



Bezpečnostní ovládací panel AX

Zákonné informace

©2019 Hangzhou Hikvision Digital Technology Co., Ltd. Všechna práva vyhrazena.

O této příručce

Příručka obsahuje pokyny pro použití a správu produktu. Obrázky, grafy, zobrazení a všechny ostatní informace zde uvedené slouží výhradně k popisu a vysvětlení. Informace obsažené v příručce podléhají změnám bez oznámení z důvodu aktualizací firmwaru nebo z jiných důvodů. Aktuální verzi naleznete na firemní webové stránce (<https://www.hikvision.com/>).

Tuto příručku používejte pod vedením a s pomocí odborníků vyškolených pro podporu tohoto výrobku.

Obchodní známky

HIKVISION a další obchodní známky a loga jsou majetkem společnosti Hikvision v různých jurisdikcích.

Ostatní uvedené obchodní známky a loga jsou majetkem příslušných vlastníků.

Odmítnutí odpovědnosti

V MAXIMÁLNÍM ROZSAHU POVOLENÉM PLATNÝMI ZÁKONY JE TENTO MANUÁL A POPSANÝ PRODUKT SE SVÝM HARDWAREM, SOFTWAREM A FIRMWAREM DODÁN „JAK STOJÍ A LEŽÍ“ A „SE VŠEMI ZÁVADAMI A CHYBAMI“. SPOLEČNOST HIKVISION NEPOSKYTUJE ŽÁDNÉ ZÁRUKY, VÝSLOVNÉ NEBO PŘEDPOKLÁDANÉ, MIMO JINÉ VČETNĚ ZÁRUKY PRODEJNOSTI, USPOKOJIVÉ KVALITY A VHODNOSTI PRO KONKRÉTNÍ ÚČEL. VÝROBEK POUŽÍVÁTE NA SVÉ VLASTNÍ RIZIKO. SPOLEČNOST HIKVISION NENESE V ŽÁDNÉM PŘÍPADĚ ODPOVĚDNOST ZA JAKÉKOLIV ZVLÁŠTNÍ, NÁSLEDNÉ, NÁHODNÉ NEBO NEPŘÍMÉ ŠKODY, MIMO JINÉ VČETNĚ DALŠÍCH ŠKOD ZE ZTRÁTY PODNIKÁNÍ, PŘERUŠENÍ PODNIKÁNÍ NEBO ZTRÁTY ÚDAJŮ, NARUŠENÍ SYSTÉMŮ NEBO ZTRÁTY DOKUMENTACE, AŽ JIŽ K TOMU DOŠLO PORUŠENÍM SMLOUVY, V DŮSLEDKU PŘEČINU (VČETNĚ NEDBALOSTI), ODPOVĚDNOSTI ZA VÝROBEK NEBO JINAK VE SPOJENÍ S POUŽÍVÁNÍM VÝROBKU, A TO I V PŘÍPADĚ, ŽE BYLA SPOLEČNOST HIKVISION UPOZORNĚNA NA MOŽNOST TAKOVÝCH ŠKOD.




BERETE NA VĚDOMÍ, ŽE CHARAKTER INTERNETU UMOŽŇUJE VZNIK VNITŘNÍCH BEZPEČNOSTNÍCH RIZIK A SPOLEČNOST HIKVISION NEPŘEBÍRÁ ZODPOVĚDNOST ZA ABNORMÁLNÍ PROVOZ, NARUŠENÍ SOUKROMÍ NEBO JINÉ ŠKODY PLYNOUCÍ Z KYBERÚTOKU, ÚTOKU HACKERŮ, VIROVÉ KONTROLY NEBO JINÝCH RIZIK PRO BEZPEČNOST INTERNETU; V PŘÍPADĚ POTŘEBY VŠAK SPOLEČNOST HIKVISION POSKYTNE VČASNOU TECHNICKOU PODPORU.

SOUHLASÍTE S TÍM, ŽE BUDETE TENTO VÝROBEK POUŽÍVAT V SOULADU SE VŠEMI PLATNÝMI ZÁKONY A ŽE JSTE ODPOVĚDNÍ ZA ZAJIŠTĚNÍ TOHO, ŽE VAŠE POUŽÍVÁNÍ BUDE V SOULADU S PLATNÝMI ZÁKONY. ZEJMÉNA NESETE ODPOVĚDNOST ZA TO, ŽE BUDETE TENTO VÝROBEK POUŽÍVAT TAKOVÝM ZPŮSOBEM, ABY NEDOŠLO K PORUŠENÍ PRÁV TŘETÍCH STRAN, MIMO JINÉ VČETNĚ OMEZENÍ PRÁV NA PUBLICITU, PRÁV DUŠEVNÍHO VLASTNICTVÍ NEBO OCHRANY DAT A DALŠÍCH PRÁV NA OCHRANU SOUKROMÍ. NEBUDETE TENTO VÝROBEK POUŽÍVAT PRO ŽÁDNÉ ZAKÁZANÉ KONCOVÉ POUŽITÍ VČETNĚ VÝVOJE NEBO VÝROBY ZBRANÍ HROMADNÉHO NIČENÍ, VÝVOJE NEBO VÝROBY CHEMICKÝCH NEBO BIOLOGICKÝCH ZBRANÍ, JAKÉKOLIV ČINNOSTI V


KONTEXTU SOUVISEJÍCÍM S JAKÝMKOLIV NUKLEÁRNÍM VÝBUŠNÝM NEBO NEBEZPEČNÝM NUKLEÁRNÍM PALIVOVÝM CYKLEM NEBO NA PODPORU PORUŠOVÁNÍ LIDSKÝCH PRÁV. V PŘÍPADĚ JAKÉHOKOLI NESOULADU MEZI TOUTO PŘÍRUČKOU A PLATNÝM ZÁKONEM MÁ PŘEDNOST PLATNÝ ZÁKON.


Vysvětlení symbolů

Tyto symboly, které se mohou nacházet v dokumentu, jsou definovány následovně:

Symbol	Popis
 Nebezpečí	Označuje nebezpečnou situaci, která, pokud jí není zamezeno, způsobí nebo může způsobit smrt nebo vážné zranění.
 Upozornění	Označuje potenciálně nebezpečnou situaci, která by, pokud by jí nebylo zamezeno, mohla vést k poškození zařízení, ztrátě dat, zhoršení výkonu nebo neočekávaným výsledkům.
 Poznámka	Poskytuje další informace k zdůraznění nebo doplnění důležitých bodů hlavního textu.





Informace o předpisech

<p>EN 50131-1:2009+A2:2017 EN 50131-3:2009 EN 50131-6:2017 EN 50131-5-3:2017 EN 50131-10: 2014 EN 50136-2: 2013</p>	<p>Bezpečnostní stupeň (SG): 2 Třída ochrany životního prostředí (EC): II</p> <p style="text-align: center;">  Potvrzeno společností Telefication </p>
--	--

 **Poznámka** EN50131 značení dodržování předpisů by mělo být odstraněna, pokud jsou používány konfigurace, které předpisy nesplňují.

EU prohlášení o shodě

Tabulka 1-1

	<p>Tento výrobek a případně také dodávané příslušenství mají označení „CE“, a tudíž splňují požadavky platných harmonizovaných evropských norem uvedených ve směrnici EMC 2014/30/EU, směrnici RE 2014/53/EU a směrnici RoHS 2011/65/EU</p>
 	<p>2012/19/EU (nařízení WEEE): Výrobky označené tímto symbolem nelze v Evropské unii likvidovat jako netříděný komunální odpad. Pro správnou recyklaci vraťte tento výrobek místnímu dodavateli při zakoupení ekvivalentního nového zařízení nebo jej zlikvidujte na určených sběrných místech. Více informací naleznete na: www.recyclethis.info</p>
	<p>2006/66/ES (směrnice o bateriích): Tento výrobek obsahuje baterii, kterou v Evropské unii nelze likvidovat jako netříděný komunální odpad. Podrobné informace o bateriích naleznete v dokumentaci k výrobku. Baterie je označena tímto symbolem, který může obsahovat písmena označující kadmium (Cd), olovo (Pb) nebo rtuť (Hg). Pro správnou recyklaci vraťte baterii dodavateli nebo na určené sběrné místo. Více informací naleznete na: www.recyclethis.info</p>

Obsah

Kapitola 1 Úvod	1
1.1 Popis systému	1
1.2 Specifikace	2
1.3 Kategorie ATS	4
1.4 Vzhled	6
Kapitola 2 Připojení	10
Kapitola 3 Instalace	12
Kapitola 4 Konfigurace	16
4.1 Aktivace	16
4.1.1 Aktivace zařízení prostřednictvím webového prohlížeče	16
4.1.2 Aktivace zařízení prostřednictvím klientského softwaru	17
4.1.3 Aktivace prostřednictvím SADP	17
4.2 Použití klientského softwaru	18
4.3 Použití webového klienta	19
4.3.1 Nastavení komunikace	19
4.3.2 Správa zařízení	32
4.3.3 Nastavení oddílu	41
4.3.4 Správa videí	45
4.3.5 Správa povolení	49
4.3.6 Údržba	53
4.3.7 Systémová nastavení	55
4.3.8 Zkontrolovat stav	61
4.4 Použití mobilního klienta	61
4.4.1 Stažení a přihlášení mobilního klienta	61
4.4.2 Aktivace ovládacího panelu prostřednictvím Hik-Connect	62
4.4.3 Přidání ovládacího panelu k mobilnímu klientovi	63
4.4.4 Přidání periférií k ovládacímu panelu	64
4.4.5 Přidání karty	65
4.4.6 Přidat klíčenku	66

4.4.7 Správa uživatelů	67
4.4.8 Nastavení systému	68
4.4.9 Aktivace/Deaktivace zóny.....	71
4.4.10 Přemostění zóny.....	73
4.4.11 Nastavení zóny	73
4.4.12 Nastavení plánu aktivace/deaktivace	75
4.4.13 Kontrola stavu systému (Stav zóny/Stav komunikace)	77
4.4.14 Kontrola oznámení alarmu	78
4.4.15 Nastavení kanálu síťové kamery	79
4.4.16 Nastavení video událostí.....	80
4.4.17 Přidání kamery k zóně.....	81
Kapitola 5 Operace.....	83
5.1 Aktivace	83
5.2 Deaktivace	84
5.3 Použití klíčenky.....	84
5.4 Použití karty.....	87
5.5 Použití klientského softwaru	88
5.5.1 Přidání zařízení do klientského softwaru.....	88
5.5.2 Přidání zařízení do klientského softwaru prostřednictvím Cloud P2P.....	89
5.5.3 Fungování oddílu	90
5.5.4 Fungování relé	91
5.5.5 Fungování sirény	91
5.6 Použití webového klienta.....	92
5.6.1 Přidat/Upravit/Smazat kartu.....	93
5.6.2 Přidat/Upravit/Smazat klíčenku.....	93
5.6.3 Přidat/Upravit/Smazat uživatele.....	94
5.6.4 Zkontrolovat stav	96
A. Řešení problémů.....	97
A.1 Porucha komunikace	97
A.1.1 Konflikt IP.....	97
A.1.2 Webová stránka není přístupná.....	97

A.1.3 Hik-Connect je offline	97
A.1.4 Síťová kamera často vypadává	97
A.1.5 Nepodařilo se přidat zařízení na APP	97
A.1.6 Informace o alarmu nejsou podávány do APP/4200/Centra alarmů	98
A.2 Vzájemné vyloučení funkcí	98
A.2.1 Nelze vstoupit do režimu registrace	98
A.2.2 Nelze vstoupit do režimu zadání hledání RF signálu	98
A.3 Vada zóny	98
A.3.1 Zóna je offline	98
A.3.2 Odolnost proti manipulaci se zónou	99
A.3.3 Spuštěná zóna/chyba	99
A.4 Problémy při aktivaci	99
A.4.1 Porucha aktivace (Když se proces aktivace nespustí)	99
A.5 Provozní závada	99
A.5.1 Nepodařilo se vstoupit do režimu testu	99
A.5.2 Operace smazání alarmu na panelu nevede k vytvoření zprávy o vymazání alarmu	99
A.6 Porucha doručení e-mailu	100
A.6.1 Nepodařilo se odeslat e-mail o testu	100
A.6.2 Nepodařilo se odeslat e-mail během používání	100
A.6.3 Nepodařilo se odeslat e-maily na Gmail	100
A.6.4 Nepodařilo se odeslat e-maily na QQ nebo Foxmail	100
A.6.5 Nepodařilo se odeslat e-maily na Yahoo	101
A.6.6 Konfigurace e-mailu	101
B. Typy vstupů	102
C. Typy výstupů	105
D. Typy událostí	106
E. Úrovně přístupu	107
F. SIA a kód CID	109
G. Zařízení v certifikátu EN Standardní/Základní norma	114

Kapitola 1 Úvod

1.1 Popis systému

Bezdrátový bezpečnostní ovládací panel AX obsahující 32 bezdrátových zón podporuje komunikační metody Wi-Fi, TCP/IP a GPRS/3G/4G. Podporuje také ISAPI, Hik-Connect a DC-09, které lze použít v prostředí trhů, obchodů, domácností, výrobních závodů, skladů, kanceláří atd.

- TCP/IP, Wi-Fi, a sítě GPRS/3G/4G
- Připojuje až 32 bezdrátových zón, 4 bezdrátové výstupy, 8 klíčenek, 32 relé a 4 sirény
- Podporuje až 13 uživatelů sítě, včetně 1 technika, 1 správce, 1 výrobce a 10 běžných uživatelů

Poznámka

Přednastavené heslo **technika** je **installer12345** a přednastavené heslo **výrobce** je **hik12345**. Tyto kódy je třeba po prvním připojení změnit.

- Podporuje funkci zvonku: Detektor při spuštění ve stavu deaktivace zvoní jako dveřní zvonek
 - Hlasový pokyn
 - Nastavení Wi-Fi v režimu AP
 - Konfigurace prostřednictvím webového klienta nebo mobilního klienta
 - Oznámení o alarmu předává pomocí zpráv nebo telefonních hovorů
-

Poznámka

Tuto funkci podporuje pouze zařízení obsahující komunikační metodu GPRS/3G/4G

- Zobrazuje videozáznamy v přímém přenosu a posílá e-maily videí spojených s alarmem prostřednictvím mobilního klienta
 - Odesílá zprávy do centra alarmů
 - Obousměrná dálková komunikace se šifrováním AES-128
 - Podporuje indikátor LED na indikaci stavu systému
 - Lithiová záložní baterie 4520 mAh, podporuje napájení až na 12 h
 - Kompatibilní s protokolem SIA-Contact ID
-

Poznámka

V souladu s požadavkem EN bude systém průběžně evidovat stejný záznam pouze třikrát.

- Po 3 neplatných pokusech o přihlášení během jedné minuty bude zařízení na 90 sekund zablokováno

Objednávání

Tabulka 1-1

Model	Popis
-------	-------

Bezpečnostní ovládací panel AX

Model	Popis
DS-PWA32-HSR (černobílý)	podporuje Ethernet/WI-FI, 3G/4G a kartu IC
DS-PWA32-HGR (černobílý)	podporuje Ethernet/WI-FI, GPRS a kartu IC
DS-PWA32-HR (černobílý)	podporuje Ethernet/WI-FI a kartu IC
DS-PWA32-HS (černobílý)	podporuje Ethernet/WI-FI a kartu 3G/4G
DS-PWA32-HG (černobílý)	podporuje Ethernet/WI-FI a GPRS
DS-PWA32-H (černobílý)	podporuje Ethernet/WI-FI

1.2 Specifikace

DS-PW32-H(R)(S)(G)		
Připojení bezdrátového zařízení	Vstup alarmu	32
	Výstup alarmu	32
	Siréna	4
	Klíčenka	8
	Klávesnice	4
	Čtečka štítků	4
	Oddíl	4
Interakce	Zvukový výstup	1, 1,5 W
RF	Frekvence RF	433/868 MHz (závisí na modelu)
	RF modulace	GFSK
	RF vzdálenost	800 m (v otevřeném prostoru)
Připojená síť	Ethernet	10M/100M autoadaptivní
Mobilní síť	GPRS, 3/4G	Podporuje podávání oznámení na ARC a Cloud, textové oznámení prostřednictvím SMS a zvukové oznámení prostřednictvím telefonního hovoru
Wi-Fi	Standard	802.11b/g/n
	Šifrování	Podporováno

Bezpečnostní ovládací panel AX

DS-PW32-H(R)(S)(G)		
	Kanál	2,4 G
Použití a protokol	Použití	iVMS-4200 a Hik-Connect
	Protokol	Protokol RTC: DC-09(ADM-CID)/ DC-09(SIA-DCS) EHome
Uživatel	IC karta	12 (pouze pro model s -R)
	Uživatel	12 (1 technik, 1 správce, 1 výrobce a 10 běžných uživatelů)
Komunikace	Provozní režim	Průchozí
Přihlášení	Uloženo ve FLASH (chráněno proti přepsání)	Max. 4700 přihlašovacích položek, z nichž 1000 je povinných
Napájení	Typ	A
	Model	Adaptér AC/DC napájený z hlavní sítě Shenzhen Honor Electronic Co., Ltd ADS-12B-06 05010E Vstup 100–240 V 50/60 Hz Max 0,3 A Výstup 5 V DC 2,0 A střed pozitivní
	Nízkonapěťová zpráva	3,55 V
	Výstup	Žádné výstupy
	Proud při napájení z baterie	300 mA
Baterie	Typ	Dobíjitelná polymerová lithium-iontová baterie Model: 765965 Jmenovité napětí: Kapacita 3,8 V: 4520 mAh 17,176 Wh 24 hodin pro dobítí na 80 %
Servis	Neobsahuje žádné díly, jejichž servis by mohl provádět uživatel	
Ostatní	Napájení	5 VDC, 10 W
	Proud	Proud alarmu: 300 mA Proud, který není určen pro

Bezpečnostní ovládací panel AX

DS-PW32-H(R)(S)(G)	
	alarm: 240 mA
Spotřeba (bez HDD)	< 5,6 W
Provozní teplota	-10 °C až 55 °C
Provozní vlhkost	10 % až 90 %
Materiál pláště	PC+ABS
Rozměr (Š x V x H)	155 × 155 × 35 mm
Hmotnost	410 g
Napájení z baterie	12 H

Poznámka

Ehome5.0: internetový protokol pro ochranu osobních dat, jenž se používá pro přístup k platformě třetích stran podporující nahrávání alarmových zpráv, správu ovládacího panelu pro zajištění bezpečnosti a nahrávání krátkých videí.

Poznámka

Standardní protokol DC-09

ADM-CID: Metoda prezentování dat DC-09 je CID, které není zašifrované a je určeno pouze pro odeslání zprávy alarmu.

*ADC-CID: Metoda prezentování dat DC-09 je CID, které je zašifrované a je určeno pouze pro odeslání zprávy alarmu.

SIA-DCS: Metoda prezentování dat DC-09 je DCS (také nazývané SIA protokol), které není zašifrované a je určeno pouze pro odeslání zprávy alarmu.

*SIA-DCS: Metoda prezentování dat DC-09 je DCS (nazývané také SIA protokol), které je zašifrované a je určeno pouze pro odeslání zprávy alarmu.

1.3 Kategorie ATS

Tabulka 1-2 Kategorie ATS

Kategorie	Model
DP2	DS-PWA32-HSR
	DS-PWA32-HS
	DS-PWA32-HGR

Bezpečnostní ovládací panel AX

Kategorie	Model
	DS-PWA32-HG
SP4	DS-PWA32-HR DS-PWA32-H

Poznámka

Pokud je zaznamenána závada ATP, tak ovládací panel vygeneruje a podá zprávy. Pokud je zaznamenána závada ATP, tak ovládací panel vygeneruje a podá zprávy, signalizuje poruchu pomocí výstražné LED (svítí oranžovou barvou) a v případě, že je systém deaktivován autorizovanými uživateli, vyzve k detekci poruchy.

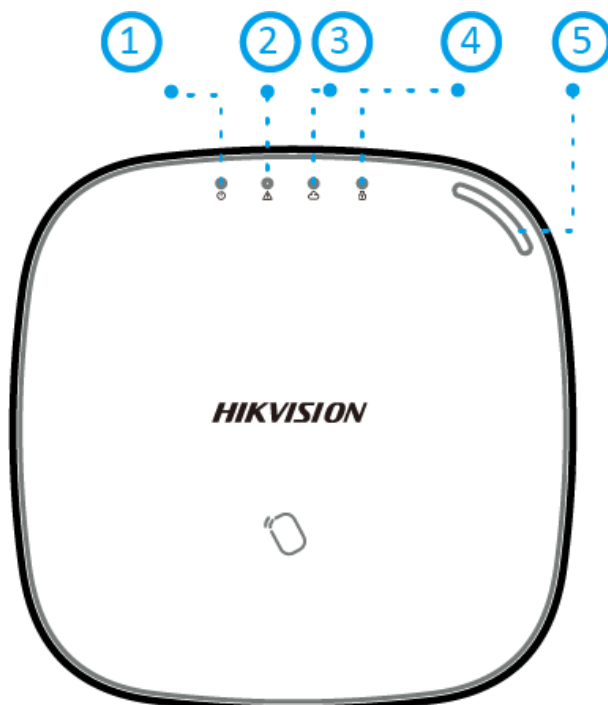
DP2: Když je centrum přijímání alarmů povoleno. Ovládací panel nahraje zprávu alarmu do přijímacího centra přes hlavní cestu (LAN nebo Wi-Fi) nebo záložní cestu (3G/4G). Pokud je ovládací panel správně připojen k síti LAN nebo Wi-Fi, je jako přenosová cesta vybrána hlavní cesta. Pokud se připojení hlavní cestou nezdaří, přepne se cesta na 3G/4G. A pokud je připojení hlavní cestou obnoveno, přepne se cesta zpět na LAN nebo Wi-Fi. Ovládací panel nepřetržitě kontroluje stav připojení a generuje poruchu přenosu protokolů pro jakoukoli cestu. Ačkoliv jsou obě cesty neplatné, ovládací panel určí chybu ATS.

SP: Ovládací panel může nahrávat pouze zprávy prostřednictvím LAN nebo Wi-Fi. Když je připojení neúspěšné, určí ovládací panel chybu ATS a uloží protokol událostí.

Informace o chybě naleznete v protokolech ovládacího panelu.


1.4 Vzhled

Přední panel



Obrázek 1-1 Přední panel

Tabulka 1-3 Popis předního panelu

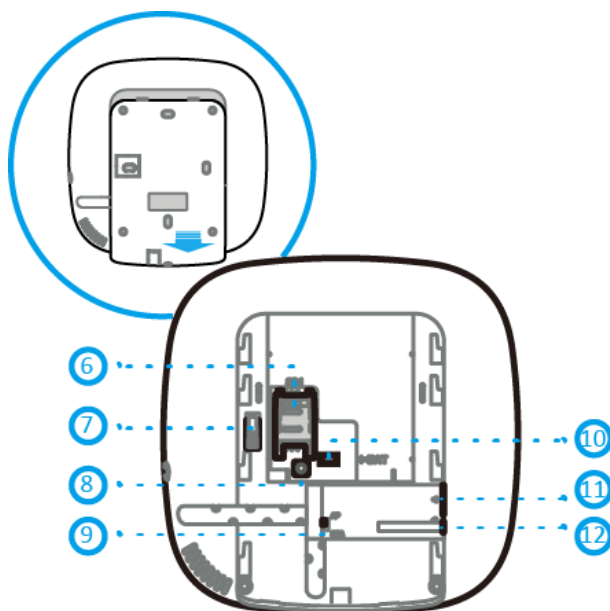
Č.	Název indikátoru	Popis
1	Napájení střídavým proudem	Svíí zeleně: Zapnutí Vypnutí: Vypnuto
2	Upozornění	Svíí oranžově: Ve stavu deaktivace LED signalizuje alarm (například alarm paniky, alarm zóny, alarm proti manipulaci atd.) a poruchu (jako je porucha provozu, porucha připojení atd.) <hr/>  Poznámka Hlasová oznámení, která není povoleno zobrazovat/pouštět uživatelům úroveň 1, budou slyšet pouze po předložení platné visačky nebo klíčenky. Když budou oprávnění uživatelé systém deaktivovat, poskytnete zařízení podrobné informace o alarmu nebo poruše. Při aktivaci na webovém klientu můžete nastavit indikaci závady.

Bezpečnostní ovládací panel AX

Č.	Název indikátoru	Popis
		*Není v souladu s požadavkem EN.
3	Odkaz	Svíí zeleně: Panel je spojen s účtem Hik-connect Vypnutí: Panel není spojen s účtem Hik-connect
4	Aktivovat/Deaktivovat	Nepřerušované modré světlo na 5 s: Aktivováno i Poznámka Při aktivaci na webovém klientovi můžete nastavit indikátor aktivace na trvale zapnuto. *Není v souladu s požadavkem EN. Vypnutí: Deaktivováno
5	Alarm	Blikající červená: Spustil se alarm Svíí červeně: Manipulace se zařízením Vypnutí: Žádný alarm

Komponent a rozhraní

Sejměte zadní kryt a některé součásti a rozhraní jsou na zadním panelu.



Obrázek 1-2 Komponent a rozhraní

Tabulka 1-4 Popis zadního panelu

Číslo	Popis
6	Slot SIM karty
	 Poznámka Funkce GPRS nebo 3G/4G (realizováno s vestavěným slotem SIM karty) se liší v závislosti na modelu zařízení.
7	MANIPULACE
8	Tlačítko Reset
9	Spínač AP&STA
10	Konektor baterie
11	Síťové rozhraní
12	Rozhraní napájení

Funkční tlačítko

Funkční tlačítko je na straně ovládacího panelu.



Obrázek 1-3 Funkční tlačítko

Použijte funkční tlačítko pro přidání bezdrátových zařízení a kontrolu signálu RF.
 Pokud ovládací panel není v režimu konfigurace, stiskněte jednou funkční tlačítko na straně

Bezpečnostní ovládací panel AX

ovládacího panelu a spusťte periferní zařízení.

Pokud ovládací panel není v režimu konfigurace, stiskněte dvakrát funkční tlačítko a můžete zkontrolovat sílu signálu RF na periferním zařízení.

