Instrukcja AX PRO

Informacje prawne

Instrukcja obsługi

O instrukcji

Niniejsza instrukcja podlega krajowej i międzynarodowej ochronie praw autorskich. Hangzhou Hikvision Digital Technology Co., Ltd. („Hikvision") zastrzega sobie wszelkie prawa do niniejszej instrukcji. Dokument nie może być powielany, zmieniany, tłumaczony ani rozpowszechniany, częściowo lub w całości, w jakikolwiek sposób, bez uprzedniej pisemnej zgody Hikvision. Z instrukcji obsługi korzystaj pod okiem profesjonalistów.

Znaki towarowe

HIKVISION a także inne znaki Hikvision są własnością Hikvision i są zastrzeżonymi znakami towarowymi lub przedmiotami ich zgłoszenia przez Hikvision i/lub podmioty stowarzyszone. Inne znaki handlowe wymienione w niniejszej instrukcji są własnością ich właścicieli. Znaki towarowe innych firm nie podlegają licencji bez wyraźnej zgody ich właścicieli.

Zrzeczenie się odpowiedzialności

W MAKSYMALNYM ZAKRESIE DOZWOLONYM PRZEZ OBOWIĄZUJĄCE PRAWO, NINIEJSZA INSTRUKCJA ORAZ OPISANY PRODUKT, WRAZ Z JEGO SPRZĘTEM, OPROGRAMOWANIEM I OPROGRAMOWANIEM UKŁADOWYM, SĄ DOSTARCZANE „w stanie zgodnym z rzeczywistością" ORAZ „ZE WSZYSTKIMI WADAMI I BŁĘDAMI". HIKVISION NIE UDZIELA ŻADNYCH GWARANCJI, WYRAŹNYCH ANI DOROZUMIANYCH, W TYM DOROZUMIANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ I PRZYDATNOŚCI DO OKREŚLONEGO CELU. UŻYTKOWNIK KORZYSTA Z NINIEJSZEJ INSTRUKCJI ORAZ OPIERA DZIAŁANIA NA JEJ TREŚCI NA WŁASNE RYZYKO I ODPOWIEDZIALNOŚĆ. W ŻADNYM WYPADKU HIKVISION NIE PONOSI ODPOWIEDZIALNOŚCI ZA SZKODY SZCZEGÓLNE, WTÓRNE, PRZYPADKOWE LUB POŚREDNIE, W TYM MIĘDZY INNYMI, ZA UTRATĘ ZYSKÓW BIZNESOWYCH LUB UTRATĘ DANYCH, USZKODZENIE SYSTEMÓW, USZKODZENIE, NA SKUTEK NARUSZENIA UMOWY, CZYNU NIEDOZWOLONEGO (W TYM NIEBEZPIECZEŃSTWA), ODPOWIEDZIALNOŚCI ZA PRODUKT LUB W INNY SPOSÓB, W ZWIĄZKU Z KORZYSTANIEM Z PRODUKTU, NAWET JEŚLI HIKVISION ZOSTAŁO POINFORMOWANE O MOŻLIWOŚCI WYSTĄPIENIA TAKICH SZKÓD LUB STRAT.
W ODNIESIENIU DO PRODUKTU Z DOSTĘPEM DO INTERNETU, WYKORZYSTANIE PRODUKTU ODBYWAĆ SIĘ BĘDZIE CAŁKOWICIE NA WŁASNE RYZYKO UŻYTKOWNIKA. HIKVISION NIE BIERZE ŻADNEJ ODPOWIEDZIALNOŚCI ZA NIEWŁAŚCIWE DZIAŁANIE, WYCIEK PRYWATNYCH INFORMACJI LUB INNE SZKODY WYNIKAJĄCE Z ATAKU HAKERSKIEGO, DZIAŁANIA WIRUSA KOMPUTEROWEGO LUB INNEGO RODZAJU RYZYKA INTERNETOWEGO; JEDNAKŻE, W TAKICH SYTUACJACH, HIKVISION ZAOFERUJE WSPARCIE TECHNICZNE.

KLIENT ZGADZA SIĘ KORZYSTAĆ Z TEGO PRODUKTU ZGODNIE ZE WSZYSTKIMI OBOWIĄZUJĄCYMI PRAWAMI I BYĆ WYŁĄCZNIE ODPOWIEDZIALNY ZA ZAPEWNIENIE, ŻE KORZYSTANIE Z TEGO PRODUKTU JEST ZGODNE Z OBOWIĄZUJĄCYM PRAWEM. W SZCZEGÓLNOŚCI UŻYTKOWNIK JEST ODPOWIEDZIALNY

ZA KORZYSTANIE Z TEGO PRODUKTU W SPOSÓB, KTÓRY NIE NARUSZA PRAW OSÓB TRZECICH, W TYM BEZ OGRANICZEŃ PRAW DO UPUBLICZNIANIA, PRAW WŁASNOŚCI INTELEKTUALNEJ LUB OCHRONY DANYCH ORAZ INNYCH PRAW PRYWATNOŚCI. NIE NALEŻY UŻYWAĆ TEGO PRODUKTU DO ŻADNYCH ZABRONIONYCH ZASTOSOWAŃ, W TYM ROZWOJU LUB PRODUKCJI BRONI MASOWEGO ZNISZCZENIA, ROZWOJU LUB

PRODUKCJA BRONI CHEMICZNEJ LUB BIOLOGICZNEJ, WSZELKICH CZYNNOŚCI ZWIĄZANYCH Z PRÓBAMI JĄDROWYMI LUB NIEBEZPIECZNYM JĄDROWYM CYKLEM PALIWOWYM, LUB DZIAŁAŃ WSPIERAJĄCYCH NARUSZANIE PRAW CZŁOWIEKA.

W PRZYPADKU JAKICHKOLWIEK NIEZGODNOŚCI MIĘDZY NINIEJSZĄ INSTRUKCJĄ A OBOWIĄZUJĄCYM PRAWEM PIERWSZEŃSTWO MA TO DRUGIE.

Znaczenie symboli

Symbole, które można znaleźć w dokumencie zdefiniowane zostały w następujący sposób.

Symbol	Opis
Niebezpieczeństwo	Oznacza niebezpieczną sytuację, która, jeśli się jej nie uniknie, doprowadzi lub może doprowadzić do śmierci lub poważnych obrażeń.
Uwaga	Oznacza potencjalnie niebezpieczną sytuację, która, jeśli się jej nie uniknie, może doprowadzić do uszkodzenia sprzętu, utratę danych, pogorszenie wydajności lub nieoczekiwane wyniki.
Wskazówka	Oznacza dodatkowe informacje w celu podkreślenia lub uzupełnienia ważnych punktów tekstu głównego.

Informacje prawne

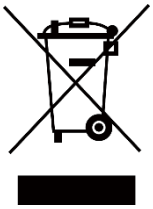
EN 50131-1:2006+A1:2009+A2:2017
EN 50131-3:2009
EN 50131-6:2017
EN 50131-5-3:2017
EN 50131-10: 2014
EN 50136-2: 2013

Stopień bezpieczeństwa (SG): 2
Klasa środowiskowa (WE): II
DP2
Certyfikowany przez Telefication

telefication

Uwaga Jeśli używane są niezgodne konfiguracje eEtykieta zgodności z normą EN50131 powinna zostać usunięta.

Oświadczenie o zgodności UE

CE	Niniejszy produkt i - w stosownych przypadkach - dostarczone akcesoria również są oznaczone symbolem „CE” i zgodne z obowiązującymi zharmonizowanymi normami europejskimi wymienionymi w Dyrektywie EMC 2014/30/UE, Dyrektywie RE 2014/53/UE, Dyrektywie RoHS 2011/65/EU
	Dyrektywie 2012/19/UE (dyrektywa WEEE): Produkty oznaczone tym symbolem nie mogą być usuwane jako nieposortowane odpady komunalne w Unii Europejskiej. Właściwe czynności związane z recyklingiem wymagają zwrócenia produktu do lokalnego dostawcy po zakupie równoważnego nowego sprzętu lub zutylizowanie go w wyznaczonych punktach zbiórki. Aby uzyskać więcej informacji zobacz: www.recyclethis.info
	2006/66/EC (Dyrektywa dotycząca baterii): Produkt zawiera baterię, która nie może być usunięta jako nieposortowane odpady komunalne w Unii Europejskiej. Szczegółowe informacje na temat baterii znajdują się w dokumentacji produktu. Bateria oznaczona jest symbolem, który zawiera litery wskazujące na kadm (Cd), ołów (Pb) lub rtęć (Hg). W celu prawidłowego recyklingu, zwróć baterię dostawcy lub wyznaczonemu punktowi zbiórki. Aby uzyskać więcej informacji, wejdź na: www. recyclethis.info

	Ostrzeżenie Jest to produkt klasy A. W środowisku domowym ten produkt może powodować usterki radiowe, w którym to przypadku użytkownik może być zmuszony do podjęcia odpowiednich środków zaradczych.
	Informacje FCC Pamiętaj, że zmiany lub modyfikacje, które nie zostały wyraźnie zatwierdzone przez stronę odpowiedzialną za kwestie zgodności, mogą pozbawić użytkownika prawa do korzystania z urządzenia. Zgodność z FCC: Urządzenie zostało przetestowane i uznane za zgodne z ograniczeniami dla urządzeń cyfrowych klasy B, zgodnie z częścią 15 przepisów FCC. Limity zostały opracowane w celu zapewnienia ochrony przed szkodliwymi zakłóceniami w instalacjach domowych. Urządzenie generuje, wykorzystuje i może emitować energię o częstotliwości radiowej, a jeśli nie zostanie zainstalowane i nie będzie używane zgodnie z instrukcją, może powodować szkodliwe usterki w komunikacji radiowej. Nie ma niestety gwarancji, że w przypadku konkretnej instalacji nie pojawią się usterki. Jeśli urządzenie powoduje szkodliwe usterki w odbiorze radiowym lub telewizyjnym, co można ustalić przez wyłączenie i włączenie urządzenia, użytkownik zachęcany jest do podjęcia próby usunięcia zakłóceń za pomocą jednego lub większej ilości następujących środków: —Zmień orientację lub położenie anteny odbiorczej. —Zwiększ odległość między urządzeniem a odbiornikiem. —Podłącz urządzenie do gniazdka w obwodzie innym niż ten, do którego podłączony jest odbiornik. —Skonsultuj się ze sprzedawcą lub doświadczonym technikiem RTV Urządzenie powinno być instalowane i obsługiwane w odległości co najmniej 20 cm między chłodnicą a ciałem. Warunki FCC Urządzenie jest zgodne z częścią 15 przepisów FCC. Działanie urządzenia podlega następującym dwóm warunkom: 1. Urządzenie nie może powodować szkodliwych zakłóceń. 2. Urządzenie musi przyjmować wszelkie odbierane usterki, w tym usterki, które mogą powodować niepożądane działanie.

Spis treści

Rozdział 1 Wstęp

1.1 Opis systemu

AX Pro to bezprzewodowy system alarmowy, co do których zachodzi wymóg ochrony przed włamaniem. Obsługuje LAN/Wi-Fi jako podstawową sieć transmisyjną oraz GPRS/3G/4G LTE jako drugorzędną sieć transmisyjną. System ma zastosowanie w scenariuszach marketu, sklepu, domu, fabryki, magazynu, biura itp.

• Innowacyjna dwukierunkowa technologia bezprzewodowa Tri-X.

• Dwukierunkowa komunikacja z szyfrowaniem AES-128.

• Widmo rozproszone z przeskokiem częstotliwości (FHSS) jest wykorzystywane w celu uniknięcia zakłóceń, zapobiegania podsłuchiwaniu i umożliwienia komunikacji z wielokrotnym dostępem z podziałem kodowym (CDMA).

• Przewodnik głosowy dla ostrzeżenia o alarmie, wskazania stanu systemu, podpowiedzi operacyjnej itp.

• Konfiguracja za pośrednictwem klienta internetowego, klienta mobilnego i chmury Convergence.

• Przesyłanie powiadomień o alarmie za pośrednictwem komunikatów lub połączeń telefonicznych.

• Wyświetlanie filmów z życia z Hik-Connect i klipów wideo alarmowych za pośrednictwem komunikatów e-mail, Hik-ProConnect i Hik-Connect.

• Przesyłanie raportów o alarmach do SMA.

• Protokół SIA-DC09 i obsługuje zarówno format danych Contact ID, jak i SIA.

• Zapasowa bateria litowa 4520 mAh z 12-godzinnym czasem czuwania.

Zamawianie

Model	Opis
DS-PWA64-L-WE	Obsługuje Ethernet/Wi-Fi i GPRS
DS-PWA96-M-WE	Obsługuje Ethernet/Wi-Fi, 3G/4G LTE i kartę IC

1.2 Specyfikacja

		AX PRO	
		Seria 64	**Seria 96**
Wydajność	Obszary	16	32
	Strefy	Do 64	Do 96
	Wyjścia		
	Czytniki znaczników	Do 8	Do 8
	Klawiatury		
	Sygnalizatory	4	6
	Wzmacniaki	2	4
	Piloty	32	48
	Znaczniki	32	48
	Wbudowany czytnik znaczników	X	V
Użytkownik	Instalator	1	1
	Administrator	1	1
	Normalny użytkownik	30	46
Bezprzewodowe właściwości techniczne	Częstotliwość RF	868 Mhz (865 Mhz dla wykrywacza kamery PIR)/433 Mhz	
	Rodzaj bezprzewodowy	Dwukierunkowa łączność bezprzewodowa	
	Ochrona bezprzewodowa	Szyfrowanie AES z przeskokiem częstotliwości	
Funkcje	Komunikaty głosowe	V	V
	Język komunikatów głosowych	angielski, włoski, hiszpański, francuski, rosyjski, portugalski, niemiecki, polski	
	Klient sieciowy	V	V
	Diagnostyka	V	V
	Powiadomienie SMS	V	V
	Powiadomienie o połączeniu głosowym	V	V
	Zapisy dziennika zdarzeń	5000 w tym 1000 obowiązkowo[a]	
	Obsługa kamer PIR	V	V
	IVaaS Storage	X	4 klipsy x 7 sekund
Interfejsy komunikacyjne	Ethernet	Samoadaptacja 10/100 Mb/s	
	Wi-Fi	802.11b/g/n	(2.4GHz)
	GPRS	V	X
	3G/4G LTE	X	V
	Gniazdo karty SIM	Pojedyncze	Podwójne
Sygnalizacja ARC	Kategoria ATS[a]	DP2	
	Podstawowa ścieżka transmisji	LAN / WiFi	
	Druga ścieżka transmisji	GPRS lub 3G/4G LTE	
	Operacje potwierdzenia	przejściowe	

	Protokoły	SIA-DC09[b], ISUP 5.0	
Usługi w chmurze	Usługa Hik-ProConnect	V	V
	Usługa Hik-Connect	V	V
Automatyzacja	Czujnik naścienny	V	V
	Moduł przekaźnika	V	V
	Inteligentna wtyczka	V	V
Zasilanie	Rodzaj PS[c]	Type A	
	Wejście sieciowe	~ 100-240V 50/60Hz 0.3A(Max)	
	Pojemność baterii[d]	4520 mAh	
	Tryb gotowości baterii[e]	Up to 12 hrs	
	Rodzaj baterii	Built-in rechargeable Lithium-ion polymer battery Model: 765965	
	Aktualne zużycie	With an alarm: 405mA Without an alarm: 340mA	
	Prąd przy włączonej baterii	340 mA	
	Okres doładowania	4 hrs to 80%	
	Komunikat o niskim napięciu	3.55 V	
Serwis	Wewnątrz nie ma części, które użytkownik mógłby serwisować		
Wymogi środowiskowe	Temperatura robocza	-10°C do 50°C - 10°C do+40°C (Certyfikowana temperatura)	
	Wilgotność względna	10% ~ 90% bez kondesnacji	
Rozmiar oraz waga	Wymiar (SxWxG)	170.0 mm (6.7") x 170.0 mm (6.7") x38.6 mm (1.5")	
	Waga	557.5 g (19.7 oz)	
Zatwierdzenia	EN 50131	SG 2 EC II	
	CE	V	
	Rohs/Reach/WEEE	V	
a	Zgodnie z wymaganiami określonymi w normie EN 50131-1: 2006 + A1: 2009 + A2: 2017 bezprzewodowa centrala alarmowa AX Pro przyjmuje tryb przekazywania potwierdzeń. Nagrane zostanie zarówno pozytywne, jak i negatywne potwierdzenie z nadajnika-odbiornika centrum odbiorczego. Opis dziennika zdarzeń Pozytywne uznanie Przesłano ARC Negatywne potwierdzenie Błąd komunikacji ARC		

b	Bezprzewodowy panel sterowania AX Pro jest kompatybilny z raportowaniem SIA IP (UDP/TCP-2013) zgodnie z ANSI/SIA DC-09-2013: Raportowanie zdarzeń protokołu internetowego. Centrala obsługuje tokeny (protokoły) ADM-CID i SIA-DCS zdefiniowane w SIA DC-07-2001.04, które zostaną zmodyfikowane, aby wprowadzić „*" przed nazwą tokena jako * ADM-CID i * SIA-DCS, gdy dane i znacznik czasu komunikatów transmisji są zaszyfrowane AES. Obsługiwane są AES-128, AES-192 i AES-256.
c	Zgodnie z EN 50131-1: 2006 + A1: 2009 + A2: 2017, 9.1 Rodzaje zasilania
d	Wartość nominalna. Rzeczywista pojemność może się nieznacznie różnić. Rzeczywista pojemność baterii dla każdego pojedynczego urządzenia może być nieco wyższa lub niższa od nominalnej pojemności baterii. Wyjęcie baterii może spowodować uszkodzenie urządzenia. Aby wymienić lub naprawić baterię, skontaktuj się z instalatorem.
e	W przypadku połączenia Wi-Fi, połączenia GPRS/3G/4G LTE, połączenia SMA (czas między odpytaniami: 1800 s), uzyskania dostępu do 8 wejść i 1 klawiatury oraz dostępu do usługi w chmurze.

UWAGA

ISUP5.0: protokół internetowy zapewniający prywatność, który jest używany do uzyskiwania dostępu do platformy strony trzeciej, która obsługuje przesyłanie raportów alarmowych, zarządzanie AX PRO i przesyłanie krótkich filmów.
Priorytety komunikatów i wskazania są takie same. AXPRO przesyła komunikatów i podaje wskazania synchronicznie.

UWAGA

Standardowy protokół DC-09:
ADM-CID: Metodą prezentacji danych DC-09 jest CID, który nie jest szyfrowany i służy tylko do przesyłania raportu alarmowego.
* ADC-CID: Metodą prezentacji danych DC-09 jest CID, który jest szyfrowany i służy tylko do przesyłania raportu alarmowego.
SIA-DCS: Metodą prezentacji danych DC-09 jest DCS (zwany także protokołem SIA), który nie jest szyfrowany i służy tylko do przesyłania raportu alarmowego.
SIA-DCS: Dane prezentujące metodę DC-09

Instrukcja RSSI dla urządzeń peryferyjnych
W odniesieniu do EN 50131-5-3 4.2.2 Wymóg odporności na tłumienie.

Siła sygnału	**Wartość RSSI**	**Oznaczenie**	**Uwagi**

Silny	>120	Zielony	Instalacja dozwolona
Średni	81 to 120	Żółty	Instalacja dozwolona
Słaby	60 to 80	Czerwony	Instalacja nie jest zalecana, ale może działać
Niedopuszczalny	0 to 59	Czerwony (miga)	Nie można zainstalować, nie działa prawidłowo

UWAGA

Instaluj urządzenia peryferyjne tylko wtedy, gdy siła sygnału przekracza 80. Aby uzyskać znacznie lepsze funkcjonowanie systemu, instalację wykonuj na 120 i więcej.

Opcje powiadomień AX PRO

AX PRO jest odpowiedni dla poniższych wymagań powiadamiania wraz z wymaganymi sygnalizatorami.

Sprzęt powiadamiający	I&HAS Grade 2		
	Opcje		
	C	E	F
Dźwiękowy WD z własnym zasilaniem	2	1	Opcjonalnie
ATS	DP1	Opcjonalnie	DP2

1.3 Wygląd

Panel przedni

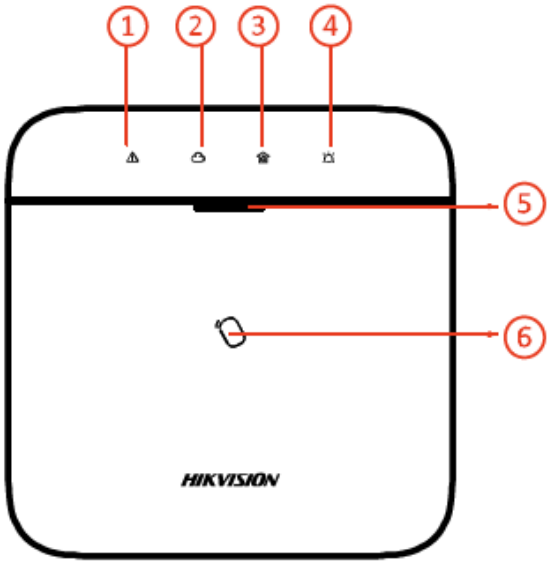


Tabela 1-2 Opis panelu przedniego

Nr	Nazwa	Opis
1	Wskaźnik alertów	Świeci na pomarańczowo: w stanie rozbrojenia dioda LED wskazuje alarm (taki jak alarm napadowy, alarm strefy, alarm sabotażowy itp.) oraz błąd (taki jak błąd działania, błąd połączenia itp.)
		UWAGA • Wskaźnik lub powiadomienia głosowe nie będą reagować na żadną operację wykonaną przez użytkowników poziomu 1. Powiadomienia będą odpowiadać tylko wtedy, gdy użytkownik poziomu 1 przedstawi lub użyje ważny znacznik lub pilot. • Urządzenie wyświetli szczegółowe informacje o alarmie lub błędzie, podczas gdy autoryzowani użytkownicy rozbroją system.
2	Wskaźnik łącza	Świeci na zielono: panel jest powiązany z kontem Hik-connect Wył.: panel nie jest powiązany z kontem Hik-connect
3	Wskaźnik uzbrojenia/rozbrojenia	Świeci na niebiesko przez 5 sekund: uzbrojony Miga na zielono dwa razy: rozbrojony

Nr	Nazwa	Opis
		UWAGA Jeśli funkcja wskaźnika uzbrojenia stale się świeci jest włączona, dioda LED świeci na niebiesko, gdy jest uzbrojona, i gaśnie, gdy jest rozbrojona. Funkcja nie jest zgodna z normą EN.
4	Wskaźnik alarmu	Miga na czerwono: wystąpił alarm Świeci na czerwono: sabotaż urządzenia Wył.: brak alarmu
5	Wskaźnik zasilania	Świeci na zielono: zasilanie włączone Wył.: wyłączone
6	Obszar obecności znacznika	**UWAGA** Funkcja różni się w zależności od modelu urządzenia.

Komponent i interfejs

Zdejmij tylną pokrywę; niektóre komponenty i interfejsy zlokalizowane są na panelu tylnym.

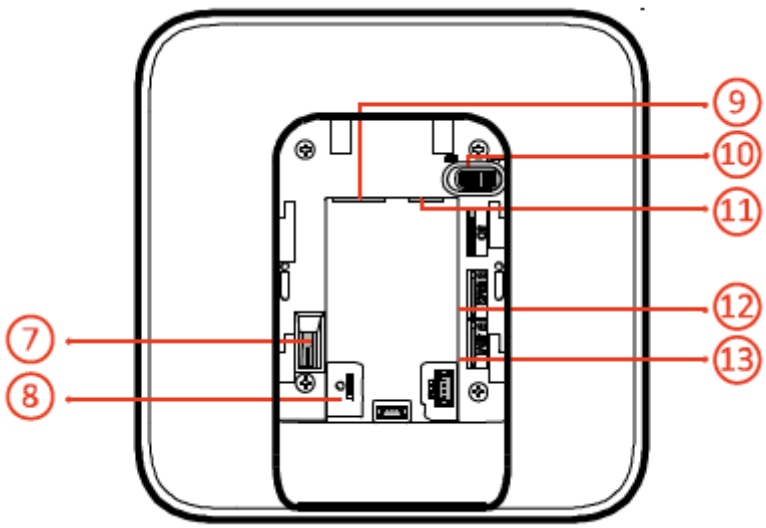


Tabela 1-3 Opis panelu tylnego

Numer	Opis
7	Włącznik zabezpieczający
8	Przycisk resetowania

Numer	Opis
	UWAGA Uruchom ponownie urządzenie, dioda LED zasilania miga 3 razy; przytrzymaj przycisk resetowania przez 5 sekund. Komunikat głosowy wskazuje wynik operacji. Naciśnij przycisk, aby przełączyć tryb STA i Hotspot.
9	Interfejs zasilania
10	Włącznik zasilania
11	Interfejs sieciowy
12	Gniazdo karty SIM 1
	UWAGA Funkcja GPRS lub 3G/4G (wdrażana z wbudowanym gniazdem na kartę SIM) różni się w zależności od modelu urządzenia.
13	Gniazdo karty SIM 2
	UWAGA Funkcja GPRS lub 3G/4G (wdrażana z wbudowanym gniazdem na kartę SIM) różni się w zależności od modelu urządzenia.

Rozdział 2 Uruchomienie

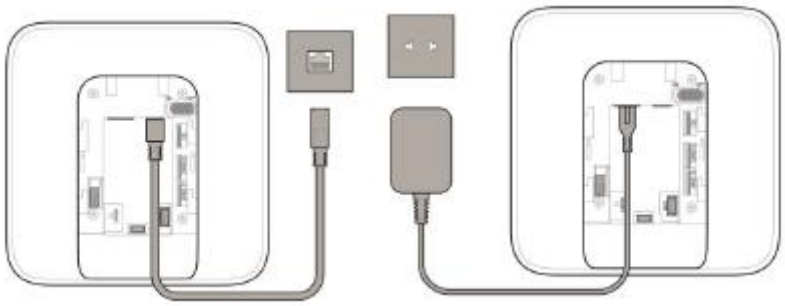
2.1 Inicjalizacja urządzenia

Podczas inicjalizacji urządzenia za pomocą Hik-ProConnector, zawsze dodaj najpierw AX Pro do konta instalatora. Konto instalatora przeniesie własność na konto administratora później, po zakończeniu wszystkich początkowych ustawień i testów.

Aby zainicjować bezprzewodowy system alarmowy, wykonaj poniższe czynności.

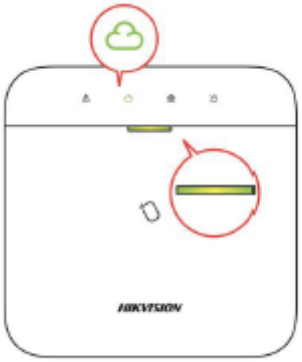
1. Połącz się z siecią.

Podłącz urządzenie do sieci Ethernet i włącz je.



UWAGA

Gdy urządzenie jest włączone, dioda LED zasilania i dioda LED połączenia zmieniają kolor na zielony.



2. Utwórz lokalizację

Otwórz Hik-ProConnect i zaloguj się na konto instalatora.

Lokalizacja to miejsce, w którym został wdrożony system alarmowy. Utwórz lokalizację, do której można dodać urządzenie, podając jego nazwę i adres. Właścicielem lokalizacji będzie użytkownik końcowy, zwykle uważany za administratora.

3. Dodaj urządzenie

Otwórz lokalizację. Dotknij Dodaj urządzenie i zeskanuj kod QR na etykiecie panelu.

Panel sterowania zostanie dodany do lokalizacji utworzonej i zarządzanej przez konto instalatora, co oznacza również, że konto instalatora zostało utworzone w panelu.

Instalator może teraz przeprowadzić konfigurację i testy panelu przed wdrożeniem. Za pomocą konta instalatora Hik-ProConnect można zalogować się zarówno do usługi Hik-ProConnect, jak i do lokalnego klienta internetowego.

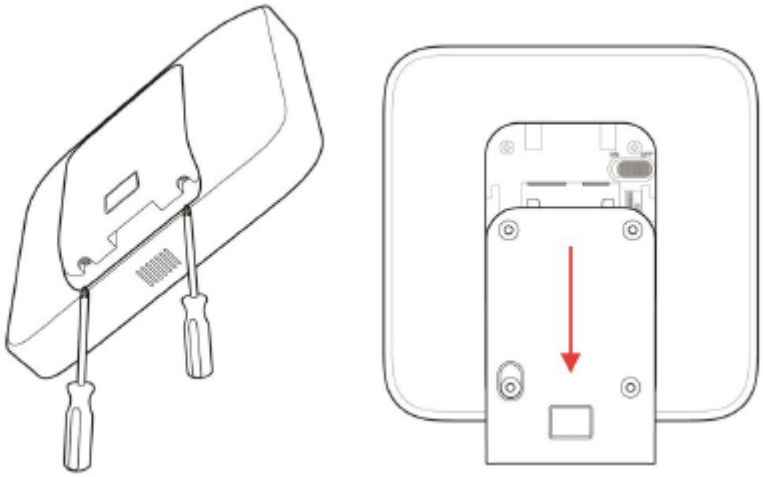
UWAGA

Podczas inicjalizacji urządzenia za pomocą Hik-connect, nie musisz najpierw tworzyć lokalizacji. Pobierz i zaloguj się do aplikacji, a następnie dodaj urządzenie, skanując kod QR lub wprowadź numer seryjny urządzenia.

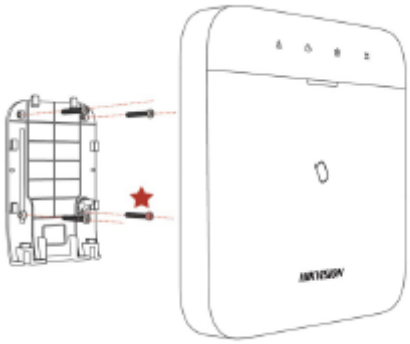
2.2 Zainstaluj urządzenie

Kroki

1. Odkręć śrubę na tylnej pokrywie. Zsuń tylną pokrywę i zdejmij ją z AX PRO.



2. Zabezpiecz tylną pokrywę w pozycji montażowej za pomocą dostarczonych śrub. Przymocuj AX PRO do tylnej pokrywy i dokręć śrubę tylnej pokrywy, aby zakończyć instalację.



