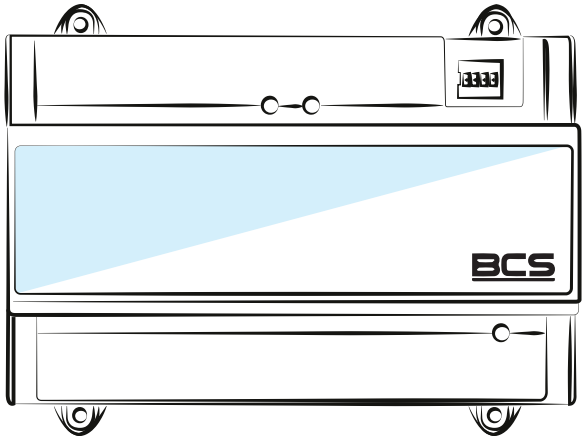
PL

BCS-KKD-J222

Dwudrzwiowy jedno kierunkowy kontroler dostępu

Instrukcja obsługi



www.bcs.pl

NSS Sp. z o.o. ul. Modularna 11 (Hala IV), 02-238 Warszawa
tel. +48 22 846 25 31, fax. +48 22 846 23 31 wew.140
e-mail: info@bcscctv.pl, NIP: 521-312-46-74

Aktualizacja: 08.04.2022

WSTĘP

OGÓLNE:

Dokument opisuje budowę, instalację i okablowanie dwudrzwiowego dwukierunkowego kontrolera dostępu.

INSTRUKCJA BEZPIECZEŃSTWA:

W instrukcji mogą pojawić się następujące słowa sygnałowe o zdefiniowanym znaczeniu.

Hasła ostrzegawcze	Znaczenie
OSTRZEŻENIE!	Wskazuje na wysokie potencjalne zagrożenie, którego zlekceważ e nie spowoduje śmierć lub poważne obrażenia
PRZESTROGA!	Wskazuje na średnie lub niskie potencjalne zagrożenie, które może spowodować lekkie lub umiarkowane obrażenia
UWAGA!	Wskazuje na potencjalne ryzyko, które może spowodować uszkodzenie mienia, utratę danych, niższą wydajność lub nieprzewidziany wynik
WSKAZÓWKI	Zawiera podpowiedzi, które pomogą rozwiązać problem lub zaoszczędzić czas
NOTA	Zapewnia dodatkowe informacje jako uzupełnienie tekstu

INFORMACJA O OCHRONIE PRYWATNOŚCI:

Jako użytkownik urządzenia lub administrator danych możesz gromadzić dane osobowe innych osób, takie jak twarz, odciski palców, numer rejestracyjny samochodu, adres e mail, numer telefonu, GPS i tak dalej. Musisz przestrzegać lokalnych przepisów i rozporządzeń dotyczących ochrony prywatności, aby chronić prawa i interesy innych osób poprzez środki wykonawcze, które obejmują między innymi: poinformowanie osoby, której dotyczą dane o istnieniu obszaru nadzoru i zapewnienie kontaktu.

O INSTRUKCJI

- Instrukcja służy wyłącznie jako odniesienie . Jeżeli istnieją różnice pomiędzy rzeczywistym produktem, a instrukcją, pierwszeństwo ma produkt rzeczywisty.
- Nie ponosimy odpowiedzialności za jakiekolwiek straty spowodowane działaniami niezgodnymi z instrukcją.
- Instrukcja zostanie zaktualizowana zgodnie z najnowszymi przepisami i regulacjami obowiązującymi w regionie. Aby uzyskać szczegółowe informacje, zobacz papierową Instrukcje użytkownika, płytę CD ROM, kod QR lub naszą oficjalną stronę internetową. W przypadku niezgodności między papierową Instrukcja obsługi, a wersją elektroniczną to wersja elektroniczna ma pierwszeństwo.
- Wszystkie projekty i oprogramowanie mogą ulec zmianie bez uprzedniego pisemnego powiadomienia . Aktualizacje produktu mogą powodować pewne różnice między faktycznym produktem, a instrukcją. Skontaktuj się z obsługą klienta, aby uzyskać najnowsze oprogramowanie i dodatkową dokumentację.
- Mogą występować odstępstwa w danych technicznych, opisach funkcji i operacji lub błędy w druku. W razie wątpliwości zapoznaj się z naszym wyjaśnieniem.
- Jeżeli nie można otworzyć Instrukcji obsługi w formacie PDF należy zaktualizować oprogramowanie czytnika PDF lub wypróbować inne oprogramowanie.
- Wszystkie znaki handlowe, zastrzeżone znaki handlowe i nazwy firm w Instrukcji są własnością ich właścicieli.
- Jeśli wystąpi jakiś problem podczas korzystania z urządzenia odwiedź naszą stronę internetową, skontaktuj się z dostawcą lub obsłu gą klienta.
- W razie wątpliwości zapoznaj się z naszym wyjaśnieniem.