Výsledek	RSSI	Opatření
Silné	Více než 160	Odsouhlasení instalace
Střední	80 až 160	Odsouhlasení instalace
Slabé	0 až 79	Viz níže uvedená poznámka.
Neplatné	-	Nesouhlas s instalací

Poznámka

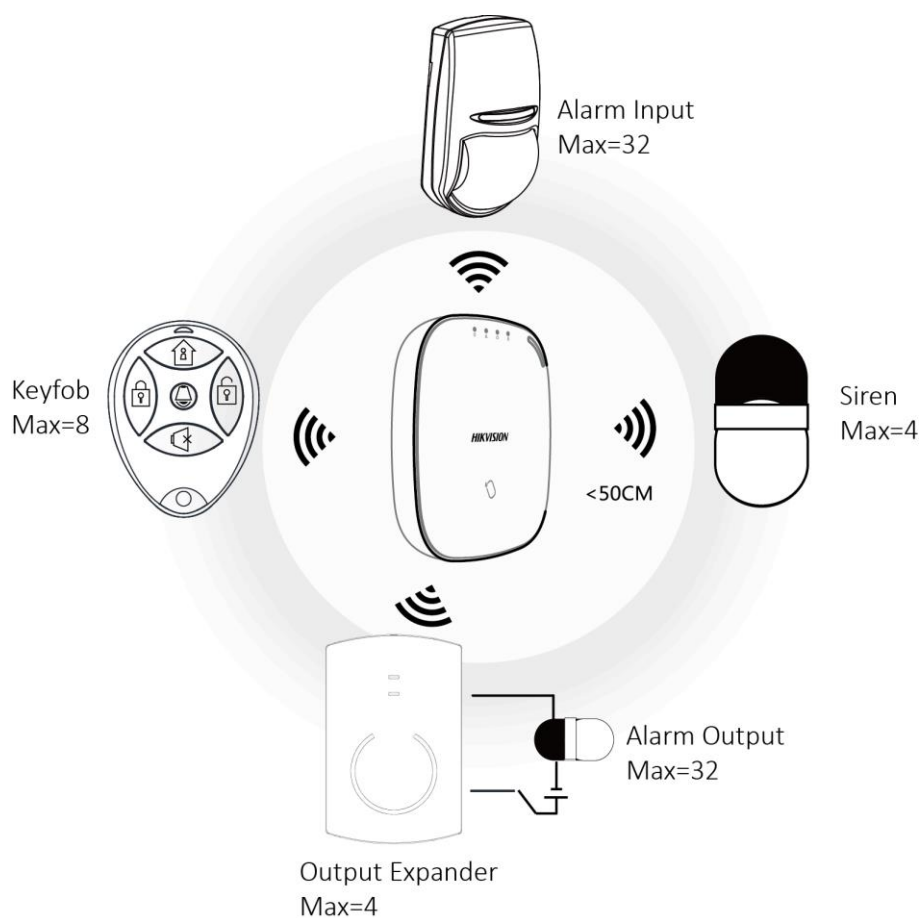
Periferie instalujte pouze v případě, že je síla signálu 100 nebo vyšší. Pro mnohem lepší systém instalujte při 120 a více.

Kapitola 2 Připojení

Můžete připojit periferní zařízení k ovládacímu panelu místně, prostřednictvím klientského softwaru, webového klienta nebo mobilního klienta.

Poznámka

Před připojením a instalací periferních zařízení zkontrolujte sílu signálu RF. Pokud ovládací panel není v režimu registrace, dvakrát stiskněte funkční tlačítko a spusťte bezdrátové zařízení (poplach událostí nebo poplach při manipulaci). Indikaci síly signálu RF můžete vidět na periferním zařízení.



Obrázek 2-1 Připojení

Místní připojení

Poznámka


Před přidáním periferního zařízení přidejte prostřednictvím webového klienta kartu nebo klíčenku, čímž vyrušíte alarm proti manipulaci.

Vzdálenost mezi ovládacím panelem a bezdrátovým zařízením by měla být menší než 50 cm.

Pokud ovládací panel není v režimu registrace, stiskněte jednu funkční tlačítko na straně ovládacího panelu a spusťte periferní zařízení.

Připojení prostřednictvím klientského softwaru

Přidejte ovládací panel ke klientskému softwaru.

V klientském softwaru klikněte na **Správa zařízení** →  → **Bezdrátové zařízení**. Zvolte zónu/relé/sirénu a vstupte na stránku **Nastavení**. Zadejte číslo sériového zařízení pro připojení.

Poznámka

Podrobnosti naleznete v kapitole *Konfigurace-Konfigurace prostřednictvím webového klienta-Nastavení alarmu*.

Připojení prostřednictvím webového klienta

Na webovém klientovi klikněte na **Bezdrátové zařízení**. Zvolte zónu/relé/sirénu a vstupte na stránku **Nastavení**. Zadejte číslo sériového zařízení pro připojení.

Poznámka

Podrobnosti naleznete v kapitole *Konfigurace-Konfigurace prostřednictvím webového klienta-Nastavení alarmu*.

Připojení prostřednictvím mobilního klienta

Přidejte ovládací panel k mobilnímu klientovi.

Na stránce nastavení ovládacího panelu klikněte na +, naskenujte kód QR na bezdrátovém zařízení nebo zadejte sériové číslo zařízení.

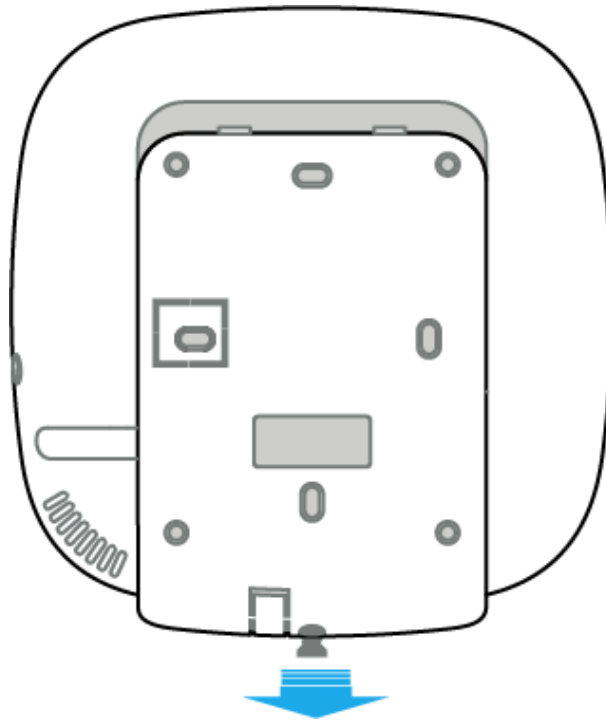
Poznámka

Podrobnosti naleznete v kapitole *Konfigurace-Konfigurace prostřednictvím mobilního klienta-Přidání periferního zařízení na ovládací panel*.

Kapitola 3 Instalace

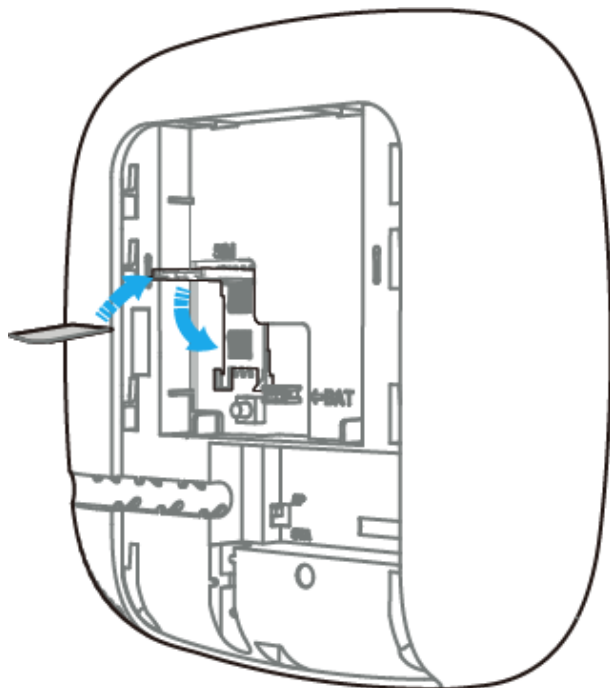
Postup

1. Uvolněte šroub na zadním krytu. Posuňte zadní kryt směrem dolů a sejměte jej z ovládacího panelu.



Obrázek 3-1 Odstraňte zadní kryt

2. Vložte SIM kartu do slotu na SIM kartu.

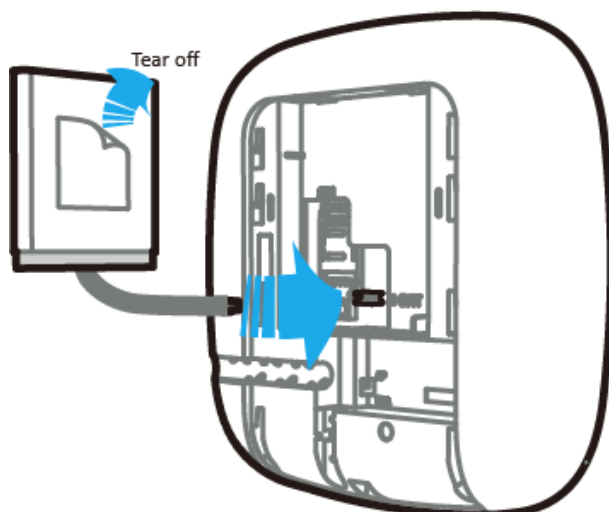


Obrázek 3-2 Vložte SIM kartu

Upozornění

Zkontrolujte, zda byla SIM karta otestována, protože u některých poskytovatelů může dojít k problémům s komunikací.

3. Připojte baterii k ovládacímu panelu.

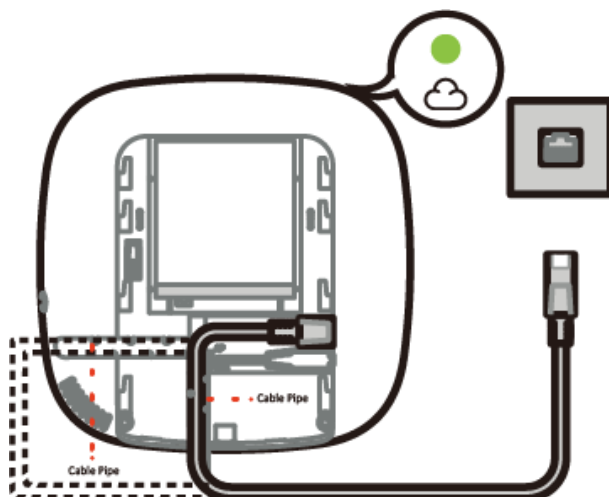


Obrázek 3-3 Připojte baterii

4. Síťový adaptér připojte k ovládacímu panelu a zásuvce. Indikátor napájení se asi po 30 s rozsvítí zeleně, což znamená, že je zařízení zapnuté.

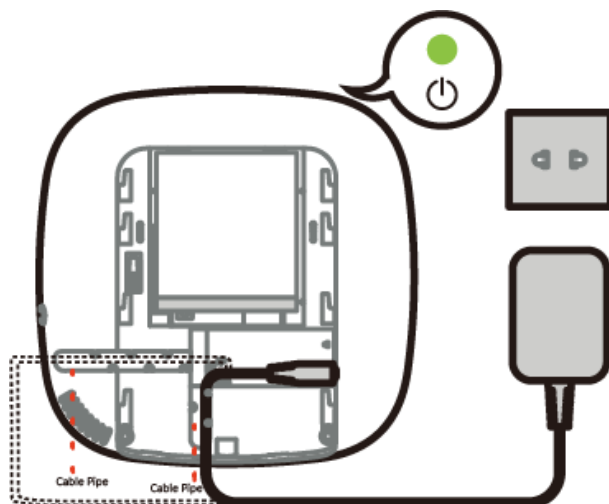
Poznámka

Stavy bez SIM karty, bez baterie, bez přívodu proudu nebo odpojení od sítě způsobí poruchu ovládacího panelu.



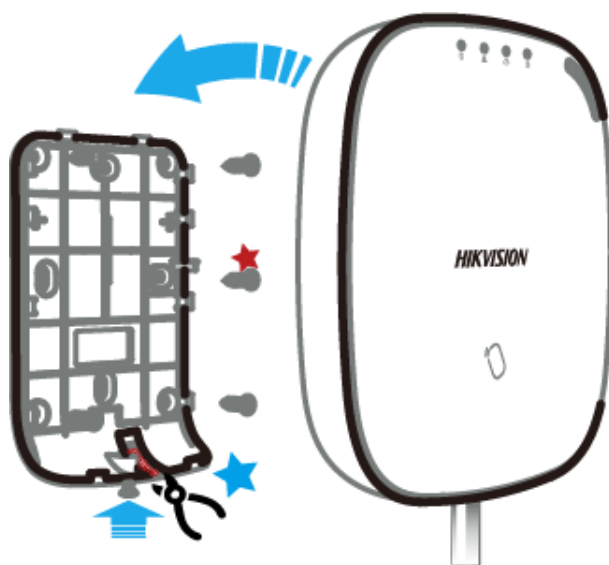
Obrázek 3-4 Zapnutí

5. Připojte ethernetový kabel k internetové zásuvce. Po přidání zařízení k účtu Hik-Connect se indikátor spojení rozsvítí zeleně.



Obrázek 3-5 Připojení k ethernetu

6. Připevněte zadní kryt k místu instalace - použijte k tomu dodané šrouby. Připevněte ovládací panel k zadnímu krytu a utažením šroubu na zadním krytu dokončete instalaci.



Obrázek 3-6 Dokončete instalaci

Poznámka

- Modrá hvězdička: Otevření boční stěny. Potřebujete-li kabel protlačit spodní částí panelu, odstraňte plech bočního otvoru.
 - Červená hvězdička: Šroub PROTI MANIPULACI. Je třeba připevnit šroub proti MANIPULACI.
 - Není nutné provádět žádné úpravy.
 - Určeno pouze pro použití v rámci prostor pod dohledem.
-

Kapitola 4 Konfigurace

Nakonfigurujte ovládací panel zabezpečení ve webovém klientovi nebo na stránce vzdálené konfigurace v klientském softwaru.

4.1 Aktivace

Pro ochranu bezpečnosti a soukromí osob a zlepšení úrovně zabezpečení sítě byste měli zařízení aktivovat při prvním připojení zařízení k síti.

4.1.1 Aktivace zařízení prostřednictvím webového prohlížeče

Zařízení aktivujete pomocí webového prohlížeče. Pomocí softwaru SADP nebo PC klienta vyhledejte online zařízení, získáte IP adresu zařízení a aktivujete zařízení na webové stránce.

Než začnete

Zařízení a váš PC musí být připojeny ke stejné LAN.

Postup

1. Otevřete webový prohlížeč a zadejte IP adresu zařízení.

Poznámka

Pokud zařízení připojíte přímo k počítači, musíte změnit IP adresu vašeho počítače na stejnou podsít' jako zařízení. Přednastavená IP adresa zařízení je 192.0.0.64.

2. Vytvořte a potvrďte heslo správce.

Upozornění

DOPORUČENO SILNÉ HESLO – Doporučujeme, abyste si vytvořili silné heslo podle vlastního výběru (použití minimálně 8 znaků, které by měly zahrnovat velká písmena, malá písmena, čísla a speciální znaky) za účelem zvýšení zabezpečení vašeho výrobku. A doporučujeme vám pravidelně resetovat heslo, zejména v systému s vysokým zabezpečením vám resetování hesla jednou za měsíc nebo jednou za týden může pomoci ochránit váš výrobek.

3. Kliknutím na **OK** dokončíte aktivaci.
4. Upravte IP adresu zařízení.
 - 1) Otevřete stránku úpravy IP adresy.
 - 2) Změňte IP adresu.
 - 3) Uložte nastavení.

4.1.2 Aktivace zařízení prostřednictvím klientského softwaru

Než začnete


- Stáhněte si klientský software iVMS-4200 z dodaného disku nebo oficiální webové stránky <http://www.hikvision.com/en/>. Software nainstalujte v souladu s pokyny.
- Zařízení a PC, které používají software, by měly být v rámci stejné podsítě.

Postup

1. Spustíte klientský software.
2. Otevřete stránku **Správa zařízení**.
3. Klikněte na **Online zařízení**.
4. Zkontrolujte stav zařízení v seznamu online zařízení a vyberte neaktivní zařízení.
5. Klikněte na tlačítko **Aktivovat**.
6. Vytvořte a potvrďte heslo správce zařízení.

Upozornění

DOPORUČENO SILNÉ HESLO – Doporučujeme, abyste si vytvořili silné heslo podle vlastního výběru (použití minimálně 8 znaků, které by měly zahrnovat velká písmena, malá písmena, čísla a speciální znaky) za účelem zvýšení zabezpečení vašeho výrobku. A doporučujeme vám pravidelně resetovat heslo, zejména v systému s vysokým zabezpečením vám resetování hesla jednou za měsíc nebo jednou za týden může pomoci ochránit váš výrobek.

7. Kliknutím na **OK** spustíte aktivaci.
Po úspěšné aktivaci se stav zařízení změní na **Aktivní**.
8. Upravte IP adresu zařízení.
 - 1) Zvolte zařízení a klikněte na  v seznamu online zařízení.
 - 2) Změňte IP adresu zařízení na stejnou podsít jako váš počítač a nastavte číslo portu na 80.
 - 3) Zadejte heslo správce zařízení a kliknutím na **OK** úpravu dokončíte.
9. Volitelně: Zkontrolujte zařízení v seznamu online zařízení a kliknutím na **Přidat** přidáte zařízení do seznamu zařízení.

4.1.3 Aktivace prostřednictvím SADP

SADP je nástroj určený ke zjištění, aktivaci a úpravě IP adresy zařízení na LAN.

Než začnete

- Získejte software SADP z dodaného disku nebo oficiální webové stránky <http://www.hikvision.com/en/> a nainstalujte SADP v souladu s pokyny.
- Zařízení a PC, které pracují na zařízení SADP, by měly být v rámci stejné podsítě.

Následující kroky ukazují, jak aktivovat zařízení a upravit jeho IP adresu. Informace o aktivaci dávky a úpravě IP adresy naleznete v *Uživatelské příručce SADP*.

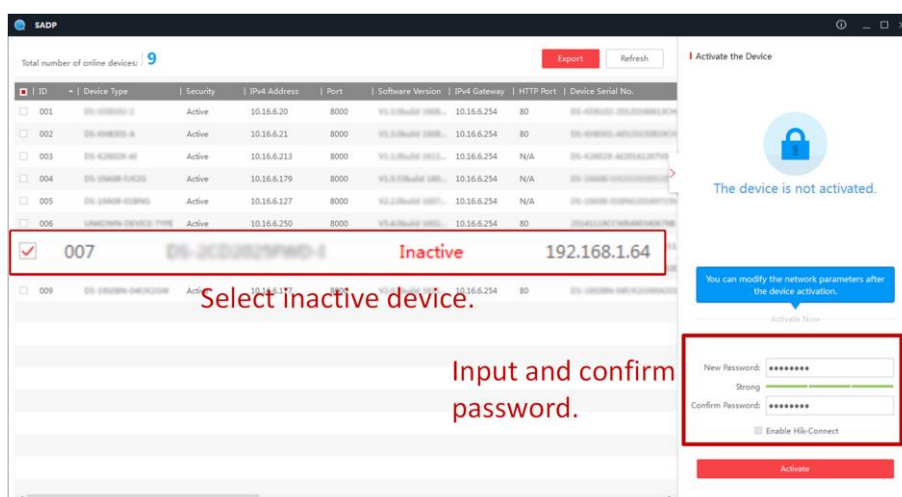
Postup

1. Spustíte software SADP a vyhledejte online zařízení.
2. Najděte a vyberte své zařízení v seznamu online zařízení.
3. Zadejte nové heslo (heslo správce) a potvrďte je.

⚠ Upozornění

DOPORUČENO SILNÉ HESLO – Doporučujeme, abyste si vytvořili silné heslo podle vlastního výběru (použití minimálně 8 znaků, které by měly zahrnovat velká písmena, malá písmena, čísla a speciální znaky) za účelem zvýšení zabezpečení vašeho výrobku. A doporučujeme vám pravidelně resetovat heslo, zejména v systému s vysokým zabezpečením vám resetování hesla jednou za měsíc nebo jednou za týden může pomoci ochránit váš výrobek.

4. Klikněte na tlačítko **Aktivovat** pro zahájení aktivace.



Stav zařízení se po úspěšné aktivaci změní na **Aktivní**.

5. Upravte IP adresu zařízení.
 - 1) Zvolte zařízení.
 - 2) Změňte IP adresu zařízení na stejnou podsít' jako váš počítač buď tím, že manuálně upravíte IP adresu nebo zaškrtnutím možnosti **Povolit DHCP**.
 - 3) Zadejte heslo správce a kliknutím na tlačítko **Upravit** aktivujete vaši úpravu IP adresy.


4.2 Použití klientského softwaru

Postup

1. Stáhněte, nainstalujte a zaregistrujte klientský software.
2. Na stránce **Správa zařízení** → **Zařízení** přidejte zařízení.

📖 Poznámka

- Nastavte č. portu zařízení na 80.
- Uživatelské jméno a heslo při přidávání zařízení jsou uživatelské jméno a heslo aktivace.

3. Kliknutím na tlačítko  otevřete stránku Vzdálená konfigurace poté, co bylo zařízení zcela přidáno.

4.3 Použití webového klienta

Postup

1. Připojte zařízení k ethernetu.
2. Vyhledejte IP adresu zařízení prostřednictvím klientského softwaru a softwaru SADP.
3. Do adresní lišty zadejte hledanou IP adresu.

Poznámka

Při používání mobilního prohlížeče je přednastavená IP adresa 192.168.8.1. Zařízení musí být v režimu AP.

Poznámka

Při přímém připojení síťového kabelu s počítačem je přednastavená IP adresa 192.0.0.64.

4. Pro přihlášení použijte aktivační uživatelské jméno a heslo.

Poznámka

Podrobnosti naleznete v kapitole *Aktivace*.

4.3.1 Nastavení komunikace

Připojená síť

Pokud je zařízení připojeno k pevné síti, můžete, když chcete změnit IP adresu zařízení a další síťové parametry, nastavit parametry připojené sítě.

Postup

Poznámka

Některé modely zařízení funkci nepodporují.

1. V klientském softwaru otevřete stránku **Správa zařízení**.
2. V seznamu zařízení pro správu zvolte zařízení a klikněte na **Vzdálená konfigurace**.

3. Kliknutím na **Komunikační parametry** → **Ethernet** otevřete stránku parametry připojené sítě.

Wired Network Settings

DHCP	<input type="checkbox"/>
IP Address	<input type="text" value="10.6.112.14"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway Address	<input type="text" value="10.6.112.254"/>
MAC Address	<input type="text" value="58:03:fb:b4:3b:6a"/>
DNS1 Server Address	<input type="text" value="8.8.8.8"/>
DNS2 Server Address	<input type="text" value="8.8.4.4"/>
HTTP Port	<input type="text" value="80"/>

Save

Obrázek 4-1 Stránka nastavení připojené sítě

4. Nastavte parametry.

Automatické nastavení: Aktivujte **DHCP** a nastavte port HTTP. Manuální nastavení: Vypnuté **DHCP** a nastavená **IP adresa, maska podsítě, adresa brány, adresa DNS serveru**.

 **Poznámka**

Port HTTP je ve výchozím nastavení 80.

5. Volitelné: Nastavte správnou adresu DNS serveru, pokud zařízení potřebuje navštívit server Hik-Connect prostřednictvím názvu domény.

6. Klikněte na **Uložit**.

Wi-Fi

Parametry Wi-Fi můžete nastavit v případě, že jsou v blízkosti bezpečné a důvěryhodné sítě Wi-Fi.

Postup

1. Kliknutím na **Komunikační parametry** → **Wi-Fi** otevřete stránku Wi-Fi.

Bezpečnostní ovládací panel AX

Wi-Fi Access point WLAN

Status of STA/AP Swit...

Switch Mode: STA Mode

Wi-Fi

SSID Wi-Fi

Wi-Fi Password

Encryption Mode WPA2-personal

Network List

Name	Channel No.	Signal Strength	Encryption Mode	Operation
MERCURY_1F32	13	100	WPA2-personal	Connect
gaoke_3E64E0	13	100	WPA2-personal	Connect
linksys_test	8	90	WPA2-personal	Connect
rongyao-pro	6	88	WPA2-personal	Connect
NETGEAR91	1	84	WPA2-personal	Connect
HAP_Q00197765	11	76	WPA2-personal	Connect
TP-LINK_DD63	1	72	WPA2-personal	Connect

Save

Obrázek 4-2 Stránka nastavení Wi-Fi

2. Provedte připojení k Wi-Fi.

Manuální připojení: Zadejte **SSID Wi-Fi** a **Wi-Fi heslo**, zvolte **režim kódování** a klikněte na **Uložit**.
Vyberte ze seznamu sítě: Ze seznamu sítě vyberte cílové Wi-Fi. Klikněte na **Připojit** a zadejte heslo Wi-Fi a poté klikněte na **Připojit**.

3. Kliknutím na **WLAN** otevřete stránku WLAN.

Wi-Fi Access point WLAN

DHCP :

IP Address 0.0.0.0

Subnet Mask 0.0.0.0

Gateway Address

MAC Address 00:95:69:f2:b6:a5

DNS1 Server Address

DNS2 Server Address

Save

Obrázek 4-3 Stránka nastavení WLAN

4. Nastavte **IP adresu**, **masku podsítě**, **adresu brány** a **adresu DNS serveru**.

Poznámka

Pokud aktivujete DHCP, zařízení vám automaticky poskytne parametry Wi-Fi.

5. Klikněte na **Uložit**.

Mobilní síť

Nastavte mobilní síťové parametry, pokud vložíte SIM kartu do zařízení. S použitím mobilní sítě může zařízení oznámení o alarmu nahrát do centra alarmů.

Než začnete

Vložte SIM kartu do slotu na SIM kartu na zařízení.

Postup

1. Kliknutím na **Komunikační parametry** → **Mobilní datová síť** otevřete stránku Nastavení mobilní datové sítě.

Cellular Data Network Settings

Enable GPRS/3G/4G	<input checked="" type="checkbox"/>
Access Number	<input type="text" value="*99***1#"/> ⓘ
User Name	<input type="text"/>
Access Password	<input type="text"/>
APN	<input type="text"/>
MTU	<input type="text" value="1400"/>
PIN Code	<input type="text"/>
Data Usage Limit	<input checked="" type="checkbox"/>
Data Used This Month	<input type="text" value="0.0"/> M
Data Limited per Month	<input type="text" value="100"/> M

Save

Obrázek 4-4 Stránka nastavení mobilní datové sítě

2. Aktivujte bezdrátové vytáčení.
3. Nastavte parametry mobilní datové sítě.

Přístupové číslo

Zadejte vytáčené číslo operátora.

Uživatelské jméno

Požádejte provozovatele sítě o uživatelské jméno a zadejte je.

Přístupové heslo

Požádejte provozovatele sítě o heslo a zadejte je.

APN

Požádejte provozovatele sítě o informace o APN a zadejte informace o APN.

Limit používání dat

Aktivovat funkci a nastavovat limit dat můžete každý měsíc. Pokud je využití dat vyšší než nastavený práh, spustí se alarm a nahraje se do centra alarmů a mobilního klienta.

Data používaná tento měsíc

Použitá data budou shromážděna a zobrazena v tomto textovém okně.

4. Klikněte na **Uložit**.

Centrum alarmu

Můžete nastavit parametry centra alarmu a všechny alarmy budou odeslány do nakonfigurovaného centra alarmu.

Postup

1. Kliknutím na **Komunikační parametry** → **Centrum přijímání alarmů** otevřete stránku Centrum přijímání alarmů.

Alarm Receiving Center

Alarm Reciever Center	1
Enable	<input checked="" type="checkbox"/>
Protocol Type	
Alarm Receiver Type	IP
Alarm Receiver IP Addr...	0.0.0.0
Port No.	0
Account Code	

Save

Obrázek 4-5 Parametry centra přijímání alarmů

2. Vyberte **Centrum přijímání alarmů** jako **1** nebo **2** pro konfiguraci a posunutím posuvníku povolte vybrané centrum přijímání alarmů.

Poznámka

Centrum přijímání alarmů 2 můžete nastavit jako **záložní kanál** a upravit parametry kanálu pouze v případě, že je aktivováno centrum přijímání alarmů 1.