UWAGA

- Czerwona Gwiazdka: Śruba TAMPER. Obowiązkowe jest zabezpieczenie śruby chronionej przed odkręceniem.
- Nie są wymagane żadne regulacje.
- Do użytku tylko w nadzorowanych pomieszczeniach.

UWAGA

Sprawdź siłę sygnału RF przed podłączeniem i instalacją urządzenia peryferyjnego. Możesz wyświetlić wskazanie siły sygnału RF na urządzeniu peryferyjnym.

Rozdział 3 Zarządzanie użytkownikami

3.1 Zarządzanie użytkownikami

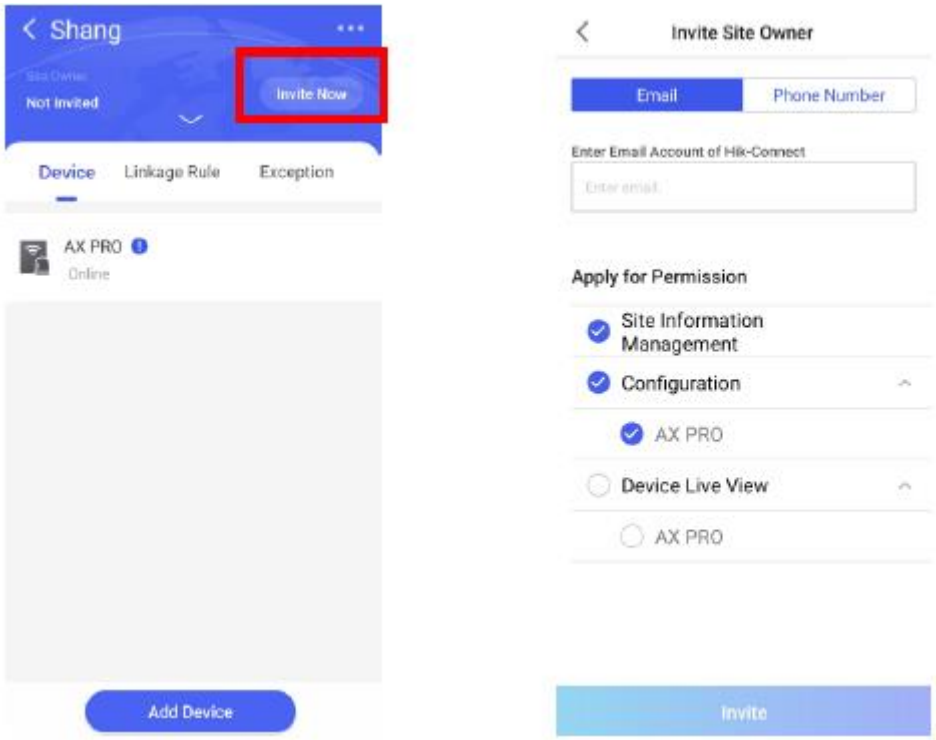
UWAGA

● Użytkowników można tworzyć w klientach.

● Nazwa i hasło użytkownika sieciowego (klienta sieciowego i użytkownika aplikacji) może mieć od 1 do 32 znaków i od 8 do 16 znaków.

3.1.1 Zaproszenie Administratora

Administrator znany jako właściciel lokalizacji w usłudze Hik-ProConnect.

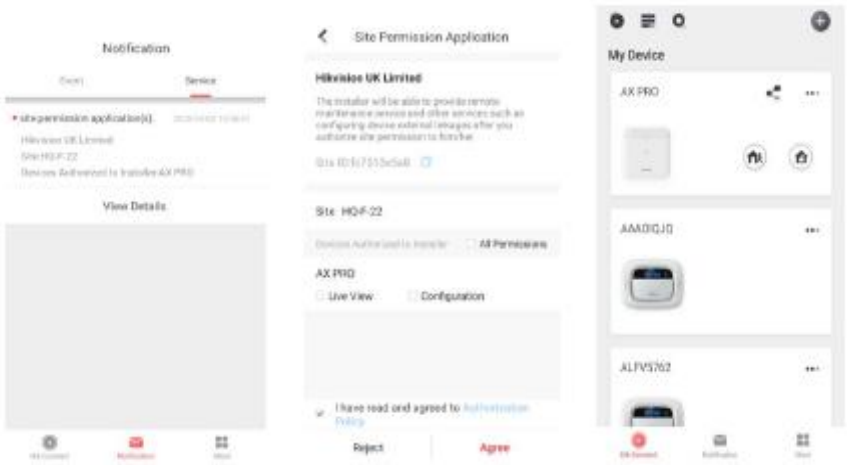


Po zakończeniu wstępnej konfiguracji instalator zaprosi właściciela lokalizacji i zastosuje pozwolenie na zarządzanie lokalizacją i konfigurację urządzenia z konta administratora. Konto administratora byłoby kontem użytkownika końcowego w usłudze Hik-Connect.

Naciśnij przycisk „Zaproś teraz” i wprowadź konto e-mail lub numer telefonu, aby przenieść własność lokalizacji na administratora. Jednocześnie instalator zastosuje uprawnienia od właściciela lokalizacji, takie jak konfiguracja i zarządzanie.

Otwórz aplikację Hik-Connect i zaloguj się na konto administratora. Żądanie usługi instalatora zostanie odebrane na stronie powiadomienia. Otwórz szczegóły powiadomienia, aby zaakceptować uprawnienia usługi instalatora i konfiguracji. Panel sterowania i inne urządzenia w lokalizacji zostaną wyświetlone na liście urządzeń.

Konto administratora zostanie dodane do panelu sterowania, za pomocą którego będzie można zalogować się do aplikacji Hik-Connect i lokalnego klienta sieciowego.



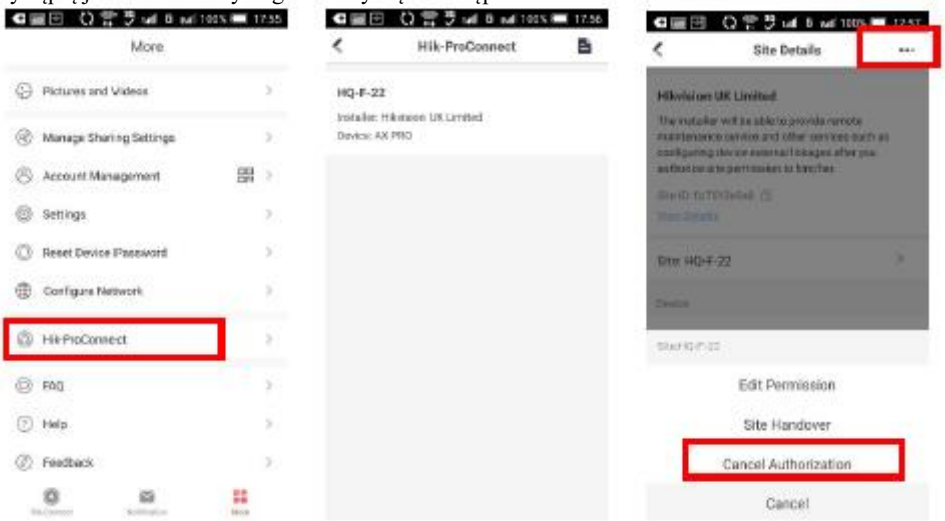
3.1.2 Anulowanie dostępu instalatora

Administrator może anulować uprawnienia dostępu instalatora.

1. Wejdź na stronę Więcej i kliknij Hik-ProConnect. Wszystkie lokalizacje zarządzane przez usługę Hik-ProConnect są wymienione na stronie.

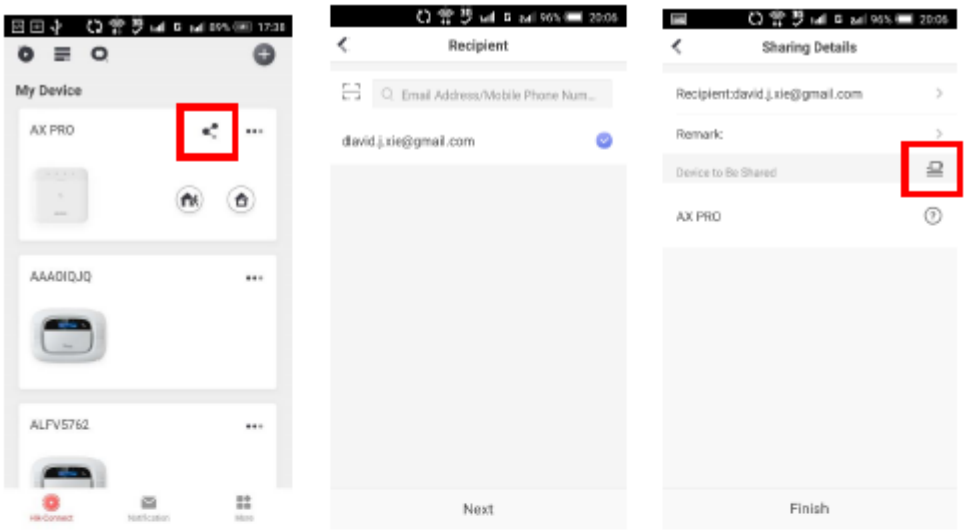
2. Kliknij przycisk opcji w prawym górnym rogu strony szczegółów lokalizacji, a następnie kliknij Anuluj autoryzację w menu kontekstowym.

3. Potwierdź operację; autoryzacja instalatora zostanie anulowana. Po anulowaniu autoryzacji instalator musi zastosować ją ponownie, jeśli wystąpią jakiekolwiek wymagania dotyczące dostępu.



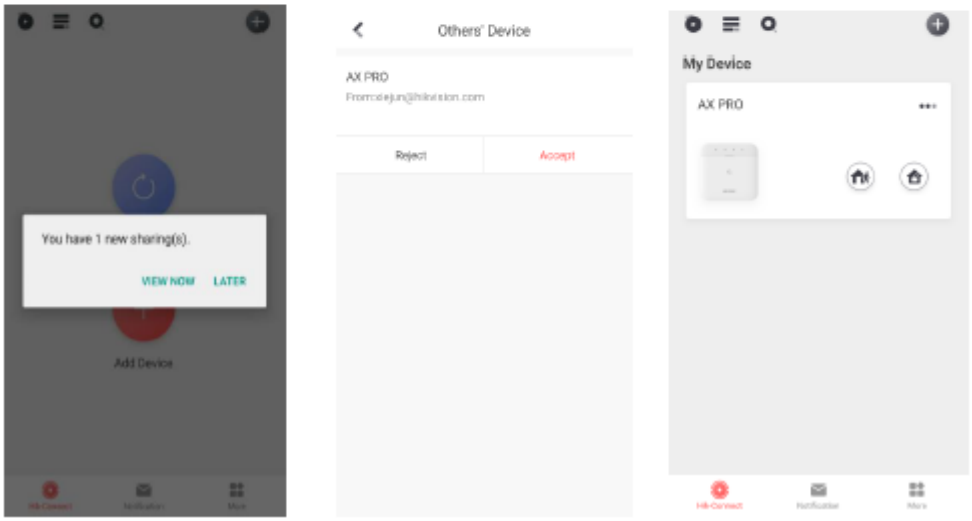
3.1.3 Dodaj operatora

Administrator może udostępniać urządzenie innym operatorom.



1. Kliknij (przycisk udostępniania) na liście urządzeń.
2. Wprowadź konto operatora Hik-Connect.

Administrator może również wybrać, które urządzenie ma zostać udostępnione.



Komunikat o udostępnieniu zostanie wysłany na konto operatora, a operator może go przeczytać w aplikacji Hik-Connect.

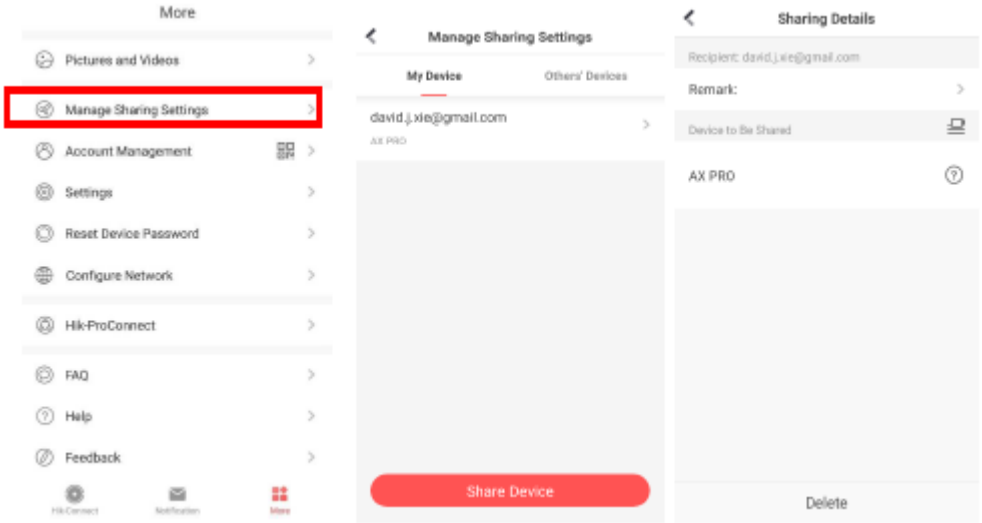
3. Zaakceptuj zaproszenie, a urządzenie zostanie umieszczone na liście urządzeń.

Konto operatora zostanie dodane do panelu sterowania, za pomocą którego można będzie zalogować się do aplikacji Hik-Connect i lokalnego klienta sieciowego.

3.1.4 Usuń operatora

Administrator może usunąć operatora.

1. Wejdź na stronę Więcej i kliknij Zarządzaj ustawieniami udostępniania.
2. Usuń wybranego operatora lub usuń go z urządzenia.



3.2 Wejściowe dane dostępowe

Instalatorowi i operatorom AXPRO przydzielono różne poziomy dostępu, które określają funkcje systemu, które z kolei może wykonywać pojedynczy użytkownik. Dostępne są różne wpisy użytkowników dla różnych ról użytkowników z określonym poziomem dostępu.

Wpisy dostępu dla instalatorów (poziom dostępu 3)

• Usługa Hik-ProConnect

Hik-ProConnect to usługa dla instalatorów służąca do zdalnego zarządzania systemami alarmowymi klientów zlokalizowanymi w różnych lokalizacjach. Panele sterowania można dodać do konta instalatora w usłudze Hik-ProConnect i zarządzać nimi w lokalizacjach.

• Lokalny klient sieciowy

Odwiedź adres IP urządzenia, który można znaleźć za pomocą narzędzia SADP. Instalator może zalogować się za pomocą konta usługi Hik-ProConnect po dodaniu panelu.

• Starsze wpisy

Numery PIN i znaczniki klawiatury można również przypisać użytkownikowi instalatora na określonym poziomie dostępu w celu

wykonywania podstawowych operacji.

Wejściowe dane dostępowe dla administratora i operatorów (poziom dostępu 2)

• Usługa Hik-Connect

Z usługi Hik-Connect mogą korzystać użytkownicy końcowi w celu uzyskania dostępu do urządzeń i zarządzania nimi.

• Lokalny klient sieciowy (dla administratora)

Po dodaniu panelu do konta użytkownika końcowego w usłudze Hik-Connect, konta Hik-Connect można używać do logowania się do wbudowanego klienta sieciowego.

Operatorzy nie mogą zalogować się do klienta sieciowego.

• Starsze wpisy

Można również przypisać numery PIN i znaczniki klalwiatury do użytkownika końcowego na określonym poziomie dostępu w celu wykonania niezbędnych operacji.

Rozdział 4 Konfiguracja

4.1 Konfiguracja za pomocą Hik-Proconnect

Instalator może użyć Hik-Proconnect do skonfigurowania AX PRO, na przykład aktywacji, rejestracji urządzenia itp.

Pobierz i zaloguj się do Hik-ProConnect

Pobierz klienta mobilnego Hik-ProConnect i zaloguj się do klienta przed uruchomieniem AX PRO.

Kroki

1. Pobierz klienta mobilnego Hik-ProConnect.
2. Opcjonalnie: Jeśli po raz pierwszy używasz klienta mobilnego Hik-ProConnect, zarejestruj nowe konto.

UWAGA

• Aby uzyskać szczegółowe informacje, patrz Instrukcja obsługi klienta mobilnego Hik-ProConnect.

• Do rejestracji potrzebny jest kod zaproszenia. Skontaktuj się ze wsparciem technicznym.

3. Uruchom i zaloguj się do klienta.

Dodaj AX PRO do klienta mobilnego

Przed rozpoczęciem innych operacji, dodaj AX PRO do klienta mobilnego.

Kroki

1. Włącz AX PRO.
2. Utwórz lub wyszukaj lokalizację.

- Dotknij +, ustaw nazwę lokalizacji, strefę czasową, adres, miasto, stan/prowincję/region i dotknij OK, aby utworzyć lokalizację.
- Wprowadź nazwę lokalizacji w obszarze wyszukiwania i dotknij ikony wyszukiwania, aby przeszukać lokalizację.

3. Kliknij Dodaj urządzenie.

- Kliknij opcję Skanuj kod QR, aby przejść do strony skanowania kodu QR. Zeskanuj kod QR w AX PRO.

UWAGA

Zwykle kod QR jest wydrukowany na etykiecie przyklejonej na tylnej okładce AX PRO.

Kliknij opcję Dodawanie ręczne, aby przejść do strony Dodaj urządzenie. Wprowadź numer seryjny urządzenia i kod weryfikacyjny, aby dodać urządzenie.

4. Aktywuj urządzenie.

Dodawanie urządzenia peryferyjnego do AX PRO

Dodawanie urządzenia peryferyjnego do AX PRO.

Kroki

1. Wybierz lokalizację.
2. Wybierz urządzenie sterujące (AX PRO).
3. Kliknij ikonę +.

- Kliknij opcję Skanuj kod QR, aby przejść do strony skanowania kodu QR. Zeskanuj kod QR na urządzeniu peryferyjnym.
- Kliknij opcję Dodawanie ręczne, aby przejść do strony Dodaj urządzenie. Wprowadź numer seryjny urządzenia i kod weryfikacyjny, aby dodać urządzenie.

Zarządzanie użytkownikami

Instalatorzy (użytkownik Hik-ProConnect) mogą zarządzać użytkownikami. Jeśli jesteś administratorem, możesz dodawać, edytować i usuwać użytkowników oraz przypisywać różne uprawnienia nowo dodanym użytkownikom.

Kroki

UWAGA

Istnieją cztery typy użytkowników AX PRO obejmujące administratora (lub właściciela), operatora i instalatora (lub ustawiającego). Różne typy użytkowników mają różne uprawnienia dostępu do funkcjonalności AX PRO.

1. Wejdź na stronę, kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli jest to wymagane), aby wejść na stronę AX PRO.
2. Kliknij Dalej, aby zaprosić użytkownika.

UWAGA

Odbiorca musi zaakceptować zaproszenie.

3. Kliknij → Zarządzanie użytkownikami → Użytkownik.
4. Kliknij użytkownika, aby wejść na stronę zarządzania użytkownikami.
5. Opcjonalnie: W razie potrzeby wykonaj następujące czynności.

Zezwolenie użytkownika	Możesz dotknąć użytkownika docelowego na liście użytkowników, a następnie dotknąć ikony Edytuj, aby ustawić uprawnienia przypisane dla użytkownika docelowego. **UWAGA** Wyłącznie administrator może wykonać taką operację.
Ustaw powiązane obszary	Jeśli użytkownik docelowy jest operatorem, dotknij użytkownika docelowego na liście użytkowników, a następnie dotknij Powiązane obszary, aby ustawić obszar powiązany z użytkownikiem docelowym.

UWAGA

Wyłącznie administrator może wykonać taką operację.

Edytuj hasło klawiatury	Jeśli docelowym użytkownikiem jest administrator, instalator lub operator, możesz dotknąć użytkownika docelowego na liście użytkowników, a następnie dotknąć opcji Edytuj hasło klawiatury, aby ustawić hasło klawiatury dla użytkownika docelowego.
Edytuj hasło przymusu	Jeśli użytkownik docelowy jest administratorem lub operatorem, możesz dotknąć użytkownika docelowego na liście użytkowników, a następnie dotknąć opcji Edytuj hasło przymusu, aby ustawić hasło przymusu dla użytkownika docelowego.

UWAGA

W warunkach przymusu, możesz wprowadzić kod przymusu na klawiaturze, aby uzbroić i rozbroić obszar(y) i przesłać alarm przymusu.

Sterowanie automatyzacją	Administrator, instalator lub operator może sterować modułem przekaźnikowym, czujnikiem naściennym i inteligentną wtyczką.

UWAGA

● Pozycje konfiguracji i uprawnienia użytkownika będą się różnić w zależności od typu użytkownika.

● Możesz przeglądać połączone karty/znaczniki i piloty użytkownika, ale nie masz uprawnień do ich konfigurowania.

Zarządzanie kartami/znacznikami

Po dodaniu kart/znaczników do bezprzewodowego AX PRO, możesz przeciągnąć kartę/znacznik, aby uzbroić lub rozbroić wszystkie wykrywacze dodane do określonego obszaru (obszarów) AX PRO i wyciszyć alarmy.

UWAGA

ID/PIN znacznika to 32-bitowa liczba całkowita, a wariantem może być 42949672956.

Kroki

1. Wejdź na stronę, kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli jest to wymagane), aby wejść na stronę.
2. Kliknij → Zarządzani użytkownikiem → Karta/znacznik, aby wejść na stronę Zarządzanie znacznikiem.
3. Kliknij +, aby dodać znacznik.
4. Po usłyszeniu komunikatu głosowego „Swipe Tag” umieść znacznik w obszarze przedstawienia znacznika AX PRO.

● Wygenerowanie sygnału dźwiękowego oznacza, że znacznik został rozpoznany.

● Znacznik zostanie wyświetlony na stronie Znacznik.

5. Opcjonalnie: kliknij znacznik, aby przejść do strony ustawień.

6. Kliknij ikonę Edytuj, aby edytować Nazwę znacznika.

UWAGA

● Jeśli logujesz się jako instalator, pomiń ten krok. Edycja Nazwy znacznika jest dostępna tylko dla administratora.

● Nazwa powinna zawierać od 1 do 32 znaków.

7. Przesuń znacznik aktywacji...

8. Wybierz połączonego użytkownika.

9. Wybierz typ znacznika

UWAGA

Różni połączeni użytkownicy mają różne uprawnienia w zakresie znaczników.

Znacznik obsługi

Możesz przesunąć znacznik, aby uzbroić lub rozbroić.

Znacznik patrolowy

Kiedy przesuniesz znacznik, system wczyta zapis.

10. Opcjonalnie: Kliknij Usuń, aby usunąć znacznik.

Ustawienia systemowe

Konfiguracja systemu

Możesz ustawić strefę czasową urządzenia i czas DST.

Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne).

Kliknij → System → Konfiguracja, aby wejść na stronę konfiguracji.

Możesz kliknąć, aby wybrać strefę czasową.

Możesz włączyć czas letni i ustawić odchylenie czasu letniego, datę rozpoczęcia czasu letniego i zakończenia czasu letniego.

Opcje systemu

Ustaw opcje systemu.

Zarządzanie opcjami

Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne).

Kliknij → System → System

Opcje → Zarządzanie systemem, aby wejść na stronę.

Wymuszone automatyczne uzbrojenie

Jeżeli opcja jest włączona, a w strefie są aktywne usterki, wejście jest blokowane automatycznie.

Raport o stanie systemu

Przełącznik do przesyłania raportów systemowych.

Komunikat głosowy

Jeśli opcja jest włączona, AX PRO włączy tekstowe podpowiedzi głosowe.

Dźwiękowy alarm sabotażowy

Jeżeli opcja jest włączona, system poinformuje za pomocą brzęczyka o alarmie sabotażowym.

Jeśli opcja jest wyłączona, urządzenia peryferyjne będą komunikować otwarcie pokrywy, ale nie będą łączyć się z alarmami.

Głośność systemu

Dostępny zakres głośności systemu wynosi od 0 do 10.

Przycisk blokady panelu

Jeśli opcja jest włączona, instalator może użyć funkcji przycisku blokady, aby zablokować AX PRO. Po zablokowaniu użytkownicy nie mogą obsługiwać urządzenia i odbierać komunikatów.

Czas trwania alarmu panelu

Ustaw czas trwania alarmów panelu.

Czasy strat zapytywania

Ustaw maksymalny czas trwania straty zapytywania. System zgłosi błąd, jeśli czas trwania przekroczy limit.

Pomiń przy ponownym uzbrojeniu

Pominięta strefa zostanie ponownie uzbrojona, jeśli usterki w jej obrębie zostaną usunięte.

Kontrola usterki

Na stronie kliknij AX PRO. Kliknij → System → Opcje systemowe → Kontrola usterki panelu, aby wejść na stronę.

Wykrycie odłączenia kamery sieciowej

Jeśli opcja jest włączona, po odłączeniu podłączonej kamery sieciowej zostanie uruchomiony alarm.

Kontrola usterki baterii

Jeżeli opcja jest włączona, przy odłączonej lub wyładowanej baterii urządzenie nie będzie przesyłać zdarzeń.

Kontrola usterki sieci LAN

Jeżeli opcja jest włączona, przy rozłączeniu sieci przewodowej lub przy innych uszkodzeniach wywołany zostanie alarm.

Kontrola usterki Wi-Fi

Jeżeli opcja jest włączona, przy rozłączeniu Wi-Fi lub przy innych awariach wywołany zostanie alarm.

Sprawdzanie błędów sieci komórkowej

Jeżeli opcja jest włączona, przy rozłączeniu sieci komórkowej lub przy innych awariach wywołany zostanie alarm.

Czas kontroli wyłączenia zasilania prądem przemiennym

System sprawdza usterkę po skonfigurowanym czasie od wyłączenia zasilania AC.

Aby zachować zgodność z normą EN 50131-3, czas kontroli powinien wynosić 10 s.

Instrukcje systemowe

Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne). Kliknij → System → Opcje systemu → Instrukcje systemowe, aby wejść na tę stronę.

Uzbrojenie z usterką

Jeżeli opcja jest włączona, gdy podczas procedury uzbrajania wystąpi błąd, możesz przerwać uzbrajanie ręcznie.

Lista kontrolna

System sprawdzi, czy urządzenie ma błędy na liście kontrolnej podczas procedury uzbrajania.

Uzbrojenie z listą kontrolną usterek

Sprawdź błędy na liście kontrolnej usterek, a urządzenie nie przerwie procedury uzbrajania, gdy wystąpią błędy.

Dioda LED Uzbrojenia pozostaje włączona

Jeśli urządzenie stosuje normę EN, domyślnie funkcja jest wyłączona. W takim przypadku, jeśli urządzenie jest uzbrojone, dioda LED będzie świecić ciągłym niebieskim światłem przez 5 sekund. A jeśli urządzenie jest rozbrojone, dioda LED zamiga 5-krotnie.

Gdy funkcja jest włączona, a urządzenie jest uzbrojone, dioda LED będzie świecić przez cały czas. A jeśli urządzenie jest rozbrojone, dioda LED zgaśnie.

Komunikaty o błędach podczas uzbrajania

Jeśli urządzenie stosuje normę EN, domyślnie funkcja jest wyłączona. W takim przypadku urządzenie nie będzie sygnalizowało błędów podczas procedury uzbrajania.

Błędne monity przy rozbrojeniu

Jeśli urządzenie stosuje normę EN, domyślnie funkcja jest wyłączona. W takim przypadku urządzenie nie będzie sygnalizować błędów podczas procedury rozbrajania.

Wczesny alarm

W przypadku włączenia funkcji, gdy strefa jest uzbrojona i nastąpi wyzwolenie, po upływie czasu opóźnienia zostanie wywołany alarm.

Czas alarmu wczesnego

Gdy funkcja wczesnego alarmu jest włączona ustaw czas wczesnego alarmu. Alarm zostanie wyzwolony po skonfigurowanym czasie wczesnego alarmu.

Metoda rejestracji

1. Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne).
2. Kliknij → System → Opcje systemu → Metoda rejestracji, aby wejść na stronę.
3. Kliknij Wejdź do trybu rejestracji.
4. Postępuj zgodnie z instrukcjami na stronie, aby dodać urządzenie.
5. Kliknij Wyjdź z trybu rejestracji.

Kamera sieciowa

Dodaj kamery do AX PRO

Kroki

1. Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne).
2. Kliknij → IPC → Zarządzanie IPC, aby wejść na stronę.
3. Kliknij Dodaj.
4. Wprowadź adres IP, port, nazwę użytkownika i hasło kamery.
5. Kliknij ikonę Zapisz.
6. Opcjonalnie: dotknij Edytuj lub Usuń, aby edytować lub usunąć wybraną kamerę.

Ustawianie parametrów wideo

Kroki

1. Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne).
2. Kliknij → IPC → Ustawienia wideo wydarzenia, aby wejść na stronę.
3. Wybierz kamerę i ustaw parametry wideo.

Typ strumienia

Strumień główny: używany do nagrywania i podglądu HD, ma wysoką rozdzielczość, współczynnik kodowania i jakość obrazu.

Podstrumień: Służy do transmisji sieciowej i podglądu obrazów jako strumień wideo z funkcjami o niższej rozdzielczości, szybkości transmisji i jakości obrazu.

Typ szybkości transmisji

Wybierz typ szybkości transmisji jako stałą lub zmienną.

Rozdzielczość

Wybierz rozdzielczość danych wyjściowych wideo.

Szybkość transmisji wideo

Wyższa wartość odpowiada wyższej jakości wideo, ale wymagana jest większa przepustowość.