WAŻNE ZABEZPIECZENIA I OSTRZEŻENIA:

Poniższy opis jest prawidłową metodą zastosowania urządzenia. Przed użyciem należy dokładnie przeczytać instrukcję, aby uniknąć niebezpieczeństwa i utraty mienia. Ściśle przestrzegaj instrukcji podczas stosowania urządzenia i stosuj się do niej po przeczytaniu.

WYMAGANIA OPERACYJNE

- Nie należy umieszczać i instalować urządzenia w miejscu narażonym na bezpośrednie działa nie promieni słonecznych lub w pobliżu urządzenia wytwarzającego ciepło.
- Nie instaluj urządzenia w wilgotnym, zakurzonym lub pełnym ciepła miejscu.
- Proszę urządzenie zainstalować poziomo lub w stabilnych miejscach i zabezpieczyć przed upadkiem.
- Proszę nie rozpryskiwać płynów na urządzenie, nie kłaść na urządzenie niczego wypełnionego płynami, aby nie dopuścić do przedostania się płynów do urządzenia.
- Zainstaluj urządzenie w dobrze wentylowanych miejscach. Nie blokuj otworu wentylacyjnego.
- Używaj urządz enia tylko w nominalnym zakresie wyjścia i wejścia.
- Nie demontuj urządzenia samowolnie.
- Proszę transportować, używać i przechowywać urządzenia w dopuszczalnym zakresie wilgotności i temperatury.

WYMAGANIA ZASILANIA

- Upewnij się, że używasz baterii zgodnie z wymaganiami, w przeciwnym razie może dojść do pożaru, wybuchu lub poparzenia baterią!
- Do wymiany baterii, można używać tylko tego samego rodzaju baterii.
- W produkcie należy stosować kable elektryczne (kable zasilające) zalecane na tym obszarze, należy stosować je zgodnie ze specyfikacją znamionową!
- Użyj standardowego zasilacza dopasowanego do urządzenia. W przeciwnym razie użytkownik zobowiązuje się do zranienia personelu lub uszkodzenia urządzenia.
- Należy używać zasilacza spełniającego wymagania SELV (bezpieczne bardzo niskie napięcie) i zasilać napięciem zgodnym z ograniczonym źródłem zasilania w IEC60950-1. Szczegółowe wymagania dotyczące zasilania można znaleźć na etykietach urządzeń.
- Produkty z kategorii I należy podłączyć do gniazda sieciowego, k tóre jest wyposażone w uziemienie ochronne.
- Łącznik urządzenia jest urządzeniem rozłączającym. Podczas użytkowania należy zachować kąt ułatwiający obsługę.

SPIS TREŚCI

1. PRZEGLĄD

Dwudrzwiowy jednokierunkowy kontroler dostępu to urządzenie sterujące, które równoważy nadzór wideo i wizualny domofon. Ma schludny i nowoczesny design o dużej funkcjonalności, odpowiedni do budynków komercyjnych, nieruchomości korporacyjnych i inteligentnej społeczności.

1.1 CECHY URZĄDZENIA

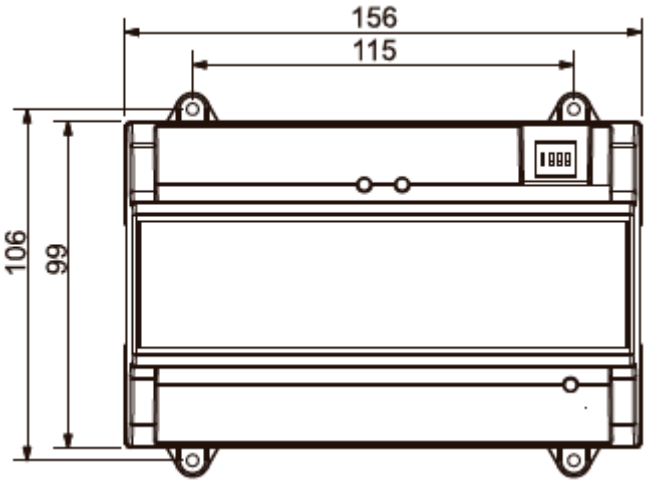
Jego bogate funkcje są następujące:

