نصاب به صورت عملی تمرین کرده است.

تصاویر این راهنما از محیط واقعی دستگاه با نسخهٔ میان افزار ۳/۰/۱ تهیه شده است؛ در سایر نگارش ها ممکن است برخی جزئیات ظاهری تفاوت داشته باشد. در صورت بروز هرگونه ابهام یا نیاز به راهنمایی بیشتر، با نصاب مجاز یا واحد پشتیبانی فنی شرکت کی دی تی تماس حاصل فرمایید.