Ustaw harmonogram uzbrajania/rozbrajania

1. Ustaw harmonogram uzbrajania/rozbrajania, aby automatycznie uzbroić/rozbroić określoną strefę.
2. Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne).
3. Kliknij → Obszar, aby wejść na stronę.
4. Kliknij obszar na liście, aktywuj go i wybierz połączone obszary.
5. Włącz funkcję automatycznego uzbrajania/rozbrajania i ustaw czas automatycznego uzbrojenia/automatycznego rozbrojenia. Można również ustawić czas opóźnienia rozbrajania, czas opóźnienia wejścia, czas opóźnienia wyjścia, czas opóźnienia sygnalizatora, wyjątek świąteczny i wyjątek weekendowy.

Automatyczne uzbrojenie

Umożliwia obszarowi automatyczne uzbrojenie się w określonym momencie.

Czas automatycznego uzbrojenia

Ustawia harmonogram automatycznego uzbrajania obszaru.

Automatyczne rozbrojenie

Aktywuje obszar, aby automatycznie rozbroił się w określonym momencie.

Czas automatycznego rozbrojenia

Ustawia harmonogram automatycznego rozbrojenia obszaru.

Opóźnienie rozbrojenia

Włącz urządzenie, aby wysyłało powiadomienie do telefonu lub tabletu, aby przypomnieć użytkownikowi o rozbrojeniu obszaru, gdy obszar jest nadal uzbrojony po określonym czasie.

UWAGA

Zalecamy włączenie funkcji Powiadomienia zarządzania panelem w kliencie sieciowym Parametry komunikacji → Komunikowanie o zdarzeniu przed włączeniem funkcji opóźnienie rozbrojenia.

Czas opóźnienia rozbrojenia

Ustaw punkt czasowy wskazany w Opóźnionym rozbrojeniu.

Wyjątek weekendowy

Jeśli funkcja jest włączona, Automatyczne uzbrojenie, Automatyczne rozbrojenie i Opóźnione rozbrojenie są wyłączone na weekend.

Wyjątek świąteczny

Po aktywacji tej funkcji strefa nie będzie uzbrajana/rozbrajana w święta. Harmonogram świąteczny należy ustawić po włączeniu.

UWAGA

Można ustawić do 6 grup świątecznych.

Komunikacja

Sieć danych komórkowych

Wprowadź tutaj krótki opis zadania (opcjonalnie).

Kroki

1. Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne).
2. Kliknij → Parametry komunikacji → Ustawienia sieci danych komórkowych, aby wejść na stronę.
3. Włącz sieć komórkową.
4. Dotknij opcji Konfiguracja parametrów → Ikona edycji i ustaw parametry, w tym nazwę użytkownika, hasło dostępu, APN, MTU i warunek PIN.
5. Kliknij ikonę Zapisz.
6. Włącz limit wykorzystania danych.
7. Edytuj dane używane w tym miesiącu i dane ograniczone miesięcznie.

Powiadomienia push

Po wyzwoleniu alarmu, jeśli chcesz wysłać powiadomienie o alarmie na telefon komórkowy, możesz ustawić parametry powiadomień push.

Kroki

1. Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne).
2. Kliknij → Parametry komunikacji → Powiadomienia push, aby wejść na stronę.
3. Kliknij Połączenie telefoniczne i SMS.
4. Kliknij + lub + Dodaj numer telefonu, aby wprowadzić numer telefonu.
5. Kliknij dodany numer telefonu, aby włączyć połączenia telefoniczne i SMS-y zgodnie z potrzebami.
6. (W przypadku połączenia telefonicznego) Ustaw liczbę połączeń.
7. (dla SMS) Ustaw zezwolenie na uzbrojenie, zezwolenie na rozbrojenie i zezwolenie na kasowanie alarmu dla obszarów.
8. Sprawdź powiadomienia.

Alarm strefy/Powiadomienia dotyczące pokrywy

Urządzenie będzie wysyłać powiadomienia, gdy zostanie wyzwolony alarm strefy lub zostanie otwarta, lub przywrócona do stanu pierwotnego pokrywa strefy.

UWAGA

Musisz ustawić interwał filtrowania zdarzeń dla połączeń telefonicznych.

Otwarta pokrywa urządzeń peryferyjnych

Urządzenie będzie wysyłać powiadomienia po otwarciu lub przywróceniu pokrywy dowolnego urządzenia peryferyjnego.

Otwarta pokrywa panelu

Urządzenie będzie wysyłać powiadomienia, gdy otwarta pokrywa panelu sterowania zostanie wyzwolona lub przywrócona.

Alarm napadowy

Urządzenie będzie wysyłać powiadomienia o wyzwoleniu lub przywróceniu do stanu pierwotnego alarmu napadowego przez wejścia, klawiatury lub piloty.

Alarm medyczny

Urządzenie będzie wysyłać powiadomienia, gdy zostanie wyzwolony alarm medyczny.

Alarm gazowy

Urządzenie będzie przesyłać powiadomienia, gdy zostanie uruchomiony alarm gazowy.

Stan panelu

Urządzenie będzie wysyłać powiadomienia, gdy zmieni się stan systemu panelu sterowania.

Stan strefy

Urządzenie będzie wysyłać powiadomienia o zmianie stanu strefy.

Stan urządzeń peryferyjnych

Urządzenie będzie wysyłać powiadomienia w przypadku zmiany stanu któregokolwiek z urządzeń peryferyjnych.

Obsługa panelu

Urządzenie będzie wysyłać powiadomienia, gdy użytkownik będzie obsługiwał AX PRO.

Inteligentne powiadomienie o alarmie

Urządzenie będzie wysyłać powiadomienia, gdy alarm zostanie wyzwolony w kamerach termowizyjnych.

Centrum odbioru alarmów (ARC)

Możesz ustawić parametry centrum alarmowego, a wszystkie alarmy zostaną wysłane do skonfigurowanego centrum alarmowego.

Kroki

1. Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne).
2. Kliknij → Parametry komunikacji → Centrum odbioru alarmów (SMA), aby wejść na tę stronę.
3. Wybierz ARC i włącz je.
4. Wybierz typ protokołu jako ADM-CID, ISUP, SIA-DCS, * SIA-DCS lub * ADM-CID, aby ustawić tryb przesyłania.

ADM-CID lub SIA-DCS

Wybierz typ adresu jako adres IP lub nazwę domeny i wprowadź adres IP/nazwę domeny, numer portu, kod konta, tryb transmisji, limit czasu ponowienia, liczbę prób, opcję zapytywania i test okresowy.

UWAGA

Ustaw interwał testu okresowego w zakresie od 10 sekund do 24 godzin.

ISUP

Nie ma potrzeby ustawiania parametrów protokołu ISUP.

* SIA-DCS lub * ADM-CID

Zalecamy wybór typu adresu jako IP lub nazwę domeny i wprowadzenie adresu IP/nazwy domeny, numeru portu, kodu konta, trybu transmisji, limitu czasu ponowienia, próby, opcji zapytywania, arytmetyki szyfrowania, długości hasła, tajnego klucza i testu okresowego.

UWAGA

Ustaw interwał testu okresowego w zakresie od 10 sekund do 24 godzin.

Dla arytmetyki szyfrowania: Panel obsługuje format szyfrowania zapewniający bezpieczeństwo informacji zgodnie z DC-09, AES-128, AES-192 i AES-256, które są obsługiwane podczas konfigurowania centrum alarmowego.

W przypadku tajnego klucza: W przypadku korzystania z zaszyfrowanego formatu DC-09 ustaw klucz podczas konfigurowania SMA. Klucz zostałby wydany w trybie offline przez ARC, który zostałby użyty do zaszyfrowania wiadomości w celu zapewnienia bezpieczeństwa zastępczego.

Konserwacja urządzenia

Możesz zrestartować urządzenie.

Kroki

1. Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne).
2. Kliknij → Konserwacja → Konserwacja urządzenia, aby wejść na stronę.
3. Kliknij Test, a następnie Start Walk Test, aby sprawdzić, czy urządzenie działa prawidłowo.
3. Kliknij Konserwacja → Uruchom ponownie urządzenie.

AX PRO uruchomi się ponownie.

Zarządzanie urządzeniami

Wpisz tutaj krótki opis swojej koncepcji (opcjonalnie).

To jest początek twojej koncepcji.

Strefa

Możesz ustawić parametry strefy na stronie strefy.

Kroki

1. Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne).
2. Kliknij strefę w zakładce Urządzenie.
3. Kliknij .
4. Kliknij ikonę Edytuj nazwę strefy.
5. Wybierz typ strefy.

Strefa natychmiastowa

Ten typ strefy natychmiast wyzwoli zdarzenie alarmowe po uzbrojeniu.

Strefa opóźniona

Opóźnienie przy wyjściu: Opóźnienie przy wyjściu zapewnia czas na opuszczenie strefy chronionej bez alarmu.
Opóźnienie przy wejściu: Opóźnienie przy wejściu zapewnia czas na wejście do strefy chronionej w celu rozbrojenia systemu bez alarmu.
System podaje czas opóźnienia wejścia/wyjścia, gdy zostanie uzbrojony lub ponownie włączony. Zwykle jest używany na drodze wejścia/wyjścia (np. drzwi frontowe/główne wejście), co jest kluczową drogą do uzbrajania/rozbrajania za pomocą klawiatury operacyjnej dla użytkowników.

UWAGA

W Opcjach systemu → Harmonogram i Regulator czasowy można ustawić 2 różne czasy trwania.
W celu zachowania zgodności z normą EN50131-1 upewnij się, że regulator czasowy nie jest ustawiony na czas dłuższy niż 45 sekund.
Jeśli strefa jest strefą opóźnioną, można ustawić parametry opóźnienia wejścia/wyjścia.

Strefa śledzenia

Strefa działa jako strefa opóźniona, gdy wykryje zdarzenie wyzwalające podczas Opóźnienia wejścia w systemie, podczas gdy w przeciwnym razie działa jako strefa natychmiastowa.

Całodobowa cicha strefa napadowa

Ten typ strefy jest aktywny przez całą dobę, jest używany do alarmów napadowych lub HUD (urządzeń napadowych), a nie do czujników dymu lub zbicia szyby.

Strefa napadowa

Strefa jest aktywna przez cały czas. Zwykle stosowana jest w obiektach wyposażonych w przycisk napadowy, czujnik dymu i czujnik zbicia szyby.

Strefa zagrożona pożarem

Wejście jest aktywowane za każdym razem z wyjściem dźwiękowym/sygnalizatorem w przypadku wystąpienia alarmu. Zwykle jest stosowana w strefach zagrożonych pożarem, wyposażonych w czujniki dymu i czujniki temperatury.

Strefa zagrożona wyciekiem gazu

Wejście jest aktywowane za każdym razem z wyjściem dźwiękowym/sygnalizatorem w przypadku wystąpienia alarmu. Zwykle jest stosowana w pomieszczeniach wyposażonych w wykrywacze gazu (np. kuchnia).

Strefa medyczna

Strefa aktywowana jest za każdym razem z potwierdzeniem dźwiękowym w przypadku wystąpienia alarmu. Zwykle stosowana jest w miejscach wyposażonych w medyczne przyciski ratunkowe.

Strefa przekroczenia czasu

Strefa jest aktywna przez cały czas. Typ strefy jest używany do monitorowania i raportowania stanu „AKTYWNA" strefa, ale będzie raportować i alarmować o tym stanie dopiero po upływie zaprogramowanego czasu. (1 do 599) sekund. Może być stosowana w miejscach wyposażonych w styki magnetyczne, które wymagają dostępu, ale tylko przez krótki czas (np. drzwiczki do hydrantu przeciwpożarowego lub inne zewnętrzne drzwiczki do skrzynki antywłamaniowej)

Strefa przełącznika kluczykowego

Połączony obszar zostanie uzbrojony po wyzwoleniu i rozbrojony po przywróceniu do stanu poprzedniego. W przypadku alarmu sabotażowego operacja uzbrojenia i rozbrojenia nie zostanie wyzwolona.

Strefa nieaktywna

Strefa nieaktywna, ignorująca każde zdarzenie alarmowe. Zwykle służy do dezaktywacji wadliwych czujników.

6. Aktywuj obejście uzbrojenia w trybie STAY, dzwonek, podwójne pukanie, cichy alarm i inne funkcje zgodnie z rzeczywistymi potrzebami.

UWAGA

● Niektóre strefy nie obsługują tej funkcji. Zapoznaj się z aktualną strefą, aby ustawić funkcję.

● Różne typy stref mają różne parametry.

7. Ustaw częstotliwość zapytywania.

8. Opcjonalnie: Kliknij Usuń, aby usunąć urządzenie.

Klawiatura

Możesz ustawić parametry klawiatury przypisanej do AX PRO.

Kroki

1. Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne).
2. Kliknij klawiaturę na karcie Urządzenie.
3. Kliknij .
4. Kliknij ikonę Edytuj nazwę klawiatury.
5. Włącz opcję aktywacji klawiatury.
6. Wybierz połączonych użytkowników.
7. Kliknij Ustawienia klawiszy funkcyjnych, aby ustawić funkcje pojedynczych klawiszy i kombinacji klawiszy.
8. Opcjonalnie: Kliknij Usuń, aby usunąć urządzenie.

Sygnalizator

Sygnalizator jest przypisany do AX PRO za pośrednictwem bezprzewodowego modułu odbiornika, a bezprzewodowy sygnalizator 868 MHz można przypisać do hybrydowego AX PRO za pośrednictwem bezprzewodowego odbiornika znajdującego się pod adresem 9.

Kroki

1. Na stronie kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne).
2. Kliknij sygnalizator na karcie Urządzenie.
3. Kliknij .
4. Kliknij ikonę Edytuj nazwę sygnalizatora.
5. Wybierz połączone obszary.
6. Ustaw czas trwania alarmu i głośność alarmu.
7. Włącz diodę LED uzbrojenia/rozbrojenia, brzęczyk uzbrajania/rozbrajania, wskaźnik alarmu zgodnie z aktualnymi potrzebami.
8. Ustaw cykl impulsu.
9. Opcjonalnie: Kliknij Usuń, aby usunąć urządzenie.

4.1.2 Korzystanie z Portalu Hik-ProConnect

W przypadku centrali alarmowej AX Pro można wykonywać operacje, w tym uzbrajanie/rozbrajanie obszaru, wyciszenie alarmu, obejście strefy itp. oraz zdalnie konfigurować panel sterowania na Portalu. Możesz również ubiegać się o PIN (wymagany do aktualizacji oprogramowania AX Pro) i zmienić język AX Pro.

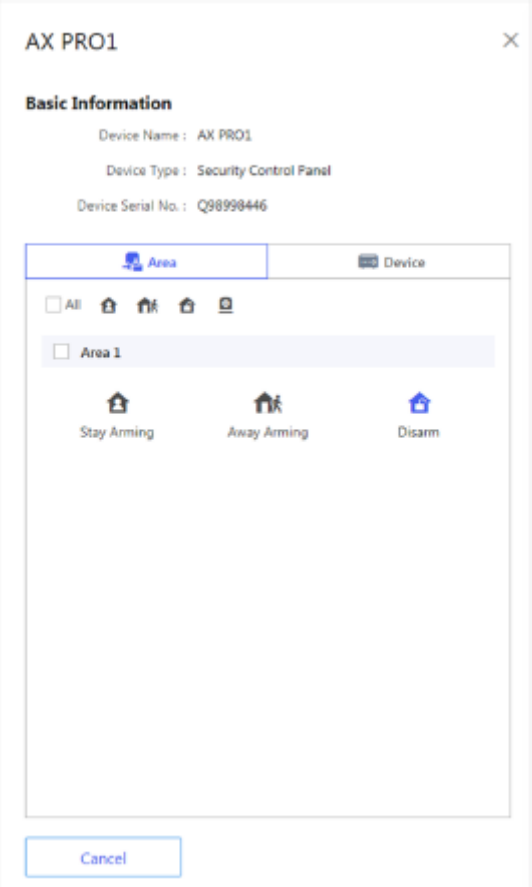
Kliknij Lokalizacja, aby przejść do strony z listą lokalizacji, a następnie kliknij nazwę lokalizacji, aby przejść na stronę szczegółów lokalizacji.

Zdalna obsługa AX Pro

Kliknij AX Pro, aby otworzyć panel operacyjny. Możesz wykonać następujące operacje.

Tabela 4-3 Opis obsługi

Obsługa	Opis
Uzbrojenie w trybie STAY określonego obszaru	Wybierz zakładkę Obszar, a następnie kliknij Uzbrojenie w trybie STAY, aby uzbroić obszar.
Uzbrojenie w trybie AWAY określonego obszaru	Wybierz zakładkę Obszar, a następnie kliknij Uzbrojenie w trybie AWAY, aby uzbroić obszar.
Rozbrojenie określonego obszaru	Wybierz zakładkę Obszar, a następnie kliknij Rozbrojenie.
Uzbrojenie w trybie STAY wielu obszarów	Wybierz zakładkę Obszar, a następnie wybierz obszary i kliknij .
Uzbrojenie w trybie AWAY wielu obszarów	Wybierz zakładkę Obszar, a następnie wybierz obszary i kliknij .
Rozbrojenie wielu obszarów	Wybierz zakładkę Obszar, a następnie wybierz obszary i kliknij .
Wyciszenie alarmów wielu obszarów	Wybierz zakładkę Obszar, a następnie wybierz obszary i kliknij .
Filtrowanie urządzenia peryferyjnego według obszaru	Wybierz zakładkę Urządzenie, a następnie kliknij i wybierz obszar, aby wyświetlić tylko urządzenia peryferyjne połączone z wybranym obszarem lub wybierz opcję Wszystkie, aby wyświetlić wszystkie urządzenia peryferyjne połączone ze wszystkimi obszarami.
Przekaźnik kontrolny	Wybierz zakładkę Urządzenie, a następnie wybierz ekspandor wyjść bezprzewodowych, aby wyświetlić sygnalizatory z nim połączone, a następnie wybierz sygnalizatory, aby je włączyć/wyłączyć.
Obejście strefy	Wybierz zakładkę Urządzenie, a następnie wybierz strefę (tj. czujnik) i włącz przełącznik obejściowy, aby ominąć strefę.



Zdalna konfiguracja AX Pro

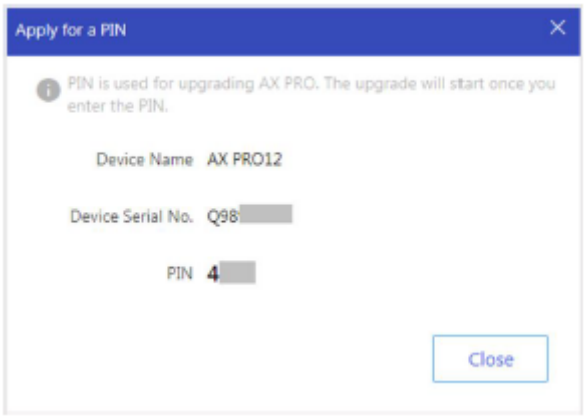
Kliknij , aby wejść na stronę internetową panelu sterowania zabezpieczeniami i skonfigurować urządzenie.

Uwaga

Aby uzyskać szczegółowe informacje na temat konfiguracji panelu sterowania bezpieczeństwem, zapoznaj się z instrukcją obsługi urządzenia.

Uzyskaj kod PIN

Kliknij → aby otworzyć okno Uzyskaj kod PIN. Wyświetlony zostanie kod PIN.

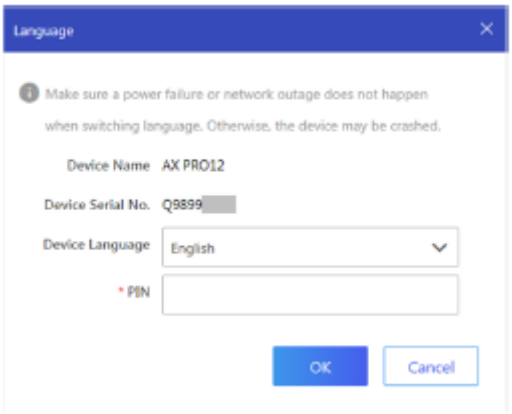


Zmiana języka

UWAGA

Konieczne jest uzyskanie kodu PIN.

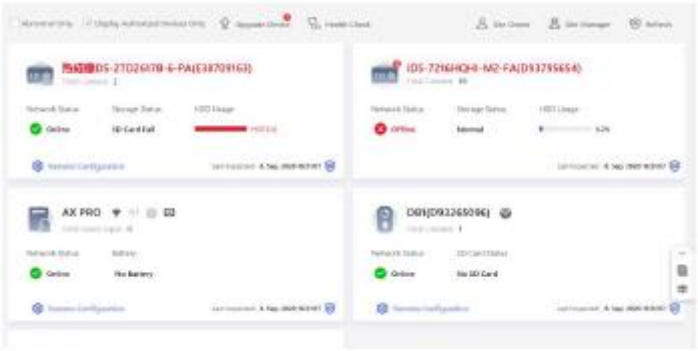
Kliknij • • • → ⇆, aby otworzyć okno Język, a następnie ustawić język urządzenia i wprowadź kod PIN.



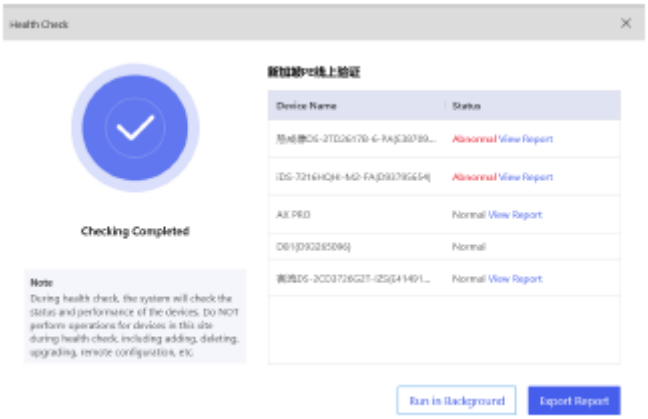
Monitorowanie stanu

1. Wejdź na stronę internetową portalu Hik-ProConnect i kliknij Monitorowanie stanu → Stan, aby wejść na stronę.

2. Wybierz lokalizację.



3. Kliknij Kontrolastanu, a następnie kliknij Sprawdź teraz. Po zakończeniu kontroli można wyświetlić stan i raporty urządzeń. Możesz także wyeksportować raport.



4. Kliknij , aby uzyskać najnowsze dane na temat stanu urządzenia.

4.2 Konfiguracja za pomocą Hik-Connect

Operator może użyć Hik-Connect do sterowania urządzeniem, na przykład do ogólnej obsługi uzbrajania/rozbrajania, zarządzania użytkownikami itp.

Pobierz i zaloguj się do klienta mobilnego

Pobierz klienta mobilnego Hik-Connect i zaloguj się do klienta przed uruchomieniem AX PRO.

Kroki

1. Pobierz klienta mobilnego Hik-Connect.
2. Opcjonalnie: Zarejestruj nowe konto, jeśli po raz pierwszy używasz klienta mobilnego Hik-Connect.

UWAGA

Szczegółowe informacje można znaleźć w instrukcji obsługi klienta mobilnego Hik-Connect.

3. Uruchom i zaloguj się do klienta.

Dodaj AX PRO do klienta mobilnego

Przed rozpoczęciem innych operacji, dodaj AX PRO do klienta mobilnego.

Kroki

1. Włącz AX PRO.
2. Wybierz typ dodawania.

- Dotknij + → Skanuj kod QR, aby wejść na stronę skanowania kodu QR. Zeskanuj kod QR w AX PRO.

UWAGA

Zwykle kod QR jest wydrukowany na etykiecie przyklejonej na tylnej okładce AX PRO.

Dotknij + → Dodawanie ręczne, aby przejść do strony Dodaj urządzenie. Wprowadź numer seryjny urządzenia za pomocą Hik-

Podłącz typ dodawania domeny.

3. Kliknij , aby wyszukać urządzenie.
4.Kliknij Dodaj na stronie wyników.
5. Wprowadź kod weryfikacyjny i kliknij OK.
6. Po zakończeniu dodawania wprowadź alias urządzenia i dotknij Zapisz.
7. Opcjonalnie: kliknij → Usuń, aby usunąć urządzenie.
8. Opcjonalnie: kliknij → , aby edytować nazwę urządzenia.

Dodawanie urządzenia peryferyjnego do AX PRO

Dodaj urządzenie peryferyjne do AX PRO.

Kroki

1. Wybierz urządzenie sterujące (AX PRO).

2. Kliknij +.

- Kliknij Skanuj kod QR, aby przejść do strony skanowania kodu QR. Zeskanuj kod QR na urządzeniu peryferyjnym.
- Kliknij Dodawanie ręczne, aby przejść do strony Dodaj urządzenie. Wprowadź numer seryjny urządzenia i kod weryfikacyjny, aby dodać urządzenie.

Zarządzanie kartami/znacznikami

Po dodaniu kart/znaczników do bezprzewodowego AX PRO możesz przeciągnąć kartę/znacznik, aby uzbroić lub rozbroić wszystkie czujniki dodane do określonego obszaru (obszarów) AX PRO i wyciszyć alarmy.

Kroki

1. Na stronie listy urządzeń kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne), aby wejść na stronę.
2. Kliknij → Zarządzanie użytkownikiem → Karta/znacznik, aby wejść na stronę.
3. Kliknij +, aby dodać kartę/znacznik.
4. Po usłyszeniu komunikatu głosowego „Swipe Tag” przyłóż kartę/znacznik do obszaru przedstawiania karty/znacznika AX PRO.
   - Wygenerowanie sygnału dźwiękowego oznacza, że karta/znacznik zostały rozpoznane.
   - Znacznik zostanie wyświetlony na stronie karty/znacznika.
5. Opcjonalnie: Kliknij kartę/znacznik, aby wejść na stronę ustawień.
6. Kliknij, aby edytować nazwę znacznika.

UWAGA

- Jeśli logujesz się jako instalator, pomiń ten krok. Edycja nazwy znacznika jest dostępna tylko dla administratora.
- Nazwa powinna zawierać od 1 do 32 znaków.

7. Przesuń kartę/znacznik aktywacji.
8. Wybierz połączonego użytkownika.
9. Wybierz typ znacznika

UWAGA

Różni połączeni użytkownicy mają różne uprawnienia do znaczników.

Znacznik obsługi

Możesz przesunąć znacznik, aby uzbroić lub rozbroić.

Znacznik patrolu

Kiedy przesuniesz znacznik, system wczyta zapis.

10. Opcjonalnie: Kliknij Usuń, aby usunąć znacznik.

Zarządzanie użytkownikami

Administrator i instalatorzy mogą zarządzać użytkownikami. Jeśli jesteś administratorem, możesz dodać, edytować i usuwać użytkowników oraz przypisywać różne uprawnienia nowo dodanym użytkownikom.

Kroki

UWAGA

Istnieją cztery typy użytkowników AX PRO, w tym administrator (lub właściciel), operator i instalator (lub osoba ustawiająca). Różne typy użytkowników mają różne uprawnienia dostępu do funkcjonalności AX PRO.

1. Na stronie listy urządzeń kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli jest to wymagane), aby wejść na stronę AX PRO.

2. Kliknij , aby przejść do strony odbiorcy.

3. Wybierz użytkownika, którego chcesz zaprosić.

- Zeskanuj kod QR, aby zaprosić użytkownika.
- Wprowadź adres e-mail/numer telefonu komórkowego, aby zaprosić użytkownika.
- Wybierz użytkownika z listy.

4. Kliknij Dalej, aby zaprosić użytkownika.

UWAGA

Odbiorca musi zaakceptować zaproszenie.

5. Kliknij → Zarządzanie użytkownikiem → Użytkownik.

6. Kliknij użytkownika, aby wejść na stronę zarządzania użytkownikami.

7. Opcjonalnie: W razie potrzeby wykonaj następujące czynności.

Zezwolenie użytkownika	Możesz kliknąć użytkownika docelowego na liście użytkowników, a następnie kliknąć ikonę Edytuj, aby ustawić uprawnienia przypisane dla użytkownika docelowego. **UWAGA** Tylko administrator może wykonać taką operację.
Ustaw połączone obszary	Jeśli użytkownik docelowy jest operatorem, dotknij użytkownika docelowego na liście użytkowników, a następnie dotknij Obszary połączone, aby ustawić obszar połączony z użytkownikiem docelowym. **UWAGA** Tylko administrator może wykonać taką operację.
Edycja hasła klawiatury	Jeśli docelowym użytkownikiem jest administrator, instalator lub operator, możesz kliknąć użytkownika docelowego na liście użytkowników,

a następnie kliknąć Edytuj hasło klawiatury, aby ustawić hasło klawiatury dla użytkownika docelowego.

UWAGA

Hasło (kod PIN) może mieć od 4 do 6 cyfr.

Brak jest liczb niedozwolonych; nie ma limitu kombinacji cyfr.

Po dodaniu jednego manipulatora można dodać kod PIN (Hasło klawiatury) w menu użytkownika. Po kliknięciu pola wprowadzania Procedura jest taka sama dla każdego użytkownika.

Edytuj hasło przymusu

Jeśli użytkownik docelowy jest administratorem lub operatorem, możesz dotknąć użytkownika docelowego na liście użytkowników, a następnie dotknąć opcji Edytuj hasło przymusu, aby ustawić hasło przymusu dla użytkownika docelowego.

UWAGA

W warunkach przymusu, możesz wprowadzić kod przymusu na klawiaturze, aby uzbroić i rozbroić obszar(y) i przesłać alarm przymusu.

Sterowanie automatyzacją

Administrator, instalator lub operator może sterować modułem przekaźnikowym, czujnikiem naściennym i inteligentną wtyczką.

UWAGA

- Pozycje konfiguracji i uprawnienia użytkownika będą się różnić w zależności od typu użytkownika.
- Możesz przeglądać połączone karty/znaczniki i piloty użytkownika, ale nie masz uprawnień do ich konfigurowania.

8. Opcjonalnie: (tylko dla administratora) Kliknij +, aby dodać użytkownika.

Obejście strefy

Gdy obszar jest uzbrojony, możesz ominąć określoną strefę według własnego uznania.

Zanim zaczniesz

Połącz czujnik ze strefą.

Kroki

1. Na stronie listy urządzeń kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne), aby wejść na stronę obszaru.
2. Kliknij Urządzenie.
3. Kliknij strefę w zakładce Urządzenie.

