



Bezpečnostní ovládací panel Axiom

Uživatelská příručka

Informace o předpisech

O této příručce

Na tuto příručku se vztahuje ochrana podle domácích i mezinárodních předpisů o autorských právech. Všechna práva na tuto příručku si vyhrazuje společnost Hangzhou Hikvision Digital Technology Co., Ltd. („Hikvision“). Tuto příručku jako celek ani její část není dovoleno žádnými prostředky reprodukovat, měnit, překládat či distribuovat bez předchozího písemného souhlasu společnosti Hikvision.

Tuto uživatelskou příručku používejte pod dohledem odborníků

Ochranné známky

HIKVISION a další značky společnosti Hikvision jsou jejím vlastnictvím a jsou to registrované ochranné známky, případně jsou předmětem žádosti společnosti Hikvision nebo jejich dceřiných společností o ochrannou známku. Ostatní ochranné známky uvedené v této příručce jsou majetkem jejich příslušných vlastníků. Tyto ochranné známky není dovoleno používat bez výslovného souhlasu.

Odmítnutí odpovědnosti

SPOLEČNOST HIKVISION V MAXIMÁLNÍM ROZSAHU POVOLENÉM PLATNÝMI ZÁKONY NEPOSKYTUJE ŽÁDNOU VÝSLOVNOU ANI PŘEDPOKLÁDANOU ZÁRUKU NA TUTO PŘÍRUČKU, VČETNĚ PŘEDPOKLÁDANÝCH ZÁRUK PRODEJNOSTI ČI VHODNOSTI PRO KONKRÉTNÍ ÚČEL. SPOLEČNOST HIKVISION NEPOSKYTUJE ŽÁDNOU ZÁRUKU TÝKAJÍCÍ SE POUŽÍVÁNÍ TÉTO PŘÍRUČKY A NERUČÍ ZA SPRÁVNOST, PŘESNOST ČI SPOLEHLIVOST INFORMACÍ V NÍ OBSAŽENÝCH. TUTO PŘÍRUČKU POUŽÍVÁTE A SPOLÉHÁTE SE NA NI ZCELA NA VLASTNÍ RIZIKO A ODPOVĚDNOST.

POUŽÍVÁNÍ PRODUKTU S PŘÍSTUPEM NA INTERNET JE ZCELA NA VAŠE VLASTNÍ RIZIKO. SPOLEČNOST HIKVISION NERUČÍ ZA ABNORMÁLNÍ FUNKCI, ÚNIK OSOBNÍCH ÚDAJŮ ANI ZA JINÉ ŠKODY VZNIKLE V DŮSLEDKU KYBERNETICKÉHO ÚTOKU, HACKERSKÉHO ÚTOKU, PŮSOBNÍ VIRU ČI JINÝCH BEZPEČNOSTNÍCH RIZIK SOUVISEJÍCÍCH S INTERNETEM.




SPOLEČNOST HIKVISION VŠAK PODLE POTŘEBY POSKYTNE VČASNOU TECHNICKOU POMOC.

ZÁKONY O DOHLEDU SE LIŠÍ PODLE SOUDNÍ PŘÍSLUŠNOSTI. PŘED POUŽITÍM TOHOTO VÝROBKU ZKONTROLUJTE VŠECHNY RELEVANTNÍ ZÁKONY PLATNÉ DLE VAŠÍ SOUDNÍ PŘÍSLUŠNOSTI, ABY BYLO ZAJIŠTĚNO, ŽE JEHO POUŽITÍ VYHOVUJE PLATNÝM ZÁKONŮM. SPOLEČNOST HIKVISION NENESE ODPOVĚDNOST ZA PŘÍPADY POUŽITÍ TOHOTO VÝROBKU PRO NELEGITIMNÍ ÚČELY.

V PŘÍPADĚ ROZPORU MEZI TOUTO PŘÍRUČKOU A PLATNÝMI ZÁKONY PLATÍ TYTO ZÁKONY.

Ujednání o symbolech

V tomto dokumentu se nacházejí níže uvedené symboly.

Symbol	Popis
 Nebezpečí	Označuje nebezpečnou situaci, která bude nebo může mít za následek smrt nebo vážné zranění, jestliže jí nezabráníte.
 Pozor	Označuje potenciálně nebezpečnou situaci, která může mít za následek poškození zařízení, ztrátu dat, zhoršení funkčnosti nebo neočekávané následky, jestliže jí nezabráníte.
 Poznámka	Obsahuje další informace ke zdůraznění či doplnění důležitých bodů v hlavním textu.

Obsah

1	Přehled základních informací	1
2	Přístup k softwaru iVMS-4200/webovému klientu	2
2.1	Popis aktivace.....	2
2.1.1	Aktivace zařízení prostřednictvím softwaru iVMS-4200	3
2.1.2	Aktivace prostřednictvím softwaru SADP	4
2.1.3	Aktivace zařízení prostřednictvím webového prohlížeče	5
2.2	Nastavení sítě.....	6
2.2.1	Kabelová síť.....	6
2.2.2	Wi-Fi.....	7
2.2.3	Mobilní síť.....	8
2.2.4	Hik-Connect	9
2.3	Nastavení alarmu	11
2.3.1	Pult centralizované ochrany	11
2.3.2	Zasílání oznámení	12
2.3.3	Zóna	12
2.3.4	Časový plán alarmů.....	15
2.3.5	Výstup	17
2.3.6	Siréna	19
2.3.7	Opakovač	20
2.4	Správa vizuálního obsahu	21
2.4.1	Přidání kamer do bezpečnostního ovládacího panelu	21
2.4.2	Propojení kamery se zónou	22

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

2.4.3	Nastavení e-mailu pro příjem videa s alarmem	23
2.4.4	Nastavení parametrů videa	24
2.5	Správa oprávnění	25
2.5.1	Přidání/úprava/odstranění uživatele	25
2.5.2	Přidání/úprava/odstranění klíčenky	27
2.5.3	Přidání/úprava/odstranění karty	29
2.6	Nastavení systému	29
2.6.1	Nastavení systému	29
2.6.2	Zabezpečení	31
2.6.3	Zabezpečení	32
2.6.4	Prohledání místního protokolu	33
2.7	Dotaz	33
2.7.1	Stav	33
2.8	Obsluha bezpečnostního ovládacího panelu	34
2.8.1	Ovládání příčky	34
2.8.2	Ovládání zóny	35
3	Správa bezpečnostního ovládacího modulu prostřednictvím mobilního klienta	36
3.1	Stažení a přihlášení mobilního klienta	36
3.2	Přidání ovládacího panelu do mobilního klienta	36
3.3	Přidání periferie do ovládacího panelu	39
3.4	Nastavení zóny	40
3.5	Přidání kamery do zóny	42
3.6	Aktivace/deaktivace zabezpečení zóny	43

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

3.7 Nastavení časového plánu aktivace/deaktivace zabezpečení	44
3.8 Zóna bypassu	45
3.9 Přidání karty	46
3.10 Přidání klíčenky	48
3.11 Kontrola oznámení o alarmu	48
3.12 Kontrola stavu systému (stav zóny / stav komunikace)	50

1 Přehled základních informací

Bezpečnostní ovládací panel Axiom obsahující 32 bezdrátových zón podporuje komunikaci prostřednictvím Wi-Fi, TCP/IP a 3G/4G. Dále podporuje technologie ISAPI, Hik-Connect, Contact ID a NAL2300, které platí pro prostředí trhu, prodejny, domu, továrny, skladu, kanceláře atd.

- síť TCP/IP, Wi-Fi, 3G/4G
- připojení až 32 bezdrátových zón, 32 bezdrátových výstupů, 8 bezdrátových klíčenek, 4 relé, 2 opakovačů, 2 sirén
- Podporuje až 13 síťových uživatelů, včetně 1 instalátora, 1 administrátora a 11 běžných uživatelů.
- Podporuje funkci domovního zvonku: Detektor po spuštění ve stavu s vypnutým zabezpečením zvoní jako domovní zvonek.
- hlasové pokyny
- režim Wi-Fi AP
- konfigurace prostřednictvím webového klienta nebo mobilního klienta
- Zasílá oznámení o alarmu prostřednictvím zpráv nebo telefonicky.

Poznámka

Tuto funkci podporují jen zařízení s komunikační metodou 3G/4G.

- Zobrazuje živé videozáběry a zasílá e-maily či videa o alarmech přes mobilního klienta.
- Nahrává zprávy na pult centralizované ochrany.
- obousměrná dálková komunikace se šifrováním ve standardu AES-128
- podpora kontrolky LED pro indikaci stavu systému
- lithiová záložní baterie 4520 mAh pro napájení po dobu až 12 h

2 Přístup k softwaru iVMS-4200/webovému klientu

Můžete se přihlásit ke klientskému softwaru iVMS-4200 nebo webovému klientu a konfigurovat parametry zařízení. Přes webového klienta je dále možné konfigurovat síťové parametry bezpečnostního ovládacího panelu, alarm, oprávnění, systém a vyhledávání v protokolu.

Poznámka

Zařízení je nutné z bezpečnostních důvodů při prvním přístupu do sítě aktivovat. Podrobnosti viz část **Aktivace zařízení**.

Přístup ke klientskému softwaru iVMS-4200

Software si stáhněte a nainstalujte. Zaregistrujte se do softwaru a přidejte zařízení v okně **Control Panel** → **Device Management** → **Device for Management**.

Poznámka

- Číslo portu zařízení nastavte na 80.
 - Uživatelské jméno a heslo použité při přidání zařízení jsou aktivační uživatelské jméno a heslo.
-

Když dokončíte přidání zařízení, kliknutím na **Remote Configuration** otevřete stránku pro konfiguraci zařízení. Na této stránce můžete konfigurovat parametry zařízení.

Přístup k webovému klientu

Po připojení zařízení k síti můžete vyhledat IP adresu zařízení pomocí klientského softwaru iVMS-4200 a softwaru SADP. Zadejte hledanou IP adresu do adresního řádku na webové stránce a stiskněte tlačítko **Enter**. Přihlaste se pomocí aktivačního uživatelského jména a hesla. Na této webové stránce můžete konfigurovat parametry zařízení.

2.1 Popis aktivace

Za účelem ochrany osobních údajů a soukromí a zvýšení úrovně zabezpečení sítě byste měli zařízení při jeho prvním připojení k síti aktivovat.

Na ochranu svého zařízení před přihlášením jiných osob můžete vytvořit aktivační heslo.

2.1.1 Aktivace zařízení prostřednictvím softwaru iVMS-4200

iVMS-4200 je klientský software pro správu a ovládání vašich zařízení. Tento software podporuje aktivaci bezpečnostního ovládacího panelu.

Než začnete

- Klientský software je na dodaném disku nebo na oficiálním webu <http://www.hikvision.com/en/>. Software nainstalujte podle následujících pokynů.
- Zařízení a počítač se softwarem by měly být ve stejné podsíti.

Postup

1. Spusťte klientský software.
2. Zadejte **Device Management** nebo **Online Device**.
3. V seznamu zařízení zaškrtněte stav zařízení a vyberte neaktivní zařízení.
4. Klikněte na možnost **Activate**.
5. Vytvořte a potvrďte administrátorské heslo pro zařízení.