- Zastosowanie szyny ślizgowej i konstrukcji sterowanej zamkiem, wygodna instalacja i konserwacja.
- Zintegrowany alarm, kontrola dostępu, nadzór wideo i alarm przeciwpożarowy.
- Obsługa 2 zestawów czytników kart.
- Obsługa 6 grup sygnałów wejściowych (przycisk wyjścia*2, kontakt drzwi*2 i alarm włamaniowy*2).
- Obsługuje 4 grupy wyjść sterujących (zamek elektryczny *2 i wyjście alarmowe *2).
- Z portem RS485 może rozszerzyć się o moduł sterujący.
- Pojemność pamięci FLASH wynosi 16M (może wzrosnąć do 32M). Wsparcie do 100,000 kart i 150,000 rekordów odczytu kart.
- Obsługa alarmu nielegalnego włamania, odblokowanie alarmu przekroczenia czasu, karty przymusu i konfiguracji kodu przymusu. Obsługuje również konfiguracje czarno-białej listy i karty patrolowej.
- Obsługa ustawiania prawidłowego okresu czasu, hasła i daty ważności karty. W przypadku karty gościa można ustawić jej czas użytkowania.
- Obsługa 128 grup harmonogramów i 128 grup harmonogramów świątecznych.
- Stałe przechowywanie danych podczas awarii, wbudowane RTC (wsparcie DST), aktualizacja online.

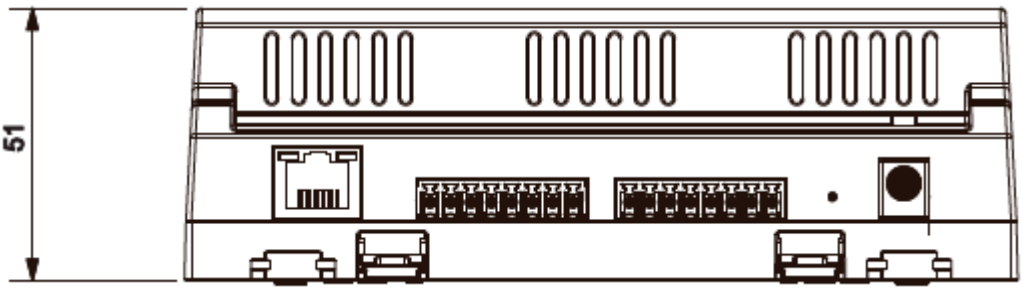
1.2 WYMIARY I WYGLĄD

Jego wygląd i rozmiary pokazano na Obrazie 1-1 i Obrazie 1-2. Jednostką długości są milimetry.

Obraz 1-1



Obraz 1-2

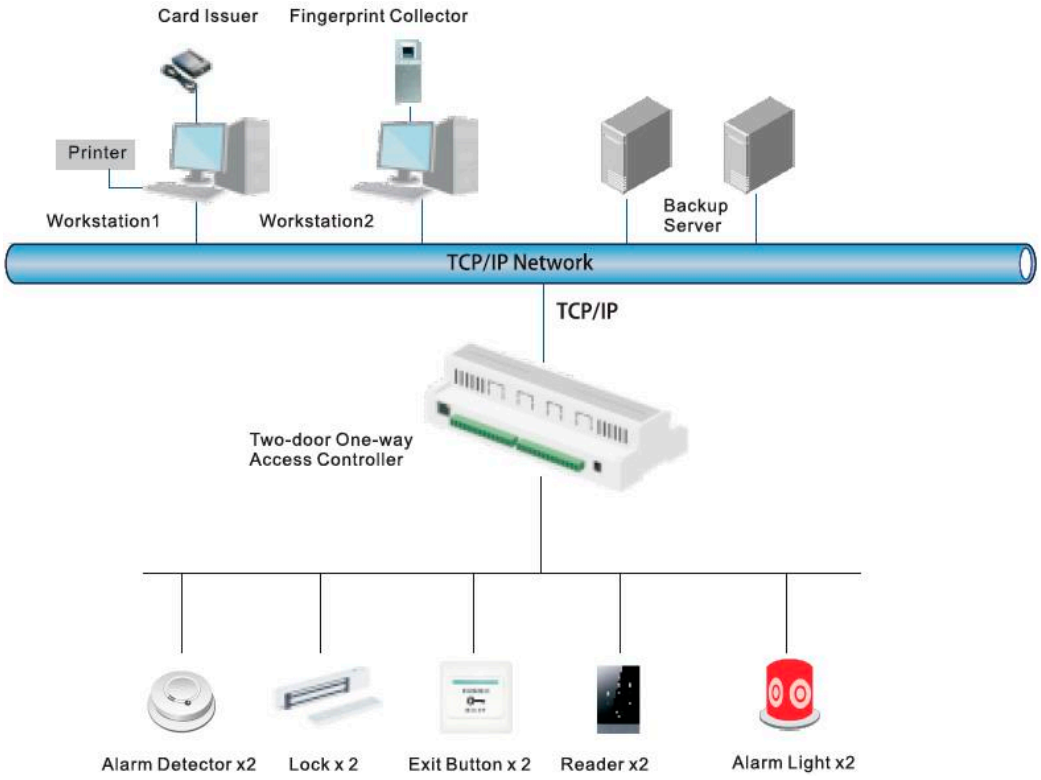


2. PRZEWODNIK INSTALACJI

2.1 STRUKTURA SYSTEMU

Struktura systemu dwudrzwiowego jednokierunkowego kontrolera dostępu, zamka drzwi i czytnika pokazano na Obrazie 2-1.