4. Kliknij , aby przejść do strony ustawień.

5. Aktywuj obejście; strefa znajdzie się w stanie obejścia.

Uzbrojenie/rozbrojenie obszaru

Możliwe jest uzbrojenie lub rozbrojenie obszaru ręcznie.

Na stronie listy urządzeń kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli jest to wymagane), aby wejść do obszaru strona.

Operacje dla jednego obszaru

• Uzbrajanie w trybie AWAY: kliknij dowolny obszar, aby uzbroić pojedynczy obszar. Kiedy wszystkie osoby w obszarze wykrywania wyjdą, włącz tryb AWAY, aby uzbroić wszystkie strefy w obszarze po określonym czasie przebywania.

• Rozbrojenie: Kliknij ikonę Uzbrajania w trybie AWAY w dowolnym obszarze, aby rozbroić pojedynczy obszar. W trybie rozbrojenia żadna strefa w obszarze nie generuje alarmu, bez względu na to, czy wystąpiły zdarzenia alarmowe, czy nie.

Operacje dla wszystkich obszarów

• Tryb AWAY: kliknij , aby uzbroić wszystkie obszary w trybie AWAY. Gdy wszystkie osoby w obszarze wykrywania opuszczą teren, włącz tryb AWAY, aby uzbroić wszystkie strefy we wszystkich obszarach po określonym czasie przebywania.

• Tryb STAY: kliknij , aby uzbroić wszystkie obszary. Gdy osoby pozostają w strefie wykrywania, włącz tryb STAY, aby uzbroić wszystkie czujniki obwodowe (takie jak czujniki obwodowe, czujniki magnetyczne, czujniki kurtynowe na balkonie) ustawione we wszystkich strefach wszystkich obszarów. W międzyczasie czujniki w obszarze wykrywania są pomijane (np. czujniki PIR). Osoby mogą poruszać się po tym obszarze, a alarm nie zostanie uruchomiony.

• Rozbrojenie: kliknij , aby rozbroić wszystkie obszary. W trybie rozbrojenia żadna strefa we wszystkich obszarach nie wywoła alarmu, bez względu na to, czy wystąpiły zdarzenia alarmowe, czy nie.

• Wyciszenie alarmu: kliknij , aby wyciszyć alarmy dla wszystkich obszarów. Usuń wszystkie alarmy wyzwolone przez wszystkie strefy we wszystkich obszarach.

Kontrola powiadomienia o alarmie

Po uruchomieniu alarmu otrzymasz powiadomienie o alarmie.

Możesz sprawdzić informacje o alarmie z poziomu klienta mobilnego.

Zanim zaczniesz

• Upewnij się, że strefa została połączona z czujnikiem.

• Upewnij się, że strefa nie znajduje się w trybie obejścia.

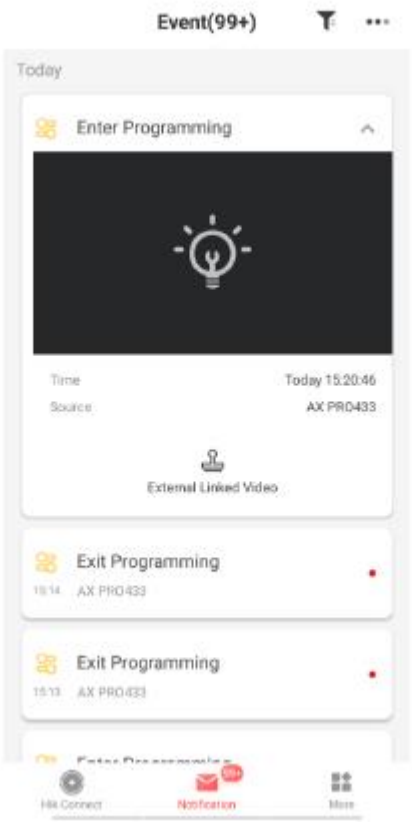
• Upewnij się, że nie została włączona funkcja cichej strefy.

Kroki

1. Kliknij Powiadomienie w kliencie mobilnym, aby wejść na stronę.

Wszystkie powiadomienia o alarmach są wymienione na stronie powiadomień.

2. Wybierz alarm, aby wyświetlić szczegóły alarmu.



3. Opcjonalnie: jeśli strefa połączyła kamerę, możesz wyświetlić odtwarzanie po wyzwoleniu alarmu.

4. Opcjonalnie: kliknij , aby wyszukiwać wydarzenia według dat lub urządzeń.

Połączenie wi-fi

Możesz połączyć AX PRO z Wi-Fi za pośrednictwem aplikacji.

Kroki

1. Na stronie listy urządzeń kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne), aby wejść na stronę.
2. Kliknij → Konfiguruj sieć Wi-Fi.
3. Postępuj zgodnie z instrukcjami na stronie i zmień AX PRO w tryb AP. Kliknij Dalej.
4. Wybierz stabilne Wi-Fi dla urządzenia w celu połączenia.
5. Wróć do strony konfiguracji, aby wprowadzić hasło Wi-Fi i kliknij Dalej.
6. Kliknij Połącz z siecią i poczekaj na połączenie.

Po nawiązaniu połączenia AX PRO wyświetli monit o wyjście z trybu AP i automatyczne przełączenie w tryb STA.

Konserwacja urządzenia

Możesz zrestartować urządzenie.

Kroki

1. Na stronie listy urządzeń kliknij AX PRO, a następnie zaloguj się do urządzenia (jeśli to konieczne), aby wejść na stronę.
2. Kliknij → Konserwacja → Uruchom ponownie urządzenie.

AX PRO uruchomi się ponownie.

4.3 Konfiguracja za pomocą klienta sieciowego

Kroki

1. Podłącz urządzenie do sieci Ethernet.
2. Wyszukaj adres IP urządzenia za pomocą oprogramowania klienckiego i oprogramowania SADP.
3. Wpisz wyszukany adres IP w pasku adresu.

UWAGA

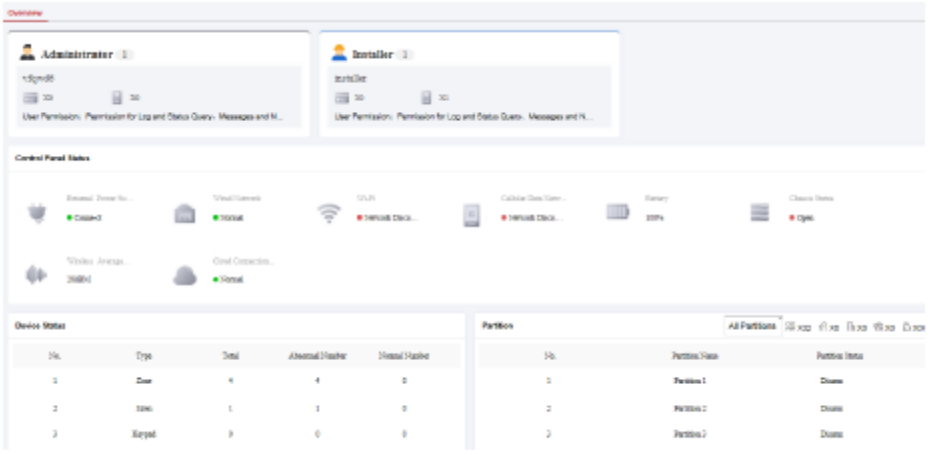
- W przypadku korzystania z przeglądarki mobilnej domyślny adres IP to 192.168.8.1.
- W przypadku bezpośredniego łączenia kabla sieciowego z komputerem domyślny adres IP to 192.0.0.64.

4. Użyj nazwy użytkownika i hasła aktywacji, aby się zalogować.

UWAGA

- Szczegółowe informacje można znaleźć w rozdziale Aktywacja.
- Tylko administrator i instalator mogą zalogować się do klienta sieciowego.

Stan użytkownika, urządzenia i obszaru można wyświetlić na stronie przeglądu.



4.3.1 Ustawienia komunikacji

Sieć przewodowa

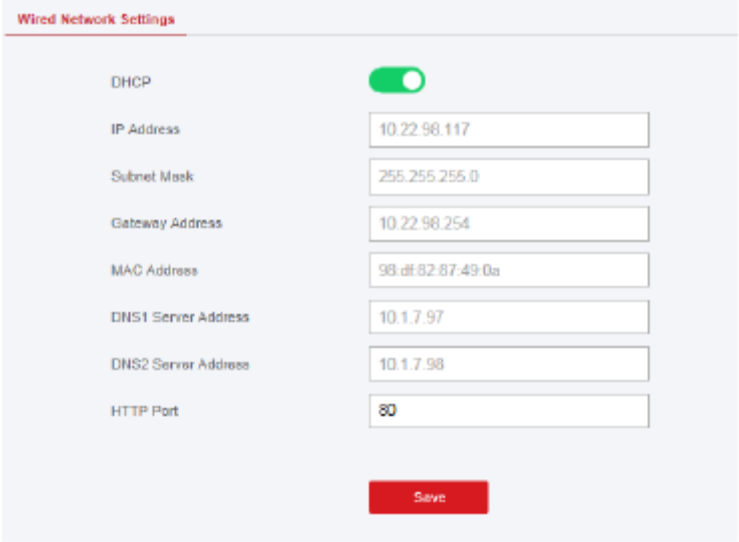
Ustaw adres IP urządzenia i inne parametry sieciowe.

Kroki

UWAGA

Funkcje różnią się w zależności od modelu urządzenia.

1. W oprogramowaniu klienckim wybierz urządzenie na stronie Zarządzanie urządzeniami i kliknij lub wprowadź adres IP radaru w pasku adresu przeglądarki internetowej i zaloguj się.



2. Kliknij Parametry komunikacji → Ethernet, aby wejść na stronę.
3. Ustaw parametry.

Ustawienia automatyczne: Włącz DHCP i ustaw port HTTP

Ustawienia ręczne: Wyłącz DHCP i ustaw adres IP, maskę podsieci, adres bramy, adres serwera DNS.

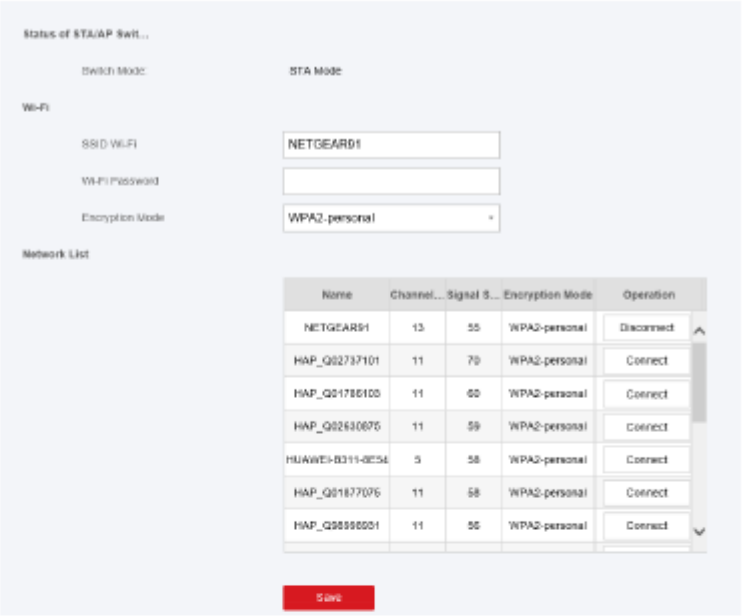
4. Opcjonalnie: Ustaw poprawny adres serwera DNS, jeśli urządzenie musi skomunikować się z serwerem Hik-Connect za pośrednictwem nazwy domeny.
5. Kliknij Zapisz.

Wi-Fi

Możesz ustawić parametry Wi-Fi, jeśli w pobliżu znajdują się bezpieczne i wiarygodne sieci Wi-Fi.

Kroki

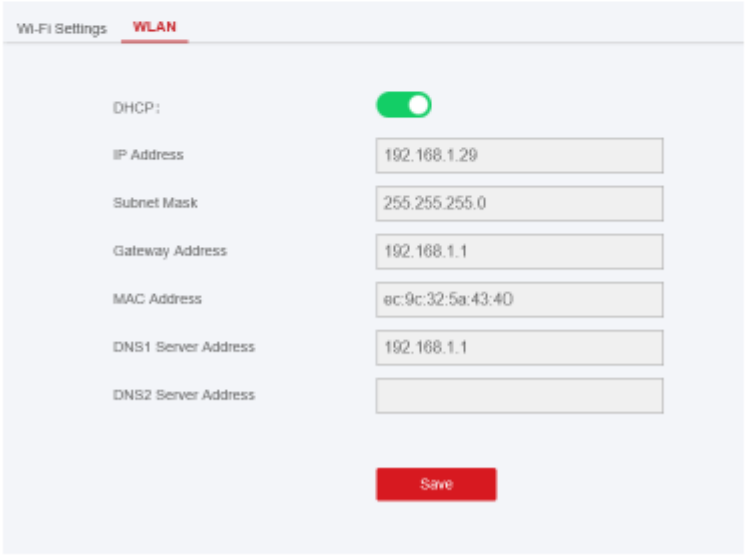
1. Kliknij Parametry komunikacji → Wi-Fi, aby przejść do strony Wi-Fi.



2. Połącz się z Wi-Fi.

Połącz ręcznie: wprowadź SSID Wi-Fi i hasło Wi-Fi, wybierz Tryb szyfrowania i kliknij Zapisz. Wybierz z listy sieci: Wybierz docelową sieć Wi-Fi z listy sieci. Kliknij Połącz i wprowadź hasło Wi-Fi, a następnie kliknij Połącz.

2. Kliknij opcję WLAN, aby przejść do strony WLAN.



4. Ustaw adres IP, maskę podsieci, adres bramy i adres serwera DNS.

UWAGA

Jeśli włączysz DHCP, urządzenie automatycznie uzyska parametry Wi-Fi.

5. Kliknij Zapisz.

Sieć komórkowa

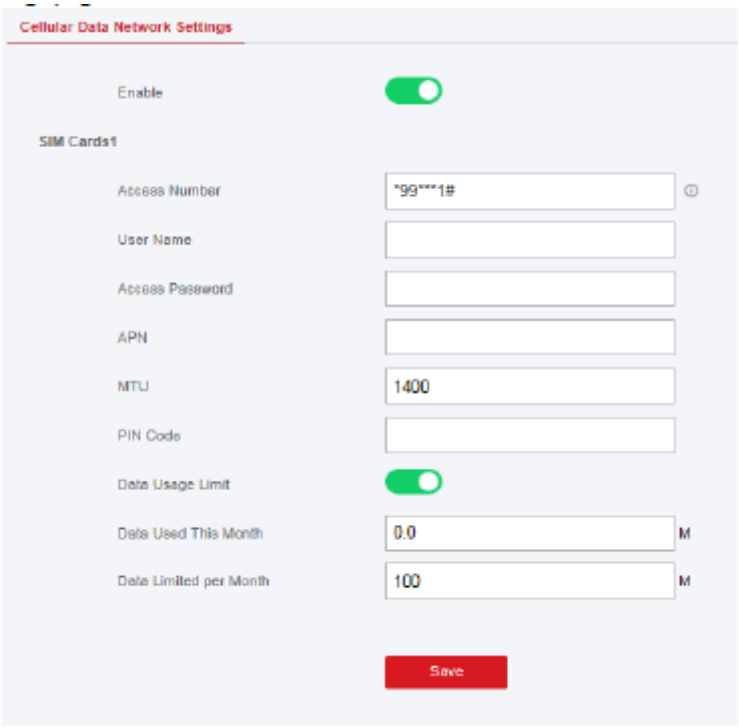
Ustaw parametry sieci komórkowej po włożeniu karty SIM do urządzenia. Korzystając z sieci komórkowej, urządzenie może przesyłać powiadomienia alarmowe do centrum alarmowego.

Zanim zaczniesz

Włóż kartę SIM do gniazda karty SIM urządzenia.

Kroki

1. Kliknij Parametry komunikacji → Sieć danych komórkowych, aby przejść do strony Ustawienia sieci danych komórkowych.



2. Włącz bezprzewodowe wybieranie numeru.
3. Ustaw parametry sieci komórkowej.

Numer dostępu

Wprowadź numer wybierania operatora.

UWAGA

Tylko użytkownik karty SIM sieci prywatnej musi wprowadzić numer dostępu.

Nazwa Użytkownika

Zapytaj operatora sieci i wprowadź nazwę użytkownika.

Hasło dostępu

Zapytaj operatora sieci i wprowadź hasło.

APN

Poproś operatora sieci o informacje dotyczące APN i wprowadź informacji o APN.

Limit wykorzystania danych

Możesz włączyć tę funkcję i ustawić próg danych co miesiąc. Jeśli wykorzystanie danych przekroczy skonfigurowany próg, zostanie wyzwolony alarm, który następnie zostanie przesłany do centrum alarmowego i klienta mobilnego.

Dane wykorzystane w tym miesiącu

Wykorzystane dane zostaną zgromadzone i wyświetlone w tym polu tekstowym.

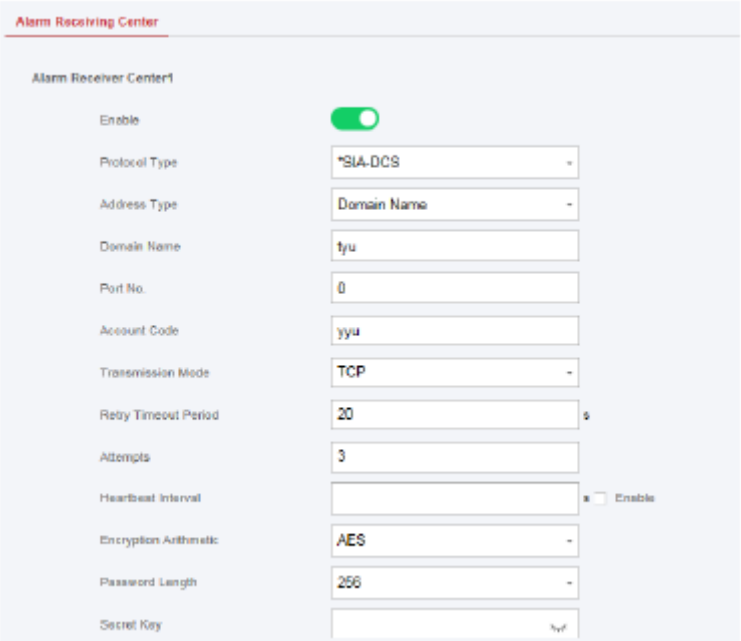
4. Kliknij Zapisz.

Centrum alarmowe

Możesz ustawić parametry centrum alarmowego, a wszystkie alarmy zostaną wysłane do skonfigurowanego centrum alarmowego.

Kroki

1. Kliknij Parametry komunikacji → Centrum monitorowania alarmów, aby przejść do strony Centrum monitorowania alarmów.



2. Wybierz Centrum odbiornika alarmu jako 1 lub 2 do konfiguracji i przesuń suwak, aby włączyć wybrane centrum odbiornika alarmu.

UWAGA

Tylko jeśli centrum odbiornika alarmu 1 jest włączony, można ustawić centrum odbiornika alarmu 2 jako kanał zapasowy i edytować parametry kanału.

3. Wybierz typ protokołu jako ADM-CID, ISUP, SIA-DCS, * SIA-DCS lub * ADM-CID, aby ustawić tryb przesyłania.

UWAGA

Standardowy protokół DC-09

ADM-CID: Metodą prezentacji danych DC-09 jest CID, który nie jest szyfrowany i służy tylko do przesyłania raportu alarmowego.

* ADC-CID: Metodą prezentacji danych DC-09 jest CID, który jest szyfrowany i służy tylko do przesyłania raportu alarmowego.

SIA-DCS: Metodą prezentacji danych DC-09 jest DCS (zwany także protokołem SIA), który nie jest szyfrowany i służy tylko do przesyłania raportu alarmowego.

* SIA-DCS: Metodą prezentacji danych DC-09 jest DCS (zwany także protokołem SIA), który jest szyfrowany i służy tylko do przesyłania raportów alarmowych.

ADM-CID lub SIA-DCS Wybierz typ odbiorcy alarmu jako adres IP lub nazwę domeny i wprowadź adres IP/nazwę domeny, numer portu, kod konta, limit czasu, czasy ponownego przesyłania i interwał impulsu.

UWAGA

Ustaw interwał impulsu w zakresie od 10 do 3888000 sekund.

ISUP Nie ma potrzeby ustawiania parametrów protokołu ISUP.

* SIA-DCS lub * ADM-CID Wybierz typ odbiorcy alarmu jako adres IP lub nazwę domeny i wprowadź adres IP/nazwę domeny, numer portu, kod konta, limit czasu ponowienia, próby, interwał impulsu, arytmetykę szyfrowania, długość hasła i tajny klucz.

UWAGA

Ustaw interwał impulsu w zakresie od 10 do 3888000 sekund.

Dla arytmetyki szyfrowania: Panel obsługuje format szyfrowania zapewniający bezpieczeństwo informacji zgodnie z DC-09, AES-128, AES-192 i AES-256, które są obsługiwane podczas konfigurowania centrum alarmowego.

W przypadku klucza tajnego: W przypadku korzystania z zaszyfrowanego formatu DC-09 ustaw klucz podczas konfigurowania SMA. Klucz wydawany jest offline przez ARC, który zostałby użyty do zaszyfrowania wiadomości w celu zapewnienia bezpieczeństwa zastępczego.

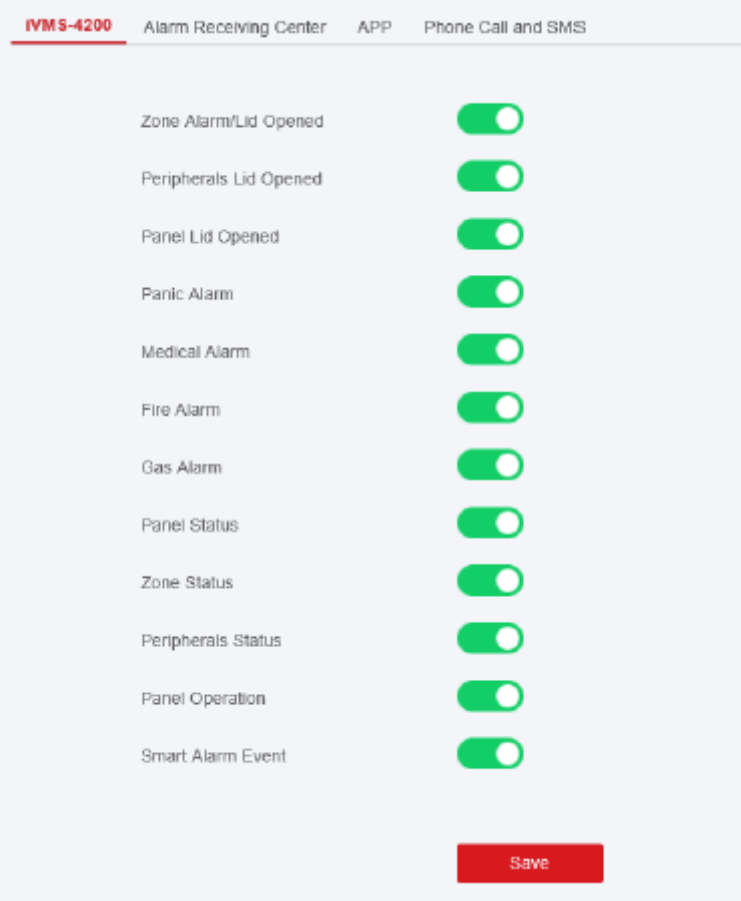
4. Kliknij Zapisz.

Powiadomienie Push

Po wyzwoleniu alarmu, jeśli chcesz wysłać powiadomienie o alarmie do klienta, centrum alarmowego, chmury lub telefonu komórkowego, możesz ustawić parametry powiadomienia push.

Kroki

1. Kliknij Parametry komunikacji → Powiadomienie o typach zdarzeń.



2. Włącz powiadomienie o celu.

UWAGA

Jeśli chcesz wysyłać powiadomienia alarmowe do klienta mobilnego, powinieneś również ustawić indeks telefonu komórkowego, numer telefonu komórkowego i sprawdzić typ powiadomienia.

UWAGA

W celu uzyskania powiadomień o komunikatach w centrum odbierania alarmów wybierz indeks centrum przed ustawieniami.

3. Kliknij Zapisz.

Wynik

Tabela 4-1 Opcje powiadomień

Opcja	Powiadomienie
iVMS-4200	Alarm strefy i otwarta pokrywa Otwarta pokrywa urządzenia bezprzewodowego Powiadomienie o naruszeniu Powiadomienie o alarmie napadowym Powiadomienie o alarmie medycznym Powiadomienie o alarmie gazowym Powiadomienie o alarmie pożarowym Powiadomienie zarządzania panelem Powiadomienie o stanie systemu Powiadomienie o stanie wykrywacza Powiadomienie o stanie urządzenia bezprzewodowego
Centrum odbioru alarmów	Centrum odbioru alarmów 1 i 2 Alarm strefy i otwarta pokrywa Otwarta pokrywa urządzenia bezprzewodowego Powiadomienie o naruszeniu Powiadomienie o alarmie napadowym Powiadomienie o alarmie medycznym Powiadomienie o alarmie gazowym Powiadomienie o alarmie pożarowym Powiadomienie zarządzania panelem Powiadomienie o stanie systemu Powiadomienie o stanie wykrywacza Powiadomienie o stanie urządzenia bezprzewodowego

Chmura	Alarm strefy i otwarta pokrywa Otwarta pokrywa urządzenia bezprzewodowego Powiadomienie o naruszeniu Powiadomienie o alarmie napadowym Powiadomienie o alarmie medycznym

Option	**Notification**
	Powiadomienie o alarmie gazowym Powiadomienie o alarmie pożarowym Powiadomienie zarządzania panelem Powiadomienie o stanie systemu Powiadomienie o stanie wykrywacza Powiadomienie o stanie urządzenia bezprzewodowego
Telefon komórkowy	Indeks telefonów komórkowych od 1 do 8 Numer telefonu komórkowego Pole wyboru typu powiadomienia SMS i połączenie głosowe Alarm strefy i otwarta pokrywa (ustaw czas filtra) Liczba połączeń Otwarta pokrywa urządzenia bezprzewodowego Powiadomienie o naruszeniu Powiadomienie o alarmie napadowym Powiadomienie o alarmie medycznym Powiadomienie o alarmie gazowym Powiadomienie o alarmie pożarowym Powiadomienie zarządzania panelem Powiadomienie o stanie systemu Powiadomienie o stanie wykrywacza Powiadomienie o stanie urządzenia bezprzewodowego

UWAGA

Dla powiadomień przez telefon komórkowy:

● Aby zakończyć połączenie, naciśnij *.

● Przy wprowadzaniu numeru telefonu komórkowego konieczne jest dodanie kodu kontrolnego.

Usługa chmury

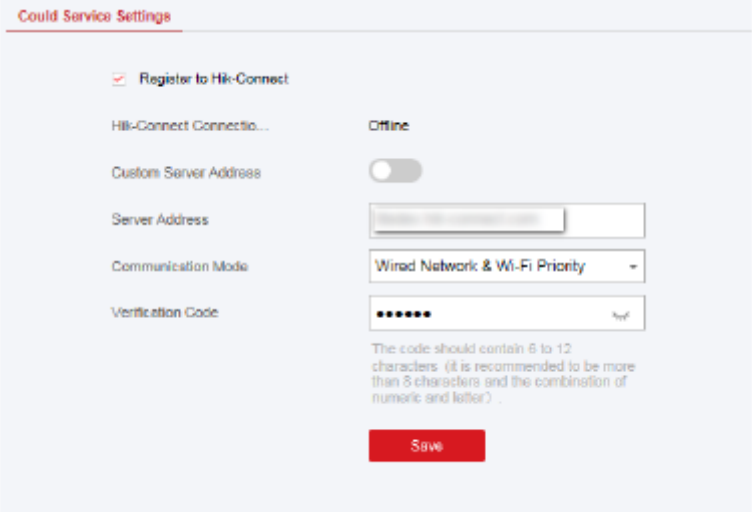
Jeśli chcesz zarejestrować urządzenie w kliencie mobilnym w celu zdalnej konfiguracji, zalecamy ustawić parametry rejestracji klienta mobilnego.

Zanim zaczniesz

- Podłącz urządzenie do sieci za pomocą połączenia przewodowego, telefonicznego lub Wi-Fi.
- Ustaw adres IP urządzenia, maskę podsieci, bramę i serwer DNS w sieci LAN.

Kroki

1. Kliknij Parametry komunikacji → Ustawienia usługi w chmurze, aby przejść do strony ustawień rejestracji Hik-Connect.\



2. Kliknij Parametry komunikacji → Rejestracja Guarding Vision, aby przejść do strony Ustawienia Rejestracji Guarding Vision.
3. Zaznacz opcję Zarejestruj się w Hik-Connect.

UWAGA

Domyślnie usługa Hik-Connect urządzenia jest włączona.

Stan urządzenia można wyświetlić na serwerze Hik-Connect (www.hik-connect.com).

4. Sprawdź stan rejestracji do Guarding Vision.

UWAGA

Domyślnie usługa Guarding Vision jest włączona.

Możesz sprawdzić stan urządzenia na serwerze Guarding Vision (www.guardingvision.com).

5. Włącz niestandardowy adres serwera.

Adres serwera jest już wyświetlany w polu tekstowym Adres serwera.

6. Wybierz tryb komunikacji z listy rozwijanej zgodnie z faktyczną metodą komunikacji urządzenia.

Tryb automatyczny

System automatycznie wybierze tryb komunikacji zgodnie z sekwencją sieci przewodowej, Wi-Fi i komórkowej sieci danych. Dopiero po odłączeniu bieżącej sieci urządzenie połączy się z inną siecią.

Sieć przewodowa i priorytet Wi-Fi

Kolejność priorytetów połączeń od wysokiego do niskiego to: sieć przewodowa, Wi-Fi, sieć danych komórkowych.

Sieć przewodowa i Wi-Fi

System najpierw wybierze sieć przewodową. Jeśli nie wykryto sieci przewodowej, wybierze sieć Wi-Fi.

Sieć danych komórkowych

System wybierze tylko sieć danych komórkowych.