DOPORUČUJE SE POUŽÍT SILNÉ HESLO – Důrazně doporučujeme vytvořit silné heslo dle svého výběru (minimálně 8 znaků obsahujících velká písmena, malá písmena, čísla a zvláštní znaky) pro lepší zabezpečení svého výrobku. Dále doporučujeme toto heslo pravidelně obměňovat, zvláště v systému s vysokým zabezpečením. Lepší ochranu vašeho výrobku zajistí obměna hesla jednou za měsíc nebo za týden.

6. Kliknutím na **OK** spusťte aktivaci.
Stav zařízení se po úspěšné aktivaci změní na **Active**.
7. Změňte IP adresu zařízení.
 - 1) Vyberte zařízení a klikněte na možnost **Modify Netinfo** u položky **Online Device**.
 - 2) Změňte IP adresu na stejnou podsít, v níž je váš počítač, buďto změnou IP adresy ručně nebo zaškrtnutím možnosti **DHCP**.
 - 3) Zadejte administrátorské heslo zařízení a kliknutím na **OK** změnu dokončete.

2.1.2 Aktivace prostřednictvím softwaru SADP

SADP je nástroj pro detekci, aktivaci a změnu IP adresy zařízení po síti LAN.

Než začnete

- Software SADP je na dodaném disku nebo na oficiálním webu <http://www.hikvision.com/en/>. Proveďte instalaci SADP podle pokynů.
- Zařízení a počítač s nástrojem SADP by měly být ve stejné podsíti.

Následující postup popisuje způsob aktivace zařízení a změnu jeho IP adresy. V případě dávkové aktivace a změny IP adres si podrobnosti přečtete v *Uživatelské příručce k softwaru SADP*.

Postup

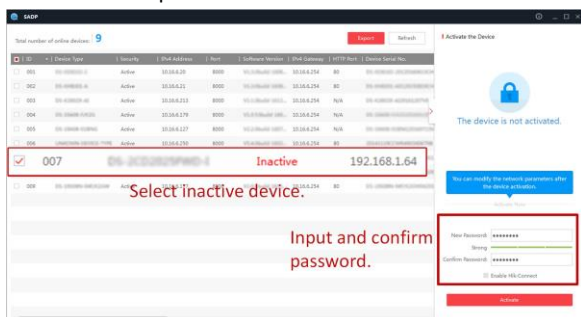
1. Spustíte software SADP a vyhledejte online zařízení.
2. Najděte a vyberte své zařízení v seznamu online zařízení.
3. Zadejte nové heslo (administrátorské heslo) a potvrďte je.



Pozor

DOPORUČUJE SE POUŽÍT SILNÉ HESLO – Důrazně doporučujeme vytvořit silné heslo dle svého výběru (minimálně 8 znaků obsahujících velká písmena, malá písmena, čísla a zvláštní znaky) pro lepší zabezpečení svého výrobku. Dále doporučujeme toto heslo pravidelně obměňovat, zvláště v systému s vysokým zabezpečením. Lepší ochranu vašeho výrobku zajistí obměna hesla jednou za měsíc nebo za týden.

4. Kliknutím na **Activate** spustíte aktivaci.



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

5. Změňte IP adresu zařízení.
 - 1) Vyberte zařízení.
 - 2) Změňte IP adresu na stejnou podsíť, v níž je váš počítač, buďto změnou IP adresy ručně nebo zaškrtnutím možnosti **Enable DHCP**.
 - 3) Zadejte administrátorské heslo a kliknutím na možnost **Modify** aktivujte změnu své IP adresy.

2.1.3 Aktivace zařízení prostřednictvím webového prohlížeče

Zařízení můžete aktivovat pomocí webového prohlížeče. Online zařízení vyhledejte pomocí softwaru SADP klientského počítače, získejte IP adresu zařízení a aktivujte je na webové stránce.

Než začnete

Ověřte, že zařízení a počítač jsou připojeny na stejnou síť LAN.

Postup

1. Otevřete webový prohlížeč a zadejte IP adresu zařízení.

Poznámka

Pokud zařízení propojíte s počítačem přímo, musíte změnit IP adresu počítače na stejnou podsíť, na níž je zařízení. Výchozí IP adresa zařízení je 192.0.0.64.

2. Vytvořte a potvrďte administrátorské heslo.

Pozor

DOPORUČUJE SE POUŽÍT SILNÉ HESLO – Důrazně doporučujeme vytvořit silné heslo dle svého výběru (minimálně 8 znaků obsahujících velká písmena, malá písmena, čísla a zvláštní znaky) pro lepší zabezpečení svého výrobku. Dále doporučujeme toto heslo pravidelně obměňovat, zvláště v systému s vysokým zabezpečením. Lepší ochranu vašeho výrobku zajistí obměna hesla jednou za měsíc nebo za týden.

3. Kliknutím na **OK** dokončete aktivaci a otevřete stránku **Live View**.
4. Změňte IP adresu zařízení.
 - 1) Otevřete stránku pro změnu IP adresy. **Configuration** → **Network** → **TCP/IP**.
 - 2) Změňte IP adresu.
 - 3) Uložte nastavení.

2.2 Nastavení sítě

2.2.1 Kabelová síť

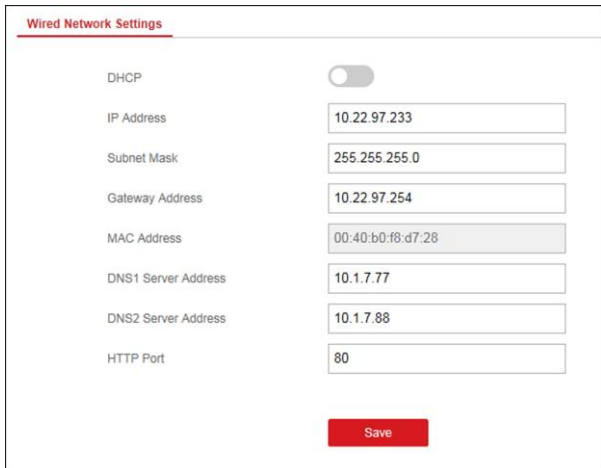
Je-li zařízení připojeno ke kabelové síti, můžete nastavit parametry kabelové sítě, až budete chtít změnit IP adresu a další parametry sítě.

Postup

Poznámka

Tuto funkci některé modely zařízení nepodporují.

1. Kliknutím na položku **Communication Parameters** → **Wired Network Parameters** otevřete stránku Wired Network Parameters.



DHCP	<input type="checkbox"/>
IP Address	<input type="text" value="10.22.97.233"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway Address	<input type="text" value="10.22.97.254"/>
MAC Address	<input type="text" value="00:40:b0:f8:d7:28"/>
DNS1 Server Address	<input type="text" value="10.1.7.77"/>
DNS2 Server Address	<input type="text" value="10.1.7.88"/>
HTTP Port	<input type="text" value="80"/>

Obrázek 2-1. Stránka Wired Network Settings

2. Nastavte parametry.
 - Automatické nastavení: Povolte možnost **DHCP** a nastavte port HTTP.
 - Ruční nastavení: Zakažte možnost **DHCP** a nastavte položky **IP Address**, **Subnet Mask**, **Gateway Address**, **DNS Server Address**.

Poznámka

Port HTTP je ve výchozím nastavení 80, což není editovatelné.

- 3. Volitelně:** Nastavte správnou adresu serveru DNS, pokud zařízení musí mít přístup k serveru Hik-Connect prostřednictvím názvu domény.
- 4.** Klikněte na tlačítko **Save**.

2.2.2 Wi-Fi

Parametry Wi-Fi můžete nastavit, pokud jsou v okolí zabezpečené a důvěryhodné sítě Wi-Fi.

Postup

- Klikněte na položku **Communication Parameters → Wi-Fi Parameters**.
- Kliknutím na **Wi-Fi** otevřete stránku Wi-Fi.
- Připojte se k síti Wi-Fi.
 - Ruční připojení: Zadejte název sítě Wi-Fi a heslo pro Wi-Fi a klikněte na tlačítko **Save**.
 - Ze seznamu sítí vyberte: Ze seznamu sítí vyberte cílovou síť Wi-Fi. Klikněte na **Connect** a zadejte heslo sítě Wi-Fi a klikněte na **Connect**.
- Kliknutím na **WLAN** otevřete stránku WLAN.

Wi-Fi	WLAN
DHCP :	<input type="checkbox"/>
IP Address	<input type="text" value="10.22.97.237"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway Address	<input type="text" value="10.22.97.254"/>
MAC Address	<input type="text" value="00:95:69:f0:9b:35"/>
DNS1 Server Address	<input type="text" value="10.1.7.77"/>
DNS2 Server Address	<input type="text" value="10.1.7.88"/>
<input type="button" value="Save"/>	

Obrázek 2-3. Stránka WLAN Settings

- 5.** Nastavte **IP Address**, **Subnet Mask**, **Gateway Address** a **DNS Server Address**.

Poznámka

Je-li možnost DHCP aktivní, zařízení si opatří parametry Wi-Fi automaticky.

- 6.** Klikněte na tlačítko **Save**.

2.2.3 Mobilní síť

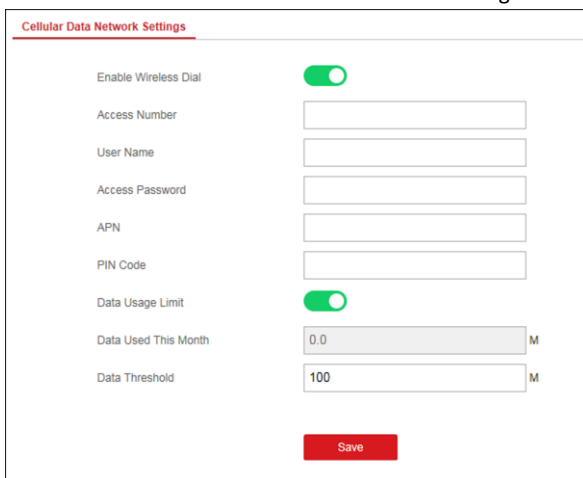
Pokud jste do zařízení vložili SIM kartu, nastavte parametry mobilní sítě. Při použití mobilní sítě může zařízení odesílat oznámení o alarmech na pult centralizované ochrany.

Než začnete

Do zdířky na SIM kartu v zařízení vložte SIM kartu.

Postup

1. Kliknutím na položku **Communication Parameters** → **Cellular Data Network Parameters** otevřete stránku Cellular Data Network Settings.



The screenshot shows the 'Cellular Data Network Settings' interface. At the top, there is a red header with the text 'Cellular Data Network Settings'. Below this, there are several settings:

- Enable Wireless Dial:** A green toggle switch is turned on.
- Access Number:** An empty text input field.
- User Name:** An empty text input field.
- Access Password:** An empty text input field.
- APN:** An empty text input field.
- PIN Code:** An empty text input field.
- Data Usage Limit:** A green toggle switch is turned on.
- Data Used This Month:** A slider control showing '0.0' on the left and 'M' on the right.
- Data Threshold:** A text input field containing the number '100' and a small 'M' unit indicator to the right.

At the bottom center of the form is a red button labeled 'Save'.

Obrázek 2-4. Stránka Cellular Data Network Settings

2. Povolte možnost Wireless Dial.
3. Nastavte parametry mobilní datové sítě.

Access Number

Zadejte vytáčené přístupové číslo operátora.

User Name

Od provozovatele sítě si vyžádejte uživatelské jméno a zadejte jej.

Access Password

Od provozovatele sítě si vyžádejte přístupové heslo a zadejte jej.

APN

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

Od provozovatele sítě si vyžádejte údaje k APN a zadejte je.