Obraz 2-1



2.2 INSTALACJA URZĄDZENIA

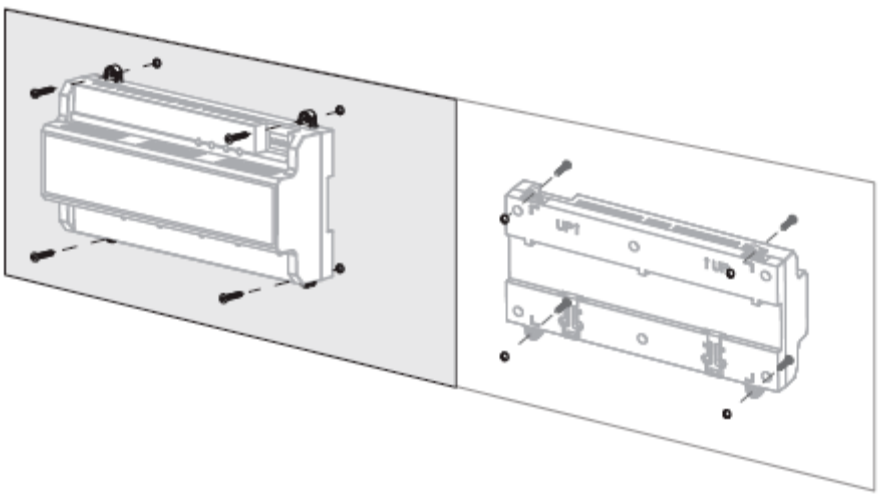
Istnieją dwa sposoby instalacji.

- Sposób 1: Przymocuj całe urządzenie do ściany za pomocą śrub.
- Sposób 2: Z szyną prowadzącą w kształcie litery U, zawiesić całe urządzenie na ścianie (Sposób 2 jest opcjonalnym montażem).

SPOSÓB 1

Schemat instalacji jest pokazany na Obrazie 2-2.

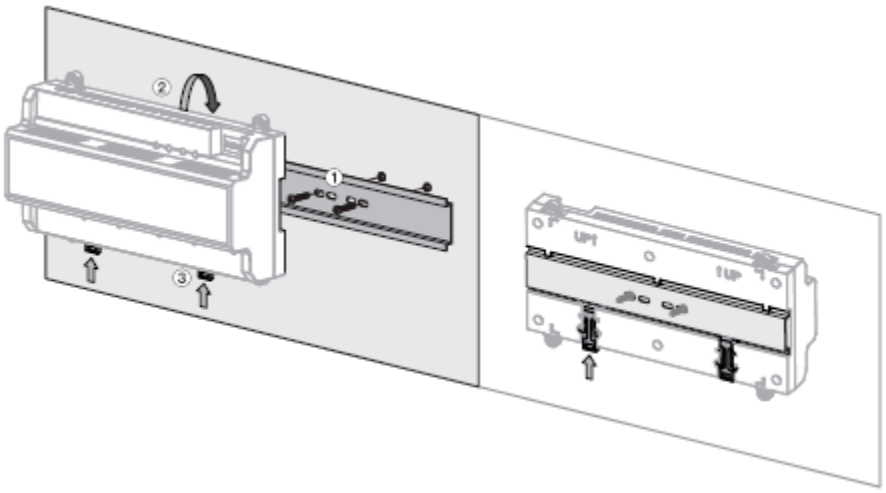
Obraz 2-2



SPOSÓB 2

Schemat instalacji jest pokazany na Obrazie 2-3.