3. Zvolte **Typ protokolu** jako **ADM-CID**, **EHome**, **SIA-DCS**, ***SIA-DCS** nebo ***ADM-CID** pro nastavení režimu odesílání.

Poznámka

Standardní protokol DC-09

ADM-CID: Metoda prezentování dat DC-09 je CID, které není zašifrované a je určené pouze pro odeslání zprávy alarmu.

*ADC-CID: Metoda prezentování dat DC-09 je CID, které je zašifrované a je určené pouze pro odeslání zprávy alarmu.

SIA-DCS: Metoda prezentování dat DC-09 je DCS (také nazývané SIA protokol), které není zašifrované a je určené pouze pro odeslání zprávy alarmu.

*SIA-DCS: Metoda prezentování dat DC-09 je DCS (nazývané také SIA protokol), které je zašifrované a je určené pouze pro odeslání zprávy alarmu.

ADM-CID nebo **SIA-DCS** Měli byste zvolit **Typ přijímače alarmu** jako **IP** nebo **název domény** a zadat IP/název domény, číslo portu, kód účtu, časový limit, časy opakovaného odesílání a interval.

Alarm Receiving Center

Alarm Receiver Center	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/>
Protocol Type	<input type="text" value="SIA-DCS"/>
Address Type	<input type="text" value="IP"/>
Server Address	<input type="text" value="10.22.96.247"/>
Port No.	<input type="text" value="6800"/>
Account Code	<input type="text" value="1106"/>
Transmission Mode	<input type="text" value="TCP"/>
Retry Timeout Period	<input type="text" value="20"/> s
Attempts	<input type="text" value="2"/>
Heartbeat Interval	<input type="text" value="300"/> s <input checked="" type="checkbox"/> Enable

Save

Obrázek 4-6 SIA-DCS

Poznámka

Nastavte interval pravidelného zvuku v rozmezí od 10 do 3888000 sekund.

EHome Nemusíte nastavovat parametry protokolu EHome.

Alarm Receiving Center

Alarm Receiver Center	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/>
Protocol Type	<input type="text" value="EHome"/>
Address Type	<input type="text" value="IP"/>
Server Address	<input type="text" value="10.22.98.247"/>
Port No.	<input type="text" value="6600"/>

Obrázek 4-7 EHome

***SIA-DCS** nebo ***ADM-CID** Měli byste zvolit **Typ přijímače alarmu** jako **IP** nebo **název domény** a zadat IP/název domény, číslo portu, kód účtu, lhůtu časového limitu pro opakované zkoušení, pokusy, interval pravidelného zvuku, aritmetické šifrování, délku hesla a tajný klíč.

Alarm Receiving Center

Alarm Receiver Center	1
Enable	<input checked="" type="checkbox"/>
Protocol Type	*ADM-CID
Address Type	IP
Server Address	10.22.96.247
Port No.	6600
Account Code	1106
Transmission Mode	TCP
Retry Timeout Period	20 s
Attempts	2
Heartbeat Interval	300 s <input checked="" type="checkbox"/> Enable
Encryption Arithmetic	AES
Password Length	128
Secret Key	

Save

Obrázek 4-8 *ADM-CID

Poznámka

Nastavte interval pravidelného zvuku v rozmezí od 10 do 3888000 sekund.

Pro aritmetické šifrování: Formát pomocného šifrování panelu pro informační bezpečnost v souladu s DC-09, AES-128, AES-192 a AES-256 je podporován, když nakonfigurujete centrum alarmů.

Pro tajnou klávesu: Když používáte zašifrovaný formát DC-09, měl by být při konfigurování ARC nastaven klíč. Klíč vydá ARC offline a měl by se použít k zašifrování zprávy pro bezpečnost náhrady.

4. Klikněte na **Uložit**.

Odesílání nabízených oznámení

Pokud je spuštěn poplach, chcete-li odeslat oznámení o alarmu klientovi, centru alarmů, cloudu nebo mobilnímu telefonu, můžete nastavit parametry odesílání nabízených oznámení.

Postup

1. Klikněte na **Komunikační parametry** → **Komunikace události**.
2. Zapněte cílové oznámení.

Alarmy a případy manipulace

Zařízení zašle oznámení tehdy, když se spustí alarm zóny, nebo při spuštění či obnovení alarmu proti manipulaci.

Alarmy pro zajištění bezpečnosti života

Zařízení zašle oznámení tehdy, když se spustí alarm požáru, alarm úniku plynu nebo alarm ohrožení zdraví.

Údržba a závady

Zařízení zašle oznámení v případě, že se jakkoliv změní stav systému.

Oznámení řízení panelu

Zařízení bude nabízet oznámení tehdy, když uživatel pracuje se zařízením.

Poznámka

Pokud chcete odeslat oznámení o alarmu mobilnímu klientovi, měli byste rovněž nastavit **Index mobilního telefonu**, **Číslo mobilního telefonu** a zaškrtnout **Typ oznámení**.

Poznámka

Pro oznámení zpráv ve středisku příjmu alarmů zvolte před nastavením index centra.

3. Klikněte na **Uložit**.

Výsledek

Tabulka 4-1 Možnosti oznámení

Možnost	Oznámení
iVMS-4200	Alarmy a případy manipulace Alarmy pro zajištění bezpečnosti života Údržba a závady Oznámení řízení panelu
Centrum příjmu alarmu	Centrum příjmu alarmů 1 a 2 Alarmy a případy manipulace Alarmy pro zajištění bezpečnosti života Údržba a závady Oznámení řízení panelu
Cloud	Alarmy a případy manipulace Alarmy pro zajištění bezpečnosti života

Možnost	Oznámení
	Údržba a závady Oznámení řízení panelu
Mobilní telefon	Index mobilního telefonu 1 až 6 Číslo mobilního telefonu Typ oznámení SMS a hlasová schránka Alarmy a případy manipulace Alarmy pro zajištění bezpečnosti života Údržba a závady

Registrace mobilního klienta

Pokud chcete zaregistrovat zařízení k mobilnímu klientovi pro vzdálenou konfiguraci, měli byste nastavit parametry registrace mobilního klienta.

Než začnete

- Připojte zařízení k síti prostřednictvím pevného připojení, vytáčeného připojení nebo Wi-Fi.
- Nastavte IP adresu zařízení, masku podsítě, adresu brány a DNS server v LAN.

Postup

1. Kliknutím na **Komunikační parametry** → **Registrace Hik-Connect** otevřete stránku Nastavení registrace Hik-Connect.

Hik-Connect Adding Settings

Register to Hik-Connect

Hik-Connect Adding Status: Online

Custom Server Address:

Server Address:

Communication Mode:

Verification Code:

The password should contain 6 to 12 characters (it is recommended to be more than 8 characters and the combination of numeric and letter) .

Obrázek 4-9 Stránka nastavení registrace Hik-Connect

2. Zaškrtněte možnost **Zaregistrovat k Hik-Connect**.

Poznámka

Ve výchozím nastavení se zapne služba zařízení Hik-Connect.

Můžete zobrazit stav zařízení na serveru Hik-Connect (www.hik-connect.com).

3. Povolte možnost **Uživatelská adresa serveru**.

Adresa serveru je již zobrazena v textovém okně Adresa serveru.

4. Z rozevřacího seznamu vyberte komunikační režim v souladu s aktuální komunikační metodou zařízení.

Auto

Systém vybere režim komunikace automaticky podle pořadí připojené sítě, sítě Wi-Fi a mobilní datové sítě. Zařízení se připojí k jiné síti pouze v případě, že aktuální síť bude odpojena.

Pořadí priority připojené sítě a Wi-Fi

Pořadí priority připojení od nejvyšší k nejnižší: pevné připojení, Wi-Fi, mobilní datová síť.

Pevné připojení a Wi-Fi

Systém nejdříve vybere pevné připojení. Není-li nalezeno žádné pevné připojení, zvolí síť Wi-Fi.

Mobilní datová síť

Systém vybere pouze mobilní datovou síť.

5. Volitelné: Změňte heslo pro ověření.

Poznámka

- Heslo pro ověření se ve výchozím nastavení zobrazí v textovém okně.
- Heslo pro ověření by mělo obsahovat 6 až 12 písmen nebo číslic. Z bezpečnostních důvodů doporučujeme osmimístné heslo, které obsahuje dva nebo více z následujících typů znaků: velká písmena, malá písmena a číslice.

6. Klikněte na **Uložit**.

EHome

V této části můžete vytvořit účet EHome a upravit IP adresu/název domény a číslo portu.

Postup

1. Kliknutím na **Komunikační parametry** → **Registrace EHome** otevřete stránku nastavení registrace Ehome.

EHome Registration Settings

Enable	<input checked="" type="checkbox"/>
EHome Protocol Version	ISUP5.0
Address Type	IP
Server Address	
Port No.	7660
Registration Status	Offline
Device ID	000000
Communication Mode	Wired Network & Wi-Fi Priority
EHome Login Password	

Save

Obrázek 4-10 Registrace Ehome

2. Posunutím posuvného kontaktu zapnete protokol Ehome.
3. Zvolte **Typ adresy** jako **IP** nebo **Název domény**.
4. Zadejte IP adresu nebo název domény podle typu adresy.
5. Zadejte číslo portu pro protokol.

Poznámka

Číslo portu pro EHome je ve výchozím nastavení 7660.

6. Nastavte účet včetně **ID zařízení a přihlašovacího hesla EHome**.

7. Zvolte **Režim komunikace**.

Auto

Systém vybere režim komunikace automaticky podle pořadí připojené sítě, sítě Wi-Fi a mobilní datové sítě. Zařízení se připojí k jiné síti pouze v případě, že aktuální síť bude odpojena.

Pořadí priority připojené sítě a Wi-Fi

Pořadí priority připojení od nejvyšší k nejnižší: pevné připojení, Wi-Fi, mobilní datová síť.

Pevné připojení a Wi-Fi

Systém nejdříve vybere pevné připojení. Nemá-li nalezeno žádné pevné připojení, zvolí síť Wi-Fi.

Mobilní datová síť

Systém vybere pouze mobilní datovou síť.

8. Klikněte na **Uložit**.

NAT

Universal Plug and Play (UPnP™) je síťová architektura, která zajišťuje kompatibilitu mezi síťovými zařízeními, softwarem a dalšími hardwarovými zařízeními. Protokol UPnP umožňuje bezproblémové připojení zařízení a zjednodušení implementace sítí v domácím i podnikovém prostředí.

Zapněte funkci UPnP a nemusíte konfigurovat mapování portů pro každý port a zařízení bude připojeno k síti Wide Area Network prostřednictvím routeru.

Postup

1. Kliknutím na **Komunikační parametry** → **NAT** otevřete příslušnou stránku.

Bezpečnostní ovládací panel AX

Enable UPnP

Mapping Type -

Port Type

HTTP Port

Service Port

Status

Port Type	External Port	External IP Address	Internal Port	UPnP Status
HTTP Port	80	0.0.0.0	80	Inoperative
Service Port	8000	0.0.0.0	8000	Inoperative

Obrázek 4-11 Nastavení NAT

2. Posunutím posuvného kontaktu zapnete UPnP.
3. Volitelné: Zvolte typ mapování jako **Manuální**
4. Nastavte HTTP port a port služeb.
5. Kliknutím na **Uložit** dokončíte nastavení.

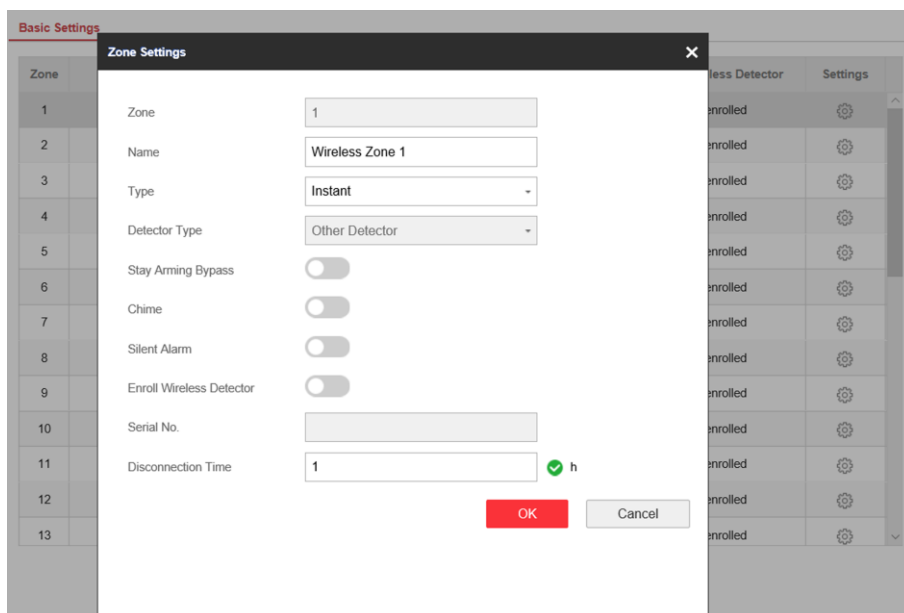
4.3.2 Správa zařízení

Zóna


Můžete nastavit parametry zóny na stránce zóny.

Postup

1. Kliknutím na položku **Správu zařízení** → **Zóna** otevřete stránku Zóna.



Obrázek 4-12 Stránka zóny

2. Zvolte zónu a kliknutím na  otevřete stránku Nastavení zóny.
3. Upravte název zóny.
4. Zvolte typ zóny.

Okamžitá zóna

Tento typ zóny spustí alarm okamžitě při aktivaci.

Opožděná zóna

Zpoždění pro odchod: Zpoždění pro odchod vám poskytne čas na to, abyste chráněnou oblast opustili bez spuštění alarmu.

Zpoždění pro příchod: Zpoždění pro příchod vám poskytne čas na to, abyste mohli vstoupit do chráněné oblasti a vypnout alarm.

System poskytně zpoždění pro odchod/příchod poté, co je aktivován nebo po novém vstupu. Obvykle se používá na vstupních/výstupních trasách (např. přední dveře/hlavní vstup), což je klíčová cesta k aktivaci/deaktivaci pomocí ovládací klávesnice pro uživatele.



Poznámka

Můžete nastavit dva různé časy trvání na stránce **Řízení oddílů** → **Plán a časovač**.

Časovač nesmí být nastaven na déle než 45 sekund, aby nedošlo k porušení normy EN 50131-1.

Následná zóna

Zóna se chová jako zpožděná zóna, když zaznamená spuštění události během Zpoždění pro příchod systému, zatímco jinak působí jako okamžitá zóna.

Obvodová zóna

Když systém po aktivaci systému zjistí spouštěcí událost, okamžitě spustí alarm. Mezi aktivací

alarmu a výstupem sirény „Čas zpoždění sirény (Obvodový alarm)“ je konfigurovatelný interval 0 až 600 sekund. Tato volba vám umožní zkontrolovat alarm a během tohoto intervalu zrušit výstup sirény v případě falešného alarmu.

Když je zóna aktivována, můžete nastavit dva různé časy zpoždění obvodového alarmu na stránce **Řízení oddílů** → **Plán a časovač**. Ve zpožděném čase můžete rovněž sirénu ztlumit.

Zóna tiché paniky

Tento typ zóny je aktivní 24 hodin, používá se pro paniku nebo HUD (Hold Up Devices), nepoužívá se pro kouřové senzory nebo detektory rozbitého skla.

Zóna paniky

Zóna se aktivuje vždy. Používá se obvykle v místech vybavených tlačítkem pro případ paniky, detektorem kouře a detektorem proti rozbití skla.

Požární zóna

Zóna se aktivuje vždy s výstupem zvuku/sirény, když se spustí alarm. Používá se obvykle v místech s nebezpečím požáru vybavených detektorem kouře a teplotními senzory.

Plynová zóna

Zóna se aktivuje vždy s výstupem zvuku/sirény, když se spustí alarm. Používá se obvykle v místech vybavených detektorem plynu (např. v kuchyni).

Zóna ochrany před ohrožením zdraví

Zóna se aktivuje vždy s potvrzujícím pípnutím, když se spustí alarm. Používá se obvykle v místech vybavených tlačítky pro situace ohrožení zdraví.

Zóna časového limitu

Zóna se aktivuje vždy. Typ zóny se používá ke sledování a hlášení stavu „AKTIVNÍ“ zóny, ale tento stav bude hlásit a alarm spustí až po uplynutí naprogramovaného času. (1 až 599) sekund. Může se používat na místech vybavených magnetickými kontakty, které vyžadují přístup, ale pouze na krátkou dobu (např. dveře požární hydrantové skříně nebo jiné vnější bezpečnostní dveře)

Klíčová zóna

Propojený oddíl se aktivuje po spuštění a deaktivuje po obnovení. V případě alarmu proti manipulaci se operace aktivace a deaktivace nespustí.

Vypnutá zóna

Při spuštění zóny nebo manipulaci s ní se alarmy neaktivují. Obvykle se používá k vypnutí vadných detektorů.

5. Zapněte **Přemostění aktivace v době přítomnosti**, **Vyzvánění** nebo **Tichý alarm** v souladu s vašimi aktuálními potřebami.

Poznámka

Některé zóny funkci nepodporují. Ohledně nastavení funkce viz aktuální zóna.

6. Aktivujte **Zapojený bezdrátový detektor**, zadejte sériové číslo a nastavte č. připojené kamery.

Poznámka

868 Zařízení nepodporují zadávání sériového čísla

- Nastavte **Dobu odpojení** a systém určí chybu připojení, pokud je doba odpojení zařízení delší než nakonfigurovaná hodnota.
- Klikněte na **OK**.

Poznámka

Po nastavení zóny můžete zadat **Status** → **Zóna** pro zobrazení stavu zóny.

Poznámka

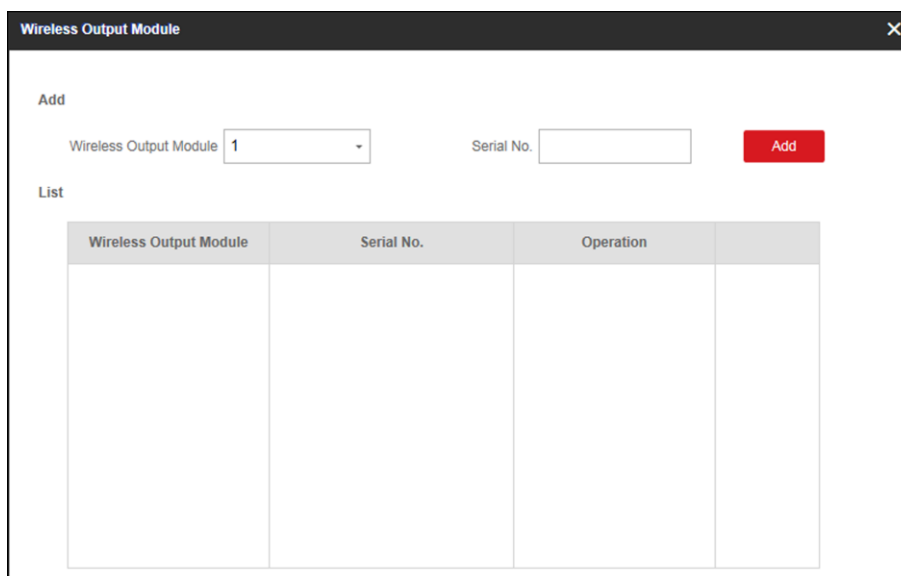
V možnostech systému webové platformy Engineer Axiom existuje možnost nazvaná Časný poplach, která musí být vypnuta pro Švédsko.

Výstup

Pokud chcete spojit zařízení s výstupem relé k výstupu alarmu, nastavte výstupní parametry.

Postup

- Kliknutím na **Správa zařízení** → **Relé** otevřete stránku Výstup.
- Přidejte bezdrátový výstupní modul.
 - Klikněte na **Bezdrátový výstupní modul**.




Wireless Output Module	Serial No.	Operation
------------------------	------------	-----------

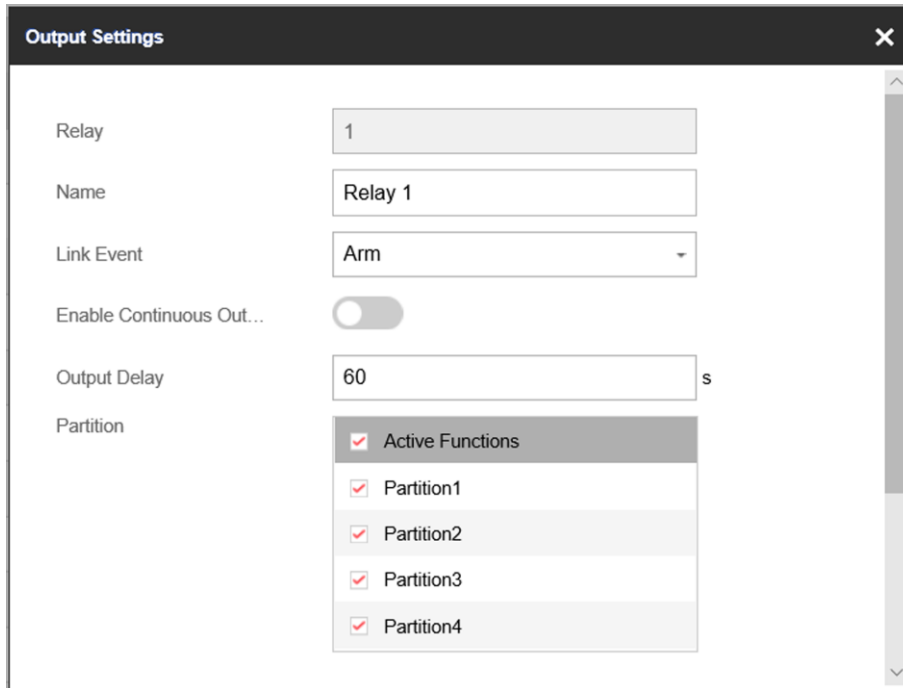
Obrázek 4-13 Nastavení bezdrátového výstupního modulu

- 2) Z rozevírací nabídky zvolte číslo bezdrátového výstupního modulu.
- 3) Zadejte sériové číslo bezdrátového výstupního modulu.

Poznámka

Zařízení v 868 MHz nemusí podporovat přidání se sériovým číslem.

- 4) Klikněte na **Přidat**.
3. Klikněte na  a vyskočí okno Nastavení výstupu.



Obrázek 4-14 Nastavení výstupu

4. Upravte název relé a zvolte událost spojení.

Poznámka

Měli byste nastavit různé parametry podle různých propojených událostí.

5. Zapněte **Zapnout průběžný výstup** nebo nastavte čas zpoždění výstupu.

Poznámka

Pokud se relé připojilo k modulu bezdrátového výstupu, informace o modulu bezdrátového výstupu se zobrazí v oblasti zapsaného bezdrátového výstupního modulu.

6. Zaškrtněte **Typ dílčí události** (Pouze pro událost **Alarmu**).
7. Zkontrolujte oddíl připojený k relé. (**Zóna** a **Manuální** událost tento obvod nemají.)
8. Klikněte na **OK**.

Poznámka

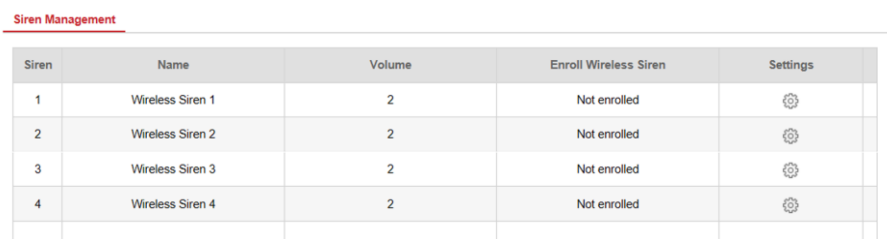
Po nakonfigurování relé můžete kliknutím **Status** → **Relé** zobrazit stav výstupu.





Siréna

Siréna je zapsána do ovládacího panelu prostřednictvím modulu bezdrátového přijímače a bezdrátová siréna 868 MHz může být zapsána do hybridního ovládacího panelu prostřednictvím bezdrátového přijímače, který je na adrese 9.

Postup

1. Kliknutím na **Správa zařízení** → **Siréna** otevřete stránku Siréna.



Siren	Name	Volume	Enroll Wireless Siren	Settings
1	Wireless Siren 1	2	Not enrolled	
2	Wireless Siren 2	2	Not enrolled	
3	Wireless Siren 3	2	Not enrolled	
4	Wireless Siren 4	2	Not enrolled	

Obrázek 4-15 Stránka Siréna

2. Kliknutím na  otevřete stránku Nastavení sirény.

Siren Settings [X]

Siren: 1

Name: Wireless Siren 1

Volume: 2

Partition:

- Active Functions
- Partition1
- Partition2
- Partition3
- Partition4

Enroll Wireless Siren:

Serial No.: [Empty]

Disconnection Time: 1 h

[OK] [Cancel]

Obrázek 4-16 Nastavení sirény

3. Nastavte název a hlasitost sirény.

 **Poznámka**

Dostupný rozsah hlasitosti sirény je od 0 do 3 (funkce se liší podle modelu zařízení).

4. Zkontrolujte propojené oddíl.

5. Volitelné: Aktivujte **Zapsat bezdrátovou sirénu** a zadejte sériové číslo sirény.

 **Poznámka**

Siréna v 868 MHz nemusí tuto funkci podporovat.

6. Nastavte **Dobu odpojení** a systém určí chybu připojení, pokud je doba odpojení zařízení delší než nakonfigurovaná hodnota.

7. Klikněte na **OK**.


 **Poznámka**

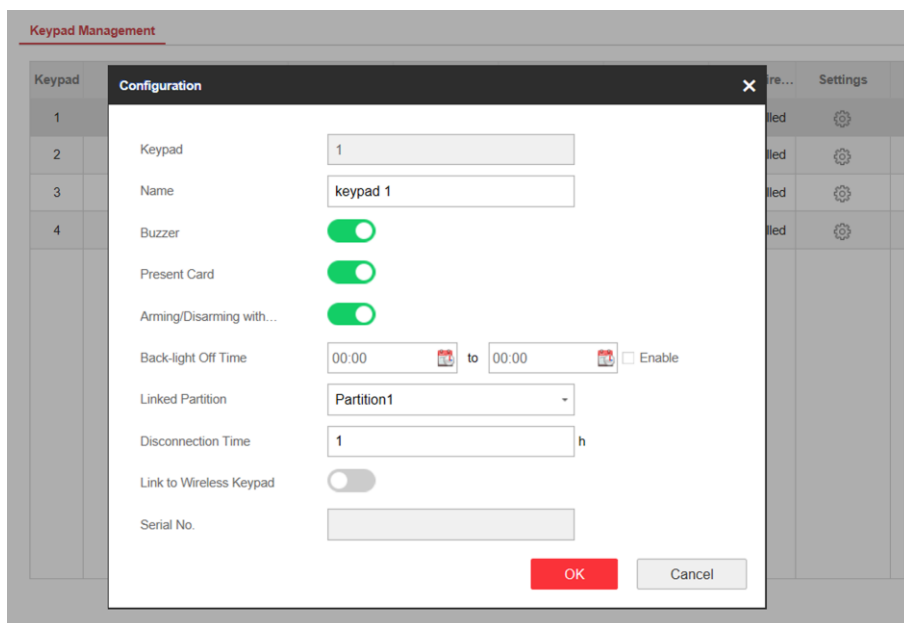
Po nakonfigurování sirény můžete kliknutím **Status** → **Siréna** pro zobrazení stavu sirény.