Data Usage Limit

Funkci omezení pro používání dat můžete povolit a každý měsíc nastavovat prahovou hodnotu pro data. Bude-li používání dat větší než konfigurovaná prahová hodnota, spustí se alarm, který bude odeslán na pult centralizované ochrany.

Data Used This Month

Data používaná tento měsíc se shromažďují a zobrazí se v tomto textovém okně.

4. Klikněte na tlačítko **Save**.

2.2.4 Hik-Connect

Chcete-li zařízení zaregistrovat k mobilnímu klientu Hik-Connect pro vzdálenou konfiguraci, je nutné nastavit parametry registrace pro Hik-Connect.

Než začnete

- Zařízení připojte k síti prostřednictvím kabelového připojení, vytáčeného připojení nebo Wi-Fi připojení.
- Nastavte IP adresu zařízení, masku podsítě, bránu a server DNS v síti LAN.

Postup

1. Kliknutím na položku **Communication Parameters** → **Hik-Connect Registration Parameters** otevřete stránku Hik-Connect Registration Settings.

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

Hik-Connect Adding Settings

Register to Hik-Connect

Hik-Connect Adding Status Online

Custom Server Address

Server Address dev.sgp.ezviz7.com

Communication Mode Wired Network Priority

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)

Save

Obrázek 2-5. Stránka Hik-Connect Registration Settings

2. Zaškrtněte možnost **Register to Hik-Connect**.

Poznámka

Ve výchozím nastavení je povolena služba Hik-Connect.

Můžete zobrazit stav zařízení na serveru Hik-Connect.

3. Povolte možnost **Custom Server Address**.
Adresa serveru se zobrazí v textovém poli Server Address.
4. Z rozbalovacího seznamu vyberte režim komunikace podle skutečného způsobu komunikace vašeho zařízení.

Auto

System vybere režim komunikace automaticky v pořadí kabelová síť, síť Wi-Fi a mobilní datová síť.

Wired Network Priority

System vybere pouze kabelovou síť.

Wired & Wi-Fi

System vybere nejdříve kabelovou síť. Není-li žádná kabelová síť zjištěna, vybere síť Wi-Fi.

Cellular Data Network

System vybere pouze mobilní datovou síť.

5. **Volitelně:** Změňte ověřovací heslo.

 **Poznámka**

- Ověřovací heslo se ve výchozím nastavení zobrazí v textovém poli.
- Ověřovací heslo by mělo obsahovat 6 až 12 písmen nebo číslic. Z bezpečnostních důvodů se doporučuje 8místné heslo obsahující dva a více těchto druhů znaků: velká písmena, malá písmena a číslice.

6. Klikněte na tlačítko **Save**.

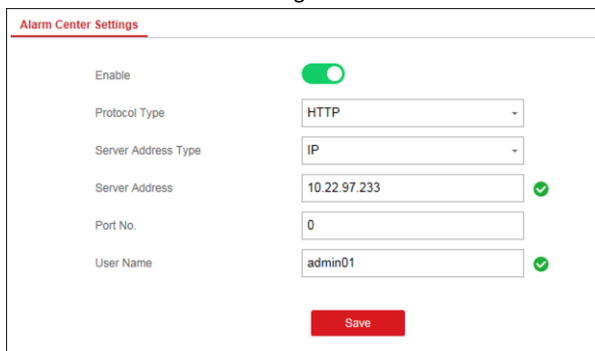
2.3 Nastavení alarmu

2.3.1 Pult centralizované ochrany

Parametry pultu centralizované ochrany můžete nastavit. Všechny alarmy pak budou odesílány na nakonfigurovaný pult centralizované ochrany.

Postup

1. Kliknutím na položku **Communication Parameters** → **Alarm Center Parameters** otevřete stránku Alarm Center Settings.




Enable	<input checked="" type="checkbox"/>
Protocol Type	HTTP
Server Address Type	IP
Server Address	10.22.97.233 ✓
Port No.	0
User Name	admin01 ✓

Save

Obrázek 2-6. Parametry pultu centralizované ochrany

2. Z rozevřacího seznamu vyberte typ protokolu, typ adresy serveru, nastavte adresu serveru, číslo portu a uživatelské jméno.

 **Poznámka**

Typ protokolu HTTP je privátní protokol Hikvision.

3. Klikněte na tlačítko **Save**.

2.3.2 Zasílání oznámení

Pokud po spuštění alarmu chcete odeslat oznámení o alarmu do klientského zařízení, na pult centralizované ochrany, cloudu nebo mobilního klienta, můžete nastavit parametry zasílání oznámení.

Postup

1. Klikněte na položku **Communication Parameters → Message Notification**.
2. Povolte cílové oznámení.

Alarm and Tampering Event Notification

Zařízení bude odesílat oznámení při spuštění alarmu zóny nebo po spuštění či obnovení alarmu neoprávněné manipulace.

Safety Event Notification


Zařízení bude odesílat oznámení při spuštění požárního alarmu, plynového alarmu nebo zdravotního alarmu.

System Status Notification

Zařízení bude odesílat oznámení v případě změny stavu systému.

Operation Event Notification

Zařízení bude odesílat oznámení při každé činnosti ovládní zařízení uživatelem.

 **Poznámka**

Chcete-li odesílat oznámení o alarmech do mobilního klienta, musíte také nastavit položky **Mobile Phone Index**, **SIM Card No.** a zaškrtnout **Notification Type**.

3. Klikněte na tlačítko **Save**.

2.3.3 Zóna

Na stránce se zónami můžete nastavit parametry zón.

Postup

1. Kliknutím na položku **Wireless Device → Zone** otevřete stránku Zone.

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

Zone Management							
Zone	Name	Type	Stay Arming Bypass	Mute	Doorbell	Link Wireless Detector	Settings
1	wirelessZone1	Panic Zone	Disable	Disable	Disable	Link	
2	wirelessZone2	24H Silent Z...	Disable	Disable	Disable	Link	
3	wirelessZone3	Instant Zone	Disable	Disable	Disable	Not Linked	
4	wirelessZone4	Instant Zone	Disable	Disable	Disable	Not Linked	
5	wirelessZone5	Instant Zone	Disable	Disable	Disable	Not Linked	
6	wirelessZone6	Instant Zone	Disable	Disable	Disable	Not Linked	
7	wirelessZone7	Instant Zone	Disable	Disable	Disable	Not Linked	
8	wirelessZone8	Instant Zone	Disable	Disable	Disable	Not Linked	
9	wirelessZone9	Instant Zone	Disable	Disable	Disable	Not Linked	
10	wirelessZone10	Instant Zone	Disable	Disable	Disable	Not Linked	
11	wirelessZone11	Instant Zone	Disable	Disable	Disable	Not Linked	
12	wirelessZone12	Instant Zone	Disable	Disable	Disable	Not Linked	
13	wirelessZone13	Instant Zone	Disable	Disable	Disable	Not Linked	

Obrázek 2-7. Stránka Zone

2. Vyberte zónu a kliknutím na otevřete stránku Zone Settings.
3. Upravte název zóny.
4. Vyberte typ zóny.

Instant Zone

Systém ihned spustí alarm, jakmile po aktivaci zabezpečení detekuje spouštějící událost. Detektory mohou být nastaveny na tento typ například v supermarketu.

Delayed Zone

Exit Delay: Exit Delay poskytuje určitý čas pro odchod chráněným prostorem bez spuštění alarmu.

Entry Delay: Entry Delay poskytuje určitý čas pro příchod chráněným prostorem a deaktivaci zabezpečovacího systému bez spuštění alarmu.

Systém poskytne čas prodlevy pro příchod/odchod, když je aktivovaný nebo při opětovném vstupu. Obvykle se používá na cestě ke vchodu/východu (např. u vstupních dveří / hlavního vchodu), která je hlavní trasou pro aktivaci/deaktivaci zabezpečení uživatelem z klávesnice.

Poznámka

Délku času prodlevy můžete nastavit v okně **System → Schedule & Timer**.

Follow Zone

Tato zóna se chová stejně jako Delayed Zone, když zjistí spouštějící událost v době Entry Delay, ale ve všech ostatních případech se chová jako Instant Zone. Obvykle se nastavuje v obývacím pokoji nebo hale zároveň se zónami perimetru s časem prodlevy.

Perimeter Zone

Systém ihned spustí alarm, jakmile po aktivaci zabezpečení detekuje spouštějící událost. Mezi spuštěním alarmu a spuštěním zvuku sirény je nastavitelný interval, který umožňuje zkontrolovat alarm a zrušit sirénu v případě falešného poplachu. Obvykle se používá v oblasti perimetru, například u dveří a oken.

Když je aktivované zabezpečení zóny, můžete nastavit čas zpoždění pro alarm perimetru v okně **System → Schedule & Timer**. V době prodlevy také můžete vypnout zvuk sirény.

24H Silent Zone

Zóna je aktivovaná stále, ale pokud dojde k alarmu, neozve se žádný zvukový výstup/siréna. Obvykle se používá v místech vybavených panikovým tlačítkem (např. v bance, zlatnictví).

Panic Zone

Zóna je aktivována stále. Obvykle se používá v místech vybavených panikovým tlačítkem, detektorem kouře a detektorem rozbití skla.

Fire Zone

Zóna je aktivovaná stále, a pokud dojde k alarmu, ozve se zvukový výstup/siréna. Obvykle se používá v prostorech s nebezpečím požáru vybavených detektory kouře a teplotními čidly.

Combustible Gas Zone

Zóna je aktivovaná stále, a pokud dojde k alarmu, ozve se zvukový výstup/siréna. Obvykle se používá v prostorech vybavených detektory plynu (např. v kuchyni).

Medical Zone

Zóna je aktivovaná stále. Když dojde k alarmu, je potvrzen pípnutím. Obvykle se používá v místech vybavených tlačítky pro přivolání neodkladné lékařské péče.


Timeout Zone

Zóna je aktivována stále. Spustí alarm, když dojde k definované události v nastavené době. Obvykle se používá v místech vybavených magnetickými kontakty (např. na dvířkách požárního hydrantu).

Shield Zone

Alarmy se při narušení zóny neaktivují. Obvykle se používají k deaktivaci vadných detektorů.

5. Podle skutečných potřeb povolte možnosti **Stay Arming Bypass**, **Doorbell**, nebo **Mute**.

 **Poznámka**

Některé zóny tuto funkci nepodporují. Při nastavování funkce si přečtěte údaje o dané zóně.

6. Povolte možnost **Link Wireless Detector**, zadejte sériové číslo a nastavte číslo připojené kamery.
 7. Klikněte na **OK**.
-

 **Poznámka**

Po nastavení zóny můžete otevřít okno **Status → Zone** a zobrazit stav zóny.

2.3.4 Časový plán alarmů

V zónách s časem prodlevy můžete nastavit délku prodlevy a dobu pro opuštění zóny. Také můžete nastavit plán alarmů. Zabezpečení zón se bude aktivovat/deaktivovat podle nastaveného časového plánu.