Obraz 2-3

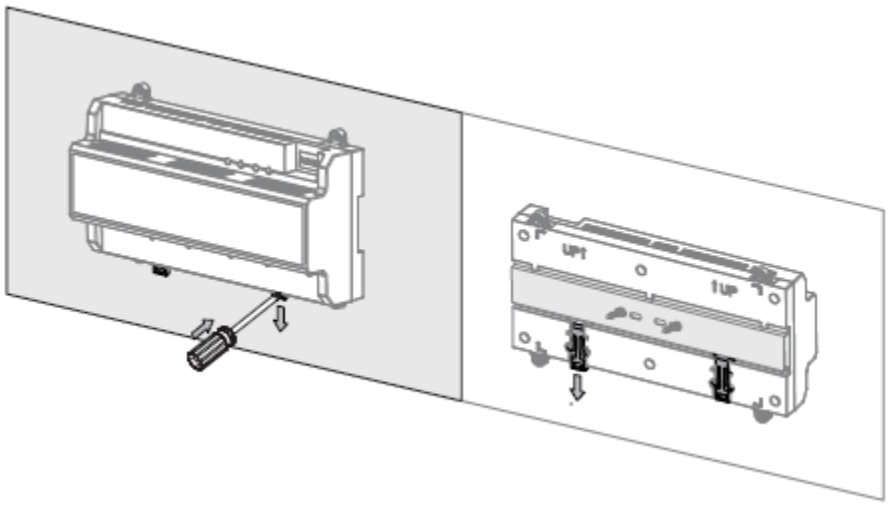


Krok 1 Przymocuj szynę prowadzącą w kształcie litery U do ściany za pomocą śrub.
Krok 2 Zapnij górną tylną część urządzenia w górnym roku szyny prowadzącej w kształcie litery U.
Krok 3 Naciśnij złącze zatrzaskowe na dole urządzenia w górę. Instalacja zostanie zakończona, gdy usłyszysz dźwięk dopasowania.

2.3 DEMONTAŻ

Jeżeli urządzenie jest zainstalowane sposobem 2, należy go zdemontować zgodnie z Obrazem 2-4. Dopasuj śrubokręt do złącza zatrzaskowego, naciśnij go, a złącze zatrzaskowe wyskoczy, aby całe urządzenie można było płynnie zdemontować.