Klávesnice

Můžete nastavit parametry klávesnice, která je zapsána do ovládacího panelu.

Postup

1. Příslušnou stránku otevřete kliknutím na položku **Správa zařízení** → **Klávesnice**.
2. Kliknutím na  pro otevřete stránku Nastavení klávesnice.



Obrázek 4-17 Stránka nastavení klávesnice

3. Nastavte název klávesnice.
4. Zaškrtnutím zaškrťovacího políčka zapnete funkci bzučáku, vložení karty a aktivaci/deaktivaci pomocí klávesnice.
5. Zaškrtněte zaškrťovací políčko **Zapnout** času vypnutí zadního světla a nastavte dobu trvání vypnutí světla.
6. Zvolte oddíl propojený s klávesnicí.
7. Volitelné: Zapněte **Odkaz na bezdrátovou klávesnici** a nastavte sériové číslo.

Poznámka

Klávesnice v 868 MHz nemusí tuto funkci podporovat.

8. Nastavte **Dobu odpojení** a systém určí chybu připojení, pokud je doba odpojení zařízení delší než nakonfigurovaná hodnota.
9. Klikněte na **OK**.

Poznámka

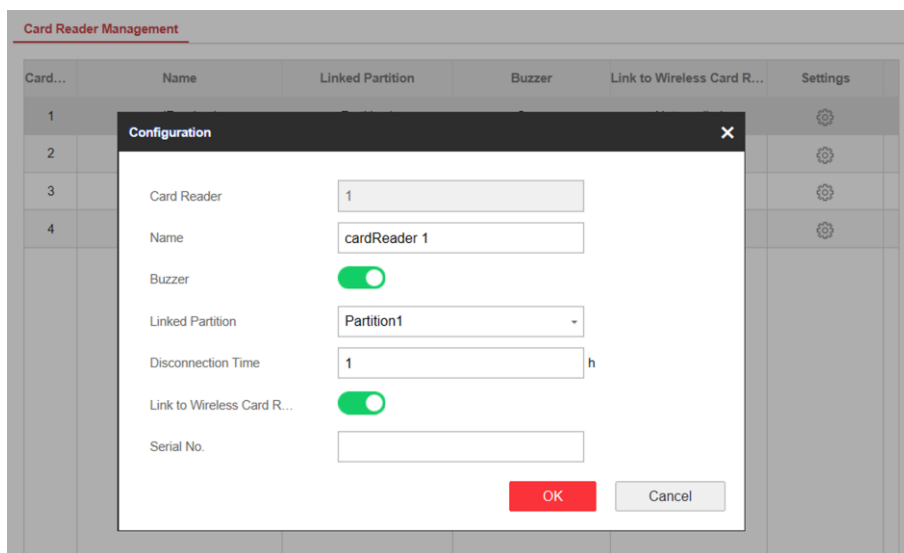
- Po nakonfigurování klávesnice můžete kliknout na **Status** → **Klávesnice** pro zobrazení stavu klávesnice.
- Můžete nastavit heslo klávesnice **Správa uživatelů** → **Uživatel** → **Provoz**.

Čtečka karty


Můžete nastavit parametry čtečky karty, která je zapsána do ovládacího panelu.

Postup

1. Stránku otevřete kliknutím na položku **Správa zařízení** → **Čtečka karty**



Obrázek 4-18 Nastavení čtečky karty

2. Kliknutím na  otevřete stránku Nastavení čtečky.
3. Nastavte název čtečky karty.
4. Aktivujte **Bzučák**.
5. Zvolte oddíl propojený s klávesnicí.
6. Nastavte **Dobu odpojení** a systém určí chybu připojení, pokud je doba odpojení zařízení delší než nakonfigurovaná hodnota.
7. Volitelné: Aktivujte **Odkaz na bezdrátovou čtečku karty** a nastavte sériové číslo.

Poznámka

Čtečka karty v 868 MHz nemusí tuto funkci podporovat.

8. Klikněte na **OK**.

Poznámka

- Všechny zóny se ve výchozím nastavení přidávají do oddílu 1
 - Po nakonfigurování klávesnice můžete kliknout na **Status** → **Klávesnice** pro zobrazení stavu klávesnice.
-

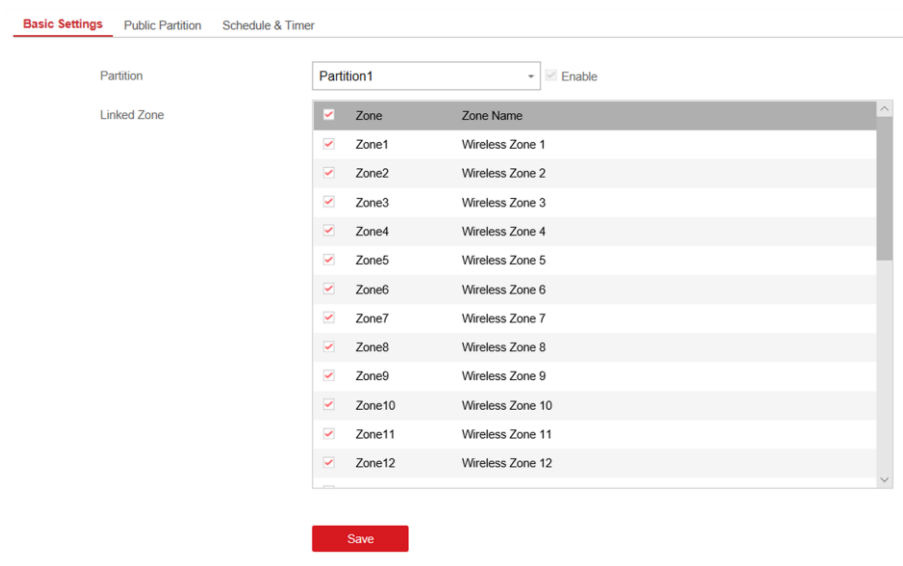
4.3.3 Nastavení oddílů

Základní nastavení

Můžete spojit zóny s vybraným oddílem.

Postup

1. Kliknutím na položku **Správa oddílů** → **Základní nastavení** otevřete příslušnou stránku.



Obrázek 4-19 Stránka správy základních informací o oddílu

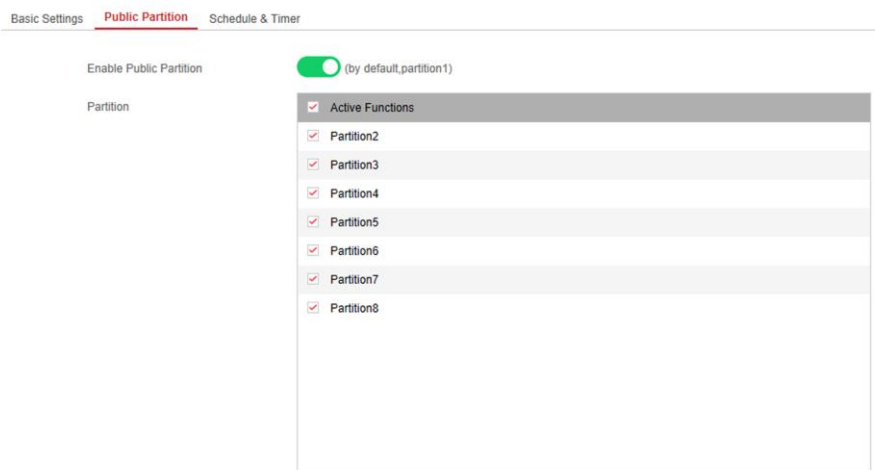
2. Vyberte oddíl.
3. Zaškrtněte **Zapnout**.
4. Zaškrtnutím políčka před zónou vyberte zóny pro oddíl.
5. Kliknutím na **Uložit** dokončíte nastavení.

Nastavení veřejných oddílů

Veřejný oddíl se považuje za zvláštní oddíl, který může být sdílen s ostatními oddíly. Obvykle se používá ke správě nebo kontrole veřejného prostoru souvisejícího s jinými oblastmi, které jsou kontrolovány jinými oddíly v jedné budově.

Postup

1. Kliknutím na položku **Správa oddílů** → **Veřejný oddíl** otevřete příslušnou stránku.



Obrázek 4-20 Nastavení veřejných oddílů

2. Zaškrtnutím políčka zapnete funkci veřejného oddílu.

Poznámka

výchozí veřejný oddíl je oddíl 1

3. V seznamu zvolte oddíl, který má být spojen s veřejným oddílem.

Poznámka

Je třeba zvolit minimálně jeden oddíl, který má být spojen s veřejným oddílem.

4. Kliknutím na **Uložit** nastavte oddíl jako veřejný.

Nastavení plánu a časovače

Můžete nastavit dobu trvání **Zpoždění pro příchod 1** a **Zpoždění pro příchod: 2** pro typ zpožděné zóny a zpožděný čas Zpoždění pro odchod pro opuštění zóny. Můžete rovněž nastavit časový plán alarmu. Zóna bude aktivována/deaktivována podle nakonfigurovaného časového plánu.

Postup

1. Kliknutím na položku **Správa oddílů** → **Časový plán a časovač** otevřete stránku Časový plán a časovač.

Bezpečnostní ovládací panel AX

Basic Settings Public Partition **Schedule & Timer**

Partition	<input type="text" value="Partition1"/>
Entry Delay 1	<input type="text" value="30"/> s
Entry Delay 2	<input type="text" value="60"/> s
Exit Delay	<input type="text" value="30"/> s
Enable auto Arming	<input type="checkbox"/>
Time	<input type="text" value="00:00"/>
Enable auto Disarm...	<input type="checkbox"/>
Time	<input type="text" value="00:00"/>
Late to Disarm	<input type="checkbox"/>
Time	<input type="text" value="00:00"/>
Weekend Exception	<input type="checkbox"/>
Excepted Holiday	<input type="checkbox"/>
Siren Delay Time (Peri...	<input type="text" value="60"/> s
Alarm Duration	<input type="text" value="90"/> s

Obrázek 4-21 Nastavení časového plánu a časovače

2. Vyberte oddíl.
3. Nastavit dobu trvání **Zpoždění pro příchod 1**, **Zpoždění pro příchod 2** nebo **Zpoždění pro odchod**.

Zpoždění pro příchod 1/Zpoždění pro příchod 2

Pokud jste nastavili zónu zpožděného příchodu, můžete zde nastavit dobu trvání zpožděného času.

Poznámka

Dostupný časový rozsah se pohybuje od 1 s do 600 s.

Zpoždění pro odchod

Pokud chcete zónu opustit bez spuštění alarmu, můžete nastavit dobu trvání opoždění odchodu.

Poznámka

Dostupný časový rozsah se pohybuje od 1 s do 600 s.

4. Volitelné: Nastavte následující parametry podle skutečných potřeb.

Zapnutí automatické aktivace

Aktivace funkce a nastavení doby zahájení aktivace. Zóna bude aktivována podle nakonfigurované doby.

Poznámka

- Čas automatické aktivace a čas automatické deaktivace nemůže být stejný.
 - Bzučák bzučí pomalu 2 minuty před spuštěním automatické aktivace a rychle 1 minutu před spuštěním automatické deaktivace.
 - Můžete se rozhodnout zapnout nucenou aktivaci na stránce Možnosti systému. Když je funkce aktivována, bude se systém aktivovat bez ohledu na poruchu.
 - Pokud je aktivován veřejný oddíl, tak dávka oddílu 1 nepodporuje automatickou aktivaci.
-

Zapnutí automatické deaktivace

Zapněte funkci a nastavte dobu zahájení deaktivace. Zóna bude deaktivována podle nakonfigurované doby.

Poznámka

- Čas automatické aktivace a čas automatické deaktivace nemůže být stejný.
 - Pokud je aktivován veřejný oddíl, tak dávka oddílu 1 nepodporuje automatickou deaktivaci.
-

Opožděná deaktivace

Zapněte funkci a nastavte čas. Pokud se po nakonfigurované době spustí alarm, bude se mít za to, že osoba má zpoždění.

Poznámka

Nejdříve byste měli zapnout funkci Oznámení řízení panelu ve volbě **Komunikační parametry** → **Komunikace události**: a teprve potom zapněte funkci Opožděná deaktivace.

Víkendová výjimka

Po zapnutí funkce nebude zóna na víkend aktivována.

Výjimka na volné dny

Po zapnutí funkce bude zóna aktivována/deaktivována na volné dny. Po aktivaci byste měli nastavit plán volných dní.

Poznámka

Lze přidat až 6 skupin volných dní.

Čas zpoždění sirény (obvodový alarm)

Pokud jste nastavili obvodovou zónu, můžete nastavit zpožděný čas pro zónu.

Poznámka

Dostupný časový rozsah se pohybuje od 0 s do 600 s.

Doba trvání alarmu

Pokud jste nastavili obvodovou zónu, můžete nastavit dobu trvání alarmu.

Poznámka

Dostupný časový rozsah se pohybuje od 1 s do 900 s.

5. Klikněte na **Uložit**.

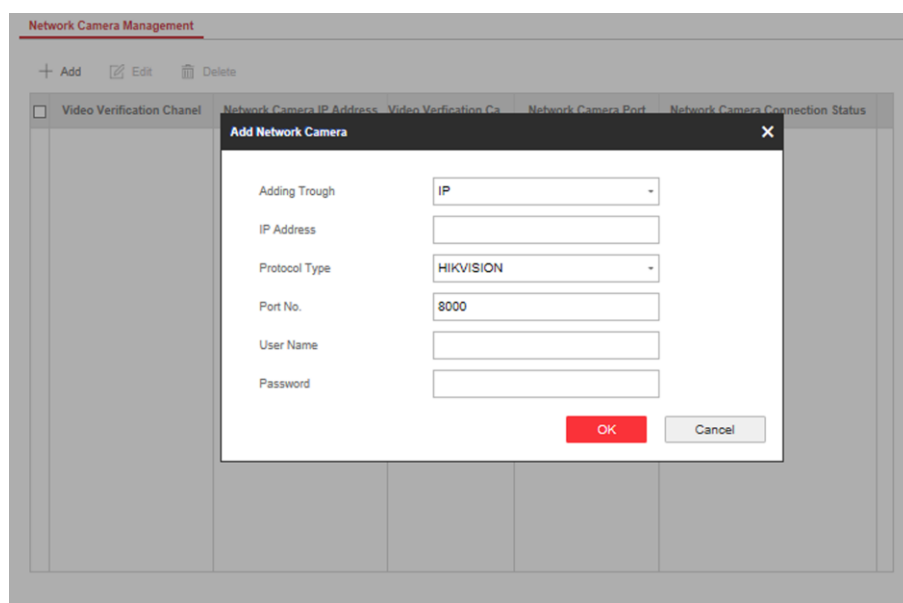
4.3.4 Správa videí

K bezpečnostnímu ovládacímu panelu můžete přidat dvě síťové kamery a spojit kameru s vybranou zónou pro video monitoring. Můžete rovněž přijmout a zobrazit video události prostřednictvím klienta a e-mailu.

Přidání kamer k bezpečnostnímu ovládacímu panelu

Postup

1. Kliknutím na **Systém** → **Síťová kamera** otevřete stránku správy síťových kamer.




Obrázek 4-22 Správa síťových kamer

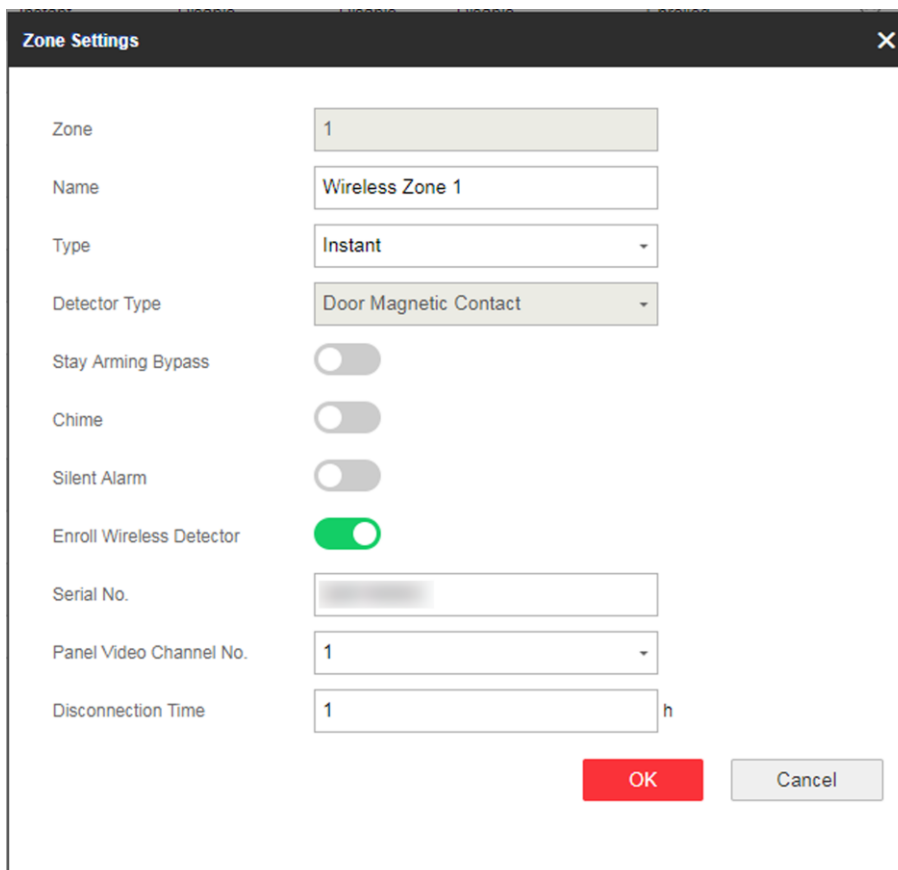
2. Klikněte na **Přidat** a zadejte základní informace o kameře, jako je IP adresa a číslo portu, a vyberte typ protokolu.

3. Zadejte jméno uživatele a heslo kamery.
4. Klikněte na **OK**.
5. Volitelné: Kliknutím na **Upravit** nebo **Smazat** upravíte nebo smažete vybranou kameru.

Spojení kamery se zónou

Postup

1. Kliknutím na **Bezdrátové zařízení** → **Zóna** otevřete konfigurační stránku.
2. Vyberte zónu, do níž chcete zahrnout video monitoring, a klikněte na .



Zone	1
Name	Wireless Zone 1
Type	Instant
Detector Type	Door Magnetic Contact
Stay Arming Bypass	<input type="checkbox"/>
Chime	<input type="checkbox"/>
Silent Alarm	<input type="checkbox"/>
Enroll Wireless Detector	<input checked="" type="checkbox"/>
Serial No.	
Panel Video Channel No.	1
Disconnection Time	1 h

Obrázek 4-23 Nastavení zóny

3. Vyberte číslo kanálu video panelu.
4. Klikněte na **OK**.

Nastavte e-mail pro přijetí videa alarmu

Můžete nastavit video alarmu nebo událost na konfigurovaný e-mail.

Postup

1. Kliknutím na **Komunikační parametry** → **Události video ověření** otevřete stránku Wi-Fi.

Video Verification Email Setting

Video Verification Events	<input checked="" type="checkbox"/>
Sender Name	<input type="text"/>
Sender	<input type="text"/>
SMTP Server address	<input type="text"/>
SMTP Port No.	<input type="text" value="25"/>
Encryption Type	<input type="text" value="None"/>
Server Authentication	<input type="checkbox"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Receiver Name	<input type="text"/>
Receiver	<input type="text"/>

Obrázek 4-24 Nastavení e-mailu na přijetí videa alarmu

2. Kliknutím zablokujete zapnutí funkce.
3. Zadejte informace odesílatele.

Poznámka

Pro odesílání e-mailů doporučujeme používat Gmail a Hotmail.

4. Zadejte informace o příjemci.
5. Klikněte na **Test adresy příjemce** a ujistěte se, že je adresa správná.
6. Klikněte na **Uložit**.

Nastavte FTP pro Uložení videa

Můžete nakonfigurovat FTP server na uložení videa alarmu.

Postup

1. Kliknutím na **Komunikační parametry** → **FTP** otevřete příslušnou stránku.

FTP Settings

FTP Type	Preferred FTP	-
Enable FTP	<input checked="" type="checkbox"/>	
Address Type	IP	-
FTP Server	<input type="text"/>	
Port No.	21	
Protocol Type	FTP	-
Enable Anonymity	<input checked="" type="checkbox"/>	
User Name	<input type="text"/>	
Password	<input type="text"/>	
Directory Structure	Save in Root Directory	-
Parent Directory	Custom	<input type="text"/>
Secondary Directory	Custom	<input type="text"/>

Obrázek 4-25 Nastavení FTP

2. Zvolte **typ FTP**.
3. Posunutím posuvného kontaktu aktivujete FTP.
4. Zvolte typ adresy jako **Jméno domény** nebo **IP**.
5. Zadejte jméno domény nebo FTP server.
6. Zadejte číslo portu, uživatelské jméno a heslo.
7. Volitelné: Posunutím posuvného kontaktu zapnete anonymitu.
8. Nastavte **Strukturu adresáře** jako uložení cesty snímků na serveru FTP.
9. Klikněte na **Uložit**.

Nastavte parametry videa

Postup

1. Kliknutím na položku **Video & Audio** → **Parametry video události** otevřete příslušnou stránku.

Event Video Settings

Panel Video Channel No.	<input type="text"/>
Stream Type	<input type="text"/>
Bitrate Type	<input type="text"/>
Resolution	<input type="text"/>
Video Bitrate	<input type="text"/> Kbps
Length of Cached Vide...	<input type="text"/> s
Length of Cached Vide...	<input type="text"/> s

Obrázek 4-26 Nastavení videozáznamů

2. Zvolte kameru a nastavte parametry videa.

Typ streamu

Hlavní stream: Používá se při záznamu a náhledu ve vysokém rozlišení, má vysoké rozlišení, rychlost kódu a kvalitu obrazu.

Dílčí stream: Používá se k přenosu sítě a náhledu obrázků jako streamování videa s vlastnostmi nižšího rozlišení, přenosové rychlosti a kvality obrazu.

Typ přenosové rychlosti

Zvolte typ přenosové rychlosti jako konstantu nebo proměnnou.

Rozlišení

Zvolte rozlišení video výstupu.

Přenosová rychlost videa

Vyšší kvalita odpovídá vyšší kvalitě obrazu, ale je vyžadována lepší pásmová šířka.

4.3.5 Správa povolení

Přidat/Upravit/Smazat uživatele

Správce může přidat uživatele na ovládací panel zabezpečení, upravit informace o uživateli nebo uživatele z ovládacího panelu zabezpečení odstranit. Můžete rovněž přidělit různá povolení novému uživateli.

Postup

1. Kliknutím na **Správa uživatelů** → **Uživatel** otevřete stránku Správa uživatelů.
2. Pro zajištění souladu s požadavkem EN posuňte blok pro aktivaci technika a výrobce.

Poznámka

- Přednastavené heslo **technika** je **installer12345** a přednastavené heslo **výrobce** je **hik12345**. Tyto kódy je třeba po prvním připojení změnit.
- Italské uživatelské jméno správce je **asmministratore**.

Tabulka 4-2 Uživatelské jméno technika

Jazyk	Uživatelské jméno	Jazyk	Uživatelské jméno
Angličtina	installer	Ruština	МОНТАЖНИК
Itaština	installatore	Francouzština	installatore
Polština	installatore	Španělština	instalador
Němčina	errichter	Portugalština	instalador
Turečtina	kurulumc	Čeština	technik

3. Klikněte na **Přidat**.

4. V automaticky otvíraném okně nastavte informace o novém uživateli, včetně typu uživatele, jména uživatele a hesla.

Obrázek 4-27 Přidání stránky uživatele

5. Nastavte heslo klávesnice (číselné, 8~16 znaků).

Poznámka

Heslo klávesnice +1 nebo -1 je tísňový kód. Použitím tísňového kódu můžete na klávesnici normálně provádět aktivaci a deaktivaci a odeslat tísňový alarm. Pokud je například heslo klávesnice 123456, je tísňový kód 123455 nebo 123457

6. Zkontrolujte oddíly
 7. Zaškrtnutím políčka nastavte oprávnění uživatele.
Uživatel může používat pouze přiřazená povolení.
 8. Klikněte na **OK**.
 9. Volitelné: Aktivací uživatele ve sloupci Aktivovat uživatele umožníte, aby aktivovaný uživatel pracoval se zařízením.
 10. Volitelné: Zvolte uživatele a klikněte na **Upravit** a potom můžete upravovat informace a povolení uživatele.
 11. Volitelné: Smažte jednoho uživatele nebo zaškrtněte více uživatelů a klikněte na **Smazat** pro smazání uživatelů v dávce.
-

Poznámka

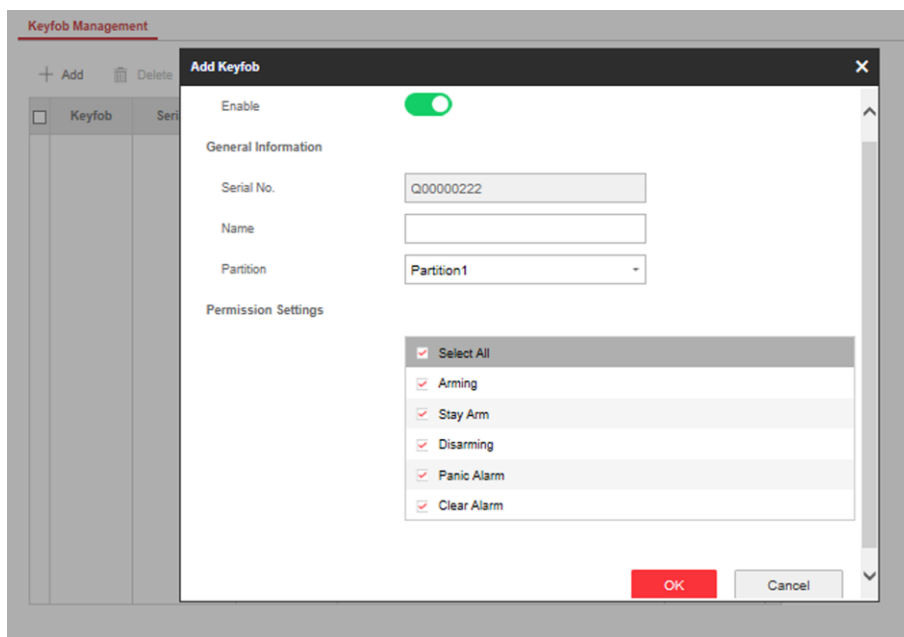
Správce, technika a výrobce nelze smazat.

Přidat/Upravit/Smazat klíčenku

Na bezpečnostní ovládací panel můžete přidat klíčenku a prostřednictvím klíčenky můžete ovládat bezpečnostní ovládací panel. Můžete rovněž upravit informace o klíčence nebo ji z ovládacího panelu zabezpečení odstranit.

Postup

1. Kliknutím na **Správa uživatelů** → **Klíčenka** otevřete stránku správy klíčenek.



Obrázek 4-28 Správa klíčenek

2. Klikněte na **Přidat** a stiskněte jakoukoliv klávesu na klíčence.
3. Nastavte parametry klíčenky.

Jméno

Upravte název klíčenky.