7. Opcjonalnie: Zmień hasło uwierzytelniania.

UWAGA

● Domyślnie hasło uwierzytelniania jest wyświetlane w polu tekstowym.

● Hasło uwierzytelnienia powinno zawierać od 6 do 12 liter lub cyfr. Ze względów bezpieczeństwa sugerowane jest 8-znakowe hasło, które zawiera co najmniej dwa z następujących typów znaków: wielkie litery, małe litery i cyfry.

8. Kliknij Zapisz.

Powiadomienie e-mailem

Możesz wysłać wideo alarmowe lub zdarzenie na skonfigurowany e-mail.

Kroki

1. Kliknij Komunikacja → Powiadomienie e-mailem, aby wejść na stronę.
2. Kliknij blok, aby włączyć funkcję wysyłania zdarzenia weryfikacji wideo.
3. Wprowadź informacje o nadawcy.

UWAGA

Do wysyłania e-maili zaleca się używanie Gmaila i Hotmaila.

4. Wprowadź informacje o odbiorcy.

5. Kliknij Test adresu odbiorcy i upewnij się, że adres jest poprawny.

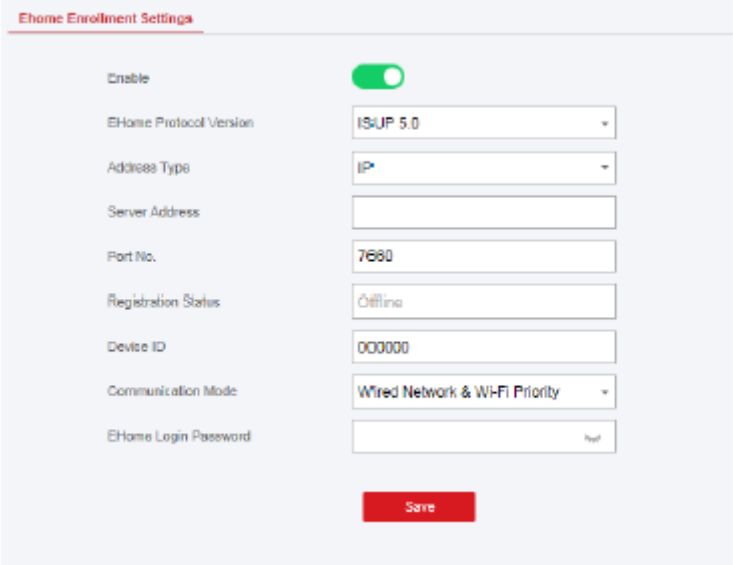
6. Kliknij Zapisz.

ISUP

W tej sekcji możesz utworzyć konto ISUP i edytować adres IP/nazwę domeny, numer portu.

Kroki

1. Kliknij Parametry komunikacji → Rejestracja ISUP, aby przejść do strony Ustawienia rejestracji ISUP.



2. Przesuń suwak, aby włączyć protokół ISUP.

3. Wybierz Typ adresu jako IP lub Nazwę domeny.

4. Wprowadź adres IP lub nazwę domeny zgodnie z typem adresu.

5. Wprowadź numer portu dla protokołu.

UWAGA

Domyślny numer portu dla ISUP to 7660.

6. Skonfiguruj konto, w tym identyfikator urządzenia i hasło logowania ISUP.

7. Wybierz Tryb komunikacji.

Tryb automatyczny

System automatycznie wybierze tryb komunikacji zgodnie z sekwencją sieci przewodowej, Wi-Fi i komórkowej sieci danych.

Dopiero po odłączeniu bieżącej sieci urządzenie połączy się z inną siecią.

Sieć przewodowa i priorytet Wi-Fi

Kolejność priorytetów połączeń od wysokiego do niskiego to: sieć przewodowa, Wi-Fi, sieć danych komórkowych.

Sieć przewodowa i Wi-Fi

System najpierw wybierze sieć przewodową. Jeśli nie wykryto sieci przewodowej, wybierze sieć Wi-Fi.

Sieć danych komórkowych

System wybierze tylko sieć danych komórkowych.

8. Kliknij Zapisz.

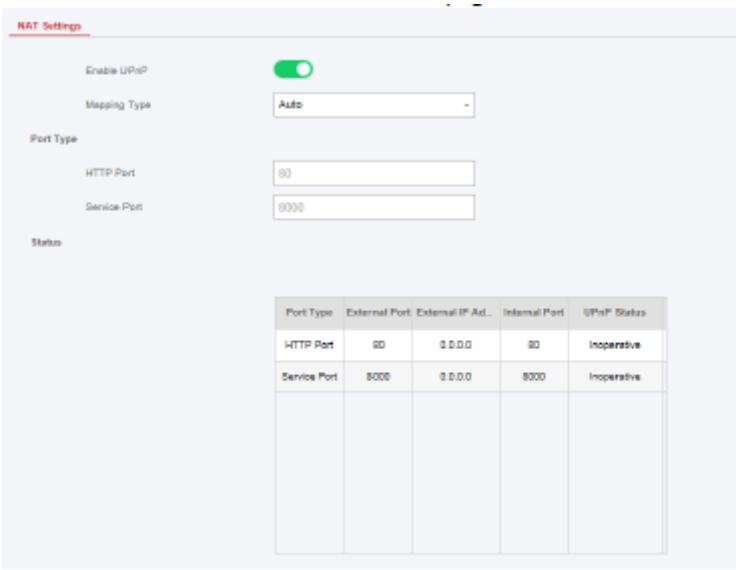
NAT

Universal Plug and Play (UPnP™) to architektura sieciowa zapewniająca zgodność sprzętu sieciowego, oprogramowania i innych urządzeń sprzętowych. Protokół UPnP umożliwia bezproblemowe łączenie urządzeń i upraszcza wdrażanie sieci w środowisku domowym i korporacyjnym.

Po włączeniu funkcji UPnP ne ma już potrzeby konfigurowania mapowania każdego portu, a urządzenie jest podłączone do sieci rozległej za pośrednictwem routera.

Kroki

1. Kliknij Parametry komunikacji → NAT, aby wejść na stronę.



2. Przeciągnij suwak, aby włączyć UPnP.
3. Opcjonalnie: Wybierz typ mapowania jako Ręczny
4. Ustaw port HTTP i port usługi.
5. Kliknij przycisk Zapisz, aby zakończyć ustawienia

FTP

Możliwe jest skonfigurowanie serwera FTP, aby zapisywał wideo alarmowe.

Kroki

1. Kliknij Komunikacja → FTP, aby wejść na stronę.
2. Skonfiguruj parametry FTP

Typ FTP

Ustaw typ FTP jako preferowany lub alternatywny.

Protokół FTP

Dostępne są opcje FTP i SFTP. Przesyłane pliki są szyfrowane przy użyciu protokołu SFTP.

Adres i port serwera

Adres serwera FTP i odpowiedni port.

Nazwa użytkownika i hasło

Użytkownik FTP powinien mieć uprawnienia do przesyłania zdjęć. Jeśli serwer FTP obsługuje przesyłanie zdjęć przez anonimowych użytkowników, możesz zaznaczyć opcję Anonimowe, aby ukryć informacje o urządzeniu podczas przesyłania.

Struktura katalogów

Ścieżka zapisu migawek na serwerze FTP.

4.3.2 Zarządzanie urządzeniami

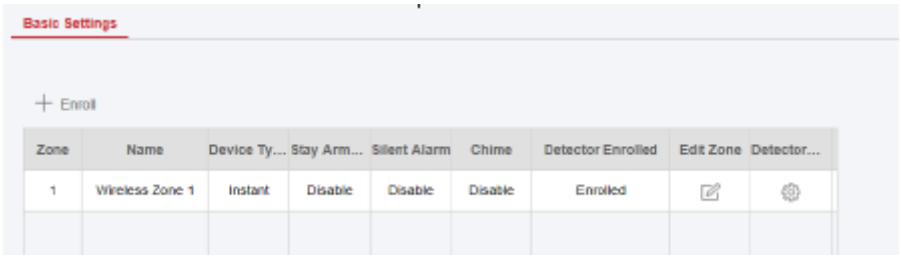
W tej sekcji możesz zarządzać zarejestrowanymi urządzeniami peryferyjnymi, w tym czujnikiem, sygnalizatorem dźwiękowym, klawiaturą itp.

Strefa

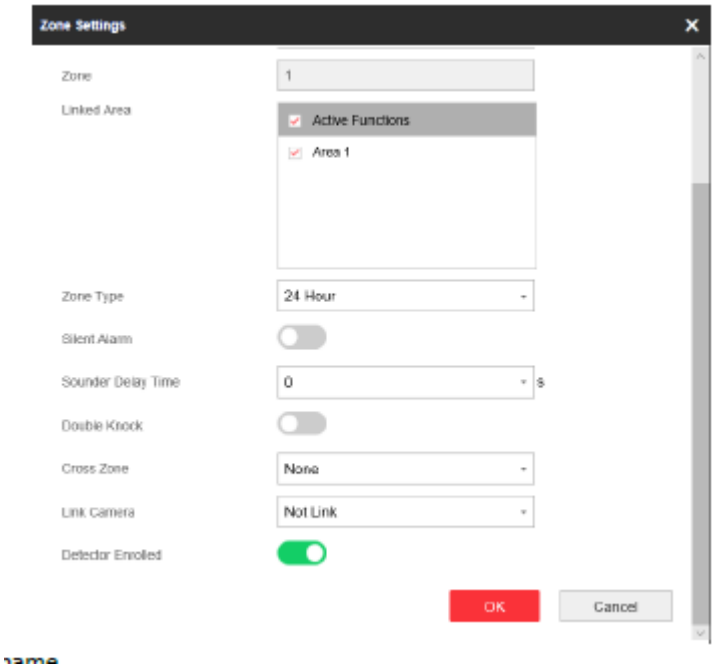
Możesz ustawić parametry strefy na stronie strefy.

Kroki

1. Kliknij Urządzenie → Strefa, aby przejść do strony Strefa.



2. Wybierz strefę i kliknij Edytuj strefę, aby przejść do strony Ustawienia strefy.



3. Edytuj nazwę strefy.

4. Sprawdź powiązane obszary.

UWAGA

- Wyświetlone zostaną tylko aktywne obszary.
- Nowo dodane urządzenie peryferyjne jest domyślnie połączone z obszarem 1.

5. Wybierz typ strefy.

Strefa natychmiastowa

Ten typ strefy natychmiast wyzwoli zdarzenie alarmowe po uzbrojeniu.

Strefa opóźniona

Opóźnienie przy wyjściu: Opóźnienie przy wyjściu zapewnia czas na opuszczenie strefy chronionej bez alarmu.

Opóźnienie przy wejściu: Opóźnienie przy wejściu zapewnia czas na wejście do strefy chronionej w celu rozbrojenia systemu bez alarmu.

System podaje czas opóźnienia wejścia/wyjścia, gdy zostanie uzbrojony lub ponownie włączony. Zwykle jest używany na drodze wejścia/wyjścia (np. drzwi frontowe/główne wejście), co jest kluczową drogą do uzbrajania/rozbrajania za pomocą klawiatury operacyjnej dla użytkowników.

UWAGA

● W Opcjach systemu można ustawić 2 różne czasy trwania→ Harmonogram i minutnik.

● Upewnij się, że regulator czasowy nie jest ustawiony na wartość większą niż 45 sekund (aby zachować zgodność z normą EN50131-1).

● Można ustawić czas opóźnienia uzbrojenia typu STAY dla strefy opóźnienia.

Strefa napadowa

Strefa jest aktywna przez cały czas. Zwykle stosowana jest w obiektach wyposażonych w przycisk napadowy, czujnik dymu i czujnik zbicia szyby.

Strefa przełącznika kluczykowego

Połączony obszar zostanie uzbrojony po aktywacji i rozbrojony po przywróceniu. W przypadku alarmu sabotażowego operacja uzbrojenia i rozbrojenia nie zostanie wywołana.

UWAGA

Dla strefy można wybrać dwa typy wyzwalania (według czasów wyzwalania i stanu strefy). W przypadku wybrania typu stanu wejścia należy ustawić operację wyzwalania (wyzwalanie uzbrojenia/rozbrojenia).

Strefa nieaktywna

Strefa wyłączona, ignorująca zdarzenie alarmowe. Zwykle służy do wyłączania wadliwych czujników.

Strefa 24-godzinna

Wejście jest aktywowane przez cały czas z wyjściem dźwiękowym/syreny w przypadku wystąpienia alarmu. Zwykle jest stosowana w strefach zagrożonych pożarem, wyposażonych w czujniki dymu i czujniki temperatury.

6. Wszelkie opcje aktywuj zgodnie z własnymi potrzebami.

UWAGA

Niektóre strefy nie obsługują tej funkcji. Zapoznaj się z aktualną strefą, aby ustawić funkcję.

7. Ustaw czas opóźnienia sygnalizatora. Sygnalizator zostanie uruchomiony natychmiast lub po ustawionym czasie.

8. W razie potrzeby połącz kamerę ze strefą.

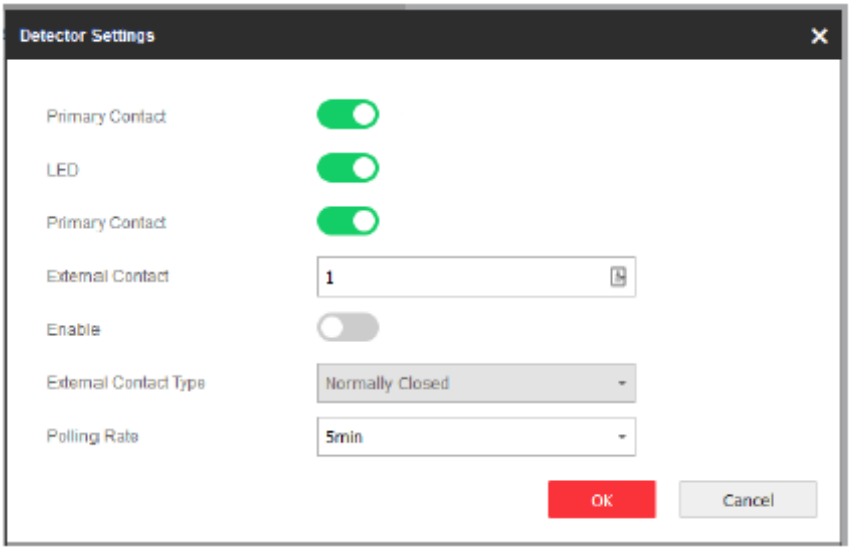
9. Włącz zarejestrowany czujnik, wprowadź numer seryjny i ustaw numer połączonej kamery.

10. Kliknij OK.

UWAGA

Po ustawieniu strefy możesz wejść w Stan → Strefa, aby zobaczyć stan strefy.

11. Kliknij Ustawienia wykrywacza, aby przejść do strony Ustawienia wykrywacza.



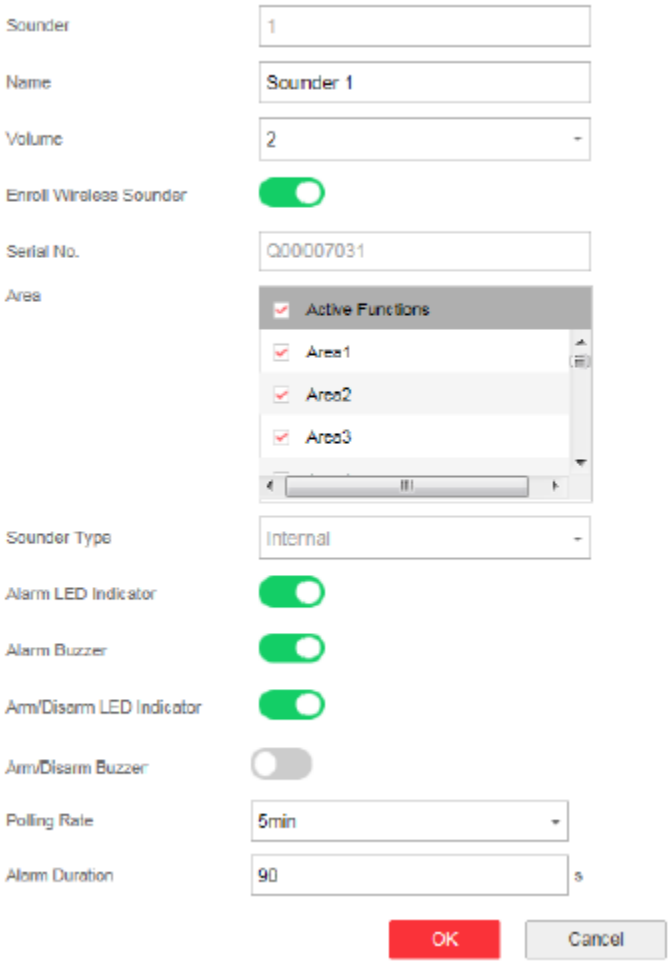
W celu zapewnienia zgodności z EN zakazane jest odłączanie styku.

Sygnalizator

Sygnalizator jest przypisany do AX PRO za pośrednictwem bezprzewodowego modułu odbiornika, a bezprzewodowy sygnalizator 868 MHz można przypisać do hybrydowego AX PRO za pośrednictwem bezprzewodowego odbiornika, który znajduje się pod adresem 9.

Kroki

1. Kliknij Urządzenie → Sygnalizator, aby przejść do strony Sygnalizator.
2. Kliknij , aby przejść do strony Ustawienia sygnalizatora.



3. Ustaw nazwę sygnalizatora i głośność.

UWAGA

Dostępny zakres głośności sygnalizatora wynosi od 0 do 3 (funkcja różni się w zależności od modelu urządzenia).

4. Włącz rejestrację bezprzewodowego sygnalizatora i ustaw numer seryjny sygnalizatora.

5. Wybierz połączony obszar.

UWAGA

- Wyświetlone zostaną tylko aktywne obszary.
- Nowo dodane urządzenie peryferyjne jest domyślnie połączone z obszarem 1.

6. Wybierz, aby włączyć wskaźnik LED alarmu, brzęczyk alarmu, wskaźnik LED uzbrojenia/rozbrojenia i brzęczyk uzbrojenia/rozbrojenia.
7. Ustaw częstotliwość zapytywania i czas trwania alarmu.
8. Kliknij OK.

UWAGA

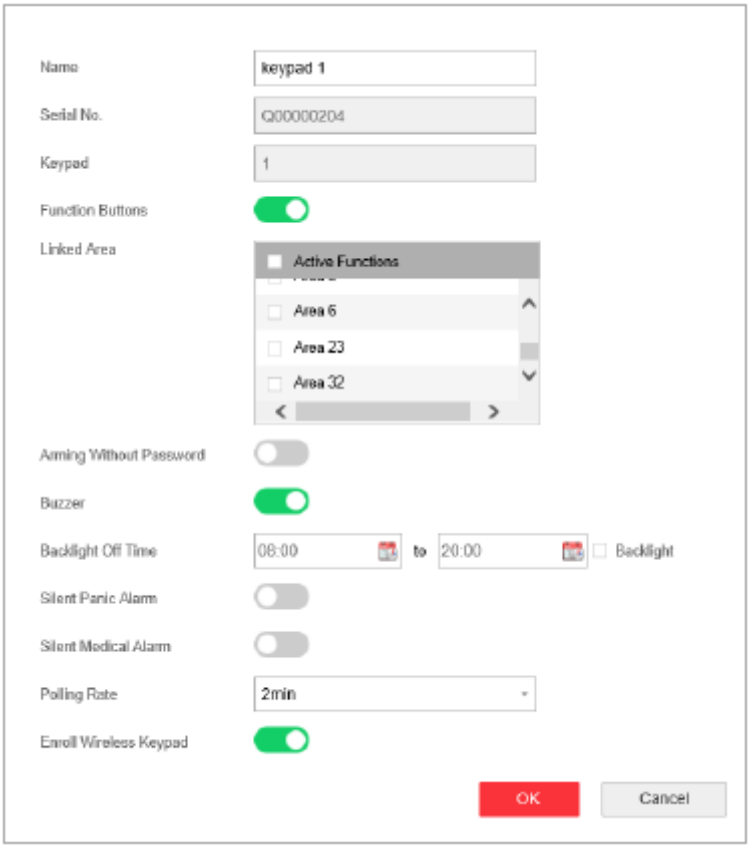
Po skonfigurowaniu sygnalizatora można kliknąć opcję Stan → Sygnalizator, aby wyświetlić stan sygnalizatora.

Klawiatura

Możesz ustawić parametry klawiatury przypisanej do AX PRO.

Kroki

1. Kliknij Urządzenie → Klawiatura, aby wejść na stronę.
2. Kliknij , aby przejść do strony Ustawienia klawiatury.



3. Ustaw nazwę klawiatury.

4. Zaznacz pole wyboru, aby włączyć funkcję brzęczyka, cichego alarmu napadowego, cichego alarmu medycznego i przycisku klawiatury.

5. Zaznacz pole wyboru, aby włączyć funkcję uzbrojenia bez hasła.

6. Zaznacz pole wyboru Aktywne w opcji Czas wyłączenia przeciwoświetlenia i ustaw czas wyłączenia podświetlenia.

7. Ustaw szybkość zwijania.

8. Wybierz obszar połączony z klawiaturą.

UWAGA

- Wyświetlone zostaną tylko włączone obszary.

● Nowo dodane urządzenie peryferyjne jest domyślnie połączone z obszarem 1.

9. Określ, czy chcesz anulować przypisanie klawiatury, czy nie. Jeśli łącze jest aktywne, urządzenie zostanie usunięte.
10. Kliknij OK.

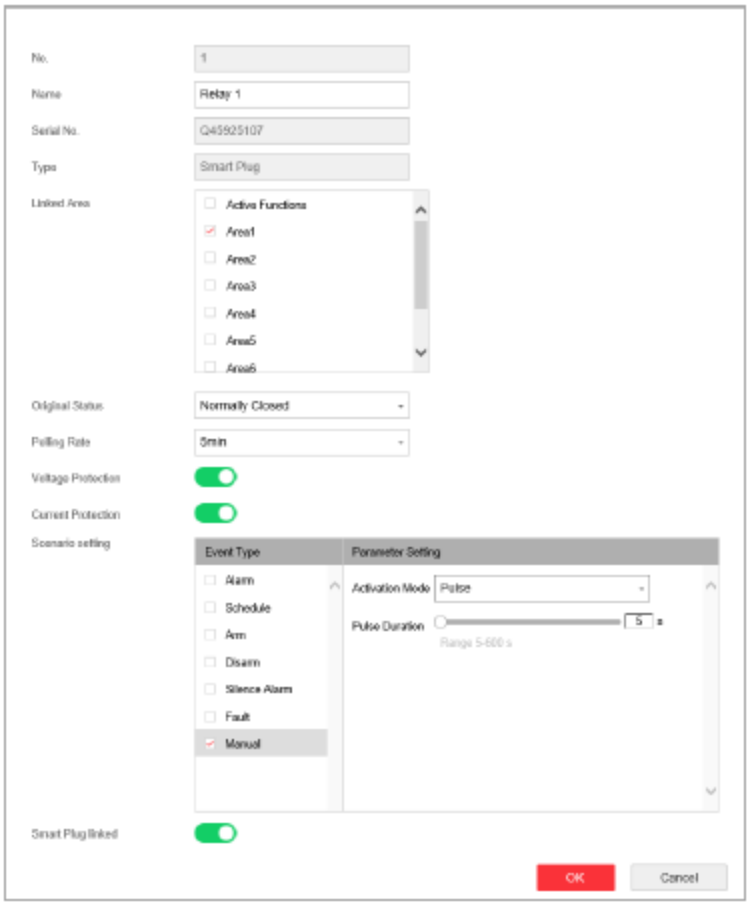
● Po skonfigurowaniu klawiatury można kliknąć Stan → Klawiatura, aby wyświetlić stan klawiatury.
● Hasło klawiatury można ustawić na stronie Zarządzanie użytkownikami → Użytkownik → Obsługa.

Automatyzacja

Możesz ustawić parametry wyjść przekaźnikowych przypisanych do AX PRO.

Kroki

1. Kliknij Urządzenie → Automatyzacja, aby wejść na stronę.
2. Kliknij Rejestrowanie, wprowadź numer seryjny i wybierz typ urządzenia, aby dodać przekaźnikowe urządzenie wyjściowe.
3. Kliknij  , aby edytować informacje o przekaźniku.



● Ustaw nazwę przekaźnika wyjściowego.

● Wybierz powiązany obszar do wyjścia.

UWAGA

● Wyświetlone zostaną tylko aktywne obszary.

● Nowo dodane urządzenie peryferyjne jest domyślnie połączone z obszarem 1.

● Funkcja różni się w zależności od różnych typów przekaźników

● Ustaw pierwotny stan na Normalnie zamknięte lub Normalnie otwarte.

● Ustaw szybkość zapytywania.

● Ustaw, czy chcesz chronić napięcie/prąd.

● Ustaw zdarzenie do wyzwolenia.

● Ustaw aktywację po wyzwoleniu.

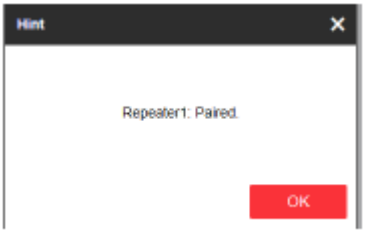
● Określ, czy połączyć się z przekaźnikowym urządzeniem wyjściowym. Jeśli łącze jest aktywne, urządzenie zostanie usunięte.

Wzmacniak

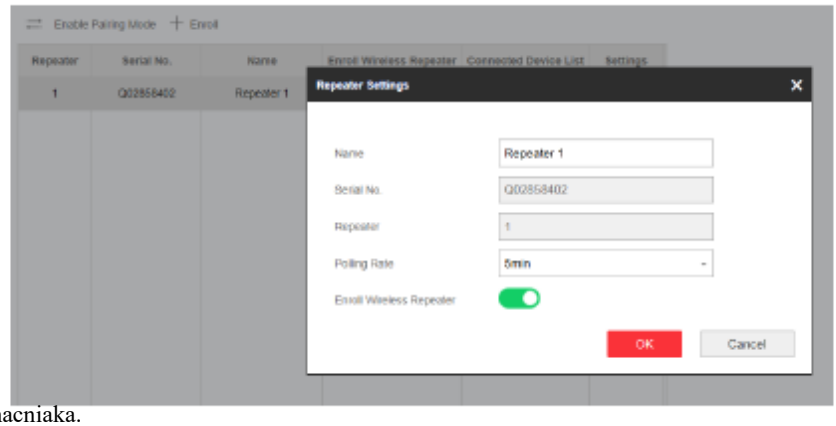
Wzmacniak może wzmacniać sygnały między panelem sterowania a urządzeniami peryferyjnymi.

Kroki

1. Kliknij Urządzenie → Wzmacniak, aby wejść na stronę.
2. Kliknij Zarejestruj, wprowadź numer seryjny i wybierz typ urządzenia, aby dodać wzmacniak.
3. Kliknij Wprowadź tryb parowania, aby wzmacniak przeszedł w tryb parowania urządzeń.
4. Gdy odległość między urządzeniem peryferyjnym a panelem sterowania jest duża, wzmacniak może służyć jako stacja transferowa do parowania. Tryb parowania trwa 3 minuty i nie można go przerwać. Po pomyślnym sparowaniu zostanie wyświetlona lista podłączonych urządzeń.



5. Kliknij , aby edytować informacje o wzmacniaku.



● Ustaw nazwę wzmacniaka.
● Ustaw częstotliwość zapytywania wzmacniaka.
● Określ, czy chcesz anulować przypisanie wzmacniaka. Jeśli łącze jest aktywne, urządzenie zostanie usunięte.

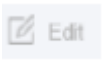
Kamera sieciowa

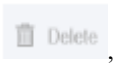
Możesz dodać kamery sieciowe do systemu.

Kroki

1. Kliknij Urządzenie → Kamera, aby wejść na stronę.
2. Kliknij opcję Rejestrowanie, wprowadź adres IP, nazwę użytkownika i hasło, aby dodać kamerę.

3. Kliknij  , aby edytować informacje o kamerze.

Możesz także kliknąć 

, aby edytować kamerę lub kliknąć 

, aby usunąć kamerę.

4.3.3 Ustawienia obszaru

Podstawowe ustawienia

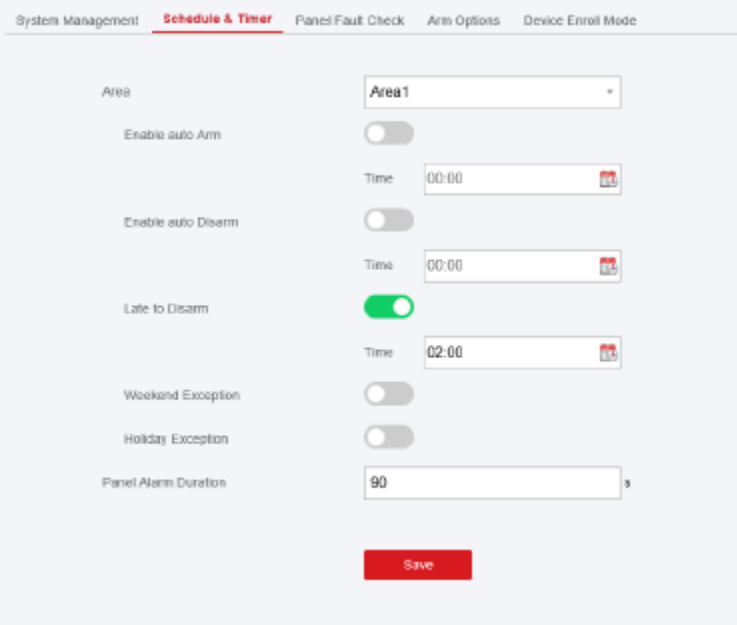
Możesz połączyć strefy z wybranym obszarem.

Kroki

1. Kliknij Obszar → Ustawienia podstawowe, aby wejść na stronę.
2. Wybierz obszar.
3. Zaznacz Aktywuj.
4. Zaznacz pole wyboru przed strefą, aby wybrać strefy dla tego obszaru.
5. Kliknij przycisk Zapisz, aby zakończyć ustawienia.