Obraz 2-4

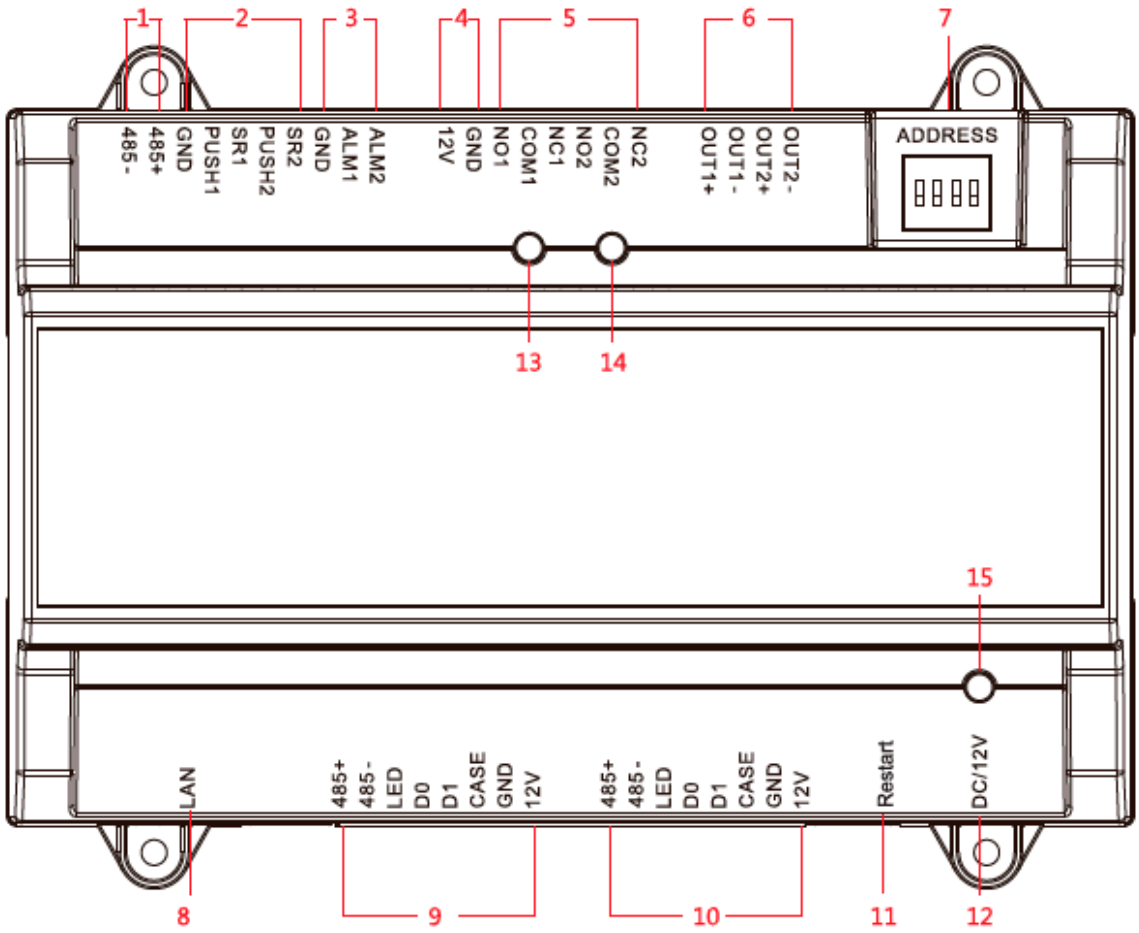


2.4 SCHEMAT OKABLOWANIA

2.4.1 OPIS OKABLOWANIA KONTROLERA DOSTĘPU

To urządzenie obsługuje dwudrzwiowe jednokierunkowe wejście lub wyjście. W przypadku wejścia alarmowego uruchom zewnętrzne urządzenie wyjściowe, aby włączyć alarm. Schemat okablowania urządzenia pokazano na Obrazie 2-5.

Obraz 2-5



Interfejsy opisano w Tabeli 2-1.

Tabela 2-1

Numer	Opis portu	Numer	Opis portu
1	Komunikacja RS485	7	Przełącznik DIP
2	Przycisk wyjścia i kontakt drzwiowy	8	TCP/IP
3	External alarm input	9	Czytnik drzwi 1
4	Wyjście zasilające zamku	10	Czytnik drzwi 2
5	Wyjście sterujące zamku	11	Restart
6	Wyjście alarmowe	12	DC 12V

Kontrolki opisano w Tabeli 2-2.

Tabela 2-2

Numer	Opis portu
13	Stan wskaźnika blokady drzwi
14	
15	Wskaźnik zasilania LED

2.4.2 OPIS OKABLOWANIA PRZYCISKU WYJŚCIA/KONTAKTU DRZWI

Odpowiednie łączenie okablowania przycisku wyjścia i kontaktu drzwi pokazano na Obrazie 2-6. Opisy łączenia przewodów znajdują się w Tabeli 2-3.

Obraz 2-6

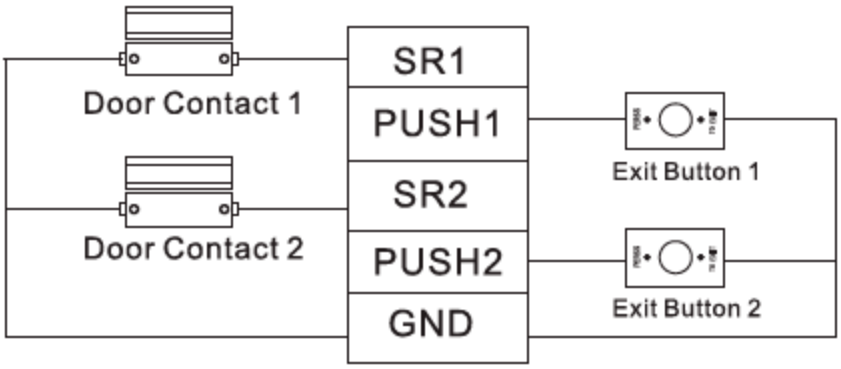


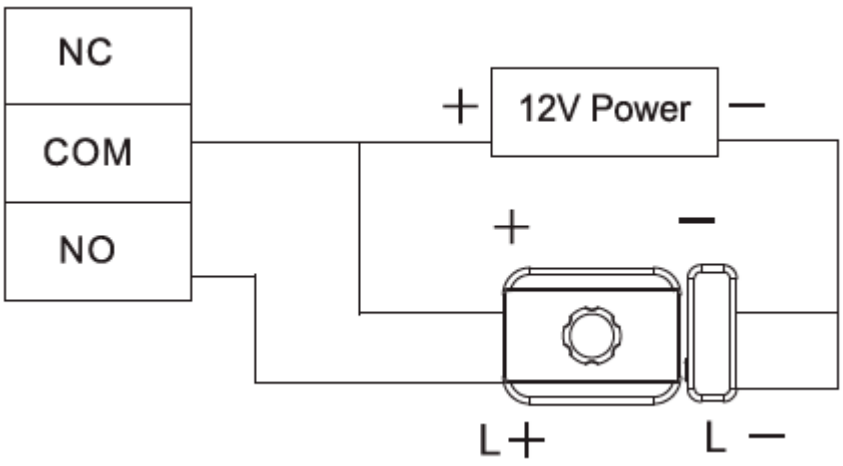
Tabela 2-3

Port	Łącze okablowania	Opis
Przycisk wyjścia i kontakt drzwi	SR1	Wejście kontaktu dla drzwi 1
	PUSH1	Przycisk wyjścia drzwi 1
	SR2	Wejście kontaktu dla drzwi 2
	PUSH2	Przycisk wyjścia drzwi 2
	GND	Współdzielone przez przycisk wyjścia, wejście kontaktu drzwi I RS485