Postup

1. Kliknutím na položku **System → Schedule & Timer** otevřete stránku Schedule & Timer.

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

Schedule & Timer Management

Delay 1	<input type="text" value="30"/>	s
Delay 2	<input type="text" value="60"/>	s
Exit Delay	<input type="text" value="60"/>	s
Auto Arming	<input type="checkbox"/>	
	Time	<input type="text" value="00:00"/>
Auto Disarming	<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"/>	
Perimeter Alarm Delayed Time	<input type="text" value="60"/>	s
Alarm Duration	<input type="text" value="60"/>	s

Obrázek 2-8 Stránka Schedule & Timer

2. Nastavte dobu **Delay 1**, **Delay 2**, případně **Exit Delay**.
Delay 1/Delay 2

Pokud jste nastavili zónu s časovou prodlevou, zde můžete nastavit délku této prodlevy.

Poznámka

Tuto dobu můžete nastavit v rozsahu od 5 s do 600 s.

Exit Delay


Chcete-li zónu opustit bez spuštění alarmu, můžete nastavit dobu prodlevy pro odchod.

Poznámka

Tuto dobu můžete nastavit v rozsahu od 5 s do 600 s.

3. **Volitelně:** Následující parametry nastavte podle svých skutečných potřeb.
Auto Arming

Povolte funkci automatické aktivace zabezpečení a nastavte dobu aktivace zabezpečení. Zabezpečení zón se bude aktivovat podle nastaveného času.

 **Poznámka**

Čas automatické aktivace a deaktivace zabezpečení nesmí být stejný.

Auto Disarming

Povolte funkci automatické deaktivace zabezpečení a nastavte dobu deaktivace zabezpečení. Zabezpečení zón se bude deaktivovat podle nastaveného času.

 **Poznámka**

Čas automatické aktivace a deaktivace zabezpečení nesmí být stejný.

Late to Disarm

Povolte funkci pozdní deaktivace zabezpečení a nastavte příslušnou dobu. Bude-li alarm spuštěn po nastavené době, příchod dotyčné osoby se bude považovat za zpoždění.

 **Poznámka**

Před povolením funkce Late to Disarm byste měli povolit funkci Operation Event Notification v okně **Communication Parameters** → **Message Notification**.

Weekend Exception

Když povolíte tuto funkci, zóna nebude o víkendu zabezpečena.

Perimeter Alarm Delayed Time


Pokud jste nastavili zónu perimetru, můžete nastavit dobu prodlevy pro tuto zónu.

 **Poznámka**

Tuto dobu můžete nastavit v rozsahu od 0 s do 600 s.

Alarm Duration

Nastavte dobu trvání alarmu.

 **Poznámka**

Tuto dobu můžete nastavit v rozsahu od 5 s do 600 s.

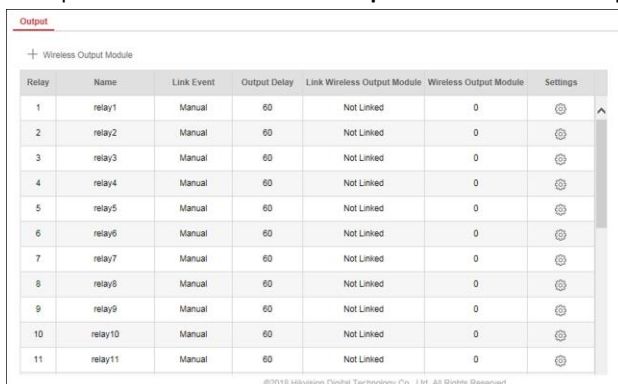
4. Klikněte na tlačítko **Save**.

2.3.5 Výstup

Chcete-li zařízení propojit s reléovým výstupem pro výstup alarmu, nastavte parametry výstupu.

Postup

1. Kliknutím na položku **Wireless Device** → **Output** otevřete stránku Output.



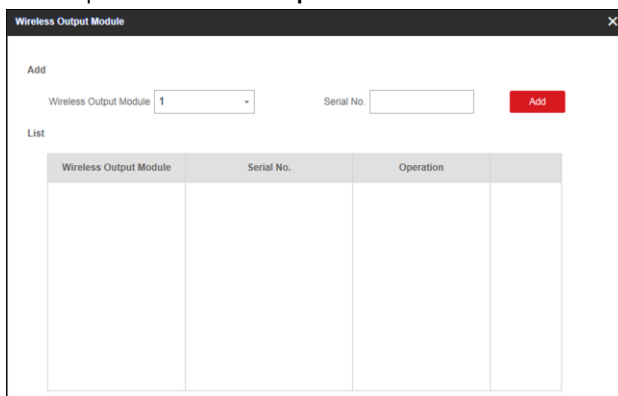
Relay	Name	Link Event	Output Delay	Link Wireless Output Module	Wireless Output Module	Settings
1	relay1	Manual	60	Not Linked	0	⚙️
2	relay2	Manual	60	Not Linked	0	⚙️
3	relay3	Manual	60	Not Linked	0	⚙️
4	relay4	Manual	60	Not Linked	0	⚙️
5	relay5	Manual	60	Not Linked	0	⚙️
6	relay6	Manual	60	Not Linked	0	⚙️
7	relay7	Manual	60	Not Linked	0	⚙️
8	relay8	Manual	60	Not Linked	0	⚙️
9	relay9	Manual	60	Not Linked	0	⚙️
10	relay10	Manual	60	Not Linked	0	⚙️
11	relay11	Manual	60	Not Linked	0	⚙️

©2016 Hikvision Digital Technology Co., Ltd. All Rights Reserved.

Obrázek 2-9. Stránka Output

2. Přidejte modul bezdrátového výstupu.

- 1) Klikněte na položku **Wireless Output Module**.



Wireless Output Module


Add

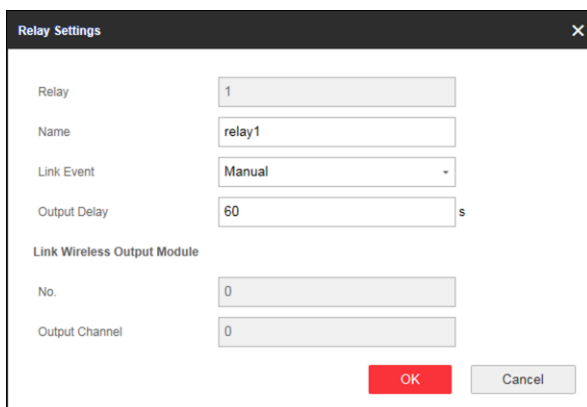
Wireless Output Module: 1 - Serial No.: **Add**

List

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

Obrázek 2-10. Nastavení modulu bezdrátového výstupu

- 2) Z rozbalovacího seznamu vyberte číslo modulu bezdrátového výstupu.
 - 3) Zadejte sériové číslo modulu bezdrátového výstupu.
 - 4) Klikněte na tlačítko **Add**.
3. Klikněte na  a zobrazí se okno Relay Settings.



Relay Settings

Relay: 1

Name: relay1

Link Event: Manual

Output Delay: 60 s

Link Wireless Output Module

No.: 0

Output Channel: 0

OK Cancel


Obrázek 2-11. Stránka Relay Settings

4. Upravte název relé, vyberte událost propojení a nastavte dobu trvání časové prodlevy výstupu.

 **Poznámka**

Je-li relé propojeno s modulem bezdrátového výstupu, informace o tomto modulu se zobrazí v oblasti Link Wireless Output Module.

5. Klikněte na **OK**.

 **Poznámka**

Po nastavení relé můžete kliknutím na položku **Status → Relay** zobrazit stav výstupu.

2.3.6 Siréna

Chcete-li bezpečnostní ovládací panel propojit se sirénou, která upozorní na spuštění alarmu, můžete nastavit parametry sirény.


Postup

1. Kliknutím na položku **Wireless Device → Siren** otevřete stránku Siren.

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

Siren Management				
Siren	Name	Volume	Link Wireless Siren	Settings
1	siren1	0	Not Linked	
2	siren2	0	Not Linked	

Obrázek 2-12. Stránka Siren

2. Kliknutím na  otevřete stránku Siren Settings.
3. Nastavte název sirény a hlasitost.



Poznámka

Hlasitost sirény můžete nastavit v rozsahu od 0 do 3.

4. **Volitelně:** Povolte možnost **Link Wireless Siren** a nastavte sériové číslo sirény.



Poznámka

Některé detektory tuto funkci nemusí podporovat.

5. Klikněte na **OK**.



Poznámka

Po nastavení sirény můžete kliknutím na položku **Status** → **Siren** zobrazit stav sirény.

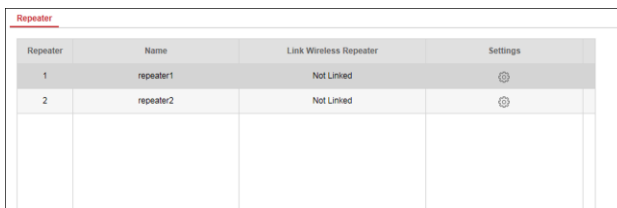
2.3.7 Opakovač

Je-li detektor od ovládacího panelu příliš vzdálen, nastavte parametry opakovače pro zesílení signálu.

Postup


1. Kliknutím na položku **Wireless Device** → **Repeater** otevřete stránku Repeater.

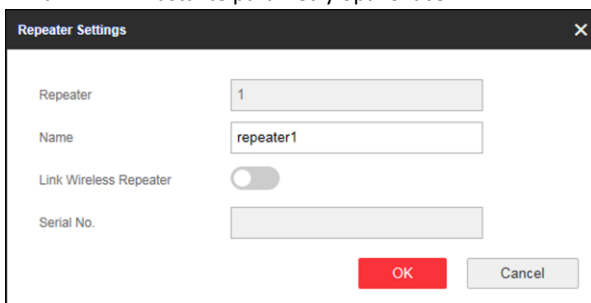
Uživatelská příručka pro bezpečnostní ovládací panel Axiom



Repeater	Name	Link Wireless Repeater	Settings
1	repeater1	Not Linked	⚙️
2	repeater2	Not Linked	⚙️

Obrázek 2-13. Stránka Repeater

2. Kliknutím na  nastavte parametry opakováče.



Repeater Settings

Repeater: 1

Name: repeater1

Link Wireless Repeater:

Serial No.:

OK Cancel

Obrázek 2-14. Nastavení opakováče

3. Upravte název opakováče.
4. Povolte možnost **Link Wireless Repeater** a zadejte sériové číslo opakováče.
5. Klikněte na **OK**.

Poznámka

Po nastavení opakováče můžete otevřít okno **Status** → **Repeater** a zobrazit stav opakováče.

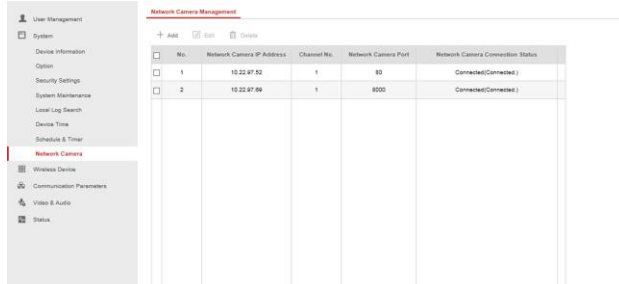
2.4 Správa vizuálního obsahu

K bezdrátovému bezpečnostnímu ovládacímu panelu můžete přidat dvě síťové kamery a propojit je s vybranou zónou monitorovanou pomocí videa. Video s událostí můžete také zobrazit v klientském zařízení a e-mailu.

2.4.1 Přidání kamer do bezpečnostního ovládacího panelu

Postup

1. Kliknutím na položku **System** → **Network Camera** otevřete stránku pro správu síťových kamer.



Obrázek 2-15. Správa síťových kamer

2. Klikněte na tlačítko **Add** a zadejte základní informace o kameře, například její název, IP adresu a číslo portu.
3. Zadejte uživatelské jméno a heslo pro kameru.
4. Klikněte na tlačítko **Save**.