Ustawienia harmonogramu i regulatora czasowego

Możesz ustawić harmonogram alarmu. Strefa zostanie uzbrojona/rozbrojona zgodnie ze skonfigurowanym harmonogramem.



Kroki

1. Kliknij System → Opcje systemu → Harmonogram i Regulator czasowy, aby przejść do strony Harmonogram i Regulator czasowy.
2. Wybierz obszar.
3. Ustaw następujące parametry zgodnie z rzeczywistymi potrzebami.

Aktywacja automatycznego uzbrojenia

Aktywuj funkcję i ustaw czas rozpoczęcia uzbrojenia. Strefa zostanie uzbrojona zgodnie ze skonfigurowanym czasem.

UWAGA

- Czas automatycznego uzbrojenia i czas automatycznego rozbrojenia nie mogą być takie same.
- Brzęczyk emituje wolny 2-minutowy sygnał dźwiękowy przed rozpoczęciem automatycznego uzbrojenia oraz szybki 1-minutowy sygnał dźwiękowy przed rozpoczęciem automatycznego uzbrojenia.
- Możliwe jest aktywowanie wymuszonego uzbrojenia na stronie Opcje systemu. Gdy funkcja jest włączona, system zostanie uzbrojony bez względu na awarię.
- Jeśli aktywny jest obszar publiczny, strefa 1 nie obsługuje automatycznego uzbrajania.

Aktywacja automatycznego rozbrojenia

Aktywuj funkcję i ustaw czas rozpoczęcia rozbrojenia. Strefa zostanie rozbrojona zgodnie ze skonfigurowanym czasem.

UWAGA

● Czas automatycznego uzbrojenia i czas automatycznego rozbrojenia nie mogą być takie same.

● Jeśli obszar publiczny jest włączony, obszar 1 nie obsługuje automatycznego rozbrajania.

Opóźnione rozbrojenie

Aktywuj funkcję i ustaw czas. Jeśli alarm zostanie wyzwolony po skonfigurowanym czasie, osoba zostanie uznana za spóźnioną.

Opóźnione rozbrojenie

Aktywuj funkcję i ustaw czas. Jeśli alarm zostanie wyzwolony po skonfigurowanym czasie, osoba zostanie uznana za intruza.

UWAGA

Zalecamy włączenie funkcji Powiadomienie zarządzania panelem w Parametry komunikacji → Komunikacja o zdarzeniu przed włączeniem funkcji Opóźnione rozbrojenie.

Wyjątek weekendowy

Po aktywowaniu funkcji strefa nie będzie uzbrojona w weekend.

Wyjątek świąteczny

Aktywuj funkcję, a strefa nie zostanie uzbrojona/rozbrojona w święta. Harmonogram świąteczny ustaw po aktywowaniu.

UWAGA

Można ustawić do 6 grup świątecznych.

Czas trwania alarmu panelu

Czas trwania alarmu panelu.

UWAGA

Dostępny zakres czasu trwania wynosi od 10 s do 900 s.

5. Kliknij Zapisz.

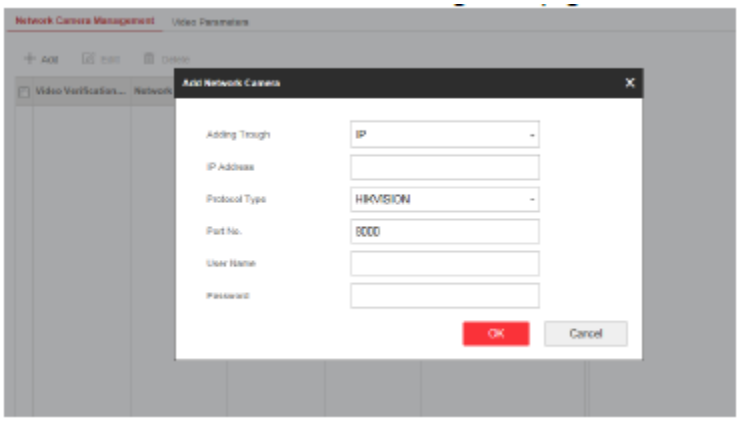
4.3.4 Zarządzanie wideo

Możliwe jest dodanie dwóch kamer sieciowych do AX PRO i połączenie kamery z wybraną strefą w celu monitorowania wideo. Możesz także odbierać i oglądać wideo z wydarzenia za pośrednictwem klienta i poczty e-mail.

Dodawanie kamer do AX PRO

Kroki

1. Kliknij Urządzenie → IPC, aby przejść do strony zarządzania kamerą sieciową.



2. Kliknij Dodaj i wprowadź podstawowe informacje o kamerze, takie jak adres IP i numer portu, a następnie wybierz typ protokołu.

3. Wprowadź nazwę użytkownika i hasło kamery.

4. Kliknij OK.

5. Opcjonalnie: Kliknij Edytuj lub Usuń, aby edytować lub usunąć wybraną kamerę.

Połączenie kamery ze strefą

Kroki

1. Kliknij Urządzenie → Strefa, aby przejść do strony konfiguracji.

2. Wybierz strefę, którą chcesz objąć monitoringiem wideo, i kliknij .

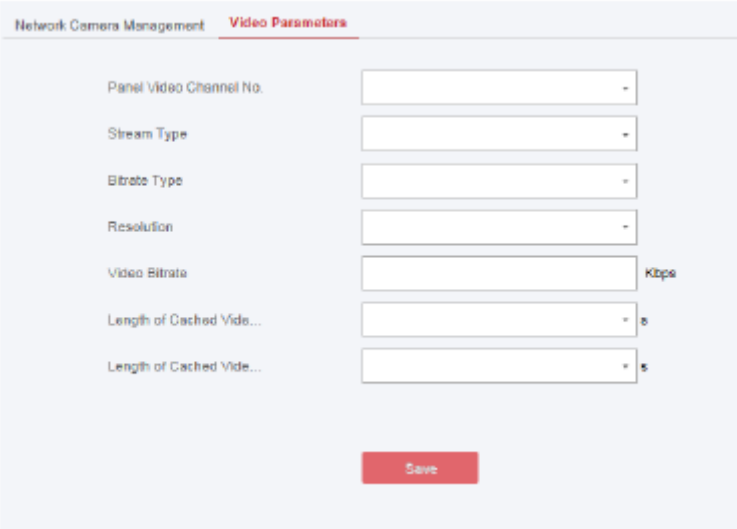
3. Wybierz numer kanału wideo panelu nr.

4. Kliknij OK.

Ustaw parametry wideo

Kroki

1. Kliknij Urządzenie → IPC → Wideo, aby wejść na stronę.



2. Wybierz kamerę i ustaw parametry wideo.

Typ strumienia

Strumień główny: używany do nagrywania i podglądu HD, ma wysoką rozdzielczość, współczynnik kodowania i jakość obrazu.

Podstrumień: Służy do transmisji sieciowej i podglądu obrazów jako strumień wideo z funkcjami o niższej rozdzielczości, szybkości transmisji i jakości obrazu.

Typ szybkości transmisji

Wybierz typ szybkości transmisji jako stałą lub zmienną.

Rozdzielczość

Wybierz rozdzielczość danych wyjściowych wideo.

Szybkość transmisji wideo

Wyższa wartość odpowiada wyższej jakości wideo, ale wymagana jest lepsza przepustowość.

4.3.5 Zarządzanie uprawnieniami

Dodawanie/edytowanie/usuwanie pilota

Możesz dodać pilota do AX PRO i sterować AX PRO za pomocą pilota. Możesz też edytować informacje o pilocie lub usuń pilota z AX PRO.

Kroki

1. Kliknij Urządzenie → Pilot, aby przejść do strony zarządzania pilotem.
2. Kliknij Dodaj i naciśnij dowolny klawisz na pilocie.

3. Ustaw parametry pilota.

Nazwa

Dostosuj nazwę pilota.

Ustawienia uprawnień

Sprawdź różne elementy, aby przypisać uprawnienia.

Ustawienia pojedynczego klucza

Wybierz z listy rozwijanej, aby ustawić funkcje klawisza I i klawisza II.

Ustawienia kombinacji klawiszy

Wybierz z listy rozwijanej, aby ustawić funkcje kombinacji klawiszy.

4. Kliknij OK.

5. Opcjonalnie: Kliknij, aby edytować informacje o pilocie.

6. Opcjonalnie: Usuń pojedynczego pilota lub zaznacz wiele pilotów i kliknij Usuń, aby usunąć piloty zbiorczo.

UWAGA

Komunikacja urządzeń bezprzewodowych w typie pilota została zidentyfikowana poprzez numer SN, który będzie szyfrowany podczas transmisji. Numer SN rozpoczyna się od znaku Q do Z i następnie po 8 cyfr, np. Q02235774. Dopuszcza się maksymalną liczbę 100 000 000 (10 do potęgi 8 [cyfr]).

Dodawanie/edytowanie/usuwanie znacznika

Możliwe jest dodanie znacznika do AX PRO i użycie go do uzbrojenia/rozbrojenia strefy. Możliwe jest także edytowanie informacji o znaczniku lub usunięcie znacznika z AX PRO.

UWAGA

Komunikacja znacznika została zidentyfikowana przez numer SN, który zostanie zaszyfrowany podczas transmisji. Numer SN rozpoczyna się od 32 cyfr; można zidentyfikować co najwyżej 4 294 967 296 numerów SN.

Kroki

1. Kliknij Urządzenie → Znacznik, aby wejść na stronę zarządzania.
2. Kliknij Dodaj i umieść znacznik w obszarze znacznika w AX PRO.
3. Dostosuj nazwę znacznika w wyskakującym okienku.

4. Wybierz typ znacznika i obszar powiązany ze znacznikiem.

5. Wybierz uprawnienia dla znacznika.

UWAGA

Zalecamy przydzielenie przynajmniej pozwolenia na znacznik.

6. Kliknij OK, a informacje o znacznikach zostaną wyświetlone na liście.

UWAGA

Znacznik obsługuje co najmniej 20 tysięcy numerów seryjnych.

7. Opcjonalnie: Kliknij , aby zmienić nazwę znacznika.
8. Opcjonalnie: Usuń pojedynczy znacznik lub zaznacz wiele znaczników i kliknij Usuń, aby usunąć je zbiorczo.

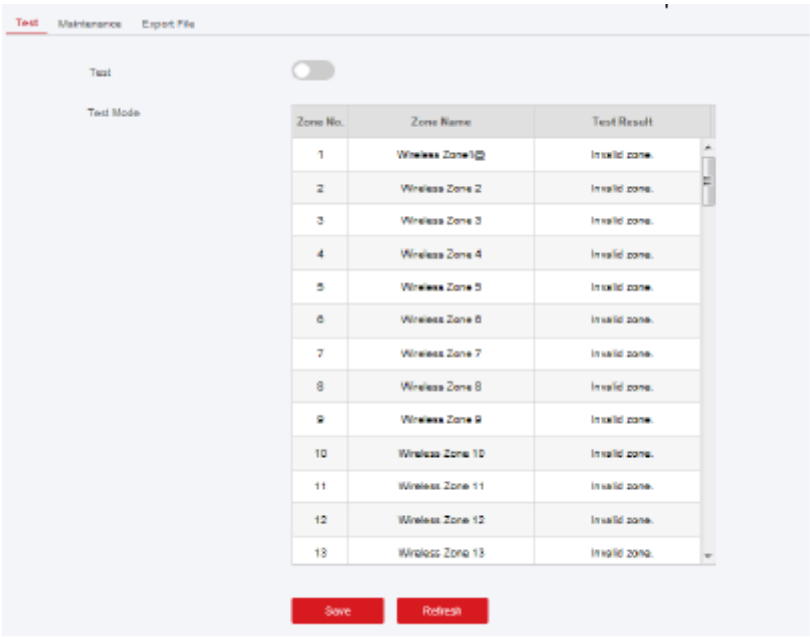
4.3.6 Konserwacja

Test

AX PRO obsługuje funkcję testu przejścia.

Kroki

1. Wejdź w Zarządzanie projektem → Konserwacja → Test →, aby włączyć funkcję.



Przejście do trybu TEST możliwe jest dopiero wówczas, gdy wszystkie czujniki są sprawne.

2. Zaznacz pole wyboru Test, aby rozpocząć test przejścia.

3. Kliknij przycisk Zapisz, aby zakończyć ustawienia.

4. Uruchom czujnik w każdej strefie.

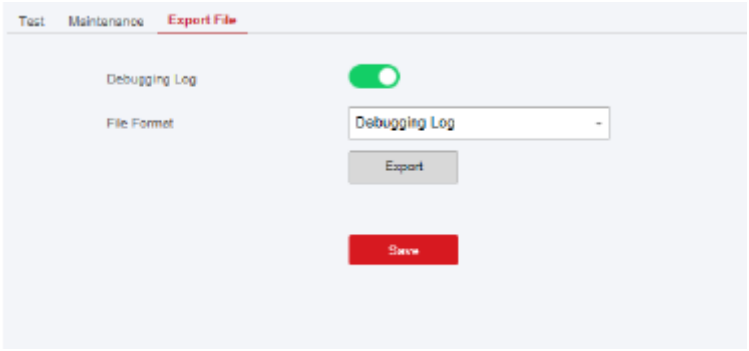
5. Sprawdź wynik testu.

Eksportowanie plik

Możesz wyeksportować plik debugowania do komputera.

Kroki

1. Kliknij Konserwacja → Eksportuj plik, aby wejść na stronę.



2. Zaznacz pole wyboru, aby włączyć funkcję.

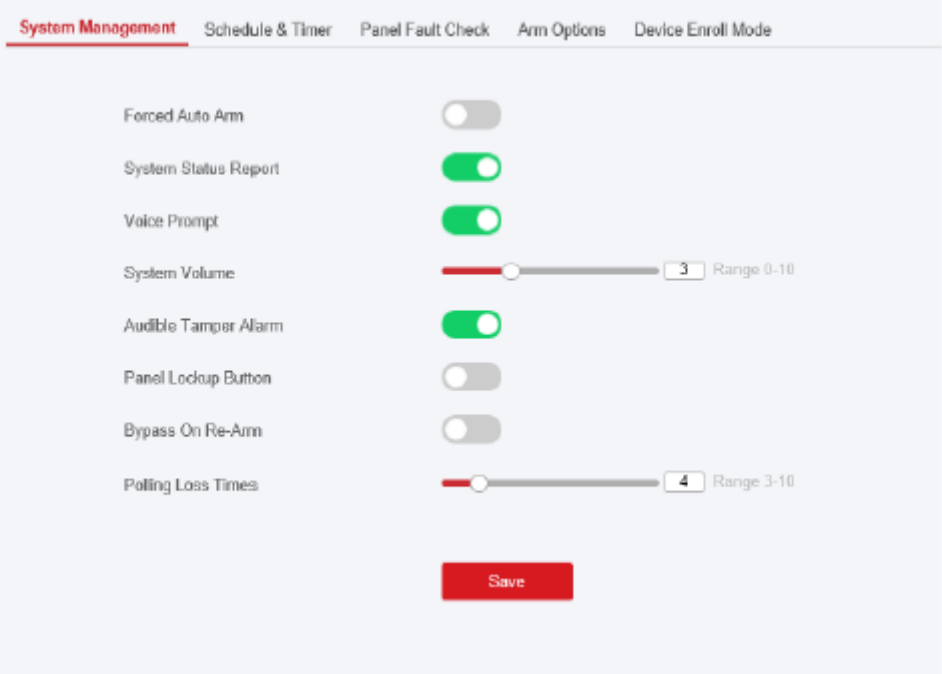
3. Kliknij Eksportuj, aby zapisać plik debugowania na komputerze.

4.3.7 Ustawienia systemowe

Zarządzanie uprawnieniami

Ustaw opcje uprawnień.

Kliknij System → Opcje systemu → Zarządzanie systemem, aby przejść do strony Zarządzanie opcjami systemu.



Wymuszone automatyczne uzbrojenie

Jeżeli opcja jest włączona, a w strefie są aktywne usterki, wejście zostanie automatycznie zablokowane podczas uzbrajania.

UWAGA

Zalecamy wyłączenie funkcji uzbrajania na stronie Ustawienia zaawansowane. Uzbrojenie AX PRO z funkcją błędu nie może zostać wykonane.

Raport o stanie systemu

Jeśli opcja jest aktywna, urządzenie automatycznie wczyta raport po zmianie stanu AX PRO.

Komunikat głosowy

Jeśli opcja jest aktywna, AX PRO włączy tekstowe podpowiedzi głosowe.

Głośność systemu

Dostępny zakres głośności systemu wynosi od 0 do 10.

Dźwiękowy alarm sabotażowy

Po aktywacji system będzie ostrzegał brzęczykiem o alarmie sabotażowym.

Przycisk blokady panelu

Włącz/wyłącz przycisk blokady panelu sterowania.

Obejście po ponownym uzbrojeniu

Gdy ta opcja jest włączona, strefa z usterką zostanie automatycznie pominięta po ponownym uzbrojeniu.

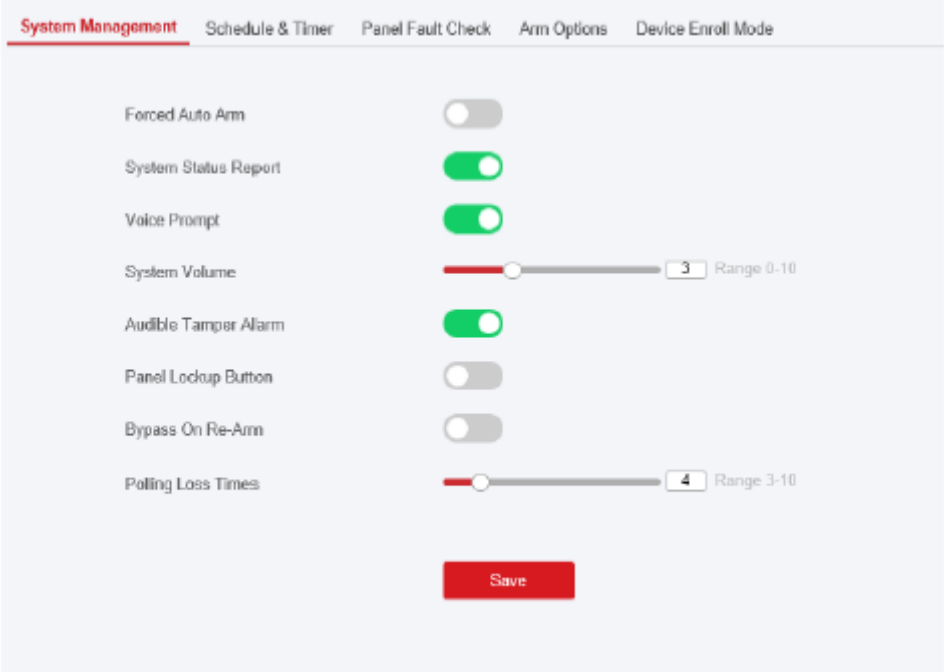
Czasy strat w ramach zapytywania

Ustaw maksymalny czas strat w ramach zapytywania. System zgłosi błąd, jeśli czas trwania przekroczy limit.

Kontrola usterek

System określa, czy sprawdzić usterki wymienione na stronie. System sprawdzi tylko wybraną usterkę.

Kliknij System → Opcje systemu → Kontrola usterki, aby wejść na stronę.



Wykrywanie odłączenia kamery sieciowej

Jeśli opcja jest aktywna, po odłączeniu podłączonej kamery sieciowej zostanie uruchomiony alarm.

Kontrola usterki baterii

Jeżeli opcja jest aktywna, gdy bateria jest odłączona lub rozładowana alarm nie zostanie wygenerowany.

Kontrola usterek sieci LAN

Jeżeli opcja jest aktywna, przy rozłączeniu sieci przewodowej lub przy innych uszkodzeniach wygenerowany zostanie alarm.

Kontrola usterek Wi-Fi

Jeżeli opcja jest aktywna, przy rozłączeniu Wi-Fi lub przy innych awariach wygenerowany zostanie alarm.

Kontrola błędów sieci komórkowej

Jeśli opcja jest aktywna, gdy sieć danych komórkowych jest odłączona lub występują inne usterki wygenerowany zostanie alarm.

Opóźnienie utraty zasilania AC

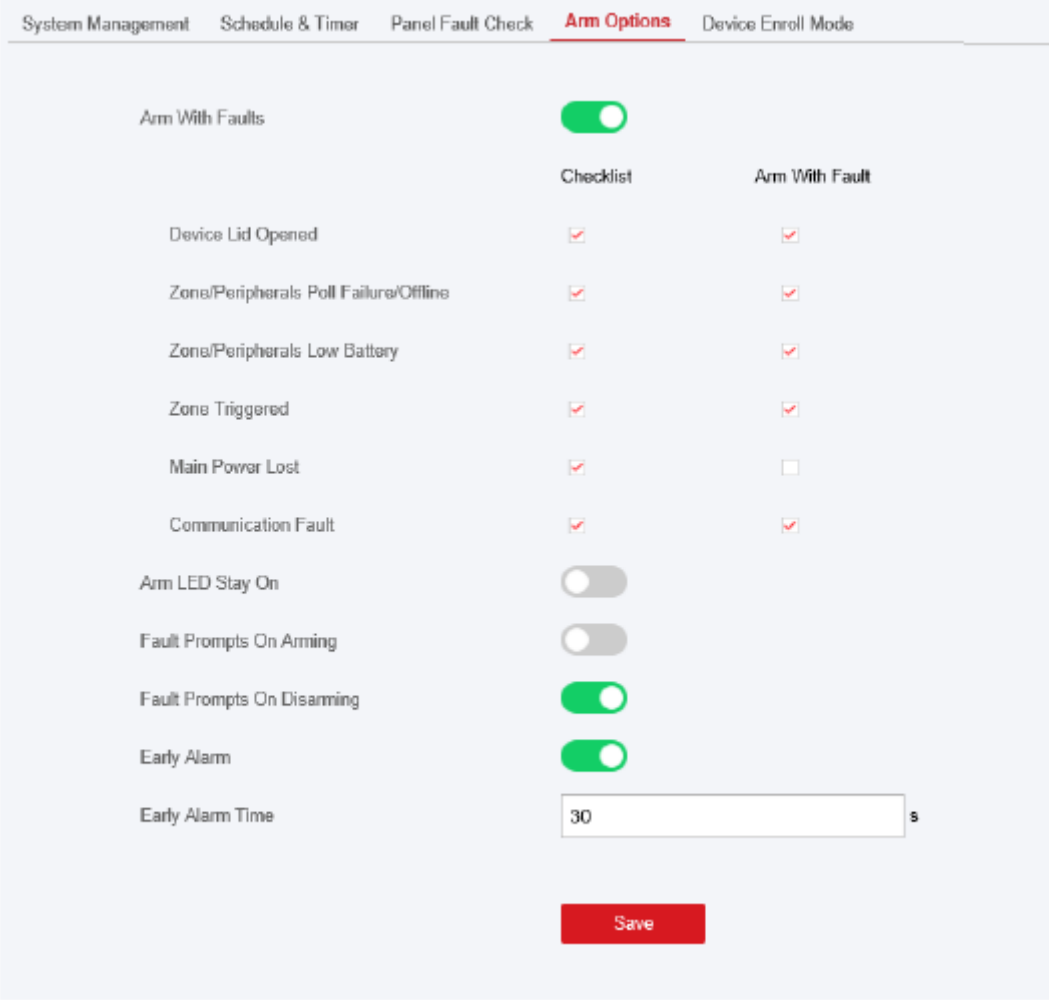
System sprawdza usterkę po skonfigurowanym czasie od wyłączenia zasilania AC.

Aby zachować zgodność z normą EN 50131-3, czas kontroli powinien wynosić 10 s.

Opcje uzbrojenia

Ustaw zaawansowane parametry uprawnień.

Kliknij System → Opcje systemu → Opcje uzbrajania, aby wejść na stronę Ustawienia zaawansowane.



Możesz ustawić następujące parametry:

Aktywacja uzbrojenia z usterką

Sprawdź błędy na liście Aktywacja uzbrojenie z usterkami; urządzenie nie zatrzyma procedury uzbrajania, gdy wystąpią usterki.

Lista kontrolna usterek

System sprawdzi, czy urządzenie ma błędy na liście kontrolnej podczas procedury uzbrajania.

Dioda LED Uzbrajania pozostaje włączona

Jeśli urządzenie stosuje normę EN, domyślnie funkcja jest wyłączona. W takim przypadku, jeśli urządzenie jest uzbrojone, wskaźnik będzie świecił ciągłym niebieskim światłem przez 5 sekund. A jeśli urządzenie jest aktywna, a urządzenie jest uzbrojone, wskaźnik będzie się świecił przez cały czas. Jeśli urządzenie jest rozbrojone, wskaźnik zgaśnie.

Komunikat o błędzie przy uzbrajaniu/rozbrajaniu

Jeśli urządzenie stosuje normę EN, domyślnie funkcja jest wyłączona. W takim przypadku urządzenie nie będzie sygnalizować usterek podczas procedury uzbrajania/rozbrajania.

Aktywacja wczesnego alarm

Po aktywacji funkcji, gdy strefa jest uzbrojona oraz nastąpi jej wyzwolenie, alarm zostanie wygenerowany po ustawionym czasie opóźnienia.

UWAGA

Alarm wczesny zacznie obowiązywać dopiero po wyzwoleniu strefy opóźnionej.

Tryb rejestracji urządzenia

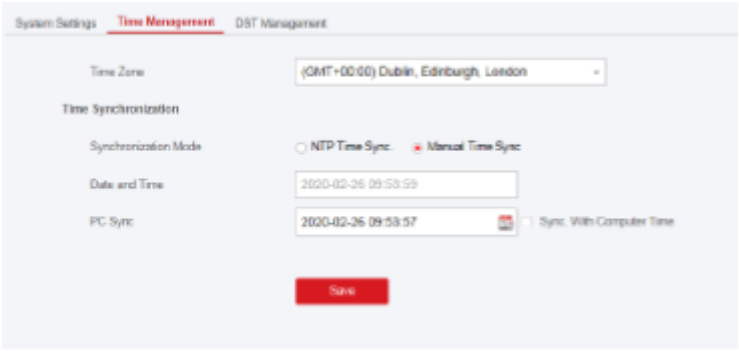
Kliknij opcję Wejdź do trybu rejestracji, aby panel przeszedł w tryb rejestracji.

Ustawienia czasu

Możliwe jest ustawienie strefy czasowej urządzenia, zsynchronizowanie czasu w urządzeniu i ustawienie czasu letniego. Urządzenie obsługuje synchronizację czasu poprzez serwer Hik-Connect Guarding Vision.

Zarządzanie czasem

Kliknij opcję System → Ustawienia systemu → Czas, aby przejść do strony Zarządzanie czasem.



Możesz wybrać strefę czasową z listy rozwijanej.

Możesz zsynchronizować czas urządzenia ręcznie z NTP. Zaznacz pole wyboru NTP Time Sync., Wprowadź adres serwera i numer portu oraz ustaw interwał synchronizacji.

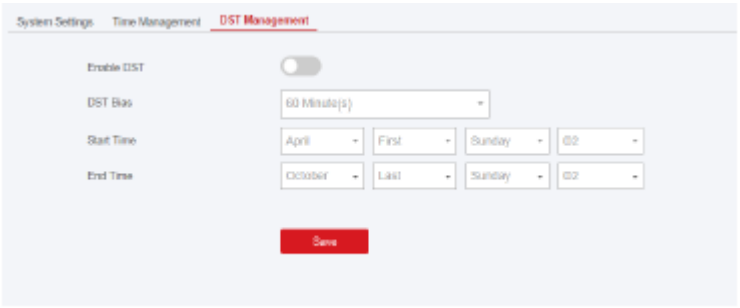
Możesz zsynchronizować czas w urządzeniu ręcznie lub zaznaczyć Synchronizuj z czasem komputera, aby zsynchronizować czas urządzenia z czasem komputera.

UWAGA

Podczas ręcznej synchronizacji czasu lub synchronizacji z czasem komputera system zapisuje w dzienniku „Synchronizacja SDK".

Zarządzanie czasem letnim

Kliknij opcję System → Ustawienia systemu → Zarządzanie czasem letnim, aby przejść do strony Zarządzanie czasem.



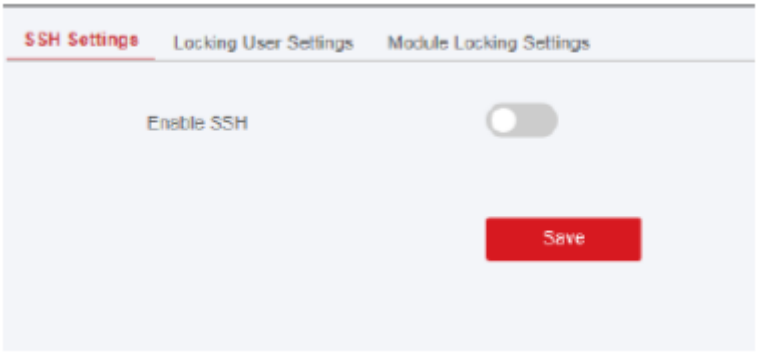
Można włączyć czas letni i ustawić odchylenie czasu letniego, czas rozpoczęcia czasu letniego i czas zakończenia czasu letniego.

Ustawienia bezpieczeństwa

Ustawienia SSH

Włącz lub wyłącz SSH (Secure Shell) zgodnie z Twoimi rzeczywistymi potrzebami.

Kliknij System → Bezpieczeństwo systemu → Ustawienia SSH, aby przejść do strony Ustawienia SSH; możesz włączyć lub wyłączyć funkcję SSH.



Blokowanie ustawień użytkownika

Urządzenie zostanie zablokowane na 90 sekund po 3 nieudanych próbach uwierzytelnienia (można ustawić w opcji Czas ponowienia przed automatyczną blokadą) w ciągu minuty.