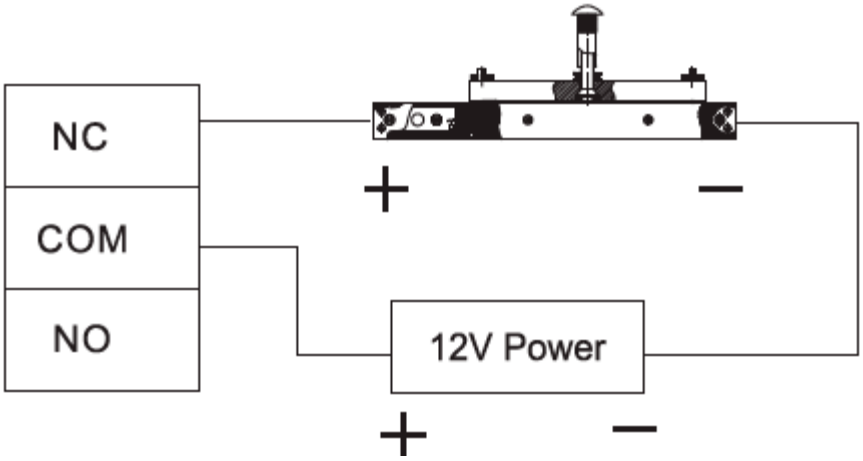
2.4.3 OPIS OKABLOWANIA ZAMKU

Obsługa 2 grup wyjść sterowania zamkiem, numery seryjne po łączeniach oznaczają odpowiednie drzwi. Wybierz odpowiedni tryb połączenia zgodnie z typem zamka, jak pokazano na Obrazie 2-7, Obrazie 2-8 i Obrazie 2-9. Opisy łączenia przewodów znajdują się w Tabeli 2-4.

Obraz 2-7



Obraz 2-8



Obraz 2-9

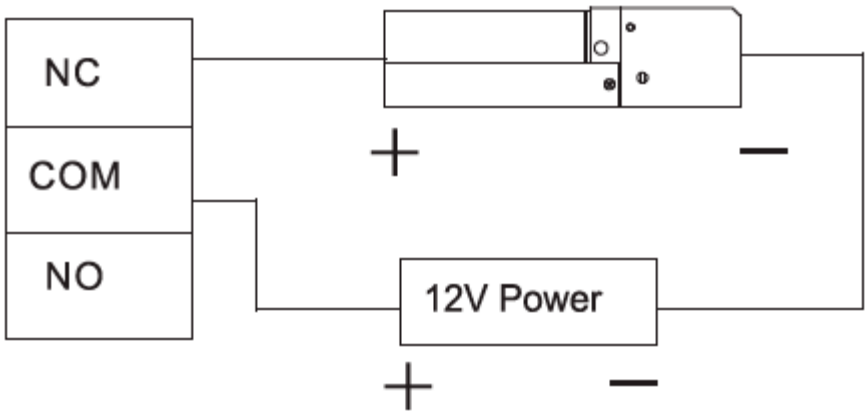


Tabela 2-4

Port	Łącze okablowania	Opis
Wyjściowy port sterowania zamku	NC1	Kontrola zamka drzwi 1
	COM1	
	NO1	
	NC2	Kontrola zamka drzwi 2
	COM2	
	NO2	

2.4.4 OPIS OKABLOWANIA CZYTNIKA

Jedne drzwi obsługują tylko jeden typ czytnika – RS485 lub Wiegand.

Opisy łączenia okablowania czytników znajdują się w Tabeli 2-5. Weźmy za przykład drzwi 1, inne czytniki są takie same. Opisy specyfikacji i długości kabla czytnika znajdują się w Tabeli 2-6.

Tabela 2-5

Port	Łącze okablowania	Kolor kabla	Opis
Wejście czytnika drzwi 1	485+	Purple	RS485
	485-	Yellow	
	LED	Brown	Wiegand
	D0	Green	
	D1	White	
	CASE	Blue	
	GND	Black	Zasilanie czytnika
	12V	Red	

Tabela 2-5

Rodzaj	Typ połączenia	Długość
RS485485	Kabel sieciowy CAT5e	100 m
Wiegand	Kabel sieciowy CAT5e	100 m

2.4.5 OPIS OKABLOWANIA ZEWNĘTRZNEGO WEJŚCIA ALARMOWEGO

2-kanałowe zewnętrzne wejście alarmowe pokazano na Obrazie 2-10. Opisy łączenia przewodów znajdują się w Tabeli 2-7.