Poznámka

Do bezdrátového bezpečnostního ovládacího panelu můžete přidat dvě síťové kamery.

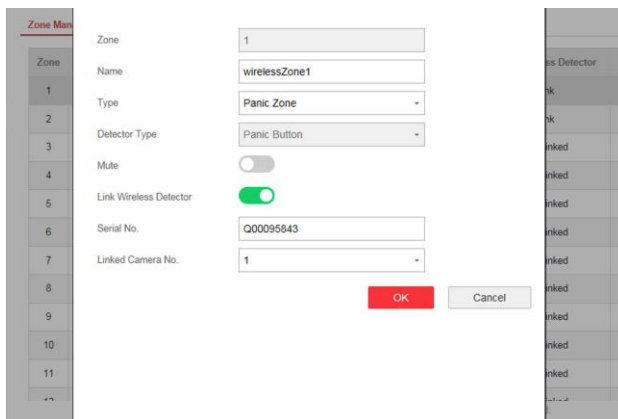
1. **Volitelně:** Kliknutím na tlačítko **Edit** nebo **Delete** můžete zvolenou kameru upravit nebo smazat.

2.4.2 Propojení kamery se zónou

Postup

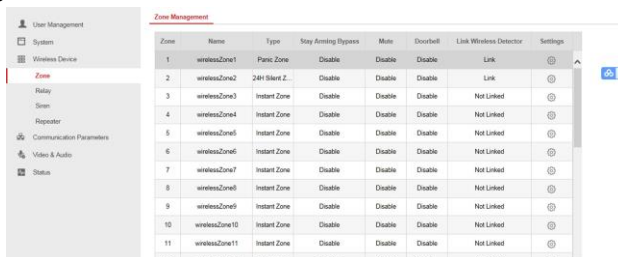
1. Kliknutím na položku **Wireless Device** → **Zone** otevřete stránku pro konfiguraci.

Uživatelská příručka pro bezpečnostní ovládací panel Axiom



Obrázek 2-16. Správa zón

2. Vyberte zónu, kterou chcete monitorovat pomocí videa, a klikněte na ikonu **Settings**.



Obrázek 2-17. Konfigurace zóny

3. Vyberte položku **Linked Camera No.**
4. Klikněte na **OK**.

2.4.3 Nastavení e-mailu pro příjem videa s alarmem

Postup

1. Kliknutím na položku **Communication Parameters** → **Event Video Transfer via Email** otevřete příslušnou stránku.

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

Event Video Transfer via Email Settings

Event Video Transfer via Email

Sender Name: vixover6

Sender: vixover6@hiktest.com

SMTP Server address: mail.hiktest.com

SMTP Port: 465

Encryption Type: SSL

Server Authentication:

User Name: vixover6

Password: *****

Confirm Password: *****

Receiver Name: yuhu7

Receiver: yuhu7@hikvision.com

Receiver Address Test

Save

Obrázek 2-18. Přenos videa s událostí e-mailem

2. Kliknutím na příslušný blok tuto funkci povolíte.
3. Zadejte údaje o odesílateli.
4. Zadejte údaje o příjemci.
5. Klikněte na položku **Receiver Address Test** a ověřte, zda je adresa správná.
6. Klikněte na tlačítko **Save**.

2.4.4 Nastavení parametrů videa

Postup

1. Kliknutím na položku **Video&Audio** → **Event Video Parameters** otevřete příslušnou stránku.

Event Video Settings

Channel No.: 1

Stream Type: Sub-stream

Bitrate Type: Variable Bitrate

Resolution: 320*240

Video Bitrate: 1024 Kbps

Length of Cached Video(before alarm): 5 s

Length of Cached Video(after alarm): 2 s

Save

Obrázek 2-19. Nastavení videa

2. Vyberte kameru a nastavte parametry videa.
Stream Type

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

Main Stream: Používá se při záznamu a HD náhledu, má vysoké rozlišení, kódový poměr a kvalitu obrazu.

Sub-Stream: Slouží k přenosu síťových a náhledových obrazů formou streamování videa s nižším rozlišením, přenosovou rychlostí a kvalitou obrazu.

Bitrate Type

Typ Bitrate vyberte jako konstantní nebo proměnný.

Resolution

Vyberte rozlišení výstupu videa.

Video Bitrate

Nejvyšší hodnota odpovídá vyšší kvalitě videa, ale je k tomu nutná lepší šířka pásma.

2.5 Správa oprávnění

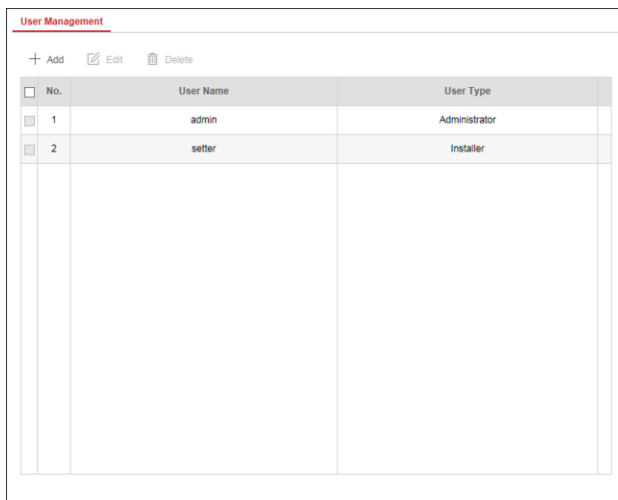
2.5.1 Přidání/úprava/odstranění uživatele

Administrátor může přidat uživatele bezpečnostního ovládacího panelu, upravit informace o uživateli nebo uživatele bezpečnostního ovládacího panelu smazat. Novému uživateli též můžete nastavit různá oprávnění.

Postup

1. Kliknutím na položku **User Management** → **User** otevřete stránku User Management.

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

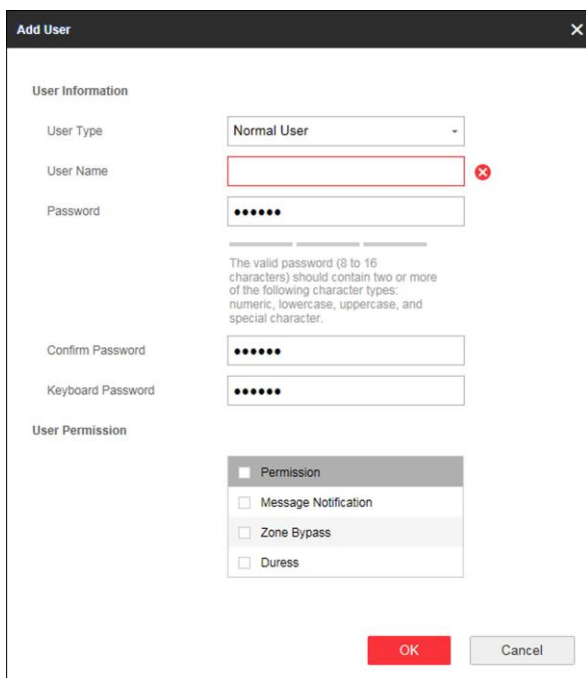


The screenshot displays the 'User Management' interface. At the top, there are three buttons: '+ Add', 'Edit' (with a pencil icon), and 'Delete' (with a trash icon). Below these buttons is a table with the following data:

<input type="checkbox"/>	No.	User Name	User Type
<input type="checkbox"/>	1	admin	Administrator
<input type="checkbox"/>	2	setter	Installer

Obrázek 2-20. Stránka User Management

2. Klikněte na tlačítko **Add**.
3. V překryvném okně nastavte údaje o novém uživateli včetně typu uživatele, uživatelského jména a hesla.



Add User

User Information

User Type: Normal User

User Name: [Red X]

Password: [Masked]

Confirm Password: [Masked]

Keyboard Password: [Masked]

User Permission

- Permission
- Message Notification
- Zone Bypass
- Duress

OK Cancel

Obrázek 2-21. Stránka Add User

4. Zaškrtnutím příslušných políček nastavte oprávnění uživatele. Uživatel může provádět úkony jen v rámci přidělených oprávnění.
5. Klikněte na **OK**.
6. **Volitelně:** Vyberte uživatele a po kliknutí na položku **Edit** můžete upravit údaje o uživateli a jeho oprávnění.
7. **Volitelně:** Můžete odstranit jednoho uživatele nebo zaškrtnout několik uživatelů a kliknutím na položku **Delete** odstranit uživatele dávkově.

Poznámka

Administrátora a instalátora není možné odstranit.

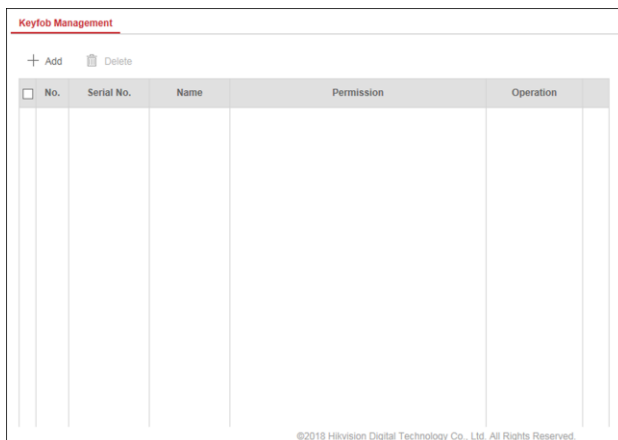
2.5.2 Přidání/úprava/odstranění klíčenky

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

Do bezpečnostního ovládacího panelu můžete přidat klíčenku, kterou pak tento panel můžete ovládat. Dále můžete upravit údaje o klíčence nebo klíčenku z bezpečnostního ovládacího panelu odstranit.

Postup

1. Kliknutím na položku **User Management** → **Keyfob** otevřete stránku Keyfob Management.



Obrázek 2-22. Správa klíčenek

2. Klikněte na položku **Add** a stiskněte libovolné tlačítko na klíčence.
3. Nastavte parametry klíčenky.

Name

Upravte název klíčenky.

Permission Settings


Zaškrtnutím různých položek přiřadíte oprávnění.

Single Key Settings

Z rozevíracího seznamu vyberte a nastavte funkce klíče I a klíče II.

Combination Keys Settings

Z rozevíracího seznamu vyberte a nastavte funkce kombinace klíčů.

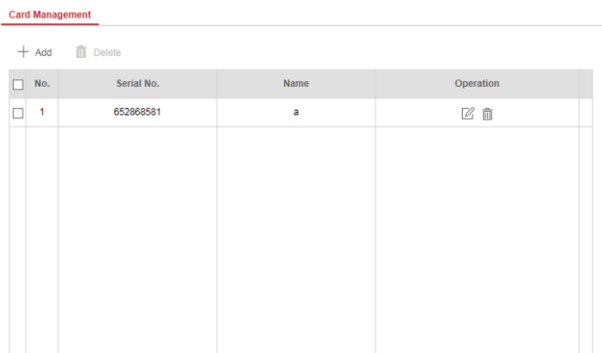
4. Klikněte na **OK**.
5. **Volitelně:** Kliknutím na  upravte údaje o klíčence.
6. **Volitelně:** Můžete odstranit jednu klíčenku nebo zaškrtnout několik klíčenek a kliknutím na položku **Delete** odstranit klíčenky hromadně.