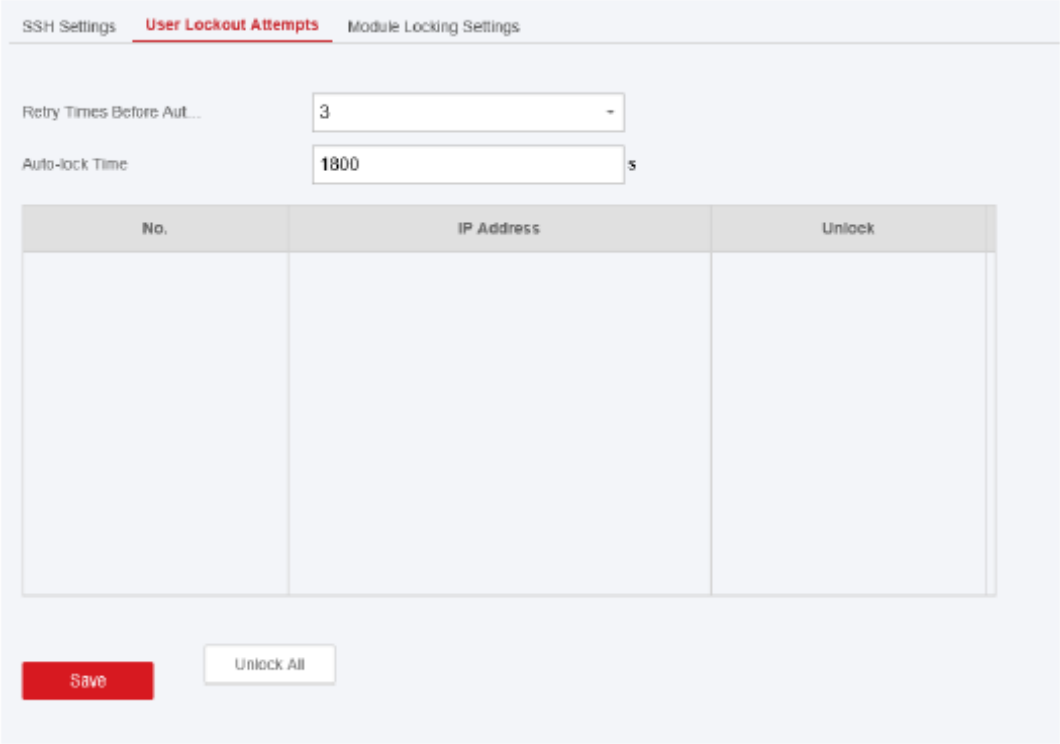
Możesz wyświetlić zablokowanego użytkownika lub odblokować użytkownika i ustawić czas trwania blokady użytkownika.

UWAGA

Aby spełnić wymagania EN, system będzie zapisywał ten sam dziennik tylko 3 razy w sposób ciągły.

Kroki

1. Kliknij System → Zabezpieczenia systemu → Próby blokady użytkownika, aby przejść do strony Ustawienia blokowania użytkownika.



2. Ustaw następujące parametry.

Czasy ponownych prób przed automatyczną blokadą

Jeśli użytkownik będzie ciągle wprowadzał nieprawidłowe hasło dłużej niż skonfigurowano, konto zostanie zablokowane.

UWAGA

Administrator ma dwie próby więcej niż skonfigurowana wartość.

Czas trwania zablokowania

Ustaw czas trwania blokady, gdy konto jest zablokowane.

UWAGA

Dostępny czas blokowania wynosi od 5 do 1800 sekund.

3. Kliknij , aby odblokować konto lub kliknij Odblokuj wszystko, aby odblokować wszystkich zablokowanych użytkowników na liście.

4. Kliknij Zapisz.

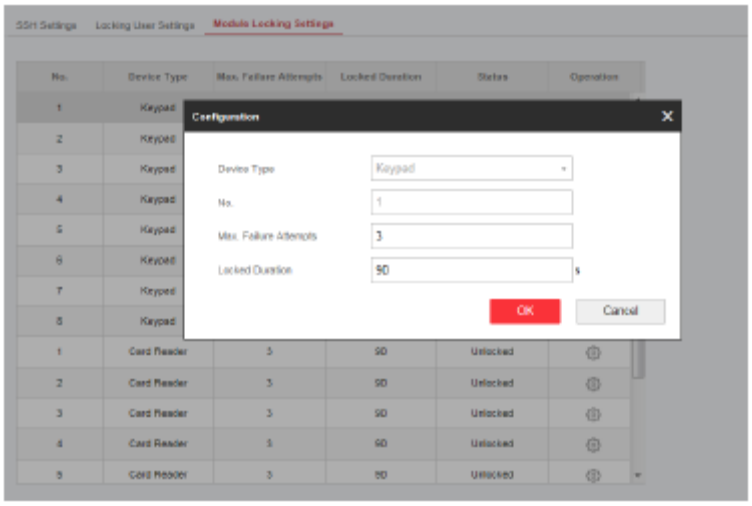
Ustawienia blokady modułu

Ustaw parametry blokowania modułu, w tym maksymalną liczbę prób zakończonych niepowodzeniem i czas trwania blokady.

Moduł zostanie zablokowany na zaprogramowany czas po nieudanej autoryzacji modułu przez określoną liczbę razy.

Kroki

1. Kliknij System → Bezpieczeństwo systemu → Ustawienia blokady modułu, aby przejść do strony Ustawienia blokady modułu.



2. Wybierz moduł z listy i kliknij ikonę .
3. Ustaw następujące parametry wybranego modułu.

Maksymalna liczba prób zakończonych niepowodzeniem

Jeśli użytkownik nieustannie próbuje uwierzytelniać hasło dłużej niż jest to dozwolone w skonfigurowanych próbach, klawiatura zostanie zablokowana na zaprogramowany czas.

Czas trwania zablokowania

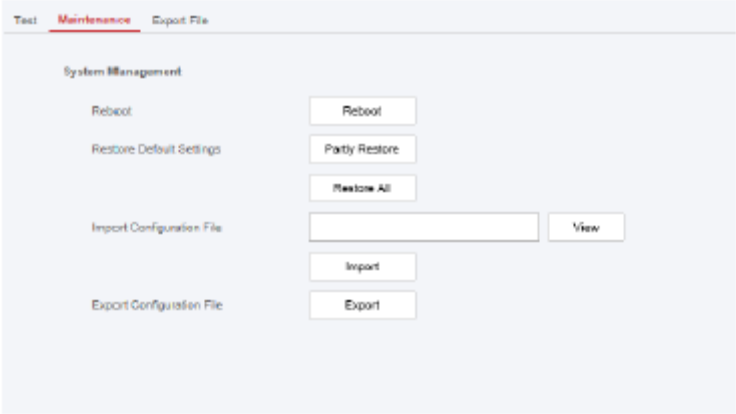
Ustaw czas zablokowania klawiatury. Po skonfigurowanym czasie klawiatura zostanie odblokowana.

4. Kliknij OK.
5. Opcjonalnie: Kliknij ikonę Zablokuj, aby odblokować zablokowany moduł.

Konserwacja systemu

Możesz zrestartować urządzenie, przywrócić ustawienia domyślne, zaimportować/wyeksportować plik konfiguracyjny lub zdalnie zaktualizować urządzenie.

Wybierz urządzenie i kliknij w oprogramowaniu klienckim lub wprowadź adres IP urządzenia w pasku adresu przeglądarki internetowej. Kliknij Zarządzanie projektem → Konserwacja, aby przejść do strony Aktualizacja i konserwacja.



Restart

Kliknij Restart, aby ponownie uruchomić urządzenie.

Przywrócenie ustawień domyślnych

Kliknij opcję Częściowe przywracanie, aby przywrócić wszystkie parametry, z wyjątkiem danych administratora, sieci przewodowej, sieci Wi-Fi, informacji o czujniku i informacji o urządzeniach peryferyjnych, do wartości domyślnych.

Kliknij przycisk Przywróć wszystko, aby przywrócić wszystkie parametry do ustawień fabrycznych.

Importowanie pliku konfiguracyjnego

Kliknij Widok, aby wybrać plik konfiguracyjny z komputera i kliknij Importuj plik konfiguracyjny, aby zaimportować parametry konfiguracyjne do urządzenia. Importowanie pliku konfiguracyjnego wymaga podania hasła ustawionego podczas eksportu.

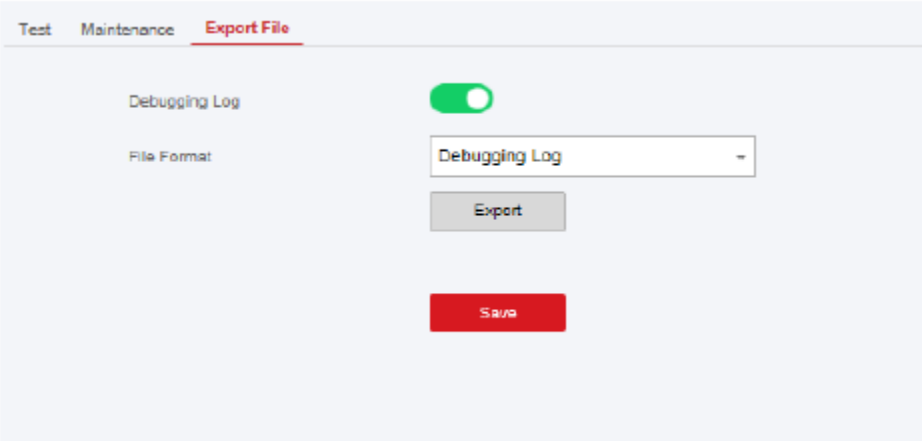
Eksportowanie pliku konfiguracyjnego

Kliknij opcję Eksportuj plik konfiguracyjny, aby wyeksportować parametry konfiguracji urządzenia do komputera. Eksportowanie pliku konfiguracyjnego wymaga podania hasła do szyfrowania plików.

Eksportowanie pliku

Kliknij Zarządzanie projektem → Zachowaj → Eksportuj plik

Aktywuj dziennik debugowania, aby włączyć tę funkcję.



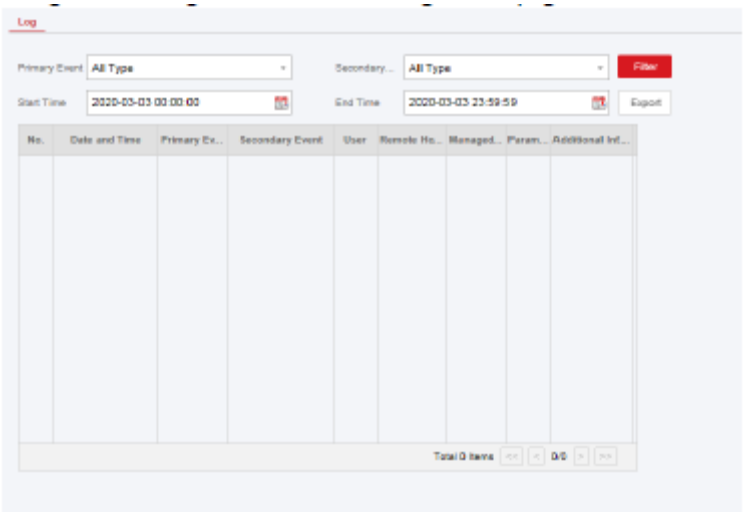
Wybierz typ pliku do wyeksportowania.

Kliknij Eksportuj, aby wyeksportować plik.

Wyszukiwanie w dzienniku lokalnym

Możesz przeszukiwać dziennik na urządzeniu.

Kliknij Zarządzanie projektem → Dziennik, aby przejść do strony Wyszukiwanie w dzienniku lokalnym.



Wybierz typ główny i typ pomocniczy z listy rozwijanej, ustaw czas rozpoczęcia i zakończenia dziennika, a następnie kliknij opcję Filtruj. Wszystkie przefiltrowane informacje dziennika zostaną wyświetlone na liście.

Możesz także kliknąć Reset, aby zresetować wszystkie warunki wyszukiwania.

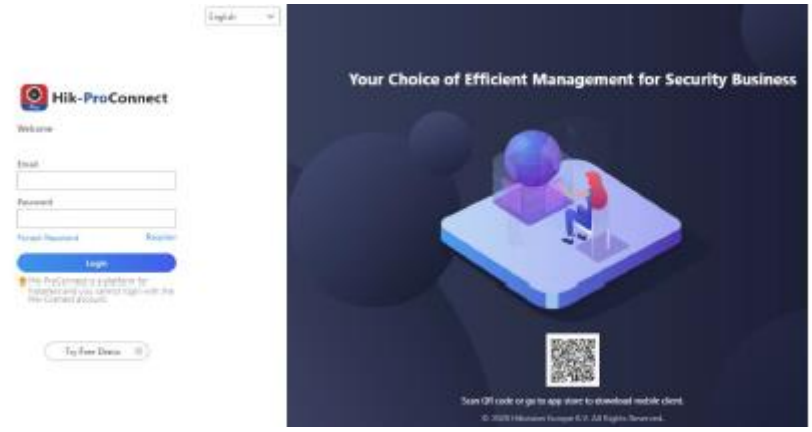
Aktualizacja urządzenia

Uzyskaj kod PIN produkcji

Aby zaktualizować urządzenie, do uwierzytelnienia potrzebny jest fabryczny kod PIN. Fabryczny kod PIN można uzyskać tylko w serwisie Hik-ProConnect, co oznacza, że instalator, który autoryzował administratora na poziomie dostępu 2, autoryzował dostęp na poziomie 4.

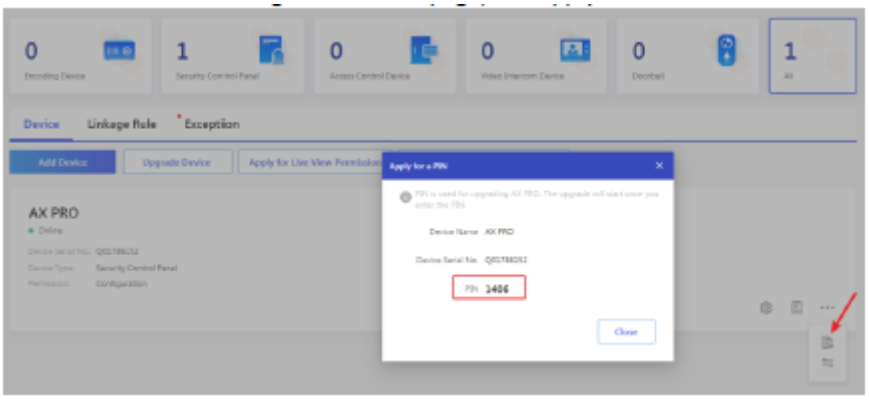
Fabryczny kod PIN może zadziałać tylko raz.

● Uzyskaj kod PIN z serwisu Hik-ProConnect



Zaloguj się na konto instalatora i wejdź na stronę aktualizowanego urządzenia. Kliknij menu Więcej w prawym dolnym rogu strony i zastosuj kod PIN.

● Uzyskaj kod PIN od działu pomocy technicznej HIKVISION



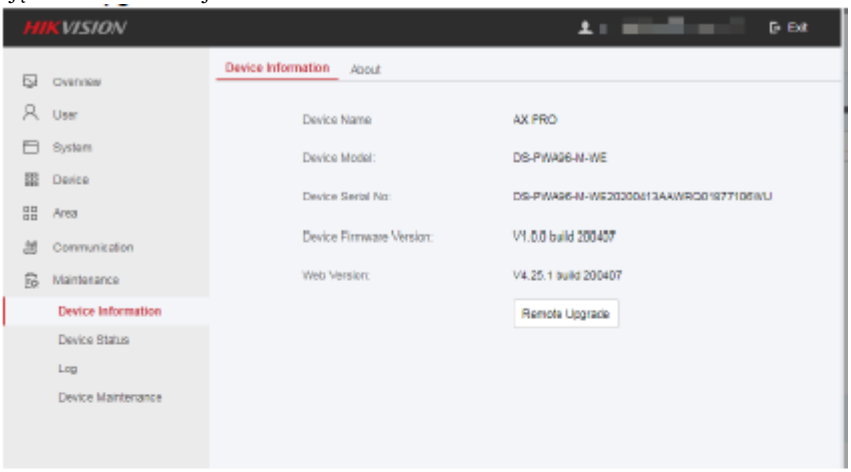
Zalecamy użycie zdalnego pulpitu, aby uzyskać dostęp do lokalnego klienta sieciowego panelu sterowania.

Kod PIN zostanie autoryzowany zgodnie ze standardową procedurą pomocy technicznej.

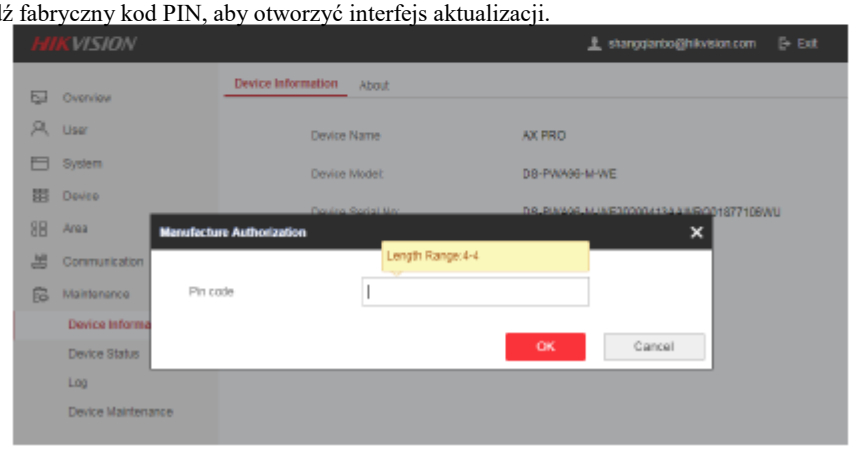
Aktualizacja oprogramowania

Kroki:

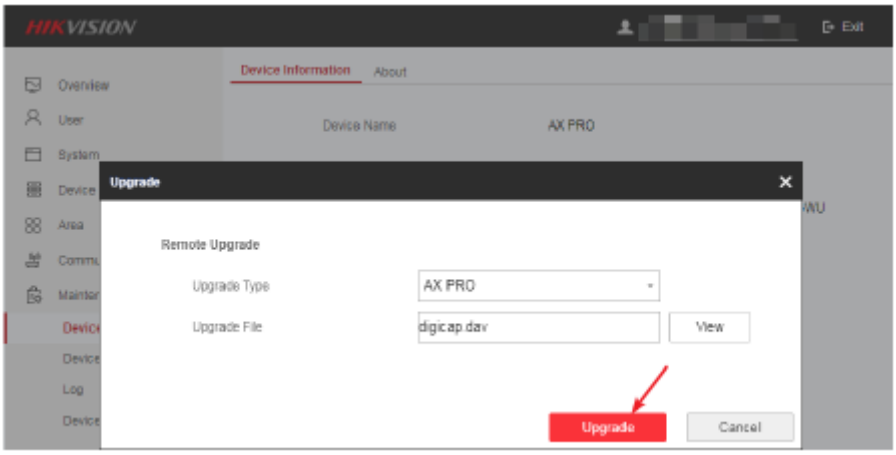
1. Kliknij Konserwacja → Informacje o urządzeniu, aby wejść na stronę.
2. Kliknij opcję Zdalna aktualizacja.



3. Wprowadź fabryczny kod PIN, aby otworzyć interfejs aktualizacji.



4. Kliknij opcję Wyświetl, aby znaleźć plik oprogramowania sprzętowego o nazwie digicap.dav.
5. Kliknij opcję Aktualizuj, aby zakończyć.



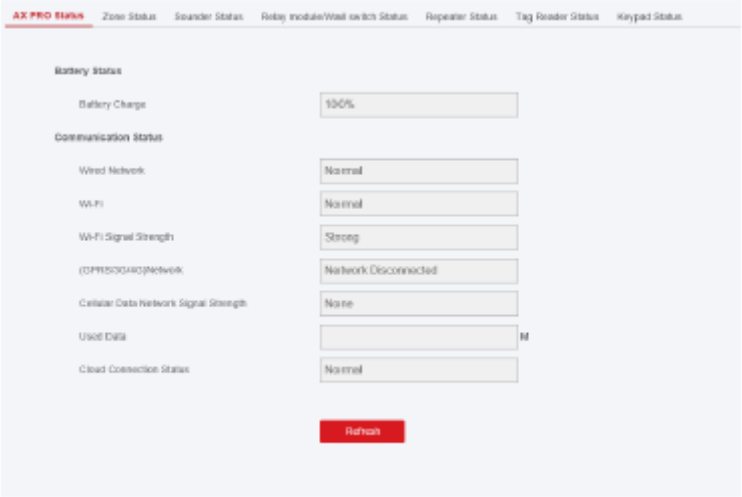
UWAGA

Po zakończeniu aktualizacji zachowani zostaną zarówno użytkownicy, jak i informacje o konfiguracji.

4.3.8 Sprawdź stan

Po ustawieniu strefy, wzmacniaka i innych parametrów można wykonać podgląd ich stanu.

Kliknij Stan. Można wyświetlić stan strefy, przekaźnika, sygnalizatora akustycznego, klawiatury, czytnika znaczników, baterii i komunikacji.



- Strefa: Możesz wyświetlić stan strefy, stan alarmu, pojemność baterii czujnika i siłę sygnału.
- Sygnalizator: Możesz wyświetlić stan sygnalizatora, stan baterii i siłę sygnału.
- Wyjście: Możesz zobaczyć stan przekaźnika, stan baterii i siłę sygnału.
- Klawiatura: Możesz wyświetlić stan klawiatury, stan baterii i siłę sygnału.

● Wzmacniak: Możesz wykonać podgląd stanu roboczego wzmacniaka.

● Czytnik znaczników: Możesz wyświetlić stan czytnika znaczników, stan baterii i siłę sygnału.

4.4 Raport do SMA (Centrum odbioru alarmów)

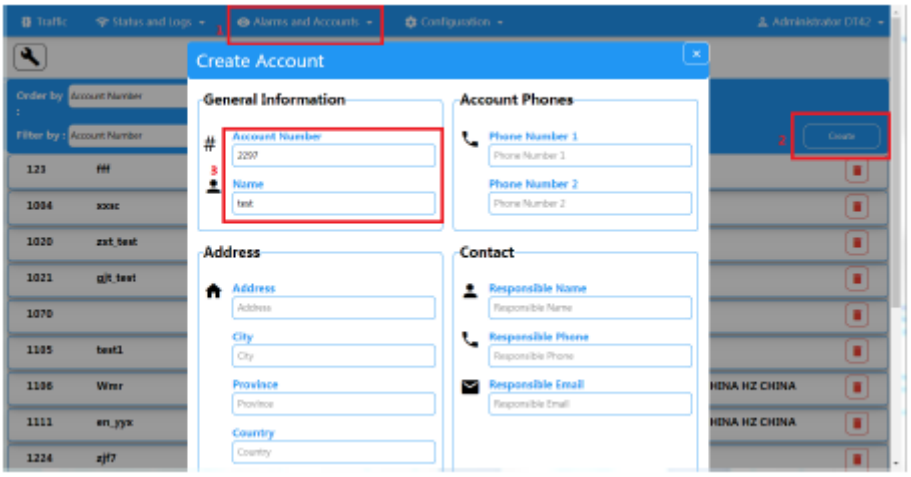
Bezprzewodowy panel sterowania AX Pro został zaprojektowany z wbudowanym nadajnikiem-odbiornikiem zgodnie z wytycznymi EN 50131-10 i EN 50136-2. Kategoria DP2 jest wyposażona w podstawowy interfejs sieciowy LAN/WiFi i dodatkowy interfejs sieciowy GPRS lub 3G/4G LTE. ATS (System Transmisji Alarmów) został zaprojektowany tak, aby zawsze używać interfejsu sieciowego LAN/Wi-Fi, gdy jest dostępny, w celu oszczędzania wykorzystania danych mobilnych. Wtórny interfejs sieciowy zapewnia odporność i niezawodność podczas awarii zasilania.

Konfiguracja ATS w nadajniku-odbiorniku centrum odbioru

Kroki:

1. Zaloguj się do klienta sieciowego odbiornika alarmów.
2. Kliknij Konfiguracja → Odbiór IP i utwórz serwer odbierający, jak przedstawiono poniżej.

3. Kliknij opcję Alarmy i konta → Zarządzanie kontami i przypisz konto do panelu, jak przedstawiono poniżej.

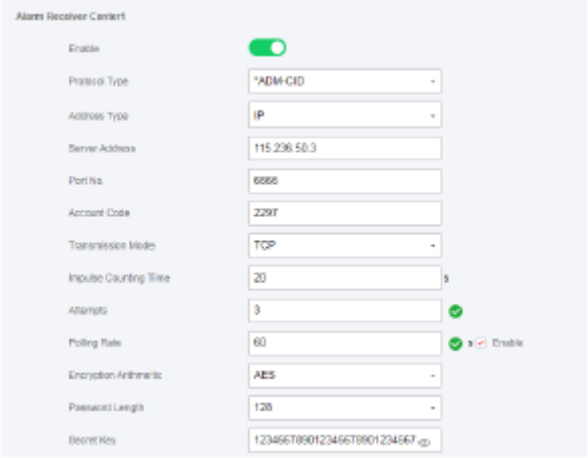


Skonfiguruj ATS w nadajniko-odbiorniku centrali

Kroki:

1. Zaloguj się przy użyciu konta instalatora z lokalnego klienta sieciowego.

2. Kliknij Komunikacja → Centrum odbioru alarmów (ARC) i aktywuj Centrum odbioru alarmów 1.



● = ustawienie protokołu

Typ protokołu

- ADM CID

- SIA DCS

*- * ID klienta ADM*

*- * SIA DCS*

Wybierz token obsługiwany przez odbiorcę w ARC.

● **= Ustawienie serwera**

● Typ adresu

- IP

- Nazwa domeny

● **Adres serwera/nazwa domeny**

● Numer portu

Wprowadź adres IP lub nazwę domeny, za pomocą której można uzyskać dostęp do centrum odbiorczego. Wprowadź numer portu serwera dostarczonego przez ARC

● **= Ustawienie konta**

● Kod konta

Wprowadź przypisane konto dostarczone przez ARC.

● = SIA DC 09 Ustawienie protokołu =

● Tryb transmisji

- TCP

- UDP

Transmisja obsługuje zarówno protokół TCP, jak i UDP. UDP jest zalecany przez standard SIA DC 09.

● **Ustawienia połączenia**

○ Czas zliczania impulsów/Czas oczekiwania na ponowienie

Ustaw limit czasu oczekiwania na odpowiedź odbiornika. Ponowna transmisja nastąpi, jeśli nadajnik-odbiornik lub odbiornik przekroczy limit czasu.

○ Próby

Ustaw maksymalną liczbę prób ponownej transmisji.

○ Szybkość zapytywania

Ustaw interwał między 2 zapytywaniami na żywo, jeśli opcja ta jest zaznaczona.

● **Ustawienia szyfrowania**

○ Arytmetyka szyfrowania

- AES

○ Długość hasła

- 128

- 192

- 256

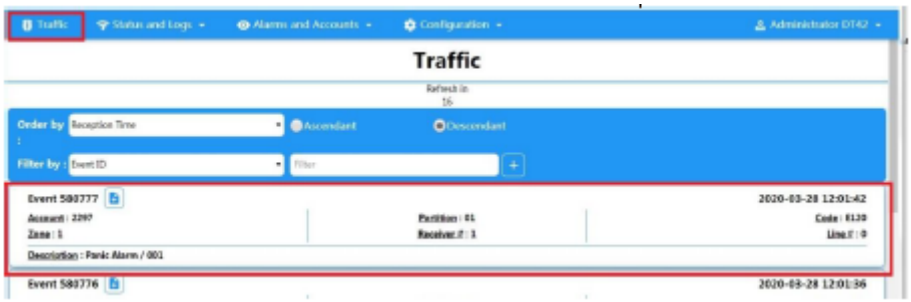
○ Tajny klucz

Ustaw długość klucza szyfrującego i wprowadź klucz dostarczony przez SM.

Test sygnalizacji

Aktywuj alarm napadowy z poziomu panelu sterowania.

Zaloguj się do odbiorcy. Kliknij Ruch, aby przejrzeć wszystkie otrzymane komunikaty.



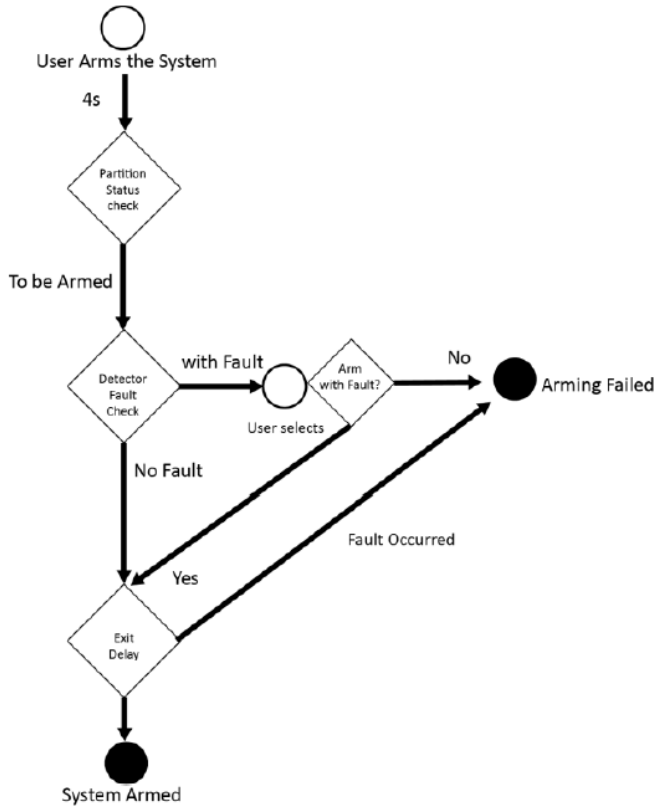
Rozdział 5 Obsługa ogólna

5.1 Uzbrojenie

Do uzbrojenia systemu możesz użyć klawiatury, pilota, znacznika, oprogramowania klienckiego, klienta mobilnego.

Po wysłaniu polecenia uzbrojenia do AX PRO, system sprawdzi stan czujnika. Jeśli czujka jest uszkodzona, konieczne będzie aby zdecydować, czy uzbroić system z usterką.