Nastavení povolení


Zaškrtněte různé položky pro přidělení povolení.

Nastavení jedné klávesy

Vyberte z rozevíracího seznamu pro nastavení funkcí klávesy I a klávesy II

Nastavení kombinačních kláves

Vyberte z rozevíracího seznamu pro nastavení funkcí kombinačních kláves.

4. Klikněte na **OK**.
5. Volitelné: Po kliknutí na  můžete upravit informace o klíčence.
6. Volitelné: Smažte jednu klíčenku nebo zaškrtněte více klíčenek a klikněte na **Smazat**, chcete-li smazat klíčenky hromadně.

Přidat/Upravit/Smazat kartu

Na bezpečnostní ovládací panel můžete přidat visačku a pomocí karty můžete aktivovat/deaktivovat zónu. Můžete rovněž upravit informace o visačce nebo visačku z bezpečnostního ovládacího panelu odstranit.

Postup

1. Kliknutím na **Správa uživatelů** → **Karta** otevřete stránku správy.
2. Klikněte na **Přidat** a vložte kartu do prostoru pro kartu ovládacího panelu.

- Upravte název karty v automaticky otevřeném okně.
- Vyberte typ karty a oddíl propojený s kartou.
- Vyberte povolení pro kartu.


Poznámka

Měli byste rozdělit alespoň povolení pro kartu.

- Klikněte na **OK** a v seznamu se zobrazí informace o visačce.

Poznámka

Karta podporuje nejméně 20 tisíc sériových čísel.

- Volitelné: Klikněte na  a můžete změnit název karty.
- Volitelné: Smažte jednu kartu nebo zaškrtněte více karet a klikněte na **Smazat** pro smazání karet v dávce.

4.3.6 Údržba

Test

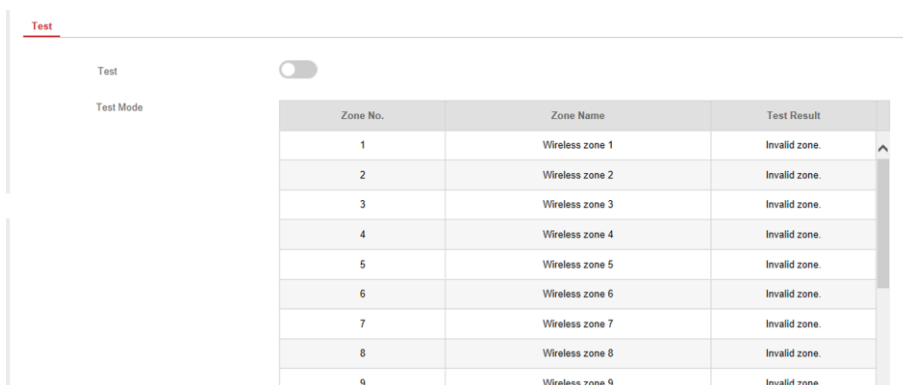
Bezpečnostní ovládací panel podporuje funkci testu chůze.

Postup

- Zadáním volby **Údržba** → **Test** → zapnete funkci.

Poznámka

Do režimu TEST můžete vstoupit pouze v případě, že všechny detektory fungují bezvadně.



Zone No.	Zone Name	Test Result
1	Wireless zone 1	Invalid zone.
2	Wireless zone 2	Invalid zone.
3	Wireless zone 3	Invalid zone.
4	Wireless zone 4	Invalid zone.
5	Wireless zone 5	Invalid zone.
6	Wireless zone 6	Invalid zone.
7	Wireless zone 7	Invalid zone.
8	Wireless zone 8	Invalid zone.
9	Wireless zone 9	Invalid zone.

- Zaškrtnutím zaškrťovacího okénka **Test** spustíte test chůze.
- Kliknutím na **Uložit** dokončíte nastavení.

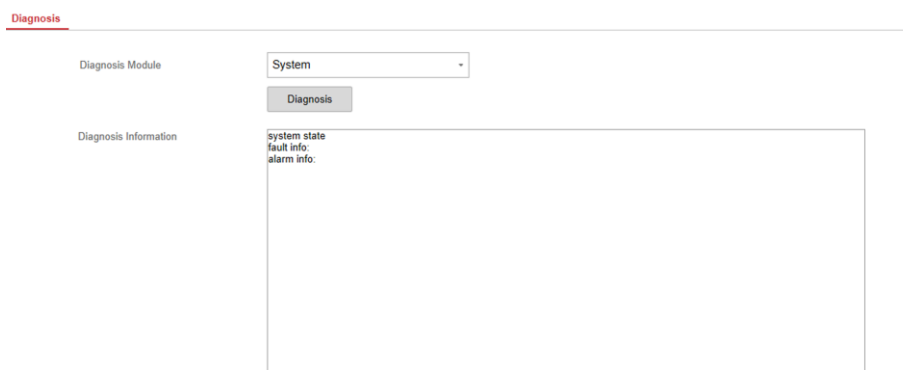
4. Spusťte detektor v každé zóně.
5. Zkontrolujte výsledek testu.

Diagnóza

Ovládací panel podporuje diagnózu systému, alarmu, bezdrátového zařízení, Wi-Fi a platformy cloudu

Postup

1. Zadejte **Údržba** → **Diagnóza**.



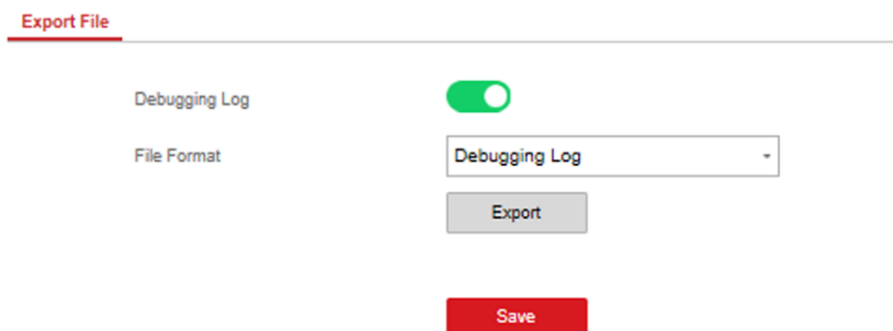
2. Zvolte systém, alarm, bezdrátové zařízení, Wi-Fi, cloudovou platformu, mobilní datovou síť, síťovou kameru a centrum přijímání alarmu jako modul diagnózy. Nebo můžete vybrat **Vlastní** a zadat vlastní příkaz (1~64) znaků.
3. Kliknutím na **Diagnóza** zahájíte operaci.
4. Výsledek diagnózy si prohlédněte v informačním okénku.

Export souboru

Soubor pro odstraňování chyb můžete exportovat do PC.

Postup

1. Pro vstup na stránku klikněte na **Údržba** → **Exportovat soubor**.



Obrázek 4-29 Stránka pro export souboru

2. Pro zapnutí funkce zaškrtněte zaškrťovací políčko.
3. Kliknutím na tlačítko **Export** uložíte soubor pro odstraňování chyb na PC.

4.3.7 Systémová nastavení

Správa oprávnění

Nastavte možnosti oprávnění.

Klikněte na **Systém** → **Možnosti systému** pro vstup na stránku správy systému.

Kontrola souboru bezdrátových zařízení

Při zapnutí této volby systém zjišťuje fungování všech radiových periferních zařízení. Pokud není fungování žádných periferních zařízení zaznamenáno, systém událost nahraje.

Poznámka

Pro EN nepřepínejte na OFF.

Aktivace ovládacího panelu se závadou

Pokud je volba zapnuta a v zóně jsou aktivní závady, bude zóna při aktivování automaticky vynechána.

Poznámka

Měli byste vypnout funkci aktivace na stránce Pokročilé nastavení. Jinak aktivace ovládacího panelu s funkcí závady nemůže být platná.

Oznámení stavu ovládacího panelu

Pokud je funkce zapnuta, zařízení zprávu automaticky nahlásí při změně stavu ovládacího panelu.

Vypnutí funkční klávesy

Při zapnutí této funkce budou vypnuty všechny klávesy.

Hlasový pokyn

Pokud je tato volba aktivována, ovládací panel zapne vydávání hlasových pokynů.

Hlasový pokyn deaktivace a vymazání alarmu

Pokud je tato volba zapnuta, ovládací panel vyše před deaktivací a vymazáním alarmu všechny systémové chyby. Před zapnutím této funkce musíte aktivovat **Hlasový pokyn**.

Hlasitost systému

Dostupný rozsah hlasitosti systému je od 0 do 10.

Pokročilé nastavení oprávnění

Nastavte pokročilé parametry oprávnění.

Klikněte na **Systém** → **Možnosti systému** → **Pokročilé nastavení** pro vstup na stránku pokročilého nastavení.

Můžete nastavit následující parametry:

Zapnutí aktivace

Když tuto funkci zapnete, systém během postupu aktivace zařízení zkontroluje nakonfigurovaný kontrolní seznam poruch. Dojde-li během procesu aktivace k poruše, postup se zastaví.

Poznámka

Klávesnice PKG a klíčenka tuto funkci nepodporují. Je-li tato funkce vypnutá, aktivace se nezdaří a dojde k chybě. Je třeba chybu odstranit nebo zavřít zapnutí aktivace.

Seznam chyb

Systém zkontroluje, jestli zařízení během postupu aktivace má v seznamu nějaké chyby.

Zapnutí aktivace s chybou

Zkontrolujte chyby v seznamu Zapnutí aktivace s chybou a zařízení pak, když dojde k chybě, postup aktivace nezastaví.

Indikátor aktivace nepřerušovaně svítí

Pokud zařízení používá normu EN, je tato funkce ve výchozím nastavení vypnutá. V tomto případě, pokud je zařízení aktivováno, bude indikátor svítit nepřerušovaným modrým světlem po dobu pěti sekund. A pokud je zařízení deaktivováno, tak indikátor pětkrát blikne.

Když je funkce zapnutá, pak, pokud je zařízení aktivováno, bude indikátor svítit nepřerušovaným světlem po celou dobu. A pokud je zařízení deaktivováno, tak bude indikátor vypnutý.

Poznámka

Tuto funkci podporuje pouze model P.

Hlášení závady při aktivaci

Pokud zařízení používá normu EN, je tato funkce ve výchozím nastavení vypnutá. V tomto případě zařízení nebude během postupu aktivace hlásit závady.

Poznámka

Tuto funkci podporuje pouze model P.

Zapnutí předčasného alarmu

Pokud zapnete funkci, když je zóna aktivována a zóna spuštěna, alarm se spustí po uplynutí zpoždění.

Poznámka

Předčasný alarm vstoupí v platnost teprve po spuštění zpožděné zóny.

Kontrola závady

Systém rozhodne, zda se mají kontrolovat závady uvedené na stránce. Systém zkontroluje pouze závadu, která byla vybrána.

Klikněte na **Systém** → **Možnosti systému** → **Seznam chyb ovládacího panelu** pro vstup na stránku.

Zjištění odpojení síťové kamery

Pokud je tato volba zapnutá, po odpojení propojené síťové kamery se spustí alarm.

Kontrola baterií

Pokud je tato možnost zapnutá, zařízení po odpojení nebo vybití baterie nahraje události.

Kontrola závady připojené sítě

Pokud je tato volba zapnutá, tak se po odpojení připojené sítě nebo při jiných závadách spustí alarm.

Kontrola závady Wi-Fi

Pokud je tato volba zapnutá, tak se po odpojení Wi-Fi nebo při jiných závadách spustí alarm.

Kontrola závady mobilní sítě

Pokud je tato volba zapnutá, tak se po odpojení mobilní datové sítě nebo při jiných závadách spustí alarm.

Kontrola závady SIM karty

Pokud je tato volba zapnutá, tak se při závadách SIM karty spustí alarm.

Čas kontroly výpadku napájení

Systém závadu zkontroluje po uplynutí nastaveného času po výpadku napájení.

Pro dodržení normy EN 50131-3 by doba trvání kontroly měla být 10 s.

Nastavení času

Můžete nastavit časové pásmo zařízení, synchronizovat čas zařízení a nastavit čas DST. Zařízení podporuje synchronizaci času prostřednictvím serveru **Hik-Connect**.

Řízení času

Klikněte na **Systém** → **Datum a čas** pro vstup na stránku Řízení času.

The screenshot displays the 'Time Management' section of the AX security control panel. It includes a dropdown menu for 'Time Zone' set to '(GMT+00:00) Dublin, Edinburgh, London'. Under 'Time Synchronization', the 'Manual Time Sync' radio button is selected. The 'Date and Time' field shows '2018-12-10 09:50:27'. The 'PC Sync' field shows '2018-12-10 09:48:48' with a small icon and a checkbox labeled 'Sync. With Computer Time'. A red 'Save' button is located at the bottom center.

Obrázek 4-30 Správa času

Z rozevíracího seznamu zvolte časovou zónu.

Čas zařízení můžete synchronizovat manuálně. Nebo zaškrtněte možnost **Synchronizovat s časem počítače** pro synchronizaci času zařízení s časem počítače.

Poznámka

Když synchronizujete čas ručně nebo s časem počítače, systém zaznamená protokol „Synchronizace SDK“.

Řízení DST

Klikněte na **System** → **Datum a čas** → **Řízení DST** pro vstup na stránku Řízení času. Můžete zapnout DST a nastavit odchylku DST, počáteční čas a konečný čas DST.

Nastavení bezpečnosti

Nastavení SSH

Podle aktuálních potřeb můžete SSH (Secure Shell) zapnout nebo vypnout.

Kliknutím na **System** → **Bezpečnost** → **Nastavení SSH** otevřete stránku Nastavení SSH a můžete funkci SSH zapnout nebo vypnout. **Zablokování nastavení uživatele**

Nastavte blokování uživatele. Můžete zobrazit uzamknutého uživatele nebo odemknout uživatele a nastavit dobu uzamknutí uživatele.

Postup

1. Kliknutím na **System** → **Bezpečnost** → **Nastavení blokování uživatele** otevřete stránku Nastavení blokování uživatele.
2. Můžete nastavit následující parametry:

Max. Nesprávné pokusy

Pokud uživatel nepřetržitě zadává nesprávné heslo po delší dobu, než je nakonfigurovaný čas, bude účet uzamknut.

Poznámka


Správce má dva další pokusy, než je nakonfigurovaná hodnota.

Doba uzamknutí

Nastavte dobu uzamknutí po uzamknutí účtu.

Poznámka


Dostupná doba blokování se pohybuje od 5 s do 1800 s.

3. Kliknutím na  účet odblokuje nebo kliknutím na **Odblokovat všechno** odblokuje všechny zablokované uživatele v seznamu.
4. Klikněte na **Uložit**.

Nastavení uzamknutí modulu

Nastavte parametry blokování modulu, včetně maximálního počtu nesprávných pokusů a doby trvání blokování. Modul bude zablokován po naprogramovanou dobu, jakmile autentizace modulu selže po určený počet nakonfigurovaných časů.

Postup

1. Kliknutím na **Systém** → **Bezpečnost** → **Nastavení blokování modulu** otevřete stránku Nastavení blokování modulu.
2. Zvolte modul ze seznamu a klikněte na ikonu .
3. Můžete nastavit následující parametry vybraného modulu.

Max. Nesprávné pokusy






Pokud se uživatel snaží o ověření hesla nepřetržitě po dobu delší, než jsou povolené nakonfigurované pokusy, klávesnice bude po naplánovanou dobu uzamknuta.

Doba uzamknutí

Nastavte dobu uzamknutí po uzamknutí klávesnice. Po uplynutí nakonfigurované doby se klávesnice odblokuje.

4. Klikněte na **OK**.
5. Volitelné: Kliknutím na ikonu **Zablokovat** odblokuje zablokovaný modul.

SSH Settings Locking User Settings Module Locking Settings

No.	Device Type	Max. Failure Attempts	Locked Duration	Status	Operation
1	Keypad	3	90	Unlocked	
2	Keypad	3	90		
3	Keypad	3	90	Unlocked	
4	Keypad	3	90	Unlocked	

Obrázek 4-31 Nastavení blokování modulu

Údržba systému

Můžete restartovat zařízení, obnovit výchozí nastavení, importovat/exportovat konfigurační soubor nebo vzdáleně upgradovat zařízení.

Vyberte zařízení a v klientském softwaru klikněte na **Vzdálená konfigurace** nebo zadejte IP adresu zařízení do adresního řádku webového prohlížeče. Kliknutím na **Systém** → **Údržba systému** otevřete stránku Upgrade a Údržba.

Obrázek 4-32 Údržba systému

Restartování

Kliknutím na **Restartovat** restartujete zařízení.

Obnovení výchozích nastavení

Klepnutím na **Částečné obnovení** obnovíte všechny parametry kromě uživatelských informací správce, připojené sítě, sítě Wi-Fi, informací o detektoru a informací o periferních zařízeních na výchozí hodnoty.

Klepnutím na **Obnovit vše** obnovíte všechny parametry továrního nastavení.

Importování konfiguračního souboru

Klikněte na **Zobrazit** pro výběr konfiguračního souboru z PC a klikněte na **Importování konfiguračního souboru** pro import parametrů konfigurace do zařízení.

Export parametrů

Klikněte na **Exportování konfiguračního souboru** pro export parametrů konfigurace zařízení do PC.

Upgradování souboru

Klikněte na **Zobrazit** pro výběr upgradování souboru z PC a klikněte na **Upgrade** pro dálkový upgrade zařízení.

Poznámka

- Při upgradování zařízení nevypínejte napájení.
 - Tuto funkci může používat pouze výrobce.
-

Norma certifikace

Kliknutím na **Systém** → **Údržba systému** → **Norma certifikace** otevřete stránku nastavení certifikace normy.

Můžete přepínat mezi režimem **EN Přednastaveno** a **Obecnou normou**.

Zařízení ve výchozím nastavení používá normu EN.

Poznámka

Zvolíte-li **Výchozí EN**, budou parametry oprávnění uživatele a aktivace v souladu s normou EN.

Místní vyhledávání záznamu

Můžete vyhledat záznam o zařizení.

Kliknutím na **Systém** → **Záznam** otevřete stránku Místní vyhledávání záznamu nastavení.

No.	Operation Time	Major Type	Minor Type	Local/Remote Operation User	Remote Host Address	Operation Method	Parameters
-----	----------------	------------	------------	-----------------------------	---------------------	------------------	------------

Obrázek 4-33 Stránka místní vyhledávání záznamu

Z rozevřacího seznamu vyberte hlavní typ a vedlejší typ, nastavte počáteční a koncový čas protokolu a klikněte na **Filtr**. Všechny filtrované informace o záznamu se zobrazí v seznamu. Pro reset všech nakonfigurovaných podmínek hledání klikněte na **Reset**.

4.3.8 Zkontrolovat stav

Po nastavení zóny, opakovače a dalších parametrů si můžete zobrazit jejich stav.

Klikněte na **Stav**. Můžete zobrazit stav zóny, relé, sirény, klávesnice, čtečky karet, baterie a komunikace.

- Zóna: Můžete zobrazit stav zóny, stav alarmu, kapacitu baterie detektoru a sílu signálu.
- Siréna: Můžete zobrazit stav sirény, stav baterie a sílu signálu.
- Relé: Můžete zobrazit stav relé, stav baterie a sílu signálu.
- Klávesnice: Můžete zobrazit stav klávesnice, stav baterie a sílu signálu.
- Čtečka karty: Můžete zobrazit stav čtečky, stav baterie a sílu signálu.
- Baterie: Můžete zobrazit nabití baterie.
- Komunikace: Můžete zobrazit stav připojené sítě, stav Wi-Fi, sílu signálu Wi-Fi, stav sítě GPRS/3G/4G, použitá data a stav připojení cloudu.

4.4 Použití mobilního klienta

4.4.1 Stažení a přihlášení mobilního klienta

Stáhněte si mobilního klienta Hik-Connect z Google Play (pro Android) nebo App store (pro iOS) a

před spuštěním bezpečnostního ovládacího panelu klienta přihlaste.

Postup

1. Vyhledejte a stáhněte si mobilního klienta Hik-Connect z Google Play (pro Android) nebo App store (pro iOS).
2. Volitelné: Pokud používáte mobilního klienta Hik-Connect poprvé, zaregistrujte si nový účet.


Poznámka

Podrobnosti *naleznete v uživatelském manuálu mobilního klienta Hik-Connect.*

3. Spusťte a přihlaste klienta.


4.4.2 Aktivace ovládacího panelu prostřednictvím Hik-Connect


Postup

1. Zapněte ovládací panel.
2. Zvolte typ přidávání.
 - Klepnutím na  → **Skenovat kód QR** otevřete stránku skenování kódu QR. Naskenujte kód QR na ovládacím panelu.

Poznámka

Normálně se kód QR vytiskne na štítku na zadním krytu ovládacího panelu.

Klepnutím na  → **Manuální přidání** otevřete stránku Přidat zařízení. Zadejte sériové číslo zařízení s typem přidání domény Hik-Connect.

3. Klepněte na  pro vyhledání zařízení.
4. Klepněte na **Další**.
5. V případě potřeby zadejte kód ověření zařízení a klepněte na **OK**.

Poznámka

Ověřovací kód se ve výchozím nastavení vytiskne na štítku zařízení.

6. Klepněte na **Bezdrátové připojení** na stránce Vybrat typ připojení.
7. Postupujte v souladu s pokyny na stránce Zapnout Hotspot a změňte ovládací panel na režim AP. Klepněte na **Další**.

Poznámka

Musíte sejmout zadní panel zařízení a spínač AP/STA je na zadní straně zařízení.

8. Pro připojení zařízení zvolte stabilní Wi-Fi a klepněte na **Další**.

Poznámka

Je důležité, aby zařízení a mobilní telefon byly připojeny ke stejné Wi-Fi.

9. Postupujte podle pokynů. Vytvořte heslo zařízení a klepněte na **Aktivní**.

Poznámka

Doporučujeme vám, abyste si vytvořili silné heslo podle vlastního výběru (použití minimálně 8 znaků, z toho nejméně tři z následujících kategorií: velká písmena, malá písmena, čísla a speciální znaky) za účelem zvýšení bezpečnosti vašeho výrobku. A doporučujeme vám pravidelně resetovat heslo, zejména v systému s vysokým zabezpečením vám resetování hesla jednou za měsíc nebo jednou za týden může pomoci ochránit váš výrobek.


10. Postupujte v souladu s pokyny na stránce Zapnout Hotspot a změňte ovládací panel na režim STA. Klepněte na **Potvrdit**.

Poznámka

Musíte sejmout zadní panel zařízení a spínač AP/STA je na zadní straně zařízení.

11. Po dokončení připojení zadejte alias zařízení a klepněte na **Uložit**.

12. Volitelné: Můžete smazat zařízení.

- 1) Na stránce se seznamem zařízení klepněte na ovládací panel zabezpečení a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku oddílu.
- 2) Klepnutím na  → **Smazat zařízení** smažete zařízení.


4.4.3 Přidání ovládacího panelu k mobilnímu klientovi

Před zahájením práce přidejte ovládací panel k mobilnímu klientovi.

Než začnete

- Ovládací panel byl aktivován.
- Ovládací panel byl zaregistrován k Hik-Connect. Podrobnosti naleznete v **Registraci mobilního klienta**.

Postup


1. Zapněte ovládací panel.
 2. Zvolte typ přidávání.
 - Klepněte na  → **Skenovat kód QR** pro vstup na stránku skenování kódu QR. Naskenujte kód QR na ovládacím panelu.
-

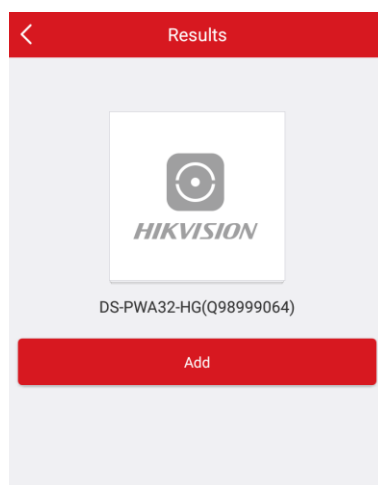
Poznámka

Normálně se kód QR vytiskne na štítku na zadním krytu ovládacího panelu.

Kliknutím na  → **Manuální přidání** otevřete stránku Přidat zařízení. Zadejte sériové číslo

zařízení s typem přidání domény Hik-Connect.

3. Klepněte na  pro vyhledání zařízení.



Obrázek 4-34 Stránka s výsledky

4. Klepněte na **Přidat** na stránce Výsledky.

5. Zadejte **Ověřovací kód** a klepněte na **OK**.

6. Po dokončení přidávání zadejte alias zařízení a klepněte na **Uložit**.

4.4.4 Přidání periférií k ovládacímu panelu

Po přidání je třeba zadat aktivační jméno a přihlašovací heslo ovládacího panelu. Během pěti minut po přihlášení zařízení jako nastavovaného zařízení nebude alarm pro případ manipulace zjištěn a zařízení nespustí.

Než začnete


Ovládací panel musí být deaktivován.

Postup

Poznámka

Některé modely ovládacích panelů nepodporují dálkové přidávání zón nebo bezdrátových zařízení. Musíte je přidat k ovládacímu panelu přímo. Podrobnosti naleznete v uživatelském manuálu bezdrátového zařízení.


1. Na stránce zařízení klepněte na ovládací panel zabezpečení a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku oddílu.

2. Klepněte na  pro vstup na stránku skenování kódu QR.

3. Naskenujte kód QR periférií.

Poznámka

Normálně se kód QR vytiskne na zadním krytu zařízení.

4. Volitelné: Nebude-li kód QR rozpoznán, klepněte na  a zadejte sériové číslo zařízení a zvolte typ zařízení.
-

Poznámka

Sériové číslo je obvykle na zadním krytu zařízení.

5. Klepněte na **Přidat**.
-

Poznámka

- Když jsou periferie přidávání detektorem, připojí se detektor k zóně. Můžete zobrazit informace o detektoru v záložce Zóna.
 - K zóně může být připojeno maximálně 32 detektorů.
-

Přidané periferie budou uvedeny v záložce Zóna nebo v záložce Periferní zařízení.

Poznámka

Jedním z nejdůležitějších faktorů pro spolehlivou instalaci zařízení je síla signálu mezi bezdrátovým zařízením a panelem. Pokud je zařízení mimo rozsah, nebude moci odesílat události na ovládací panel, proto se před provedením upevnění zařízení doporučuje provést test síly signálu. Ovládací panel má pokročilý mechanismus síly signálu, který pracuje monitorováním všech vstupů/zvonek na webovém prohlížeči. Stránku je třeba vždy obnovit pro nový test. Viz také tlačítko funkce vzhledu.

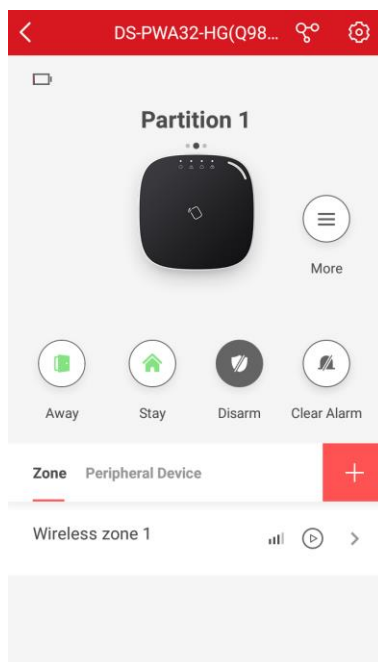
Při provádění testu síly signálu doporučujeme, aby byl systém testován ve „scénáři nejhoršího případu“. Například se všemi zavřenými dveřmi a okny.