2.5.3 Přidání/úprava/odstranění karty



Do bezpečnostního ovládacího panelu můžete přidat kartu, kterou pak můžete aktivovat/deaktivovat zabezpečení zóny. Dále můžete upravit údaje o kartě nebo kartu z bezpečnostního ovládacího panelu odstranit.

Postup


1. Kliknutím na položku **User Management** → **Card** otevřete stránku Card Management.



The screenshot shows the 'Card Management' interface. At the top, there are buttons for '+ Add' and 'Delete'. Below is a table with the following data:

No.	Serial No.	Name	Operation
1	652868581	a	 

Obrázek 2-23. Správa karet

2. Klikněte na položku **Add** a položte kartu na plochu pro přiložení karty.
3. V překryvném okně upravte název karty.
4. Klikněte na tlačítko **OK** a údaje o kartě se zobrazí v seznamu.
5. **Volitelně:** Klikněte na  a poté můžete změnit název karty.
6. **Volitelně:** Můžete odstranit jednu kartu nebo zaškrtnout několik karet a kliknutím na položku **Delete** odstranit karty dávkově.

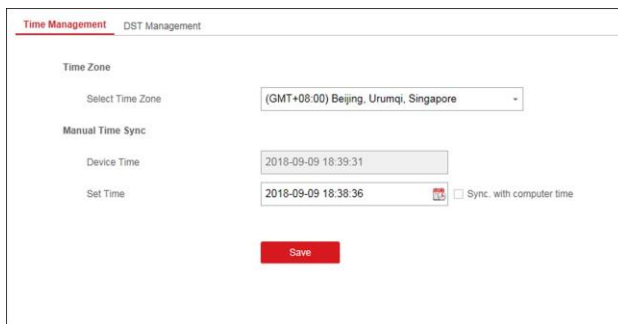
2.6 Nastavení systému

2.6.1 Nastavení systému

Můžete nastavit časovou zónu zařízení, synchronizovat čas zařízení, nastavit čas DST a nastavit parametry jednotlivých možností.

Time Management

Kliknutím na položku **System** → **Device Time** → **Time Management** otevřete stránku Time Management.



The screenshot shows the 'Time Management' page. At the top, there are two tabs: 'Time Management' (active) and 'DST Management'. Under 'Time Management', there are three sections: 'Time Zone' with a dropdown menu set to '(GMT+08:00) Beijing, Urumqi, Singapore'; 'Manual Time Sync' with a 'Device Time' field showing '2018-09-09 18:39:31' and a 'Set Time' field showing '2018-09-09 18:38:36'; and a checkbox labeled 'Sync. with computer time' which is currently unchecked. A red 'Save' button is located at the bottom center.

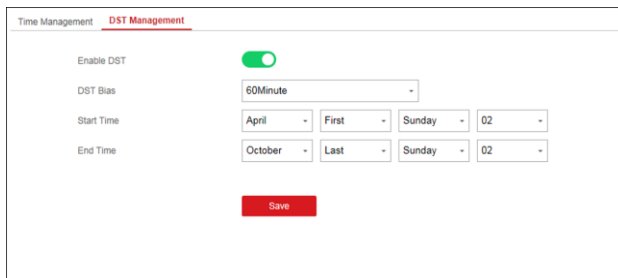
Obrázek 2-24. Řízení času

Z rozevřacího seznamu můžete vybrat časovou zónu.

Čas zařízení můžete ručně synchronizovat. Nebo můžete zaškrtnout položku **Sync. with Computer Time** a synchronizovat čas zařízení s časem počítače.

DST Management

Kliknutím na položku **System** → **Device Time** → **DST Management** otevřete stránku Time Management.



The screenshot shows the 'DST Management' page. At the top, there are two tabs: 'Time Management' and 'DST Management' (active). Under 'DST Management', there are four sections: 'Enable DST' with a green toggle switch turned on; 'DST Bias' with a dropdown menu set to '60Minute'; 'Start Time' with four dropdown menus set to 'April', 'First', 'Sunday', and '02'; and 'End Time' with four dropdown menus set to 'October', 'Last', 'Sunday', and '02'. A red 'Save' button is located at the bottom center.



Obrázek 2-25. Řízení letního času

Můžete povolit letní čas a nastavit časový rozdíl, dobu začátku letního času a dobu konce letního času.

Option Management

Kliknutím na položku **System** → **Option Management** otevřete stránku Option Management.

Podle potřeby nastavte níže uvedené parametry.

Installer Not Allowed

Je-li tato možnost povolená, instalátor se nemůže přihlásit k systému a ovládat zařízení.

Wireless Peripherals Management

Je-li tato možnost povolená, systém bude zjišťovat přítomnost periferních zařízení. Nebude-li žádné periferní zařízení zjištěno, systém odešle informaci o události.

Disarming Failed: Zone Fault

Je-li tato možnost povolena a v zóně došlo k chybě, nebudete moci aktivovat zabezpečení zóny.

System Fault Report

Je-li tato možnost povolena, zařízení automaticky odešle zprávu o chybě systému.

Disable Function Key

Je-li tato možnost povolena, tlačítka všech funkcí budou neaktivní.

Network Camera Disconnection Detection

Je-li tato možnost povolena, v případě odpojení propojené síťové kamery se spustí alarm.

System Volume

Hlasitost systému můžete nastavit v rozsahu od 0 do 10.

2.6.2 Zabezpečení

Protokol SSH (Secure Shell) můžete povolit nebo zakázat podle svých skutečných potřeb. Můžete také nastavit parametry zamknutí uživatele a uživatele odemknout.

Kliknutím na položku **System** → **Security Settings** → **SSH Settings** otevřete stránku SSH Settings, na níže můžete funkci SSH povolit nebo zakázat.

Kliknutím na položku **System** → **Security Settings** → **Locking User Settings** otevřete cílovou stránku. Můžete nastavit následující parametry:

Max. Failure Attempts

Pokud uživatel nepřetržitě zadává nesprávné heslo vícekrát, než je nastavený počet pokusů, účet se uzamkne.

Poznámka


Administrátor má o dva pokusy více, než je nastavená hodnota.

Locked Duration

Nastavte dobu, po kterou bude účet uzamčen.

Poznámka

Doba trvání uzamknutí je 5 až 1800 s.

Můžete také zobrazit údaje o uzamknutém uživateli. Kliknutím na  účet odemkněte nebo kliknutím na **Unlock All** odemkněte všechny uzamknuté uživatele v seznamu.

Klikněte na tlačítko **Save**.

2.6.3 Zabezpečení

Protokol SSH (Secure Shell) můžete povolit nebo zakázat podle svých skutečných potřeb. Můžete také nastavit parametry zamknutí uživatele a uživatele odemknout.

Kliknutím na položku **System** → **Security Settings** → **SSH Settings** otevřete stránku SSH Settings, níže můžete funkci SSH povolit nebo zakázat.

Kliknutím na položku **System** → **Security Settings** → **Locking User Settings** otevřete cílovou stránku. Můžete nastavit následující parametry:

Max. Failure Attempts

Pokud uživatel nepřetržitě zadává nesprávné heslo vícekrát, než je nastavený počet pokusů, účet se uzamkne.

Poznámka


Administrátor má o dva pokusy více, než je nastavená hodnota.

Locked Duration

Nastavte dobu, po kterou bude účet uzamčen.

 **Poznámka**

Doba trvání uzamknutí je 5 až 1800 s.

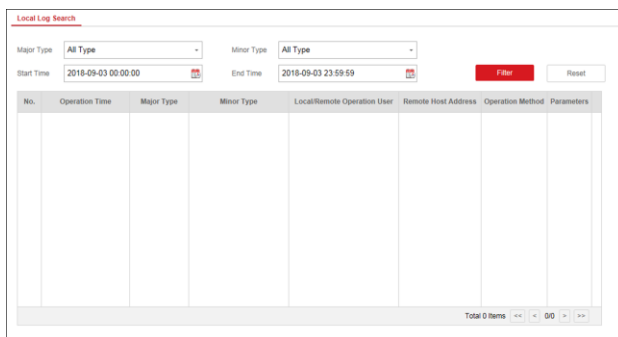
Můžete také zobrazit údaje o uzamknutém uživateli. Kliknutím na  účet odemkněte nebo kliknutím na **Unlock All** odemkněte všechny uzamknuté uživatele v seznamu.

Klikněte na tlačítko **Save**.

2.6.4 Prohledání místního protokolu

Můžete prohledat protokol s údaji o zařízení.

Kliknutím na položku **System** → **Local Log Search** otevřete stránku Local Log Search.



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

Obrázek 2-26. Stránka Local Log Search

Z rozbalovacího seznamu vyberte hlavní typ a vedlejší typ, nastavte čas začátku a čas konce prohledávání protokolu a klikněte na položku **Filter**. V seznamu se zobrazí všechny vyfiltrované údaje z protokolu.

Kliknutím na položku **Reset** můžete také resetovat všechny vyhledávané stavy.

2.7 Dotaz

2.7.1 Stav

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

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

Klikněte na položku **Status**. Můžete zobrazit stav zóny, relé, sirény, baterie, komunikace a opakovače.

2.8 Obsluha bezpečnostního ovládacího panelu

V modulu **Security Control Panel** můžete spravovat a ovládat přičky a související zóny.

Poznámka

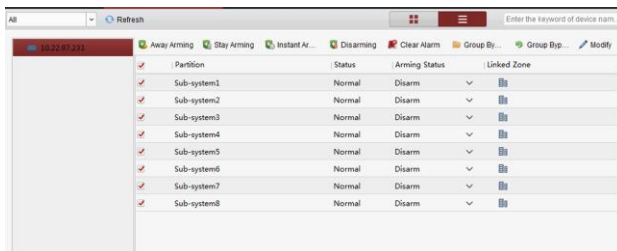
Pokud se na stránce **Control Panel** žádný **bezpečnostní ovládací panel** nezobrazí, klikněte na položku **Selecting Modules** a vyberte možnost **Security Control Panel**.

2.8.1 Ovládání přičky

V modulu **Security Control Panel** můžete ovládat vybranou přičku, například dálkovou aktivaci zabezpečení, zabezpečení při pobytu, okamžité zabezpečení, deaktivaci zabezpečení, vymazání alarmu, skupinový bypass a obnovení skupinového bypassu.

Poznámka

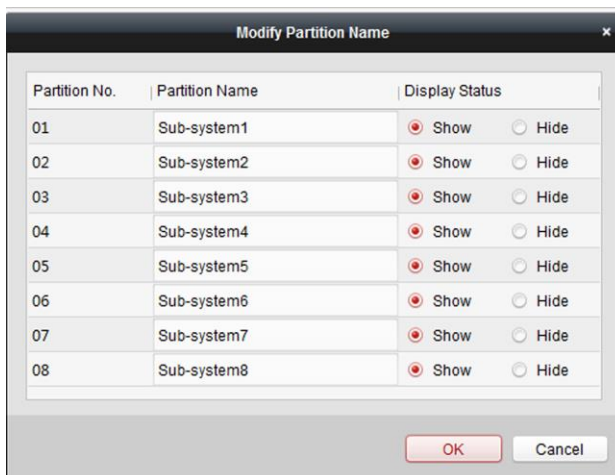
Bezdrátový bezpečnostní ovládací panel má jen jednu přičku.