Gdy system jest uzbrojony, AX PRO wyświetli monit o wynik w ciągu 5 sekund i prześle raport o uzbrojeniu.



LEGENDA:

User arms the system- użytkownik uzbraja system
Partition status check- częściowa kontrola stanu
To be armed- do uzbrojenia
Detector fault check- kontrola usterki wykrywacza
With fault- z usterką
User selects- uzytkownik wybiera
Arm with fault?- uzbrojenie z usterką?
No- nie
Arming failed- uzbrojenie się nie powiodło
No fault- brak usterki
Yes- Tak
Fault occured- wystąpienie usterki
Exit delay- opóźnienie wyjścia
System armed- system uzbrojony

Poziom dostępu do uzbrojenia

Użytkownik na poziomie 2 lub 3 ma uprawnienia do uzbrojenia lub częściowego uzbrojenia systemu.

Wskazanie uzbrojenia

Wskaźnik uzbrojenia/rozbrojenia świeci na niebiesko przez 5 sekund.

Przyczyna braku uzbrojenia

- Zadziałał czujnik wtargnięcia (z wyjątkiem czujnika na drodze wyjścia).
- Zadziałało urządzenie alarmu napadowego.
- Wystąpił alarm sabotażowy.
- Wyjątek komunikacyjny
- Wyjątek od głównego źródła zasilania

● Wyjątek dotyczący baterii zapasowej
● Usterka odbioru alarmu
● Awaria sygnalizatora
● Słaba bateria pilota
● Inne

Uzbrojenie z usterką

Podczas gdy uzbrojenie jest zatrzymane z powodu usterki, użytkownik na poziomie 2 ma uprawnienia do uzbrojenia systemu z usterką (uzbrojenie wymuszone).

Uzbrojenie wymuszone obowiązuje tylko w bieżącej operacji uzbrojenia.

Wymuszone uzbrojenie zostanie zapisane w dzienniku zdarzeń.

5.2 Rozbrajanie

Możesz rozbroić system za pomocą klawiatury, pilota, znacznika, oprogramowania klienckiego lub klienta mobilnego.

Wskazanie rozbrojenia

Wskaźnik uzbrojenia/rozbrojenia miga przez 30 sekund, podczas gdy użytkownik pomyślnie rozbraja system na drodze wejścia/wyjścia.

System poinformuje o wyniku rozbrojenia po zakończeniu operacji.

Czas trwania opóźnienia przy wejściu

Upewnij się, że regulator czasowy nie jest ustawiony na czas dłuższy niż 45 sekund, aby zachować zgodność z EN50131-1.

Wczesny alarm

Jeśli alarm włamania lub sabotażu wystąpi na drodze wejścia/wyjścia, gdy AX PRO jest w stanie opóźnienia wejścia, AX PRO przejdzie w tryb wczesnego alarmu.

Można ustawić czas trwania wczesnego alarmu (> 30 s).

AX PRO zgłosi alarm tylko wtedy, gdy zdarzenie alarmowe trwa przez czas trwania wczesnego alarmu z dodanym opóźnieniem na wejście.

5.3 Sterowanie SMS

Możesz sterować systemem bezpieczeństwa za pomocą wiadomości SMS. Polecenia przedstawiono poniżej.

Format SMS do uzbrojenia/rozbrojenia/wyciszenia alarmu:

{Polecenie} + {Typ operacji} + {Cel}

Polecenie: 2 cyfry, 00- Rozbrojenie, 01- Uzbrojenie pozycyjne, 02- Uzbrojenie obwodowe, 03- Wyciszenie alarmu

Typ operacji: 1- Obszar działania

Cel: nie więcej niż 3 cyfry, 0-działanie dla wszystkich obszarów, 1-działanie dla obszaru 1 (strefa 1); resztę można wywnioskować poprzez analogię.

A. Rozwiązywanie problemów

A.1 Błąd komunikacji

A.1.1 Konflikt adresów IP

Opis błędu:

Adres IP, który panel automatycznie uzyskał lub ustawił, jest taki sam jak innych urządzeń, co powoduje konflikty adresów IP.

Rozwiązanie:

Wyszukaj aktualny dostępny adres IP za pomocą polecenia ping. Zmień adres IP i zaloguj się ponownie.

A.1.2 Strona internetowa jest niedostępna

Opis błędu:

Użyj przeglądarki, aby uzyskać dostęp do stron internetowych i wyświetlić Niedostępne.

Rozwiązania:

1. Sprawdź, czy kabel sieciowy nie jest luźny i czy sieć panelu działa prawidłowo.
2. Port panelu został zmodyfikowany. Dodaj port do adresu internetowego, aby uzyskać dalszy dostęp.

A.1.3 Hik-Connect jest w trybie offline

Opis błędu:

Strona internetowa pokazuje, że Hik-Connect jest w trybie offline.

Rozwiązanie:

Konfiguracja sieciowa panelu jest błędna, nie można uzyskać dostępu do extranetu.

A.1.4 Kamera sieciowa często się wyłącza

Opis błędu:

System raportuje wiele dzienników zdarzeń dotyczących rozłączenia i połączenia IPC.

Rozwiązanie:

Sprawdź, czy komunikacja sieciowa lub podgląd na żywo z kamery są prawidłowe.

A.1.5 Nie udało się dodać urządzenia w aplikacji

Opis błędu:

Podczas korzystania z aplikacji APP do dodawania urządzeń pojawia się monit, że nie można dodać urządzenia, urządzenie nie może zostać odnalezione itp.

Rozwiązanie:

Sprawdź stronę internetową: czy Hik-Connect jest offline.

A.1.6 Informacje alarmowe nie są przekazywane do APP/4200/Centrum alarmowego

Opis błędu:

Po uruchomieniu alarmu aplikacja/4200/centrum alarmowe nie otrzymuje komunikatu alarmowego.

Rozwiązanie:

„Wiadomość push” - „Powiadomienie o alarmie i zabezpieczeniu przed sabotażem” nie jest aktywna. Włącz opcję „Powiadomienie o alarmie i zabezpieczeniu przed sabotażem”.

A.2 Wzajemne wykluczanie funkcji

A.2.1 Nie można wejść w tryb rejestracji

Opis błędu:

Kliknij klawisz funkcyjny panelu i klawisz zgłoszenia konwersacyjnego jest nieaktywny.

Rozwiązanie:

Panel jest w trybie „Hotspot”. Przełącz panel w tryb „stacja”, a następnie spróbuj ponownie wejść w tryb rejestracji.

A.3 Usterka strefy

A.3.1 Strefa jest offline

Opis błędu:

Wyświetl stan stref, które są wyświetlane w trybie offline.

Rozwiązanie:

Sprawdź, czy czujnik komunikuje zbyt niskie napięcie. Wymień baterię czujnika.

A.3.2 Strefa odporna na sabotaż

Opis błędu:

Wyświetla stan wejść, które są odporne na sabotaż.

Rozwiązanie:

Zabezpiecz przycisk czujnika przed sabotażem.

A.3.3 Strefa wyzwolona/usterka

Opis błędu:

Wyświetl stan stref, które wyświetlają sygnał wyzwolenia/usterki.

Rozwiązanie:

Zresetuj czujnik.

A.4 Problemy podczas uzbrajania

A.4.1 Niepowodzenie uzbrojenia (gdy proces uzbrajania nie został rozpoczęty)

Opis błędu:

Kiedy panel jest uzbrojony, szybkie uzbrojenie nie powiedzie się.

Rozwiązanie:

Panel nie daje możliwości „wymuszonego uzbrojenia”, a w przypadku usterki strefy uzbrojenie nie powiedzie się. Włącz opcję „wymuszone uzbrojenie” lub przywróć wejście do normalnego stanu.

A.5 Usterki obsługi

A.5.1 Nie udało się wejść do trybu testowego

Opis błędu:

Nie udało się włączyć trybu testowego; wyświetlenie monitu „Usterka w strefie”.

Rozwiązanie:

Stan strefy, stan alarmu lub zasilanie strefy jest nieprawidłowe.

A.5.2 Operacja kasowania alarmu na panelu nie generuje raportu kasowania alarmu

Opis błędu:

Operacja kasowania alarmu na panelu nie generuje raportu o skasowaniu alarmu.

Rozwiązanie:

W przypadku braku alarmu żaden raport nie zostanie przesłany w celu wykasowania uzbrojenia.

A.6 Niepowodzenie dostarczenia poczty

A.6.1 Nie udało się wysłać wiadomości testowej

Opis błędu:

Podczas konfigurowania informacji o poczcie kliknij „test skrzynki odbiorczej” i test zgłoszenia konwersacyjnego zakończy się niepowodzeniem.

Rozwiązanie:

Błędna konfiguracja parametrów skrzynki pocztowej. Edytuj informacje o konfiguracji skrzynki pocztowej, jak przedstawiono w tabeli 1/1.

A.6.2 Nie udało się wysłać poczty podczas użytkowania

Opis błędu:

Sprawdź dziennik wyjątków panelu. Wystąpił „błąd wysyłania poczty".

Rozwiązanie:

Serwer skrzynek pocztowych ma ograniczony dostęp. Zaloguj się do skrzynki pocztowej, aby sprawdzić, czy skrzynka pocztowa nie jest zablokowana.

A.6.3 Nie udało się wysłać wiadomości e-mail do Gmaila

Opis błędu:

Skrzynką pocztową odbiorcy jest Gmail. Kliknij „Testuj skrzynkę odbiorczą", a test zgłoszenia konwersacyjnego zakończy się niepowodzeniem.

1. Google uniemożliwia użytkownikom uzyskiwanie dostępu do Gmaila za pomocą aplikacji/urządzeń, które nie spełniają ich standardów bezpieczeństwa.

Rozwiązanie:

Zaloguj się do witryny internetowej (https://www.google.com/settings/security/lesssecureapps) i „zacznij korzystać z dostępu do aplikacji, która nie jest wystarczająco bezpieczna". Urządzenie może normalnie wysyłać maile.

2. Gmail nie usuwa uwierzytelniania CAPTCHA.

Rozwiązanie: Kliknij poniższy link, a następnie kliknij „kontynuuj" (https://accounts.google.com/b/0/displayunlockcaptcha).

A.6.4 Nie udało się wysłać wiadomości e-mail do QQ lub Foxmail

Opis błędu:

Skrzynka pocztowa odbiorcy to QQ lub foxmail. Kliknij „Testuj skrzynkę odbiorczą", a test zgłoszenia konwersacyjnego zakończy się niepowodzeniem.

1. Nieprawidłowe konto lub hasło QQ.

Rozwiązanie:

Hasło wymagane do logowania do konta QQ nie jest hasłem używanym do normalnego logowania. Konkretna ścieżka to: Wprowadź konto e-mail → urządzenie → konto →, aby wygenerować kod autoryzacji i użyj kodu autoryzacji jako hasła logowania.

2. Do otwarcia wymagane jest zezwolenie na logowanie SMTP.

A.6.5 Nie udało się wysłać wiadomości e-mail do Yahoo

Opis błędu:

Skrzynka pocztowa odbiorcy to Yahoo. Kliknij „Testuj skrzynkę odbiorczą", a test zgłoszenia konwersacyjnego zakończy się niepowodzeniem.

1. Poziom bezpieczeństwa skrzynki pocztowej jest zbyt wysoki.

Rozwiązanie:

Przejdź do swojego konta pocztowego i włącz „mniej bezpieczne logowanie".

A.6.6 Konfiguracja poczty

Tabela A-1 Konfiguracja poczty

Typ maila	Serwer maila	Port SMTP	Obsługiwane protokoły
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)

UWAGA

O konfiguracji poczty:

• Port SMTP Domyślnie używany jest port 25 bez szyfrowania lub port 465, jeśli używany jest protokół SSL/TLS. Port 587 jest używany głównie w trybie protokołu STARTTLS.

Tryb protokołu STARTTLS, który jest zwykle używany domyślnie przy wybieraniu TLS.

• Nazwa użytkownika Nazwy użytkownika programów Outlook i Hotmail wymagają pełnych nazw, a inne adresy e-mail wymagają przedrostka przed @.

B. Rodzaje danych wejściowych

Tabela B-1 Rodzaje danych wejściowych

Rodzaje danych wejściowych	Operacje
Strefa natychmiastowa	System natychmiast wygeneruje alarm natychmiast, gdy wykryje zdarzenie wyzwalające po uzbrojeniu systemu. Reakcja dźwiękowa: wyzwoli dźwięk systemowy i sygnalizator. Komunikat głosowy: Alarm w strefie X.
Strefa obwodowa	System wygeneruje alarm natychmiast, gdy wykryje zdarzenie wyzwalające po uzbrojeniu systemu. Reakcja dźwiękowa: wyzwoli dźwięk systemowy i sygnalizator. Istnieje konfigurowalny odstęp czasu między alarmem a wyjściem sygnalizatora, co umożliwia sprawdzenie alarmu i anulowanie wyjścia sygnalizatora w tym okresie. Komunikat głosowy: Alarm obwodowy strefy X.
Strefa opóźniona	System zapewnia czas na opuszczenie lub wejście do strefy chronionej bez wygenerowania alarmu. Reakcja dźwiękowa: wyzwoli dźwięk systemowy i sygnalizator. Komunikat głosowy: Alarm w strefie X
Strefa śledzenia	Strefa działa jako opóźniona, gdy wykryje zdarzenie wyzwalające podczas opóźnienia wejścia w systemie, podczas gdy w przeciwnym razie działa jako strefa natychmiastowa. Reakcja dźwiękowa: wyzwoli dźwięk systemowy i sygnalizator. Komunikat głosowy: Alarm śledzący w strefie X.
Strefa wyciszona 24H	Aktywacja strefy następuje przez cały czas bez żadnego dźwięku/sygnalizatora w przypadku wystąpienia alarmu. Reakcja dźwiękowa: Brak dźwięku systemowego (komunikat głosowy lub sygnalizator).
Strefa napadowa	Strefa jest aktywna przez cały czas. Reakcja dźwiękowa: wyzwoli dźwięk systemowy i sygnalizator. Komunikat głosowy: Alarm napadowy w strefie X.
Strefa zagrożenia pożarem	Wejście aktywuje przez cały czas wyjście dźwiękowe/sygnalizator w przypadku wystąpienia alarmu.

Rodzaje danych wejściowych	Operacje
	Reakcja dźwiękowa: wyzwoli dźwięk systemowy i sygnalizator. Komunikat głosowy: Alarm pożarowy w strefie X
Strefa zagrożona wyciekiem gazu	Wejście aktywuje przez cały czas wyjście dźwiękowe/sygnalizator w przypadku wystąpienia alarmu. Reakcja dźwiękowa: wyzwoli dźwięk systemowy i sygnalizator. Komunikat głosowy: Alarm gazowy w strefie X.
Strefa medyczna	Strefa aktywuje przez cały czas wyjście dźwiękowe w przypadku wystąpienia alarmu. Reakcja dźwiękowa: wyzwoli dźwięk systemowy i sygnalizator. Komunikat głosowy: Alarm medyczny w strefie X.
Strefa przekroczenia czasu	Strefa jest aktywna przez cały czas. Rodzaj strefy jest używany do monitorowania i raportowania stanu „AKTYWNA" strefy, ale będzie raportować i alarmować o tym stanie dopiero po upływie zaprogramowanego czasu (od 1 do 599) sekund.
Strefa nieaktywna	Alarmy nie będą aktywowane, gdy dojdzie do naruszenia lub wyzwolenia strefy.. Reakcja dźwiękowa: Brak dźwięku systemowego (komunikat głosowy lub sygnalizator dźwiękowy).
Strefa wirtualna (klawiatura/pilot)	System wygeneruje alarm natychmiast, gdy wykryje zdarzenie wyzwalające po uzbrojeniu systemu. Reakcja dźwiękowa: wyzwoli dźwięk systemowy i sygnalizator. Komunikat głosowy: Sygnał dźwiękowy brzęczyka.
Alarm sabotażowy	System wygeneruje alarm natychmiast, gdy wykryje zdarzenie wyzwalające po uzbrojeniu systemu. Reakcja dźwiękowa: wyzwoli dźwięk systemowy i sygnalizator. Komunikat głosowy: Sabotaż strefy X
Połączenie	Wyzwolenie połączonego urządzenie, gdy wystąpi zdarzenie. Na przykład- Przekaźniki połączone z ekspandorem danych wyjściowych zostaną włączone, gdy AX PRO jest uzbrojone.
Uzbrojenie	Podczas uzbrojenia: Komunikat głosowy o usterce. Usterkę można usunąć postępując zgodnie z poleceniem głosowym. • Dźwięk systemowy do uzbrajania za pomocą znacznika lub pilota. • Komunikat głosowy o usterce. Usterkę można usunąć postępując zgodnie z poleceniem głosowym.

Zdarzenie usterki jest wyświetlane na kliencie. Usterkę można usunąć za pomocą oprogramowania klienckiego lub klienta mobilnego.

Komunikat głosowy: uzbrojenie/ uzbrojenie nie powiodło się.

C. Rodzaje danych wyjściowych

Tabela C-1 Rodzaje danych wyjściowych

Rodzaje danych wyjściowych	Działanie	Przywrócenie
Uzbrojenie	Uzbrojenie AX PRO	Po skonfigurowanym opóźnieniu wyjścia.
Rozbrojenie	Rozbrojenie AX PRO	Po skonfigurowanym opóźnieniu wyjścia.
Alarm	Kiedy wystąpi zdarzenie alarmowe. Wyjściowe dane alarmowe zostaną aktywowane po skonfigurowanym opóźnieniu wyjścia/wejścia.	Po skonfigurowanym opóźnieniu wyjścia rozbrój AX PRO lub wycisz alarm.
Połączenie strefy	Gdy wystąpi zdarzenie alarmowe, połączony przekaźnik wyśle sygnał alarmowy.	Po skonfigurowanym czasie trwania wyjścia.
Obsługa w trybie ręcznym	Ręczna aktywacja przekaźnika.	W czasie wyzwalania lub wyłącz przekaźniki ręcznie.

D. Rodzaje zdarzeń

Tabela D-1 Rodzaje zdarzeń

Rodzaje zdarzeń	Zasada	Domyślnie 1 (powiadomienie oprogramowania klienckiego)	Domyślnie 2 (powiadomienie oprogramowania klienckiego1/2)	Domyślnie 3 (klient mobilny)	Domyślnie 4 (telefon)
Alarm i sabotaż	x/v	v	v	v	v
Wydarzenie związane z bezpieczeństwem życia	x/v	v	v	v	v
Stan systemu	x/v	v	x	x	x
Panel	x/v	v	x	x	x

E. Poziomy dostępu

Poziom	Opis
1	Dostęp dla każdej osoby. Ogólny dostęp.
2	Dostęp użytkownika poprzez operatora i administratora; na przykład klienci (użytkownicy systemów).
3	Dostęp użytkownika przez instalatora; na przykład profesjonalista z firmy alarmowej.

Tabela E-1 Uprawnienia poziomu dostępu

Funkcja	Uprawnienie		
	1	2	3
Uzbrojenie	Nie	Tak	Tak
Rozbrojenie	Nie	Tak	Tak
Przywracanie/kasowanie alarmu	Nie	Tak	Tak
Przechodzenie do trybu testu przejścia	Nie	Tak	Tak
Obejście (strefa)/Wyłączenie/Uzbrojenie wymuszone	Nie	Tak	Tak
Dodawanie/zmiana kodu weryfikacyjnego	Nie	Tak[d]	Tak[d]
Dodawanie/edycja kodu użytkownika i kodu weryfikacyjnego poziomu 2	Nie	Tak	Tak
Dodawanie/edycja danych konfiguracyjnych	Nie	Nie	Tak
Wymiana oprogramowania i oprogramowania sprzętowego	Nie	Nie	Nie

[a] Pod warunkiem posiadania akredytacji przez użytkownika na poziomie 2.

[b] Pod warunkiem posiadania akredytacji przez użytkownika na poziomie 2 i 3.

[d] Użytkownik może edytować tylko swój własny kod użytkownika.

● Poziom użytkownika 2 może przypisać uprawnienia logowania sterownika do poziomu użytkownika 3 na stronie ustawień.

● Poziom użytkownika 2 powinien przypisać uprawnienia poziomowi użytkownika 3, jeśli użytkownik poziomu 3 chce zdalnie zalogować się do sterownika.

● Gdy sterownik zostanie pominięty, poziom użytkownika 3 może zalogować się do sterownika bez przypisania uprawnień z poziomu użytkownika 2.

● Gdy sterownik zostanie pominięty, poziom użytkownika 3 może zalogować się do sterownika bez przydziału uprawnień z poziomu użytkownika 2.

● Użytkownik na poziomie 4 może zalogować się do sterownika tylko wtedy, gdy użytkownik na poziomie 2 lub 3 ma przypisane uprawnienia do 4 poziomu użytkownika.

F. Sygnalizacja

Wykrywanie błędów ATP/ATS

Usterki ATP (ścieżki transmisji alarmu) będą wykrywane, gdy interfejs sieciowy panelu sterowania zostanie odłączony lub ścieżka transmisji do nadajnika-odbiornika centrum odbiorczego znajdującego się w ARC zostanie zablokowana gdzieś pomiędzy. Usterka ATS (System Transmisji Alarmów) zostanie zgłoszona, gdy błędy ATP zostaną wykryte na obu ścieżkach transmisji.

Przywrócenie ATP zostanie wykryte natychmiast po podłączeniu interfejsu sieciowego i przywróceniu ścieżki transmisji do nadajnika-odbiornika centrum odbiorczego. Przywrócenie ATS zostanie zgłoszone po wykryciu przywrócenia ATP dowolnej ścieżki transmisji.

W poniższej tabeli przedstawiono wyniki czasowe wykrywania błędów ATP i przywracania.

	TN	Maksymalny czas wykrywania
Podstawowa awaria/przywrócenie ATP	LAN/WiFi	10 min
	GPRS	60 min
Wtórna awaria/przywrócenie ATP	3G/4G LTE	20 min (gdy podstawowe ATP zawiodło)

Sygnalizacja będzie zawsze przesyłana z podstawowego ATP, gdy będzie działać. W przeciwnym razie zostanie automatycznie przełączony na drugą ścieżkę transmisji, która jest w danej chwili aktywna. Zarówno pierwotne, jak i wtórne zdarzenia awarii i przywrócenia ATP będą zgłaszane do ARC, gdy ATP pozostanie w trybie roboczym. Będą również zapisywane w obowiązkowej pamięci dziennika o pojemności 1000 zapisów alokowanych w nieulotnej pamięci flash, a także w zapisie usterki ATS. Szczegóły raportów i zapisów dziennika są wymienione w poniższej tabeli.

	Kod zdarzenia podczas sygnalizacji	Opis dziennika zdarzeń
Podstawowa awaria/przywrócenie ATP	E351/R351	LAN Path Failed/LAN Path Recovery
Wtórna awaria/przywrócenie ATP	E352/R352	Mobile Net Path Failed/Mobile Net Path Recovery
Awaria/przywrócenie ATS	N/A	ATS Failed
Podstawowa awaria/przywrócenie interfejsu sieci	E351/R351	LAN Path Failed/LAN Path Recovery
Wtórna awaria/przywrócenie interfejsu sieci	E352/R352	Mobile Net Path Failed/Mobile Net Path Recovery

Kategoria ATS

Kategoria ATS w AXPRO to DP2. Gdy centrum odbioru alarmów jest aktywne. Centrala prześle raport alarmowy do centrum odbiorczego poprzez ścieżkę główną (LAN lub Wi-Fi) lub ścieżkę rezerwową (3G/4G). Jeżeli panel sterowania jest poprawnie podłączony do sieci LAN lub Wi-Fi, jako ścieżka transmisji wybierana jest ścieżka główna. Jeśli połączenie głównej ścieżki nie powiedzie się, ścieżka zostanie przełączona na 3G/4G. A jeśli połączenie głównej ścieżki zostanie przywrócone, ścieżka zostanie przełączona z powrotem na LAN lub Wi-Fi. Panel sterowania sprawdza w sposób ciągły stan połączenia i generuje dzienniki błędów transmisji dla dowolnej ścieżki. Jeśli obie ścieżki są nieprawidłowe, centrala określa awarię ATS.

G. Kod SIA i CID

Tabela Kod F-1 SIA i CID

Kod SIA	Kod CID	Opis
BA	E130	Alarm włamaniowy
BH	R130	Przywrócono alarm włamaniowy
HA	E122	Cichy alarm napadowy
HH	R122	Przywrócono cichy alarm napadowy
NA	E780	Alarm przekroczenia limitu czasu
BH	R780	Przywrócono alarm przekroczenia limitu czasu
PA	E120	Alarm napadowy
PH	R120	Przywrócono alarm napadowy
BA	E131	Alarm obwodowy
BH	R131	Przywrócono alarm obwodowy
BA	E134	Alarm wejścia/wyjścia
BH	R134	Przywrócono alarm wejścia/wyjścia
TA	E137	Wykryto sabotaż urządzenia
TR	R137	Przywrócono wykrywanie sabotażu urządzenia
TA	E383	Wykryto sabotaż wykrywacza
TR	R383	Przywrócono wykrywanie sabotażu wykrywacza
TA	E321	Wykryto sabotaż sygnalizatora bezprzewodowy
TR	R321	Przywrócono wykrywanie sabotażu sygnalizatora bezprzewodowego
TA	E334	Wykryto sabotaż wzmacniaka bezprzewodowego
TR	R334	Przywrócono wykrywanie sabotażu wzmacniaka bezprzewodowego
ES	E341	Wykryto sabotaż ekspandora lub urządzenia bezprzewodowego
EJ	R341	Przywrócono wykrywanie sabotażu ekspandora lub urządzenia bezprzewodowego
PA	E120	Alarm napadowy z klawiatury/pilota

Kod SIA	Kod CID	Opis
MA	E100	Alarm medyczny
MH	R100	Przywrócono alarm medyczny
GA	E151	Alarm wycieku gazu
GH	R151	Przywrócono alarm wycieku gazu
FA	E110	Alarm przeciwpożarowy
FH	R110	Przywrócono alarm przeciwpożarowy
OP	E401	Rozbrojenie
CL	R401	Uzbrojenie w trybie AWAY
OA	E403	Automatyczne rozbrojenie
CA	R403	Automatyczne uzbrojenie
BC	E406	Kasowanie alarmu
CL	R441	Uzbrojenie w trybie STAY
CD	E455	Automatyczne uzbrojenie nie powiodło się
BB	E570	Strefa pominięta
BU	R570	Przywrócono pominięcie blokady
CT	E452	Opóźnienie rozbrojenia
AT	E301	Utrata zasilania AC
AR	R301	Przywrócono zasilanie sieciowe
YT	E302	Słaba bateria systemowa
YR	R302	Przywrócono niski poziom baterii systemowej
XT	E384	Słaba bateria pilota
XR	R384	Przywrócono wykrywanie słabej baterii pilota
YM	E311	Awaria baterii
YR	R311	Przywrócono wykrywanie usterki baterii
DK	E501	Klawiatura zablokowana
DO	R501	Klawiatura odblokowana
TS	E607	Wprowadzono tryb testowy
TE	R607	Wyjście z trybu testowego
RN	E305	Reset AX PRO

Kod SIA	Kod CID	Opis
UY	E321	Odłączono bezprzewodowy sygnalizator dźwiękowy
UJ	R321	Podłączono bezprzewodowy sygnalizator dźwiękowy
UY	E381	Odłączono bezprzewodowy wykrywacz
UJ	R381	Podłączono bezprzewodowy wykrywacz
XT	E384	Niskie napięcie wykrywacza bezprzewodowego
XR	R384	Normalne napięcie wykrywacza bezprzewodowego
ET	E333	Odłączony ekspandor lub urządzenie bezprzewodowe
ER	R333	Podłączono ekspandor lub urządzenie bezprzewodowe
UY	E334	Odłączono bezprzewodowy wzmacniak
UJ	R334	Podłączono bezprzewodowy wzmacniak
NT	E352	Odłączono sieć danych komórkowych
NR	R352	Połączono sieć danych komórkowych
NT	E352	Wyjątek dotyczący karty SIM
NR	R352	Przywrócono kartę SIM
NT	E352	Przekroczony przepływ sieciowy
NT	E351	Konflikt adresów IP
NR	R351	Normalny adres IP
NT	E351	Wyjątek dotyczący sieci przewodowej
NR	R351	Normalna sieć przewodowa
NT	E351	Błąd komunikacji Wi-Fi
NR	R351	Połączono z Wi-Fi
XQ	E344	Wyjątek dotyczący sygnału radiowego
XH	R344	Normalny sygnał radiowy

Kod SIA	Kod CID	Opis
/	E306	Usunięto ekspandor
/	R306	Dodano ekspandor
/	E306	Usunięto wykrywacz
/	R306	Dodano wykrywacz
/	E306	Usunięto wzmacniak bezprzewodowy
/	R306	Dodano wzmacniak bezprzewodowy
/	E306	Usunięto sygnalizator bezprzewodowy
/	R306	Dodano bezprzewodowy sygnalizator dźwiękowy
BA	E130	Alarm włamaniowy
BH	R130	Przywrócono alarm włamaniowy
XT	E338	Słaba bateria urządzenia bezprzewodowego
XR	R338	Przywrócono wykrywanie niskiego poziomu naładowania baterii urządzenia bezprzewodowego
LB	E627	Wejście w tryb programowania
LX	E628	Wyjście z trybu programowania
CI	E454	Uzbrojenie nie powiodło się
/	R250	Patrol
/	E306	Usunięto urządzenie bezprzewodowe
/	R306	Dodano urządzenie bezprzewodowe
XT	E384	Niski poziom baterii sygnalizatora bezprzewodowego
XR	R384	Przywrócono niski poziom naładowania baterii sygnalizatora bezprzewodowego
NT	E351	Usterka sieci przewodowej/Wi-Fi ATP
NR	R351	Przywrócono sieć przewodową/Wi-Fi ATP
NT	E352	Błąd ATP sieci komórkowej
NR	R352	Przywrócono ATP sieci komórkowej
CS	1409	Strefa kluczowa rozbrojona
OS	3409	Strefa kluczowa uzbrojona