4.4.5 Přidání karty


Můžete přidat k ovládacímu panelu kartu. Kartu použijte pro aktivaci, deaktivaci nebo vymazání alarmu.

Postup

1. Na stránce se seznamem zařízení klepněte na ovládací panel zabezpečení a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku oddílu.



Obrázek 4-35 Stránka oddílu

2. Kliknutím na  → **Správa uživatelů** → **Správa karet/visaček** otevřete stránku Správa karet/visaček.
3. Klepněte na +.
4. Když uslyšíte hlasový pokyn „Vložte kartu“, vložte kartu na místo na ovládacím panelu vyhrazené k vložení karty.
Až uslyšíte pípnutí, znamená to, že zařízení kartu poznalo.
5. Vytvořte název karty a klepněte na **Dokončit**.

Poznámka

Jméno by mělo obsahovat 1 až 32 znaků.

Karta se zobrazí na stránce Správa karet/visaček.

4.4.6 Přidat klíčenku


Klíčenku můžete přidat k ovládacímu panelu a kontrolovat stav aktivace/deaktivace oddílu. Po spuštění alarmu můžete vymazat alarm.

Postup

Poznámka


Frekvence klíčenky musí být stejná jako frekvence ovládacího panelu.

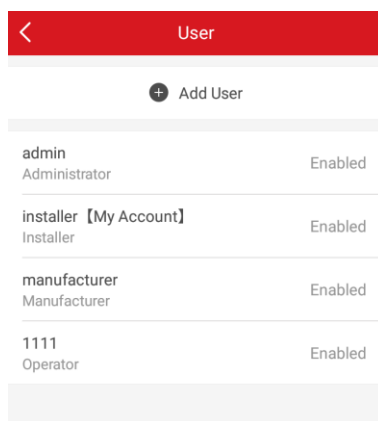
1. Na stránce se seznamem zařízení klepněte na bezpečnostní ovládací panel a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku ovládacího panelu.

2. Klepněte na  pro vstup na stránku skenování kódu QR.
3. Klepněte na možnost **Přidat klíčenku**.
4. Postupujte v souladu s pokyny na stránce a stisknutím jakékoliv klávesy na klíčence ji přidejte.
5. Vytvořte název klíčenky a klepněte na **Dokončit**.
Klíčenka je uvedena na stránce Bezdrátová zařízení.
6. Volitelné: Můžete si zobrazit sériové číslo klíčenky a můžete jej rovněž smazat.

4.4.7 Správa uživatelů

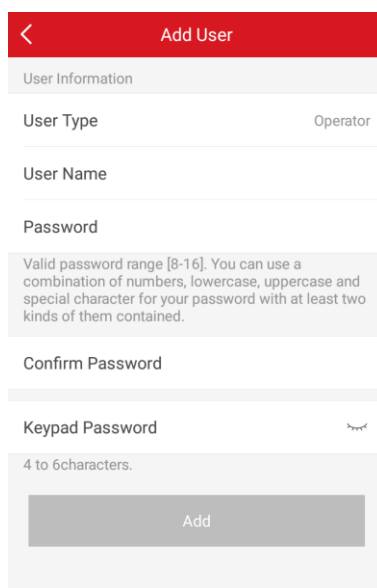
Postup

1. Na stránce se seznamem zařízení klepněte na bezpečnostní ovládací panel a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku ovládacího panelu.
2. Klepněte na  → **Správa uživatelů** → **Uživatel**.



Obrázek 4-36 Správa uživatelů

3. Klepněte na **Přidat uživatele**.



Obrázek 4-37 Přidat uživatele

4. Zvolte **Typ uživatele**. Zadejte **jméno uživatele** a **heslo**.
5. Zadejte **Heslo klávesnice**.

Poznámka

Heslo klávesnice +1 nebo -1 je tísňový kód. Použitím tísňového kódu můžete na klávesnici normálně provádět aktivaci a deaktivaci a odeslat tísňový alarm. Pokud je například heslo klávesnice 123456, je tísňový kód 123455 nebo 123457.

6. Klepnutím na **Přidat** přidáte uživatele.
7. Volitelné: Klepněte na uživatele pro přidání parametrů. Můžete si zvolit, zda uživatele povolíte nebo ne. Vyberte propojený oddíl a povolení.
8. Volitelné: Klepnutím na uživatele a tlačítko **Smazat** smažete uživatele.

Poznámka

Správce, technika a výrobce nelze smazat.

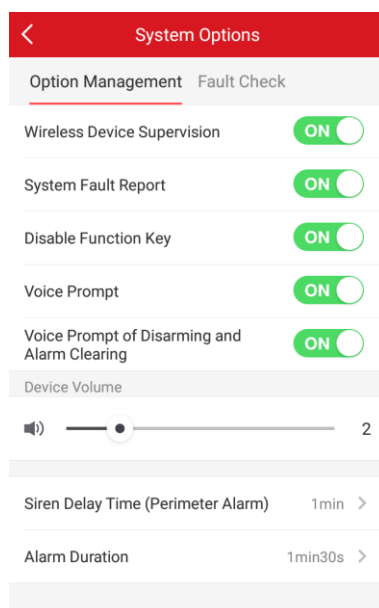
4.4.8 Nastavení systému

Možnost systému

Na stránce se seznamem zařízení klepněte na bezpečnostní ovládací panel a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku ovládacího panelu.

Klikněte na  → **Možnost systému** pro nastavení parametrů.

Správa možností:



Obrázek 4-38 Správa možností

Kontrola bezdrátových zařízení

Při zapnutí této volby systém zjišťuje status všech bezdrátových zařízení.

Zpráva systémové chyby

Pokud je funkce zapnutá, zařízení zprávu při vzniku systémových chyb automaticky odešle.

Vypnutí funkční klávesy

Při zapnutí této funkce budou vypnuty všechny klávesy.

Čas zpoždění sirény (obvodový alarm)

Pokud jste nastavili obvodovou zónu, můžete nastavit zpožděný čas pro zónu.

Poznámka

Dostupný časový rozsah se pohybuje od 0 s do 600 s.

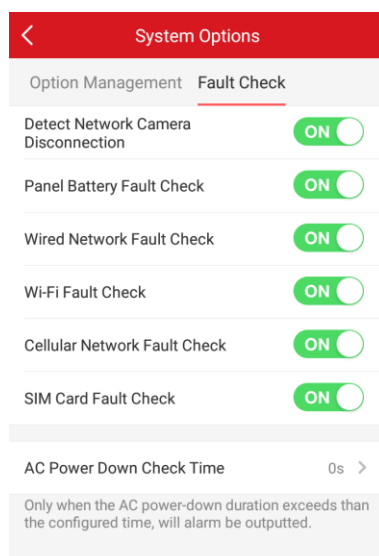
Doba trvání alarmu

Pokud jste nastavili obvodovou zónu, můžete nastavit dobu trvání alarmu.

Poznámka

Dostupný časový rozsah se pohybuje od 1 s do 900 s.

Pro kontrolu závad:



Obrázek 4-39 Kontrola závad

Zjištění odpojení síťové kamery

Pokud je tato volba zapnutá, po odpojení propojené síťové kamery se spustí alarm.

Kontrola závady baterie panelu

Pokud je tato možnost zapnutá, zařízení po odpojení nebo vybití baterie nahraje události.

Kontrola závady připojené sítě

Pokud je tato volba zapnutá, tak se po odpojení připojené sítě nebo při jiných závadách spustí alarm.

Kontrola závady Wi-Fi

Pokud je tato volba zapnutá, tak se po odpojení Wi-Fi nebo při jiných závadách spustí alarm.

Kontrola závady mobilní sítě

Pokud je tato volba zapnutá, tak se po odpojení mobilní datové sítě nebo při jiných závadách spustí alarm.

Kontrola závady SIM karty

Pokud je tato volba zapnutá, tak se při závadách SIM karty spustí alarm.


Čas kontroly výpadku napájení

Systém závadu zkontroluje po uplynutí nastaveného času po výpadku napájení.

Pro dodržení normy EN 50131-3 by doba trvání kontroly měla být 10 s.

Údržba systému

Na stránce se seznamem zařízení klepněte na bezpečnostní ovládací panel a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku ovládacího panelu.

Klikněte na  → **Údržba systému** pro nastavení parametrů.

Restartování zařízení

Zařízení vrátí všechny parametry do předvoleného nastavení.

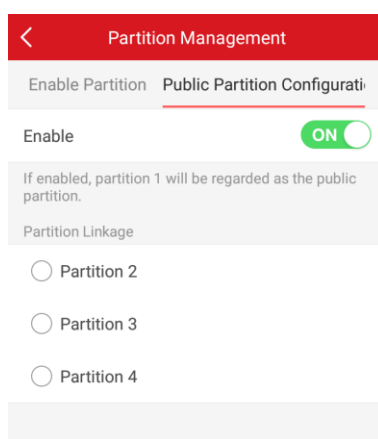
Částečné obnovení

Zařízení obnoví předvolená nastavení kromě uživatelských informací správce, parametrů připojené sítě, sítě Wi-Fi, informací o detektoru a parametrů bezdrátových zařízení na výchozí hodnoty.

Konfigurace veřejných oddílů

Na stránce se seznamem zařízení klepněte na bezpečnostní ovládací panel a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku ovládacího panelu.

Klepněte na  → **Správa oddílů** → **Konfigurace veřejného oddílu** pro nastavení parametrů.



Obrázek 4-40 Konfigurace veřejného oddílu

Po **Povolení** posunutí bude oddíl 1 považován za veřejný oddíl.

Můžete si rovněž vybrat propojený oddíl.

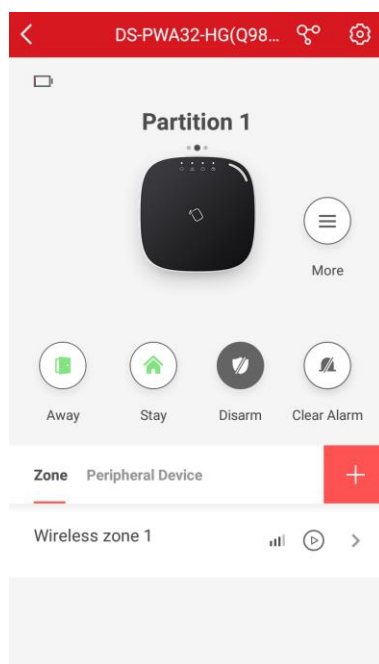
4.4.9 Aktivace/Deaktivace zóny

Zónu můžete manuálně aktivovat nebo deaktivovat podle potřeby.

Poznámka

Bezpečnostní ovládací panel systému Axiom podporuje 4 oddíly.

Na stránce se seznamem zařízení klepněte na ovládací panel zabezpečení a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku Oddíl. Pro přepínání mezi oddíly můžete posouvat doleva nebo doprava.



Obrázek 4-41 Stránka Oddíl

Operace pro jeden oddíl

- **V době nepřítomnosti:** Když všichni lidé sledovanou oblast opustí, zapnutím režimu v době nepřítomnosti aktivujete všechny zóny v oddílu poté, co uplyne definovaná doba setrvání.
- **V době přítomnosti:** Když lidé zůstanou ve sledované oblasti, zapnutím režimu V době přítomnosti aktivujete veškerou obvodovou detekci loupeží (jako je obvodový detektor, magnetické kontakty, detektor záclon na balkóně). Mezitím jsou detektory uvnitř detekční oblasti přemostěny (například detektory PIR). Lidé se mohou v této oblasti pohybovat a nedojde ke spuštění alarmu. **Deaktivace:** V režimu deaktivace nebudou všechny zóny v oddílu aktivovat alarm, bez ohledu na to, zda k události alarmu dojde nebo ne.
- **Vymazání alarmu:** Vymažte alarmy spuštěné zónami oddílu.

Operace pro všechny oddíly

- **V době nepřítomnosti:** Když všichni lidé sledovanou oblast opustí, zapnutím režimu v době nepřítomnosti aktivujete všechny zóny v oddílu poté, co uplyne definovaná doba setrvání.
- **V době přítomnosti:** Když lidé zůstanou ve sledované oblasti, zapnutím režimu V době přítomnosti aktivujete veškerou obvodovou detekci loupeží (jako je obvodový detektor, magnetické kontakty, detektor záclon na balkóně) nastavenou ve všech zónách všech oddílů. Mezitím jsou detektory uvnitř detekční oblasti přemostěny (například detektory PIR). Lidé se mohou v této oblasti pohybovat a nedojde ke spuštění alarmu. **Deaktivace:** V režimu deaktivace nebudou všechny zóny všech oddílů aktivovat alarm, bez ohledu na to, zda k události alarmu dojde nebo ne.
- **Vymazání alarmu:** Vymažte všechny alarmy spuštěné všemi zónami všech oddílů.

4.4.10 Přemostění zóny

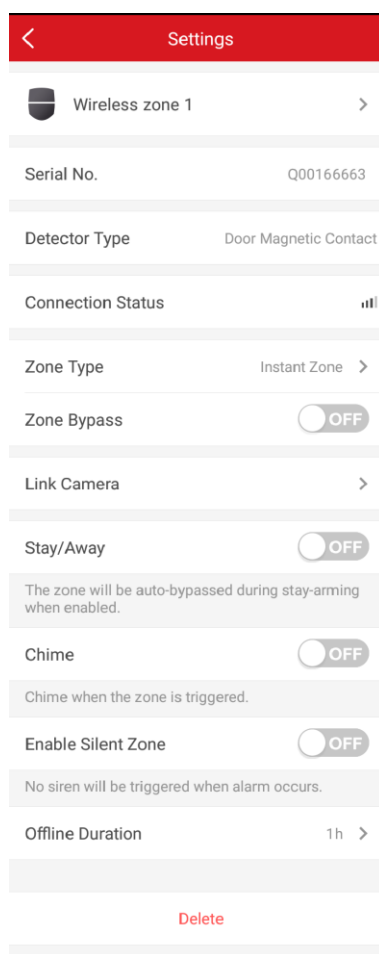
Když je oddíl aktivován, můžete podle potřeby určitou konkrétní zónu přemostit.

Než začnete

Připojte detektor k zóně.

Postup

1. Na stránce se seznamem zařízení klepněte na ovládací panel zabezpečení a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku Oddíl.
2. Zvolte zónu v záložce Zóna pro zadání stránky nastavení.
3. Zvolte zónu a vstupte na stránku Nastavení.



Obrázek 4-42 Stránka nastavení zóny

4. Povolte **Přemostění zóny** a zóna bude ve stavu přemostění. Detektor v zóně nic nezjistí a ze zóny neobdržíte žádný alarm.

4.4.11 Nastavení zóny

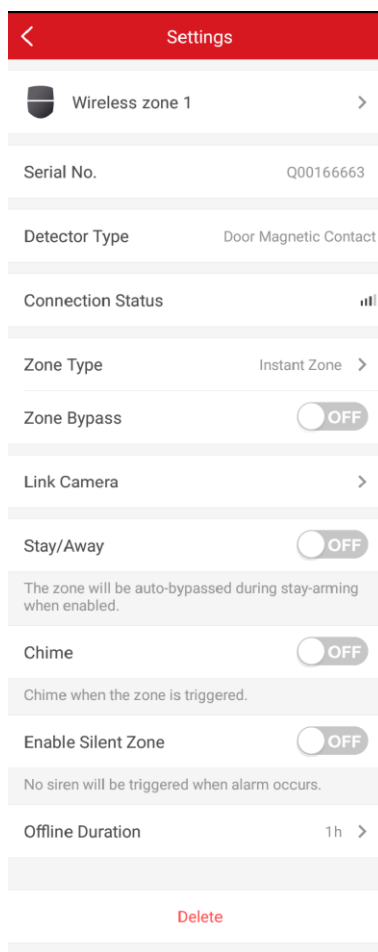
Po přidání detektoru můžete nastavit zónu, včetně názvu zóny, typu zóny, přemostění zóny,

Bezpečnostní ovládací panel AX

připojené kamery, stavu v přítomnosti/stavu v nepřítomnosti, sirény a tiché zóny. Můžete si také prohlédnout sériové číslo detektoru (pouze zařízení v 433 MHz) a typ detektoru zóny.

Postup

1. Na stránce se seznamem zařízení klepněte na bezpečnostní ovládací panel a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku ovládacího panelu.
2. Klepněte na položku **Zóna** a potom klepnutím na zónu na stránce Oddíl otevřete stránku nastavení zóny.



Obrázek 4-43 Stránka nastavení zóny

3. Podle potřeby můžete nastavit následující parametry:

Typ zóny

Ze seznamu typů zóny zvolte typ zóny.

Zvolíte-li možnost **Zpožděná zóna**, měli byste vybrat zpoždění položky (Zpoždění pro příchod 1 nebo Zpoždění pro příchod: 2) na automaticky otevírané stránce.

Pokud vyberete **Časový limit**, měli byste vybrat hodnotu časového limitu nebo klepnutím na

Vlastní nastavit vlastní hodnotu.

Přemostění zóny

Po zapnutí funkce bude zóna přemostěna. Když bude zóna přemostěna, nebude přijatý žádný alarm.

Propojení kamery

Můžete spojit zóny s kamerami. Po spuštění alarmu můžete monitorovat zónu prostřednictvím připojených kamer.

Během přítomnosti/Během nepřítomnosti

Pokud je tato možnost povolena, bude zóna automaticky přemostěna, když bude systém alarmu během přítomnosti aktivní. Pro zakázání zóny tuto volbu zrušte.

Zvonění

Po povolení funkce se v zóně spustí slyšitelný alarm, když je spuštěn.



Zapnutí tiché zóny

Po zapnutí této funkce se v případě události nebo alarmu nezapne siréna.

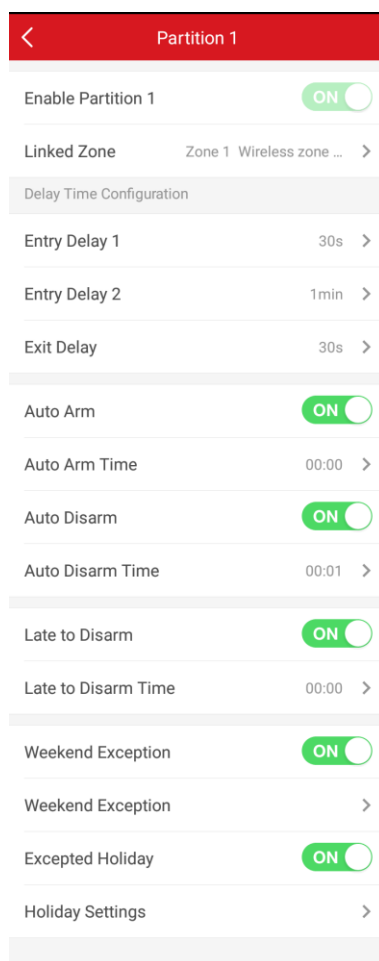
4.4.12 Nastavení plánu aktivace/deaktivace

Nastavte plán aktivace/deaktivace pro automatickou aktivaci/deaktivaci konkrétní zóny.

Na stránce se seznamem zařízení klepněte na bezpečnostní ovládací panel a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku ovládacího panelu.

Klikněte na  → **Správa oddílů** a vyberte oddíl, nebo klikněte na  na stránce Oddíl a otevřete stránku Nastavení.

Zapněte funkci automatické aktivace/deaktivace a nastavte čas automatické aktivace/deaktivace. Můžete rovněž nastavit čas opožděné deaktivace, zpoždění pro příchod, zpoždění pro odchod, čas zpoždění sirény, víkendovou výjimku a výjimku na volné dny.



Obrázek 4-44 Stránka plánu aktivace nebo deaktivace

Zpoždění pro příchod 1

Zpoždění pro příchod 2

Nastavte hodnotu **Zpoždění pro příchod 1** a **Zpoždění pro příchod 2**. Zpoždění pro příchod je časový koncept. Pokud je pro zpožděnou zónu nakonfigurováno zpoždění pro příchod, tak se při vstupu do aktivované zpožděné zóny nespustí alarm zóny až do konce zpoždění pro příchod.

Poznámka

Po nastavení hodnoty pro **Zpoždění pro příchod 1** a **Zpoždění pro příchod 2** byste měli nastavit zpoždění pro příchod konkrétní zóny na hodnotu **Zpoždění pro příchod 1** nebo **Zpoždění pro příchod 2**.

Zpoždění pro odchod

Nastavte zpoždění pro odchod pro zpožděnou zónu. Pokud je pro zpožděnou zónu nakonfigurováno zpoždění pro odchod, můžete po zapnutí zóny na vnitřní jednotce opustit zónu bez spuštění alarmu až do konce zpoždění pro odchod.

Automatická aktivace

Povolte, aby se oddíl v určitý okamžik automaticky aktivoval.

Čas automatické aktivace

Natavte časový plán toho, jak se má oddíl v určitý okamžik automaticky aktivovat.

Opožděná deaktivace

Povolte zařízení, aby vydalo oznámení telefonu nebo tabletu s cílem připomenout uživateli deaktivaci oddílu, když je oddíl po určitém časovém bodě stále aktivovaný.



Poznámka

Nejdříve byste měli povolit funkci Oznámení řízení panelu na webovém klientu **Komunikační parametry** → **Komunikace události**: a teprve potom aktivujte funkci Opožděná deaktivace.

Opožděná deaktivace

Nastavte zmíněný časový bod v **Opožděné deaktivaci**.

Víkendová výjimka

Jsou-li povoleny, tak se funkce **Automatická aktivace**, **Automatická deaktivace** a **Opožděná deaktivace** o víkendu vypínají.

Výjimka na volné dny

Po zapnutí funkce bude zóna aktivována/deaktivována na volné dny. Po aktivaci byste měli nastavit plán volných dní.



Poznámka

Lze přidat až 6 skupin volných dní.


4.4.13 Kontrola stavu systému (Stav zóny/Stav komunikace)

Stav zóny a stav komunikace můžete zobrazit prostřednictvím mobilního klienta.

Zobrazení stavu zóny

Na stránce Oddíl klepněte na položku **Zóna** a otevřete záložku Zóna. Můžete zobrazit stav každé zóny v seznamu.

Režim komunikace


Na stránce Oddíl klepněte na  → **Informace o zařízení** a otevřete příslušnou stránku. Můžete zobrazit stav komunikace zařízení, včetně baterie, sítě Ethernet, Wi-Fi, mobilní sítě, využití dat atd.

Povolení procesu aktivace

Na stránce Oddíl klepnutím na  otevřete příslušnou stránku. Přejděte na povolení **Povolení**

procesu aktivace. Po povolení zařízení automaticky zjistí své závady během procesu aktivace. Můžete určit, zda se má pokračovat v aktivaci nebo ne, jestli byly zjištěny závady.

Režim EN

Na stránce Oddíl klepnutím na  otevřete příslušnou stránku. Posunutím posuvného kontaktu aktivujete **EN Režim**.

Poznámka

Při vypnutí nebo zapnutí režimu EN se zařízení automaticky restartuje.

4.4.14 Kontrola oznámení alarmu

Když se spustí alarm a vy obdržíte oznámení alarmu. Můžete si zkontrolovat informace o alarmu z mobilního klienta.

Než začnete

- Je třeba, aby zóna byla spojená s detektorem.
- Zóna nesmí být přemostěná.
- Dávejte pozor, abyste neaktivovali funkci tiché zóny.

Postup

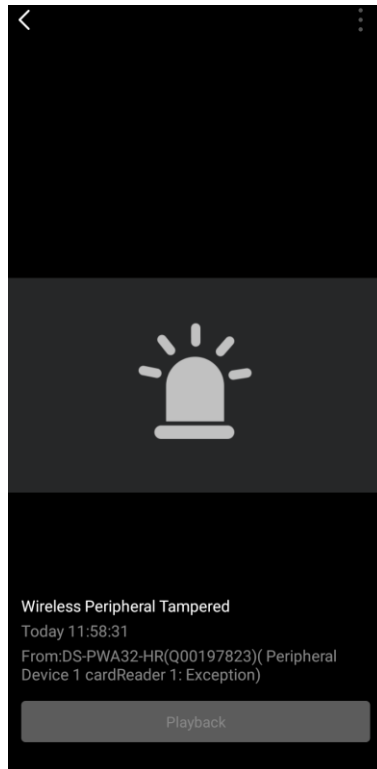
1. Pro vstup na stránku klepněte na **Oznámení** v mobilním klientovi.



Obrázek 4-45 Stránka oznámení

Všechna oznámení alarmu jsou uvedena na stránce Oznámení.

2. Zvolte alarm a můžete zobrazit údaje o alarmu.




Obrázek 4-46 Údaje o alarmu

3. Volitelné: Pokud má zóna připojenou kameru, můžete si při spuštění alarmu prohlížet přehrávání.

4.4.15 Nastavení kanálu síťové kamery


Postup

1. Na stránce se seznamem zařízení klepněte na bezpečnostní ovládací panel a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku ovládacího panelu.
2. Klepněte na  → **Kanál síťové kamery**.
3. Klepněte na **Přidat kanál**.

Bezpečnostní ovládací panel AX

Enrollment Mode	IP
IP Address	
Protocol Type	Hikvision
Port	
User Name	
Password	

4. Zadejte **IP adresu, port, jméno uživatele a heslo.**

5. Klepněte  pro přidání kanálu.

6. Volitelné: Upravte kanál.

1) Vyberte kanál ze seznamu.

Enrollment Mode	IP
IP Address	10.22.102.242
Protocol Type	Hikvision
Port	8000
User Name	admin
Password
Linked Camera	Camera 1

Delete

Obrázek 4-48 Nastavení síťové kamery

2) Klepnutím na  otevřete režim úprav.


3) Upravte parametry.

4) Klepněte na  pro uložení.

7. Volitelné: Zvolte kanál a klepnutím na tlačítko **Smazat** jej smažete.

4.4.16 Nastavení video událostí

Na stránce se seznamem zařízení klepněte na bezpečnostní ovládací panel a poté se přihlaste k

zařízení (je-li to nutné) a otevřete stránku ovládacího panelu.
Klepněte na  → **Nastavení video událostí** otevřete příslušnou stránku.
Musíte si vybrat video kanál a nastavit parametry.

Event Video Settings	
Video Channel	102 >
Stream Type	H.264 >
Bitrate Type	Variable Bitrate >
Resolution	640*480 >
Bitrate	32 Kbps
Length of Cached Video	
Before Alarm	5 >
After Alarm	2 >

Obrázek 4-49 Nastavení video události

Typ streamu

Hlavní stream: Používá se při záznamu a náhledu ve vysokém rozlišení, má vysoké rozlišení, rychlost kódu a kvalitu obrazu.

Dílčí stream: Používá se k přenosu sítě a náhledu obrázků jako streamování videa s vlastnostmi nižšího rozlišení, přenosové rychlosti a kvality obrazu.

Typ přenosové rychlosti

Zvolte typ přenosové rychlosti jako konstantu nebo proměnnou.

Rozlišení

Zvolte rozlišení video výstupu

Přenosová rychlost

Vyšší kvalita odpovídá vyšší kvalitě obrazu, ale je vyžadována lepší pásmová šířka.

Před alarmem

Délka videa v mezipaměti před alarmem.