Obrázek 2-27. Ovládání přičky

Klikněte na položku **Edit**, chcete-li upravit název přičky a zobrazit možnosti.

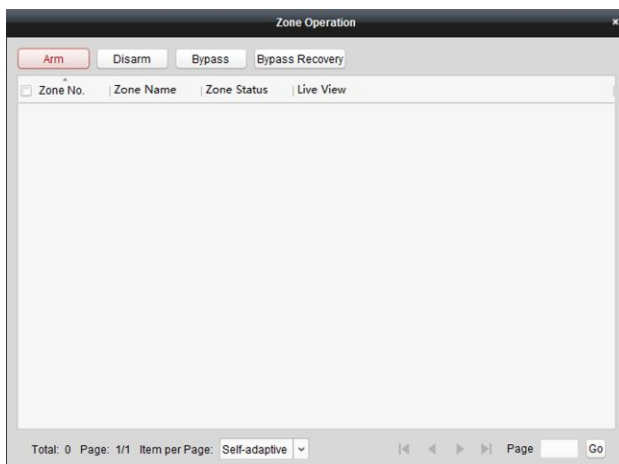
Uživatelská příručka pro bezpečnostní ovládací panel Axiom



Obrázek 2-28. Úprava údajů o příčce

2.8.2 Ovládání zóny

Klikněte na položku **Linked Zone** v seznamu příček v **bezpečnostním ovládacím modulu**. Můžete ovládat zvolené zóny související s příčkou, například aktivaci zabezpečení, deaktivaci zabezpečení, bypass nebo obnovu bypassu.



Obrázek 2-29. Ovládání zóny

3 Správa bezpečnostního ovládacího modulu prostřednictvím mobilního klienta

Zde zadejte krátký popis své koncepce (nepovinné).

Jedná se o začátek vaší koncepce.

3.1 Stažení a přihlášení mobilního klienta

Stáhněte si mobilního klienta Hik-Connect ze stránky Google Play (pro Android) nebo App store (pro iOS) a klienta přihlaste. Teprve poté můžete ovládat bezpečnostní ovládací panel Axiom.

Postup

1. Vyhledejte a stáhněte si aplikaci mobilního klienta Hik-Connect na stránce Google Play (pro Android) nebo App Store (pro iOS).
2. **Volitelně:** Jestliže mobilního klienta Hik-Connect používáte poprvé, zaregistrujte si nový účet.

Poznámka

Podrobnosti si přečtěte v *uživatelské příručce k mobilnímu klientu Hik-Connect*.

3. Klienta zapněte a přihlaste se.


3.2 Přidání ovládacího panelu do mobilního klienta


Než provedete další akce, měli byste přidat ovládací panel do mobilního klienta.

Postup

1. Zapněte napájení ovládacího panelu.
2. Vyberte typ přidání.


-

Klepnutím na  → **Scan QR Code** otevřete stránku pro naskenování QR kódu. Naskenujte QR kód na ovládací panel.

 **Poznámka**

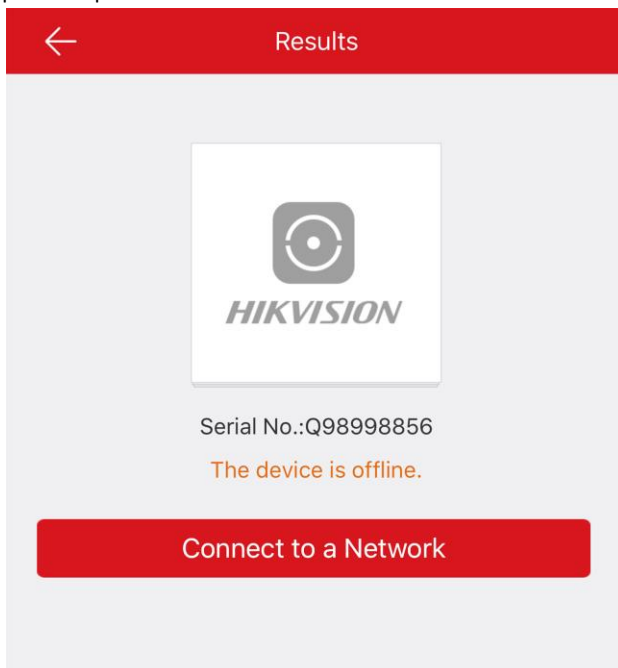
QR kód je obvykle vytištěn na štítku nalepeném na zadním krytu ovládacího panelu.



Klepnutím na  → **Manual Adding** otevřete stránku Add Device. Zadejte sériové číslo zařízení s typem přidání domény Hik-Connect.


3. Připojte se k síti.

- 1) Klepněte na položku **Connect to a Network**.



Obrázek 3-1. Stránka Connect to a Network

- 2) Klepněte na položku **Wireless Connect** na stránce Adding Type.
- 3) Podle pokynů změňte režim ovládacího panelu na režim AP. Klepněte na položku **Next**.
- 4) Vyberte stabilní síť Wi-Fi, k níže se má zařízení připojit, a klepněte na položku **Next**.

 **Poznámka**

Ověřte, že zařízení a mobilní telefon jsou připojeny ke stejné síti Wi-Fi.

4. Podle pokynů na mobilním klientu připojte mobilní telefon s ovládacím panelem pomocí bezdrátového připojení.
 5. Vytvořte heslo pro aktivaci zařízení.
-

 **Poznámka**

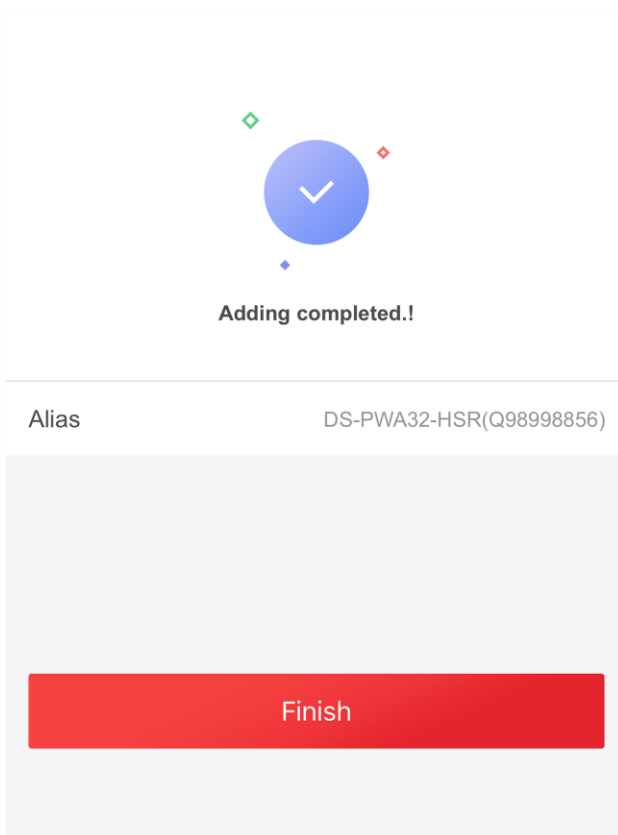
Důrazně doporučujeme vytvořit silné heslo dle svého výběru (minimálně 8 znaků obsahujících alespoň tři následující kategorie: velká písmena, malá písmena, čísla a zvláštní znaky) pro lepší zabezpečení svého výrobku. Dále doporučujeme toto heslo pravidelně obměňovat, zvláště v systému s vysokým zabezpečením. Lepší ochranu vašeho výrobku zajistí obměna hesla jednou za měsíc nebo za týden.

6. Zadejte ověřovací kód zařízení a klepněte na **OK**.
-

 **Poznámka**

Ověřovací kód je implicitně na štítku zařízení.

7. Podle pokynů změňte režim ovládacího panelu na režim Station. Klepněte na položku **Next**.
8. Po dokončení přidání ovládacího panelu klepněte na položku **Finish**.



Obrázek 3-2. Stránka Adding Completed

Ovládací panel je v seznamu na stránce Hik-Connect.

9. Klepněte na položku **Finish**.

3.3 Přidání periferie do ovládacího panelu

Před provedením dalších úkonů, například aktivace či deaktivace zabezpečení, byste měli do ovládacího panelu přidat periferie.



Než začnete

Zkontrolujte, že ovládací panel je deaktivovaný.

Postup

Poznámka

Některé modely ovládacích panelů nepodporují vzdálené přidání zón nebo bezdrátových zařízení. Do ovládacího panelu byste je měli přidat přímo. Podrobnosti si přečtěte v uživatelské příručce k bezdrátovému zařízení.

1.  Klepnutím na  otevřete stránku pro naskenování QR kódu.
 2. Naskenujte QR kód periferního zařízení, abyste je mohli přidat.
 3. Vyberte typ periferie a vytvořte název periferie.
-

Poznámka

- Když je doplněným periferním zařízením detektor, bude připojen k zóně. Údaje o detektoru se zobrazí na kartě Zone.
 - K zóně lze připojit až 32 detektorů.
-

Přidané periferní zařízení bude uvedeno na kartě Zone nebo na kartě Wireless Devices.

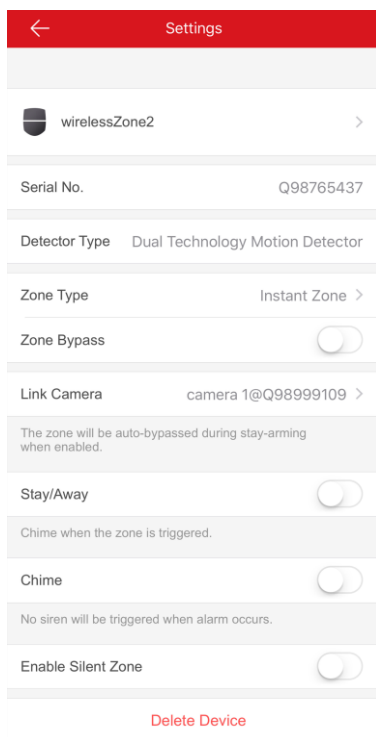
3.4 Nastavení zóny

Po přidání detektoru můžete nastavit zónu včetně jejího názvu, typu, bypassu, připojené kamery, stavu pro pobyt v zóně a mimo zónu, sirény a tiché zóny. Dále můžete zobrazit sériové číslo detektoru a typ zóny detektoru.

Postup

1. Klepnutím na zónu na stránce Partition otevřete stránku pro nastavení zóny.

Uživatelská příručka pro bezpečnostní ovládací panel Axiom



Obrázek 3-3. Stránka Zone Settings

2. Podle potřeby nastavte níže uvedené parametry.

Zone Type

Ze seznamu druhů zón vyberte druh zóny. Když klepnete na **?**, zobrazí se definice jednotlivých zón.

Zone Bypass

Když povolíte tuto funkci, zóna bude obcházena. Po dobu existence bypassu nebudou odesílány žádné alarmy.

Link Camera

Zónu můžete propojit s kamerami. V případě spuštění alarmu můžete zónu sledovat připojenými kamerami.

Stay/Away

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

Když povolíte tuto funkci, zóna bude automaticky obcházena, pokud bude ve stavu pobytu v zóně nebo mimo zónu.

Chime

Když povolíte tuto funkci, po spuštění alarmu zóny se ozve zvukový alarm.

Enable Silent Zone

Když povolíte tuto funkci, v případě vzniku události nebo alarmu se neozve siréna.

3.5 Přidání kamery do zóny

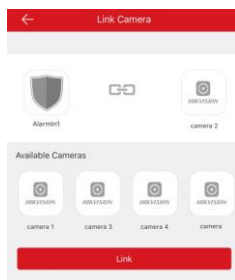
Kameru můžete propojit se zónou, kterou chcete sledovat. V případě spuštění alarmu si můžete prohlédnout videa s alarmovou situací.

Než začnete

Ověřte, že je v cílové zóně instalovaná kamera, která je připojená ke stejné síti LAN jako bezpečnostní ovládací panel.


Postup

1. Klepněte na bezpečnostní ovládací panel na stránce Hik-Connect a klepnutím na položku **Zone** otevřete stránku se seznamem zón.
2. Vyberte zónu, kterou chcete zadat na stránku pro nastavení zón.
3. Klepnutím na položku **Link Camera** otevřete stránku Link Camera.



Obrázek 3-4. Stránka Link Camera

4. Z dostupných kamer vyberte některou kameru a klepněte na položku **Link**.

Vybraná kamera se propojí se zónou. Napravo od zóny v seznamu zón se zobrazí ikona  Klepnutím na ikonu zobrazíte živý videopřenos ze zóny.



3.6 Aktivace/deaktivace zabezpečení zóny

Zabezpečení zóny můžete podle potřeby ručně aktivovat nebo deaktivovat.

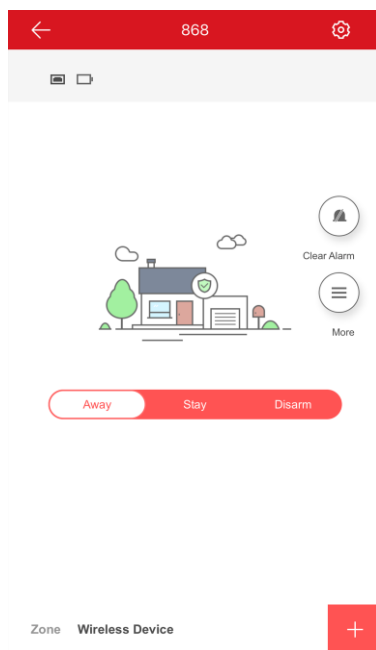
Poznámka

Bezpečnostní ovládací panel Axiom podporuje jednu příčku.

Na stránce Hik-Connect klepnutím na bezpečnostní ovládací zařízení otevřete stránku pro správu ovládacího panelu. Klepnutím na položku **Away/Stay/Disarm** můžete ovládat stav příčky.

Dále můžete klepnutím na **Clear Alarm** odstranit alarm po jeho spuštění.


Uživatelská příručka pro bezpečnostní ovládací panel Axiom



Obrázek 3-5. Stránka Control Panel Management

3.7 Nastavení časového plánu aktivace/deaktivace zabezpečení

Nastavte časový plán aktivace/deaktivace zabezpečení pro automatickou aktivaci/deaktivaci zabezpečení určité zóny. Klepnutím na bezpečnostní ovládací panel

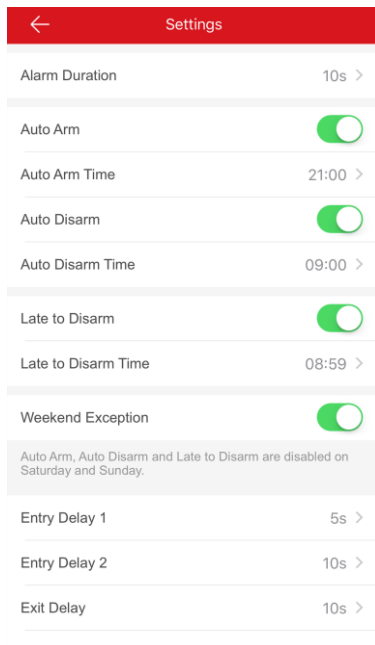
otevřete stránku pro ovládání a klepnutím na  nebo



otevřete stránku Settings.

Uživatelská příručka pro bezpečnostní ovládací panel Axiom

Povolte funkci automatické aktivace/deaktivace a nastavte čas automatické aktivace či deaktivace. Dále můžete nastavit čas pozdní deaktivace, čas prodlevy pro příchod, čas prodlevy pro odchod a čas prodlevy pro sirénu.



Obrázek 3-6 Stránka Arming or Disarming Schedule

3.8 Zóna bypassu

Když je aktivované zabezpečení příčky, můžete určitou zónu podle potřeby obejít.

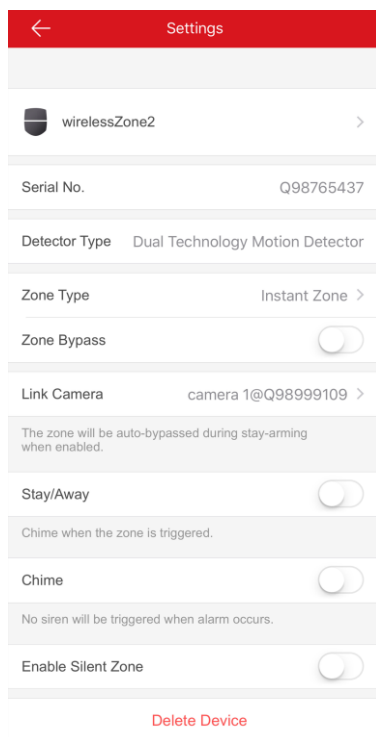
Než začnete

Propojte detektor se zónou.

Postup

1. Vyberte zónu na kartě Zone na stránce Partition.
2. Vyberte zónu a otevřete stránku Settings.

Uživatelská příručka pro bezpečnostní ovládací panel Axiom



Obrázek 3-7. Stránka Zone Settings

3. Povolte možnost **Zone Bypass** a zóna bude ve stavu obcházení.

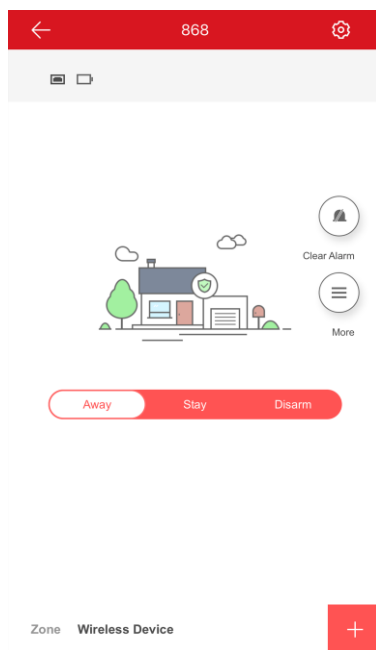
Detektor v zóně nebude nic detekovat a ze zóny nebudete dostávat žádné alarmy.

3.9 Přidání karty

Do ovládacího panelu můžete přidat kartu. Pomocí karty můžete aktivovat/deaktivovat zabezpečení nebo odstranit alarm.


Postup

1. Vyberte ovládací panel na stránce Hik-Connect a otevřete stránku pro správu ovládacího panelu.



Obrázek 3-8. Stránka Control Panel Management

2.  Klepnutím na  → **Card/Tag Management** otevřete stránku Card/Tag Management.
3.  Klepněte na  .
4. Až uslyšíte hlasovou výzvu „Swipe Card“, přiložte kartu na plochu pro přiložení karty na ovládacím panelu.
Když uslyšíte pípnutí, karta byla rozpoznána.
5. Vytvořte zástupný název (alias) karty a klepněte na **Finish**.

 **Poznámka**

Alias může obsahovat 1 až 32 znaků.

Uživatelská příručka pro bezpečnostní ovládací panel Axiom
Karta se zobrazí na stránce Card/Tag Management.



3.10 Přidání klíčenky

Na kontrolní panel můžete přidat klíčenky a ovládat jimi stav aktivace/deaktivace zabezpečení příčky. Spuštěný alarm můžete také odstranit.

Postup

Poznámka

Zkontrolujte, zda má klíčenka stejnou frekvenci jako ovládací panel.

1.  Klepnutím na  otevřete stránku pro naskenování QR kódu.
2. Naskenujte QR kód klíčenky, abyste ji mohli přidat.
3. Vytvořte název klíčenky a klepněte na **OK**.
Klíčenka se objeví v seznamu na stránce Wireless Device.
4. **Volitelně:** Můžete zobrazit sériové číslo klíčenky a můžete je také smazat.

3.11 Kontrola oznámení o alarmu

Po spuštění alarmu obdržíte oznámení o alarmu. Na mobilním klientu můžete zkontrolovat údaje o alarmu.

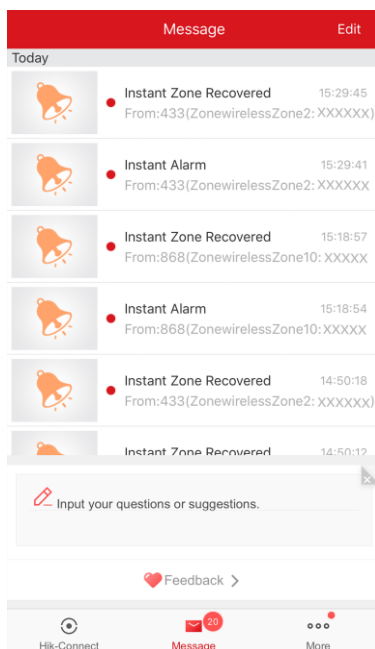
Než začnete

- Zkontrolujte, zda máte zónu propojenou s detektorem.
- Zkontrolujte, zda není aktivní obcházení (bypass) zóny.
- Zkontrolujte, zda jste nepovolili funkci tiché zóny.

Postup

1. Klepnutím na položku **Message** na stránce Hik-Connect otevřete stránku Message.

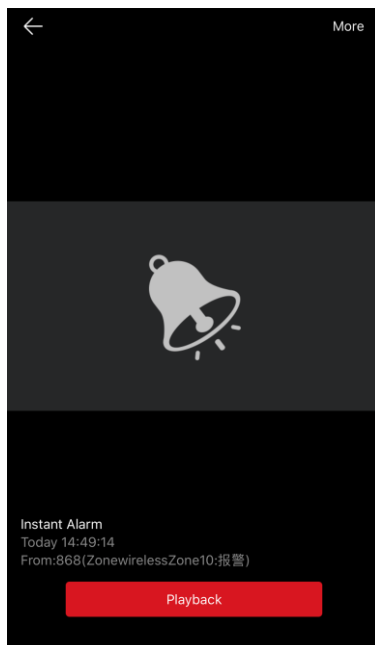
Uživatelská příručka pro bezpečnostní ovládací panel Axiom



Obrázek 3-9. Stránka Message

Na stránce Message jsou uvedena všechna oznámení.

2. Vyberte alarm a můžete zobrazit podrobnosti o něm.



Obrázek 3-10. Stránka Alarm Notification

- 3. Volitelně:** Je-li zóna propojená s kamerou, můžete si po spuštění alarmu přehrát záznam.

3.12 Kontrola stavu systému (stav zóny / stav komunikace)


Pomocí mobilního klienta můžete zobrazit stav zóny a stav komunikace.

Zobrazení stavu zóny

Na stránce Partition klepněte na položku Zone. Zobrazí se karta Zone. Můžete zobrazit stav jednotlivých zón v seznamu.

Režim komunikace



Klepnutím na  otevřete stránku pro nastavení ovládacího panelu. Můžete zobrazit stav komunikace zařízení včetně baterie, sítě Ethernet, Wi-Fi, mobilní sítě a používání dat.