Po alarmu

Délka videa v mezipaměti po alarmu.

4.4.17 Přidání kamery k zóně

Můžete kameru připojit k zóně pro monitorování zóny. Při spuštění alarmu můžete zobrazit údaje o alarmu.

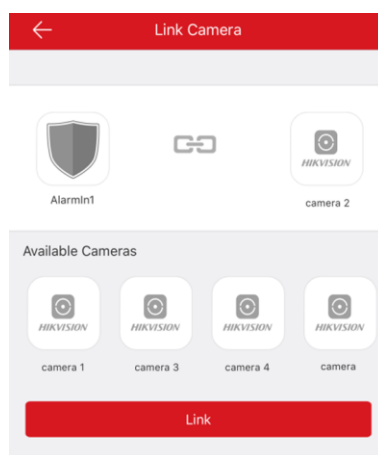
Než začnete

Ujistěte se, že máte kameru nainstalovanou v cílové zóně a kamera je připojena ke stejné LAN jako

ovládací panel zabezpečení.

Postup

1. Na stránce se seznamem zařízení klepněte na bezpečnostní ovládací panel a poté se přihlaste k zařízení (je-li to nutné) a otevřete stránku ovládacího panelu.
2. Klikněte na **Zóna** pro vstup na stránku seznam zón.
3. Zvolte zónu pro nastavení stránky nastavení zóny.
4. Klepněte na **Spojit kameru** pro vstup na stránku Spojit kameru.



Obrázek 4-50 Stránka spojit kameru

5. Zvolte kameru v dostupných kamerách a klepněte na **Spojit**.

Kapitola 5 Operace

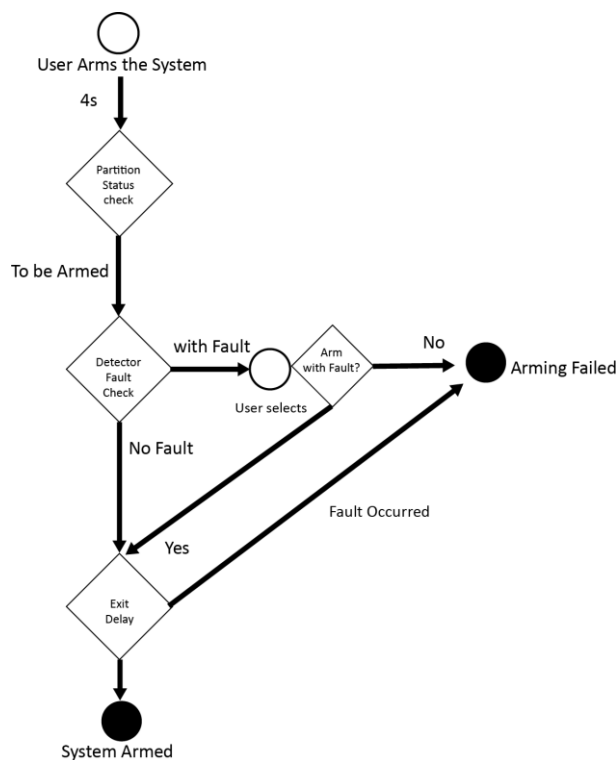
Zóny můžete aktivovat, deaktivovat, přemostovat a vypínat pomocí klíčenky klienta, karty, klientského softwaru nebo mobilního klienta.

5.1 Aktivace

System můžete aktivovat pomocí klávesnice, klíčenky, karty, klientského softwaru nebo mobilního klienta.

Po odeslání aktivačního příkazu na ovládací panel systém zkontroluje stav detektoru. Pokud je detektor vadný, budete se muset rozhodnout, zda chcete deaktivovat systém se závadou.

Když je systém aktivován, tak ovládací panel dodá výsledek během pěti sekund a odešle aktivační zprávu.



Obrázek 5-1 Proces aktivace

Úroveň přístupu aktivace

Uživatel na úrovni 2 nebo 3 má povolení k aktivaci nebo částečné aktivaci systému.

Indikace aktivace

Indikátor aktivace/deaktivace svítí nepřerušovaným modrým světlem po dobu 5 s.

Důvod poruchy aktivace

- Spuštění detektoru vniknutí (kromě detektoru na trase výstupu).
- Spuštění zařízení alarmu paniky.
- Spuštění alarmu v případě manipulace.
- Komunikační výjimka
- Výjimka hlavního napájení
- Výjimka záložní baterie
- Závada přijetí alarmu
- Závada sirény
- Vybitá baterie nebo klíčenka
- Ostatní

Aktivace se závadou

Když dojde k zastavení aktivace se závadou, má uživatel na úrovni 2 povolení k aktivaci se závadou (nucená aktivace).

K nucené aktivaci dojde pouze u operace běžné aktivace.

Operace nucené aktivace bude zaznamenána do deníku událostí.

5.2 Deaktivace

Systém můžete deaktivovat pomocí klávesnice, klíčenky, karty, klientského softwaru nebo mobilního klienta.

Indikace deaktivace

Indikátor aktivace/deaktivace bliká 30 s během doby, kdy uživatel úspěšně deaktivuje systém prostřednictvím cesty vstupu/výstupu.

Po dokončení operace systém nahlásí výsledek deaktivace.

Doba trvání zpoždění pro příchod

Časovač nesmí být nastaven na déle než 45 sekund, aby nedošlo k porušení normy EN 50131-1.

Předčasný alarm

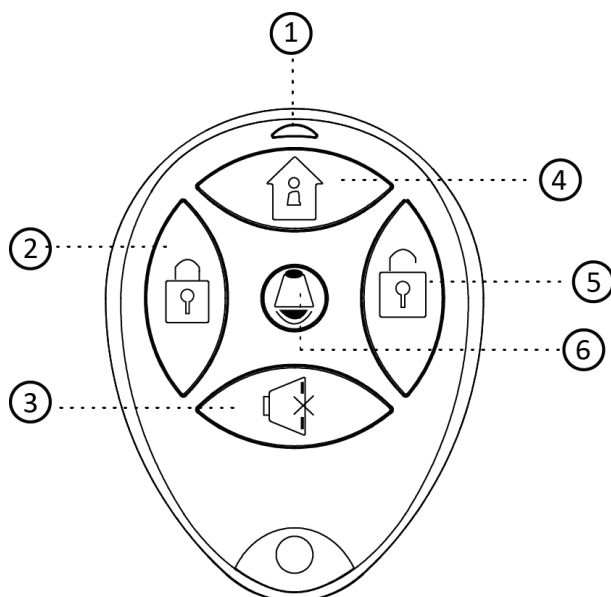
Při spuštění alarmu kvůli narušení nebo manipulaci na trase vstupu/výstupu, když je ovládací panel ve stavu zpoždění pro příchod, přejde ovládací panel do režimu předčasného alarmu.

Dobu trvání předčasného alarmu lze nastavit na (> 30 s).

Ovládací panel nahlásí alarm pouze v případě, když událost alarmu trvá po celou dobu trvání předčasného alarmu s přidáním zpoždění pro příchod.

5.3 Použití klíčenky

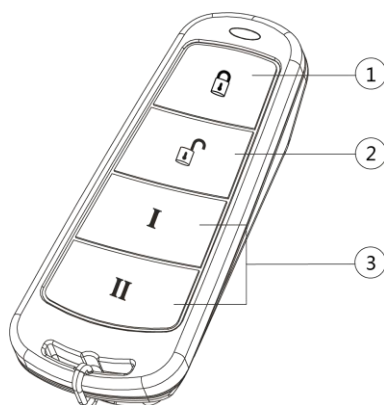
Klíčenka se používá pro aktivaci v době nepřítomnosti, aktivaci v době přítomnosti, deaktivaci, alarm paniky a vymazání alarmu.



Obrázek 5-2 Klíčenka typu I

Tabulka 5-1 Klávesy klíčenky typu I

Č.	Popis
1	Indikátor Zelený: Úspěšná operace Červená: Stiskněte tlačítko
2	Aktivace v době nepřítomnosti
3	Vymazání alarmu
4	Aktivace v době přítomnosti
5	Deaktivace
6	Alarm v případě paniky (tísňový alarm) Podržte tlačítko na dobu 2 sekund a zpráva o alarmu bude zaslána do centra alarmů tajně bez upozornění.



Obrázek 5-3 Klíčenka typu II

Tabulka 5-2 Klávesy klíčenky typu II

Č.	Popis
1	Aktivace (zámek)
2	Deaktivace (odemknutí)
3	Klávesa pro kombinaci funkcí

Kombinace funkcí dle individuálních potřeb (kromě Aktivace + II a Deaktivace + I): Aktivace v době nepřítomnosti, aktivace v době přítomnosti, deaktivace alarm paniky, vymazání alarmu, kontrola závad a kontrola stavu aktivace.

Následující tabulka zobrazuje operace klíčenky a indikace odpovědí.

Tabulka 5-3 Operace a indikace klíčenky typu III

Výsledek operace s klíčenkou	Hlasový pokyn	Indikace
Aktivováno	Stav nepřítomnosti/zůstává aktivováno	Červená dioda jednou blikne
Aktivace selhala	Aktivace selhala.	Zelená dioda jednou blikne
Aktivace	Pípnutí v prvních pěti sekundách. Chybová zpráva poté, co nastalo pípnutí kvůli poruše	Zelená dioda devětkrát blikne
Žádné povolení aktivace	Operace se nezdařila. Klíčenka nemá povolení aktivace.	Žlutá dioda čtyřikrát blikne
Kontrola závady byla dokončena	Žádný hlasový pokyn	Žlutá dioda čtyřikrát blikne
Alarm byl vymazán	Alarm byl vymazán	Zelená dioda jednou blikne

Bezpečnostní ovládací panel AX

Výsledek operace s klíčenkou	Hlasový pokyn	Indikace
Žádné povolení pro vymazání alarmu	Operace se nezdařila. Klíčenka nemá povolení aktivace.	Žlutá dioda čtyřikrát blikne
Deaktivováno	Deaktivováno	Zelená dioda jednou blikne
Žádné povolení deaktivace	Operace se nezdařila. Klíčenka nemá povolení aktivace.	Žlutá dioda čtyřikrát blikne
Odeslání alarmu pro případ paniky	Pokyn alarmu	Zelená dioda jednou blikne
Žádné povolení alarmu paniky	Operace se nezdařila. Klíčenka nemá povolení aktivace.	Žlutá dioda čtyřikrát blikne

5.4 Použití karty

S pomocí karty lze aktivovat nebo deaktivovat systém.



Když systém není aktivován, vložte platnou kartu do ovládacího panelu pro aktivaci systému. Když systém je aktivován, vložte platnou kartu do ovládacího panelu pro deaktivaci systému. Níže jsou uvedeny operace s kartou a hlasové pokyny pro reakci.

Tabulka 5-4

Výsledek operace s kartou	Hlasový pokyn
Aktivováno se zapsanou kartou	Stav nepřítomnosti/zůstává aktivováno
Aktivování se zapsanou kartou se nezdařilo	Aktivace selhala
Zahájit aktivaci se zapsanou kartou	Pípnutí v prvních pěti sekundách. Chybová zpráva poté, co nastalo pípnutí kvůli poruše
Žádné povolení pro zapsanou kartu	Žádný hlasový pokyn
Kontrola závady byla dokončena se zapsanou kartou	Žádný hlasový pokyn

Výsledek operace s kartou	Hlasový pokyn
Deaktivace se zapsanou kartou	Deaktivováno
Žádné povolení deaktivace pro zapsanou kartu	Žádný hlasový pokyn
Operace s nezapsanou kartou	Neplatný přístup


5.5 Použití klientského softwaru

Postup

1. Stáhněte, nainstalujte a zaregistrujte klientský software.
2. Na stránce **Správa zařízení** → **Zařízení** přidejte zařízení.

Poznámka

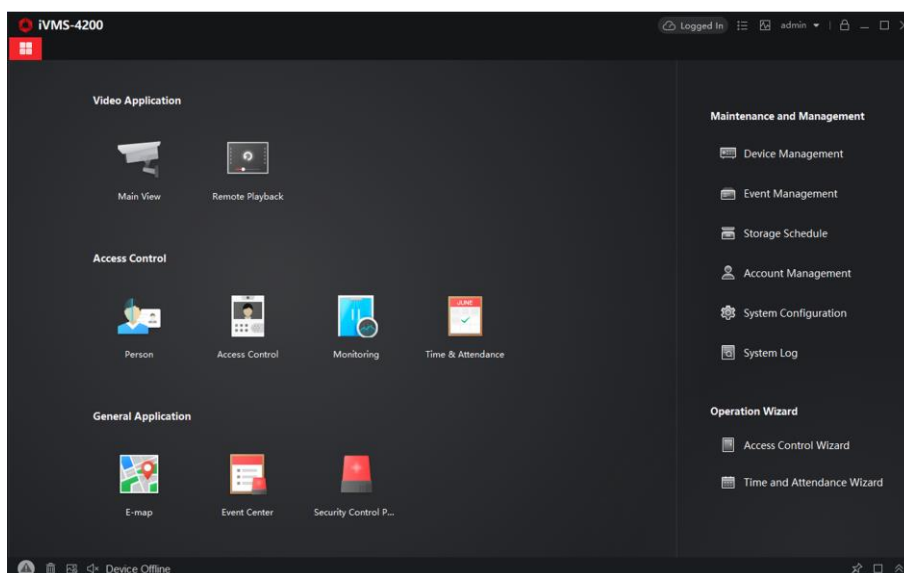
- Nastavte č. portu zařízení na 80.
- Uživatelské jméno a heslo při přidávání zařízení jsou uživatelské jméno a heslo aktivace.

3. Kliknutím na tlačítko  otevřete stránku Vzdálená konfigurace poté, co bylo zařízení zcela přidáno.

5.5.1 Přidání zařízení do klientského softwaru

Než začnete

Aktivujte zařízení a dbejte o to, aby zařízení bylo na stejné podsíti jako PC.



Obrázek 5-4 Klientský software Hlavní stránka

V klientském softwaru přejděte na položku **Správa zařízení** → **Zařízení** v seznamu **Údržba a správa**. Zařízení můžete do klientského softwaru přidávat pomocí několika metod na stránce správy zařízení. Níže je popsáno přidávání zařízení prostřednictvím IP/jména domény. Více informací naleznete v *uživatelském manuálu klientského softwaru iVMS-4200*.

Postup

1. Na stránce **Zařízení** klikněte na **Přidat**.
2. Jako režim přidávání zvolte **IP/doména**, upravte informace o zařízení, včetně **jména, adresy, portu, uživatelského jména a hesla**.

Poznámka

Č. portu je 80.

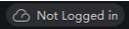
3. Zaškrtněte **Import do skupiny**.
4. Kliknutím na **Přidat** přidáte zařízení.

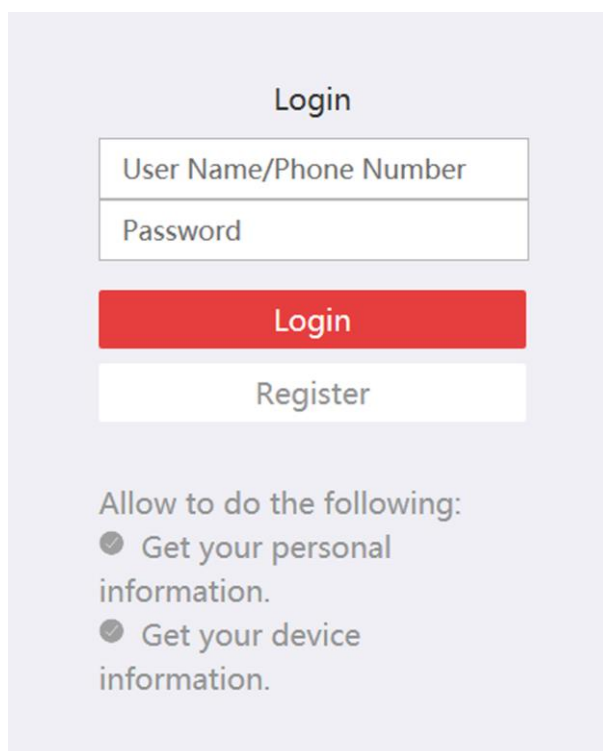
5.5.2 Přidání zařízení do klientského softwaru prostřednictvím Cloud P2P

Než začnete

Sem zadejte požadavky (nepovinné).

Postup

1. Kliknutím na **Správa zařízení** → **Zařízení** v seznamu **Údržba a správa** otevřete příslušnou stránku.
 2. Klikněte na účet Cloud P2P.
 - Klikněte na  a vyberte region. Ve vyskakovacím okně zadejte jméno uživatele a heslo. Klikněte na **Přihlásit**.
- Klikněte na **Přidat**, zvolte region a klikněte na **Přihlásit** ve vyskakovacím okně. Zadejte uživatelské jméno, heslo a klikněte na **Přihlásit**.



Login

User Name/Phone Number

Password

Login

Register

Allow to do the following:

- Get your personal information.
- Get your device information.

Obrázek 5-5 Přihlášení k účtu Cloud P2P

Poznámka

- Pokud jste přidali zařízení pro váš účet Cloud P2P, objeví se zařízení v seznamu zařízení. Pokud ne, musíte přidat zařízení prostřednictvím cloudu P2P nebo IP.
- Poté, co odejdete z vašeho účtu Cloud P2P, dojde k odstranění zařízení, které jste přidali k vašemu účtu Cloud P2P.

3. Kliknutím na **Přidat** zvolte režim přidání jako **Cloud P2P**.

4. Zadejte **Sériové č.** a **Ověřovací kód** nebo klikněte na **Online zařízení** pro výběr zařízení.

Poznámka

- Zařízení by mělo být na stejném síťovém segmentu jako počítač, abyste jej mohli najít v seznamu online zařízení.
- Můžete zkontrolovat **DDNS** a zadat parametry pro její aktivaci.

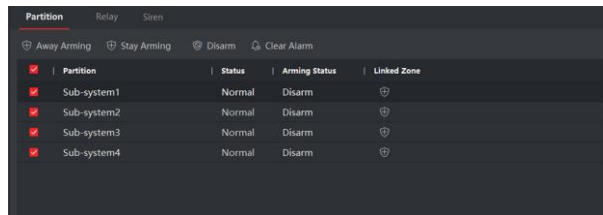
5. Zaškrtněte **Import do skupiny**.

6. Klikněte na **Přidat**.


5.5.3 Fungování oddílu

V klientském softwaru kliknutím na **Bezpečnostní ovládací panel** → **Oddíl** otevřete příslušnou stránku. Můžete ovládat vybraný oddíl, jako například **Aktivace v době nepřítomnosti**, **Aktivace v**

době přítomnosti, Deaktivace a Vymazání alarmu.

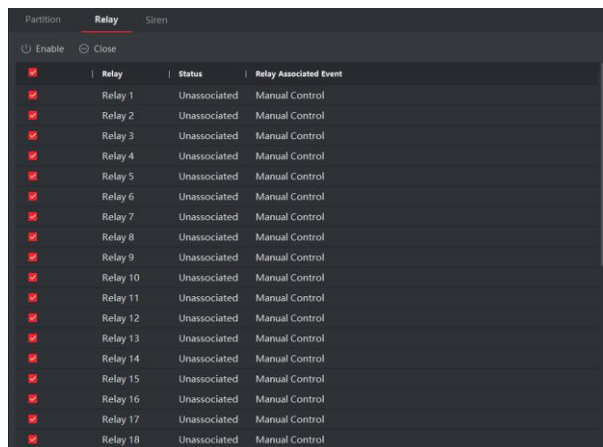


Obrázek 5-6 Operace oddílu

Kliknutím na  otevřete stránku fungování zóny. Vybrané zóny zde můžete **Přemostit** nebo **Zrušit přemostění**.

5.5.4 Fungování relé

V klientském softwaru kliknutím na **Bezpečnostní ovládací panel** → **Relé** otevřete příslušnou stránku. Vybraná relé můžete **Povolit** nebo **Zavřít**.







Obrázek 5-7 Fungování relé

5.5.5 Fungování sirény

Postup

1. V klientském softwaru kliknutím na **Bezpečnostní ovládací panel** → **Siréna** otevřete příslušnou stránku.

Partition	Relay	Siren	
 Enable	 Close	 Refresh	
<input type="checkbox"/>	 Siren	Status	Battery
<input type="checkbox"/>	Siren1	Close	Normal
<input type="checkbox"/>	Siren2	Unassociated	Invalid
<input type="checkbox"/>	Siren3	Unassociated	Invalid
<input type="checkbox"/>	Siren4	Unassociated	Invalid

Obrázek 5-8 Provoz sirény

2. Vybrané sirény můžete **Povolit** nebo **Uzavřít**.

5.6 Použití webového klienta

Postup

1. Připojte zařízení k ethernetu.
2. Vyhledejte IP adresu zařízení prostřednictvím klientského softwaru a softwaru SADP.
3. Do adresní lišty zadejte hledanou IP adresu.

Poznámka

Při používání mobilního prohlížeče je přednastavená IP adresa 192.168.8.1. Zařízení musí být v režimu AP.

Poznámka

Při přímém připojení síťového kabelu s počítačem je přednastavená IP adresa 192.0.0.64.

4. Pro přihlášení použijte aktivační uživatelské jméno a heslo.

Poznámka

Podrobnosti naleznete v kapitole *Aktivace*.

5.6.1 Přidat/Upravit/Smazat kartu

Na bezpečnostní ovládací panel můžete přidat visačku a pomocí karty můžete aktivovat/deaktivovat zónu. Můžete rovněž upravit informace o visačce nebo visačku z bezpečnostního ovládacího panelu odstranit.

Postup

1. Kliknutím na **Správa uživatelů** → **Karta** otevřete stránku správy.
2. Klikněte na **Přidat** a vložte kartu do prostoru pro kartu ovládacího panelu.
3. Upravte název karty v automaticky otevřeném okně.
4. Vyberte typ karty a oddíl propojený s kartou.
5. Vyberte povolení pro kartu.


Poznámka

Měli byste rozdělit alespoň povolení pro kartu.

6. Klikněte na **OK** a v seznamu se zobrazí informace o visačce.

Poznámka

Karta podporuje nejméně 20 tisíc sériových čísel.

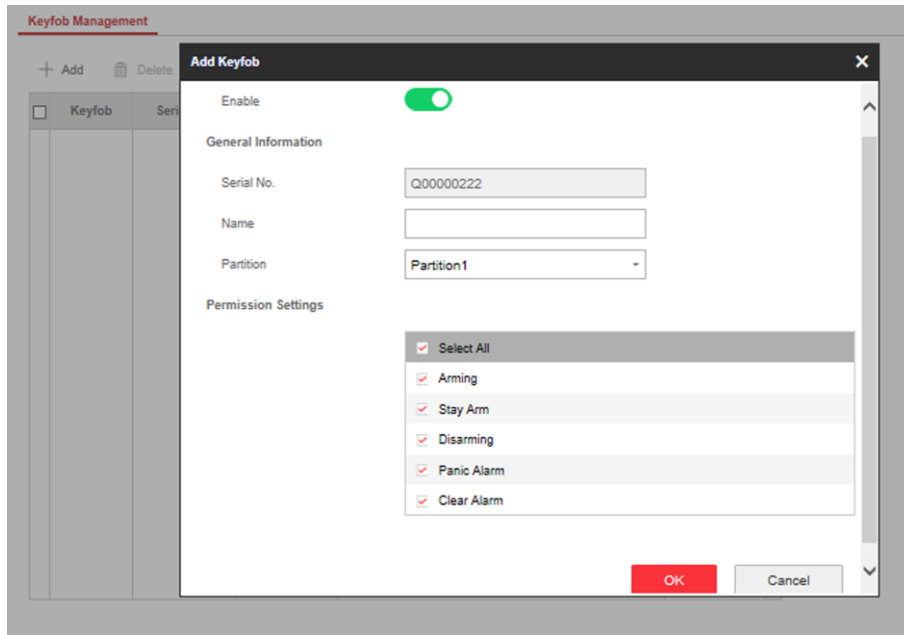
7. Volitelné: Klikněte na  a můžete změnit název karty.
8. Volitelné: Smažte jednu kartu nebo zaškrtněte více karet a klikněte na **Smazat** pro smazání karet v dávce.

5.6.2 Přidat/Upravit/Smazat klíčenku

Na bezpečnostní ovládací panel můžete přidat klíčenku a prostřednictvím klíčenky můžete ovládat bezpečnostní ovládací panel. Můžete rovněž upravit informace o klíčence nebo ji z ovládacího panelu zabezpečení odstranit.

Postup

1. Kliknutím na **Správa uživatelů** → **Klíčenka** otevřete stránku správy klíčenek.



Obrázek 5-9 Správa klíčenek

2. Klikněte na **Přidat** a stiskněte jakoukoliv klávesu na klíčence.
3. Nastavte parametry klíčenky.

Jméno

Upravte název klíčenky.

Nastavení povolení


Zaškrtněte různé položky pro přidělení povolení.

Nastavení jedné klávesy

Vyberte z rozevíracího seznamu pro nastavení funkcí klávesy I a klávesy II

Nastavení kombinačních kláves

Vyberte z rozevíracího seznamu pro nastavení funkcí kombinačních kláves.

4. Klikněte na **OK**.
5. Volitelné: Klikněte na  pro úpravu informací o klíčence.
6. Volitelné: Smažte jednu klíčenku nebo zaškrtněte více klíčenek a klikněte na **Smazat**, chcete-li smazat klíčenky hromadně.

5.6.3 Přidat/Upravit/Smazat uživatele

Správce může přidat uživatele na ovládací panel zabezpečení, upravit informace o uživateli nebo uživatele z ovládacího panelu zabezpečení odstranit. Můžete rovněž přidělit různá povolení novému uživateli.

Postup

1. Kliknutím na **Správa uživatelů** → **Uživatel** otevřete stránku Správa uživatelů.

2. Pro zajištění souladu s požadavkem EN posuňte blok pro aktivaci technika a výrobce.

Poznámka

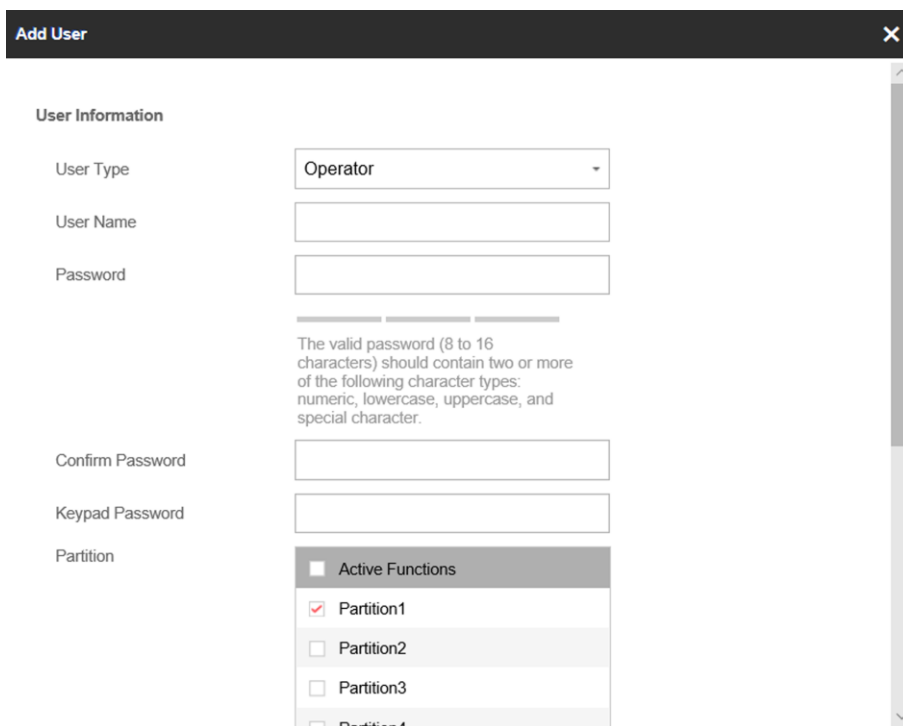
- Přednastavené heslo **technika** je **installer12345** a přednastavené heslo **výrobce** je **hik12345**. Tyto kódy je třeba po prvním připojení změnit.
- Italské uživatelské jméno správce je **asmministratore**.

Tabulka 5-5 Uživatelské jméno technika

Jazyk	Uživatelské jméno	Jazyk	Uživatelské jméno
Angličtina	installer	Ruština	МОНТАЖНИК
Italština	installatore	Francouzština	installatore
Polština	installatore	Španělština	instalador
Němčina	errichter	Portugalština	instalador
Turečtina	kurulumc	Čeština	technik

3. Klikněte na **Přidat**.

4. V automaticky otvíraném okně nastavte informace o novém uživateli, včetně typu uživatele, jména uživatele a hesla.



Obrázek 5-10 Přidat stránku uživatele

5. Nastavte heslo klávesnice (číselné, 8~16 znaků).

Poznámka

Heslo klávesnice +1 nebo -1 je tísňový kód. Použitím tísňového kódu můžete na klávesnici normálně provádět aktivaci a deaktivaci a odeslat tísňový alarm. Pokud je například heslo klávesnice 123456, je tísňový kód 123455 nebo 123457

6. Zkontrolujte oddíly
 7. Zaškrtnutím políčka nastavte oprávnění uživatele.
Uživatel může používat pouze přiřazená povolení.
 8. Klikněte na **OK**.
 9. Volitelné: Aktivací uživatele ve sloupci Aktivovat uživatele umožníte, aby aktivovaný uživatel pracoval se zařízením.
 10. Volitelné: Zvolte uživatele a klikněte na **Upravit** a potom můžete upravovat informace a povolení uživatele.
 11. Volitelné: Smažte jednoho uživatele nebo zaškrtněte více uživatelů a klikněte na **Smazat** pro smazání uživatelů v dávce.
-

Poznámka

Správce, technika a výrobce nelze smazat.

5.6.4 Zkontrolovat stav

Po nastavení zóny, opakovače a dalších parametrů si můžete zobrazit jejich stav.

Klikněte na **Stav**. Můžete zobrazit stav zóny, relé, sirény, klávesnice, čtečky karet, baterie a komunikace.

- Zóna: Můžete zobrazit stav zóny, stav alarmu, kapacitu baterie detektoru a sílu signálu.
- Siréna: Můžete zobrazit stav sirény, stav baterie a sílu signálu.
- Relé: Můžete zobrazit stav relé, stav baterie a sílu signálu.
- Klávesnice: Můžete zobrazit stav klávesnice, stav baterie a sílu signálu.
- Čtečka karty: Můžete zobrazit stav čtečky, stav baterie a sílu signálu.
- Baterie: Můžete zobrazit nabití baterie.
- Komunikace: Můžete zobrazit stav připojené sítě, stav Wi-Fi, sílu signálu Wi-Fi, stav sítě GPRS/3G/4G, použitá data a stav připojení cloudu.

A. Řešení problémů

A.1 Porucha komunikace

A.1.1 Konflikt IP

Popis závady:

IP, které panel automaticky získalo nebo nastavení je stejné jako jiná zařízení, což vede k rozporům v IP.

Řešení:

Vyhledejte aktuální dostupné IP prostřednictvím ping. Změňte IP adresu a znovu se přihlaste.

A.1.2 Webová stránka není přístupná

Popis závady:

Při použití prohlížeče pro přístup k webovým stránkám se zobrazí Nepřístupné.

Řešení:

1. Zkontrolujte, zda je síťový kabel volný a zda je síť panelu abnormální.
2. Port panelu byl upraven. Přidejte port na webovou adresu pro další přístup.

A.1.3 Hik-Connect je offline

Popis závady:

Webová stránka ukazuje, že Hik-Connect je offline.

Řešení:

Konfigurace sítě panelu je chybná, je znemožněn přístup na extranet.

A.1.4 Síťová kamera často vypadává

Popis závady:

Systém hlásí více událostí odpojení a připojení IPC.

Řešení:

Zkontrolujte, zda je síťová komunikace nebo živé zobrazení kamery v pořádku.

A.1.5 Nepodařilo se přidat zařízení na APP

Popis závady:

Při používání APP pro přidání zařízení se objevila zpráva, že se zařízení nepodařilo přidat, zařízení nemohlo být nalezeno atd.

Řešení:

Zkontrolujte webovou stránku: zda je Hik-Connect offline.

A.1.6 Informace o alarmu nejsou podávány do APP/4200/Centra alarmů

Popis závady:

Po spuštění alarmu app/4200/centrum alarmů neobdrží zprávu o alarmu.

Řešení:

„Nabízená zpráva“ – „oznámení alarmu a ochrany proti manipulaci“ není aktivováno. Nejdříve byste měli povolit „oznámení alarmu a ochrany proti manipulaci“.

A.2 Vzájemné vyloučení funkcí

A.2.1 Nelze vstoupit do režimu registrace

Popis závady:

Kliknete na tlačítko funkce panelu a objeví se zpráva, že je tlačítko neplatné.

Řešení:

Panel je v režimu „AP“. Přepněte panel na režim „stanice“ a poté znovu zkuste vstoupit do režimu registrace.

A.2.2 Nelze vstoupit do režimu zadání hledání RF signálu

Popis závady:

Dvakrát kliknete na tlačítko funkce ovládacího panelu a objeví se zpráva, že je tlačítko neplatné.

Řešení:

Panel je v režimu „AP“. Řešení: přepněte panel na režim „stanice“ a poté znovu zkuste vstoupit do režimu hledání signálu RF.

A.3 Vada zóny

A.3.1 Zóna je offline

Popis závady:

Zobrazuje se stav zón, který se zobrazuje offline.

Řešení:

Zkontrolujte, zda detektor nevykazuje podpětí. Vyměňte baterii detektoru

A.3.2 Odolnost proti manipulaci se zónou

Popis závady:

Zobrazuje se stav zón, který se zobrazí jako odolné proti manipulaci.

Řešení:

Přidrželte tlačítko odolnosti proti manipulaci na detektoru.

A.3.3 Spuštěná zóna/chyba

Popis závady:

Zobrazuje se stav zón, který se chybně zobrazuje jako spuštěné.

Řešení:

Resetujte detektor.

A.4 Problémy při aktivaci

A.4.1 Porucha aktivace (Když se proces aktivace nespustí)

Popis závady:

Když je panel aktivován, selže pokyn aktivace.

Řešení:

Panel neumožní „nucenou aktivaci“ a když v zóně dojde k poruše, aktivace selže. Zapněte „nucenou aktivaci“ nebo obnovte zónu do normálního stavu.

A.5 Provozní závada

A.5.1 Nepodařilo se vstoupit do režimu testu

Popis závady:

Nepodařilo se zapnout režim testu, zadání pokynu „porucha v zóně“.

Řešení:

Stav zóny, stav alarmu nebo síla zóny jsou abnormální.

A.5.2 Operace smazání alarmu na panelu nevede k vytvoření zprávy o vymazání alarmu

Popis závady:

Operace smazání alarmu na panelu nevede k vytvoření zprávy o vymazání alarmu.

Řešení:

Pokud nedojde k alarmu, neodešle se žádná zpráva pro smazání alarmu.

A.6 Porucha doručení e-mailu

A.6.1 Nepodařilo se odeslat e-mail o testu

Popis závady:

při konfigurování informací o e-mailu, klikněte na „testovat příchozí poštu“ a test výzvy se nezdaří.

Řešení:

Nesprávná konfigurace parametrů poštovní schránky. Upravte informace o konfiguraci poštovní schránky v souladu s tím, jak je uvedeno v tabulce 1/1.

A.6.2 Nepodařilo se odeslat e-mail během používání

Popis závady:

Podívejte se do deníku výjimek panelu. Je tam „porucha odeslání e-mailu“.

Řešení:

Server poštovní schránky má omezený přístup. Přihlaste se do poštovní schránky a zjistěte, jestli je poštovní schránka uzamknutá.

A.6.3 Nepodařilo se odeslat e-mail na Gmail

Popis závady:

Poštovní schránka příjemce je Gmail. Klikněte na „Testovat příchozí poštu“ a test výzvy se nezdaří.

1. Google neumožňuje uživatelům přístup na Gmail s použitím aplikací/zařízení, která nespĺňují bezpečnostní normy.

Řešení:

Přihlaste se k webové stránce (<https://www.google.com/settings/security/lesssecureapps>) a „začněte použitím přístupu nedostatečně zabezpečené aplikace“. Zařízení může normálně posílat e-mail.

2. Gmail neodstraňuje ověření prostřednictvím CAPTCHA.

Řešení: Klikněte na níže uvedený odkaz a poté klikněte na „pokračovat“

(<https://accounts.google.com/b/0/displayunlockcaptcha>).

A.6.4 Nepodařilo se odeslat e-mail na QQ nebo Foxmail

Popis závady:

Poštovní schránka příjemce je QQ nebo foxmail. Klikněte na „Testovat příchozí poštu“ a test výzvy se nezdaří.

1. Nesprávný účet QQ nebo heslo.

Řešení:

heslo požadované pro přihlášení k účtu QQ není heslo používané pro normální přihlášení. Konkrétní cesta je: Zadejte e-mailový účet → zařízení → účet → pro generování autorizačního kódu a použijte autorizační kód jako přihlašovací heslo.

2. Pro otevření je vyžadováno povolení přihlášení SMTP.

A.6.5 Nepodařilo se odeslat e-mail na Yahoo

Popis závady:

Poštovní schránka příjemce je yahoo. Klikněte na „Testovat příchozí poštu“ a test výzvy se nezdaří.

1. Úroveň zabezpečení poštovní schránky je příliš vysoká.

Řešení:

Přejděte do svého e-mailového účtu a zapněte „méně bezpečné přihlášení“.

A.6.6 Konfigurace e-mailu

Tabulka A-1 Konfigurace e-mailu

Typ e-mailu	Server e-mailu	Port SMTP	Podporované protokoly
Gmail	smtp.gmail.com	587	TLS/STARTTLS (TLS)
Outlook	smtp.office365.com	587	STARTTLS (TLS)
Hotmail	smtp.office365.com	587	STARTTLS (TLS)
QQ	smtp.qq.com	587	STARTTLS (TLSv1.2)
Yahoo	smtp.mail.yahoo.com	587	STARTTLS (TLSv1.2)
126	smtp.126.com	465	SSL/TLS
Sina	smtp.sina.com	25/465/587	SSL/TLS/STARTTLS (SSL/TLS)

Poznámka

O konfiguraci e-mailu

- Port SMTP Přednastavený k používání portu 25 bez kódování nebo použití portu 465, pokud se používá SSL/TLS. Port 587 se používá hlavně pro vytvořený protokol STARTTLS. Režim protokolu STARTTLS, který se obvykle používá jako výchozí při výběru TLS.
- Jméno uživatele Jméno uživatele Outlooku a Hotmailu vyžaduje celá jména a jiný e-mail vyžaduje předponu před @.

B. Typy vstupů

Tabulka B-1 Typy vstupů

Typy vstupů	Operace
Okamžitá zóna	<p>Když systém po aktivaci systému zjistí spouštěcí událost, okamžitě spustí alarm.</p> <p>Slyšitelná odpověď spustí zvuk systému a sirénu.</p> <p>Hlasový pokyn: Alarm zóny X.</p>
Obvodová zóna	<p>Když systém po aktivaci systému zjistí spouštěcí událost, okamžitě spustí alarm.</p> <p>Slyšitelná odpověď: Spustíte zvuk systému a sirénu. Mezi alarmem a výstupem sirény je nastavitelný interval, který vám umožní zkontrolovat alarm a během tohoto intervalu zrušit výstup sirény.</p> <p>Hlasový pokyn: Obvodový alarm zóny X.</p>
Zpožděná zóna	<p>Systém vám poskytne čas na to, abyste chráněnou oblast opustili bez spuštění alarmu.</p> <p>Slyšitelná odpověď: Spustíte zvuk systému a sirénu.</p> <p>Hlasový pokyn: Alarm zóny X.</p>
Následná zóna	<p>Zóna se chová jako zpožděná zóna, když zaznamená spuštění události během Zpoždění pro příchod systému, zatímco jinak působí jako okamžitá zóna.</p> <p>Slyšitelná odpověď: Spustíte zvuk systému a sirénu.</p> <p>Hlasový pokyn: Zóna X sledovat alarm.</p>
24H Zóna ticha	<p>Zóna se pokaždé aktivuje bez jakéhokoli výstupu zvuku/sirény, když se spustí alarm.</p> <p>Slyšitelná odpověď: Žádný zvuk systému (hlasový pokyn nebo siréna).</p>
Zóna paniky	<p>Zóna se aktivuje vždy.</p> <p>Slyšitelná odpověď: Spustíte zvuk systému a sirénu.</p> <p>Hlasový pokyn: Alarm zóny X paniky.</p>
Požární zóna	<p>Zóna se aktivuje vždy s výstupem zvuku/sirény, když se spustí alarm.</p>

Bezpečnostní ovládací panel AX

Typy vstupů	Operace
	<p>Slyšitelná odpověď: Spusťte zvuk systému a sirénu.</p> <p>Hlasový pokyn: Zóna X požární alarm.</p>
Plynová zóna	<p>Zóna se aktivuje vždy s výstupem zvuku/sirény, když se spustí alarm.</p> <p>Slyšitelná odpověď: Spusťte zvuk systému a sirénu.</p> <p>Hlasový pokyn: Zóna X alarm plynu.</p>
Zóna ohrožení zdraví	<p>Zóna se aktivuje vždy s potvrzujícím pípnutím, když se spustí alarm.</p> <p>Slyšitelná odpověď: Spusťte zvuk systému a sirénu.</p> <p>Hlasový pokyn: Zóna X alarm ohrožení zdraví.</p>
Zóna časového limitu	<p>Zóna se aktivuje vždy. Typ zóny se používá ke sledování a hlášení stavu „AKTIVNÍ“ zóny, ale tento stav bude hlásit a alarm spustí až po uplynutí naprogramovaného času (1 až 599) sekund.</p>
Vypnutá zóna	<p>Při spuštění zóny nebo manipulaci s ní se alarmy neaktivují.</p> <p>Slyšitelná odpověď: Žádný zvuk systému (hlasový pokyn nebo siréna).</p>
Virtuální zóna (Klávesnice/Klíčenka)	<p>Když systém po aktivaci systému zjistí spouštěcí událost, okamžitě spustí alarm.</p> <p>Slyšitelná odpověď: Spusťte zvuk systému a sirénu.</p> <p>Hlasový pokyn: Bzučák bzučí.</p>
Alarm pro případ manipulace	<p>Když systém po aktivaci systému zjistí spouštěcí událost, okamžitě spustí alarm.</p> <p>Slyšitelná odpověď: Spusťte zvuk systému a sirénu.</p> <p>Hlasový pokyn: Manipulace se zónou X.</p>
Odkaz	<p>Při vzniku události spusťte připojené zařízení.</p> <p>např. Relé připojená k expandéru výstupu se aktivují tehdy, když bude ovládací panel zapnutý.</p>
Aktivace	<p>Při aktivaci: Hlasový pokyn pro poruchu. S poruchou můžete pracovat podle hlasového pokynu.</p> <ul style="list-style-type: none"> ● Zvuk systému pro aktivaci s kartou nebo klíčenkou. ● Hlasový pokyn pro poruchu. S poruchou můžete pracovat podle hlasového pokynu.

Na klientovi se zobrazí chybová událost. Chybu můžete řešit pomocí klientského softwaru nebo

mobilního klienta.

Hlasový pokyn: Aktivováno/Aktivace selhala.

C. Typy výstupů

Tabulka C-1 Typy výstupů

Typy výstupů	Aktivní	Obnovit
Aktivace	Aktivujte ovládací panel.	Po nakonfigurovaném zpoždění výstupu
Deaktivace	Deaktivujte ovládací panel.	Po nakonfigurovaném zpoždění výstupu
Alarm	Když dojde k alarmu. Výstup alarmu bude aktivován po nakonfigurovaném zpoždění pro odchod/příchod.	Po nakonfigurovaném zpoždění výstupu deaktivujte kontrolní panel nebo vymažte alarm.
Spojení zóny	Když dojde k alarmu, spustí připojené relé signál alarmu.	Po nakonfigurované době výstupu
Manuální operace	Zapněte relé manuálně	Během doby spuštění nebo relé manuálně deaktivujte

D. Typy událostí

Tabulka D-1 Typy událostí

Typy událostí	Vlastní	Výchozí 1 (oznámení klientského softwaru)	Výchozí 2 (centrum přijímání alarmu 1/2)	Výchozí 3 (mobilní klient)	Výchozí 4 (telefon)
Alarmy a případy manipulace	x/v	√	√	√	√
Událost ohrožující bezpečnost života	x/v	√	√	√	√
Stav systému	x/v	√	x	x	x
Správa panelu	x/v	√	x	x	x

E. Úrovně přístupu

Úroveň	Popis
1	Přístup jakékoliv osoby, například veřejnosti.
2	Uživatelský přístup operátora; například zákazníci (uživatelé systému).
3	Uživatelský přístup technika; například pracovník společnosti zaměřené na alarmy.
4	Uživatelský přístup výrobce zařízení.

Tabulka E-1 Povolení úrovně přístupu

Funkce	Povolení		
1	2	3 ^a	4 ^b
Aktivace	Ne	Ano	Ano
Deaktivace	Ne	Ano	Ano
Obnovení/vymazání alarmu	Ne	Ano	Ano
Vstup do režimu testování chůze	Ne	Ano	Ano
Přemostění (zóny)/Deaktivace/Nucená aktivace	Ne	Ano	Ano
Přidání/změna ověřovacího kódu	Ne	Ano ^d	Ano ^d
Přidání/úprava úrovně 2 Uživatele a kódu ověření	Ne	Ano	Ano
Přidání/úprava data konfigurace	Ne	Ne	Ano
Výměna softwaru a firmwaru	Ne	Ne	Ne

Poznámka

^a Podmínkou akreditace uživatelem na úrovni 2. ^b Podmínkou akreditace uživatelem na úrovni 2 a 3. ^d Uživatelé mohou upravovat pouze svůj vlastní uživatelský kód.

- Uživatelská úroveň 2 může přiřadit přihlašovací oprávnění řadiče uživatelské úrovni 3 nebo 4 na stránce nastavení.
- Uživatelská úroveň 2 by měla přidělit oprávnění k uživatelské úrovni 3, pokud se uživatelská úroveň 3 chce vzdáleně přihlásit k řadiči.

- Když je ovladač přemostěn, uživatelská úroveň 3 se může přihlásit k řadiči bez přiřazení oprávnění uživatelské úrovni 2.
- Když je ovladač přemostěn, uživatelská úroveň 3 se může přihlásit k řadiči bez přiřazení oprávnění uživatelské úrovni 2.
- Uživatelská úroveň 4 se může přihlásit k řadiči pouze tehdy, když uživatelská úroveň 2 nebo úroveň 3 přidělila oprávnění uživatelské úrovni 4.

F. SIA a kód CID

F. SIA a kód CID

Kód SIA	Kód CID	Popis
BA	E130	Alarm pro případ vloupání
BH	R130	Alarm pro případ vloupání obnoven
HA	E122	Alarm tiché paniky
HH	R122	Alarm tiché paniky obnoven
NA	E780	Alarm časové zóny
BH	R780	Požární alarm napraven
PA	E120	Alarm paniky
PH	R120	Alarm paniky napraven
BA	E131	Obvodový alarm
BH	R131	Obvodový alarm obnoven
BA	E134	Alarm příchodu/odchodu
BH	R134	Alarm příchodu/odchodu obnoven
TA	E137	Manipulace se zařízením
TR	R137	Manipulace se zařízením napravena
TA	E383	Manipulace s detektorem
TR	R383	Manipulace s detektorem napravena
TA	E321	Manipulace s bezdrátovou sirénou
TR	R321	Manipulace s bezdrátovou sirénou napravena
TA	E334	Manipulace s bezdrátovým opakovačem
TR	R334	Manipulace s bezdrátovým opakovačem napravena

Bezpečnostní ovládací panel AX

Kód SIA	Kód CID	Popis
ES	E341	Manipulace s rozšířením nebo bezdrátovým zařízením
EJ	R341	Manipulace s rozšířením nebo bezdrátovým zařízením napravena
PA	E120	Alarm v případě paniky klávesnice/klíčenka
MA	E100	Alarm ochrany před ohrožením zdraví
MH	R100	Alarm ochrany před ohrožením zdraví obnoven
GA	E151	Alarm úniku plynu
GH	R151	Alarm úniku plynu obnoven
FA	E110	Požární alarm
FH	R110	Požární alarm obnoven
OP	E401	Deaktivace
CL	R401	Aktivace v době nepřítomnosti
OA	E403	Automatická deaktivace
CA	R403	Automatická aktivace
BC	E406	Vymazání alarmu
CL	R441	Aktivace v době přítomnosti
CD	E455	Automatická aktivace selhala
BB	E570	Zóna byla přemostěna
BU	R570	Přemostění zóny bylo obnoven
CT	E452	Opožděná deaktivace
AT	E301	Výpadek střídavého proudu
AR	R301	Obnova dodávky střídavého proudu
YT	E302	Vybitá baterie systému
YR	R302	Dobití baterie systému
XT	E384	Vybitá baterie v klíčence

Bezpečnostní ovládací panel AX

Kód SIA	Kód CID	Popis
XR	R384	Baterie v klíčence dobita
YM	E311	Závada baterie
YR	R311	Závada baterie napravena
DK	E501	Klávesnice uzamknuta
DO	R501	Klávesnice odemknuta
TS	E607	Zadání režimu testu
TE	R607	Odchod z režimu testu
RN	E305	Reset ovládacího panelu
UY	E321	Odpojení bezdrátové sirény
UJ	R321	Bezdrátová siréna odpojena
UY	E381	Bezdrátový detektor odpojen
UJ	R381	Bezdrátový detektor připojen
XT	E384	Nízké napětí bezdrátového detektoru
XR	R384	Normální napětí bezdrátového detektoru
ET	E333	Odpojení rozšíření nebo bezdrátového zařízení
ER	R333	Připojení rozšíření nebo bezdrátového zařízení
UY	E334	Bezdrátový opakovač odpojen
UJ	R334	Bezdrátový opakovač připojen
NT	E352	Mobilní datová síť odpojena
NR	R352	Mobilní datová síť připojena
NT	E352	Výjimka SIM karty
NR	R352	SIM karta opravena
NT	E352	Překročení síťového průtoku
NT	E351	Konflikt IP adresy
NR	R351	Normální IP adresa:
NT	E351	Výjimka připojené sítě

Bezpečnostní ovládací panel AX

Kód SIA	Kód CID	Popis
NR	R351	Normální připojená síť
NT	E351	Porucha komunikace Wi-Fi
NR	R351	Wi-Fi připojeno
XQ	E344	Výjimka signálu RF
XH	R344	Normální signál RF
/	E306	Expandér smazán
/	R306	Expandér přidán
/	E306	Detektor smazán
/	R306	Detektor přidán
/	E306	Bezdrátový opakovač smazán
/	R306	Bezdrátový opakovač přidán
/	E306	Bezdrátová siréna smazána
/	R306	Bezdrátová siréna přidána
BA	E130	Alarm pro případ vloupání
BH	R130	Alarm pro případ vloupání obnoven
XT	E338	Vybitá baterie v bezdrátovém zařízení
XR	R338	Baterie v bezdrátovém zařízení dobíjí
YC	E354	Odeslání zprávy se nezdařilo
YK	R354	Odesílání zpráv obnoveno
LB	E627	Zadání režimu programování
LX	E628	Ukončení režimu programování
CI	E454	Aktivace selhala
/	R250	Stráž
/	E306	Bezdrátové zařízení smazáno
/	R306	Bezdrátové zařízení přidáno
XT	E384	Baterie bezdrátové sirény vybitá

Bezpečnostní ovládací panel AX

Kód SIA	Kód CID	Popis
XR	R384	Baterie bezdrátové sirény dobita
NT	E351	Porucha kabelové sítě/Wi-Fi
NR	R351	Kabelová síť/Wi-Fi opraveny
NT	E352	Porucha mobilní sítě ATP
NR	R352	Mobilní síť ATP opravena

G. Zařízení v certifikátu EN Standardní/Základní norma

Tabulka G-1 Oprávnění uživatele v normě EN

Funkce	Oprávnění uživatele v normě EN					
Úroveň 1		Úroveň 2			Úroveň 3	Úroveň 4
Kdokoliv	Základní uživatel	Správce	Technik	Výrobce		
Aktivace	x	Podle nakonfigurovaného povolení.	√	√	x	
Deaktivace	x	Podle nakonfigurovaného povolení.	√	√	x	
Vymazání alarmu	x	Podle nakonfigurovaného povolení.	√	√	x	
Test chůze	x	Podle nakonfigurovaného povolení.	√	√	x	
Dotaz k záznamu	x	Podle nakonfigurovaného povolení.	√	√	x	
Přemostění/Deaktivace/Povinná aktivace	x	Podle nakonfigurovaného povolení.	√	√	x	
Přidání/změna ověřovacího kódu	x	Podle nakonfigurovaného povolení.	√	√	√	

Bezpečnostní ovládací panel AX

Přidání/odebrání úrovně 2 Uživatele a kódu ověření	x	Podle nakonfigurovaného povolení.	√	√	x
Přidání/Úprava místa	x	x	x	√	x
Vyměnit programování /Firmware	x	x	x	x	√

Tabulka G-2 Oprávnění uživatele v základní normě

Funkce	Oprávnění uživatele v základní normě					Úroveň 4
	Úroveň 1	Úroveň 2			Úroveň 3	
Kdokoliv	Základní uživatel	Správce	Technik	Výrobce		
Aktivace	x	Podle nakonfigurovaného povolení.	√	√	x	
Deaktivace	x	Podle nakonfigurovaného povolení.	√	√	x	
Vymazání alarmu	x	Podle nakonfigurovaného povolení.	√	√	x	
Test chůze	x	Podle nakonfigurovaného povolení.	√	√	x	
Dotaz k záznamu	x	Podle nakonfigurovaného povolení.	√	√	x	
Přemostění/Deaktivace/Povinná aktivace	x	Podle nakonfigurovaného	√		x	

Bezpečnostní ovládací panel AX

		povolení.			
Přidání/změna a ověřovacího kódu	x	Podle nakonfigurovaného povolení.	√	√	√
Přidání/odebrání úrovně 2 Uživatelé a kódu ověření	x	Podle nakonfigurovaného povolení.	√	√	x
Přidání/Úprava místa	x	x	√	√	x
Vyměnit programování /Firmware	x	x	√	√	√



See Far, Go Further