Obraz 2-10

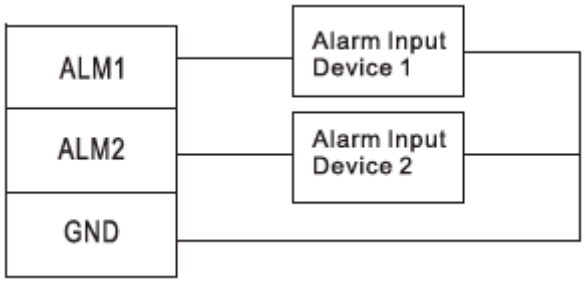


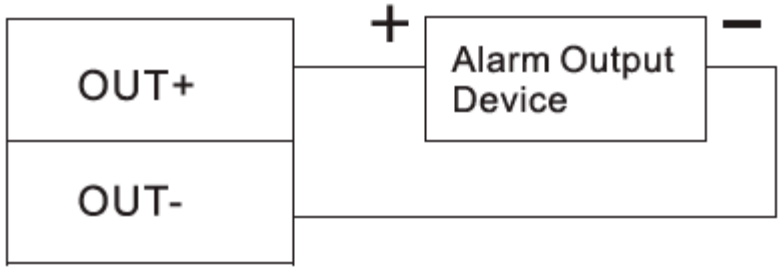
Tabela 2-7

Port	Łącze okablowania		Opis
Zewnętrzne wejście alarmowe	ALM1	Port wejściowy alarmu 1	Przez zewnętrze porty wejściowe alarmu możemy łączyć czujkę dymu, czujkę podczerwieni itp.
	ALM2	Port wejściowy alarmu 2	
	GND	Współdzielone przez port wejściowy alarmu 1 i 2	Alarm zewnętrzny może łączyć status otwarcia I zamknięcia drzwi. • ALM1 łączy wszystkie drzwi w celu normalnego otwarcia. • ALM2 łączy wszystkie drzwi w celu normalnego zamknięcia.

2.4.6 OPIS OKABLOWANIA ZEWNĘTRZNEGO WYJŚCIA ALARMOWEGO

Istnieją dwa sposoby podłączenia zewnętrznego wyjścia alarmowego, w zależności od urządzenia alarmowego. Na przykład IPC może korzystać ze sposobu 1, podczas gdy syrena dźwiękowa i wizualna może korzystać ze sposobu drugiego, jak pokazano na Obrazie 2-11 i Obrazie 2-12. Opisy łączenia okablowania znajdują się w Tabeli 2-8.

Obraz 2-11



Obraz 2-12

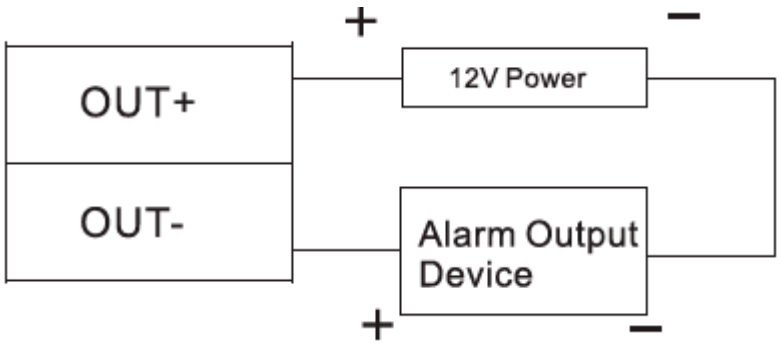


Tabela 2-8

Numer	Opis portu		Opis portu
Zewnętrzne wyjście alarmowe	OUT1+	ALM1 wyzwala wyjście alarmowe. • Wyjście alarmu o przekroczeniu limitu czasu drzwi i sygnalizacji włamania do drzwi 1. • Wyjście alarmu sabotażowego czytnika drzwi 1.	Wewnętrzne i zewnętrzne porty wyjścia alarmowego mogą łączyć syreny dźwiękowe i wizualne.
	OUT1-		
	OUT2+	ALM2 wyzwala wyjście alarmowe. • Wyjście alarmu o przekroczeniu limitu czasu drzwi i sygnalizacji włamania do drzwi 2. • Wyjście alarmu sabotażowego czytnika drzwi 2.	
	OUT2-		

2.4.7 OPIS ZASADY WEJŚCIA I WYJŚCIA ALARMOWEGO

W przypadku zdarzenia alarmowego, alarm trwa przez 15 sekund. Szczegółowe informacje dotyczące wejść i wyjść alarmowych znajdują się w Tabeli 2-9.

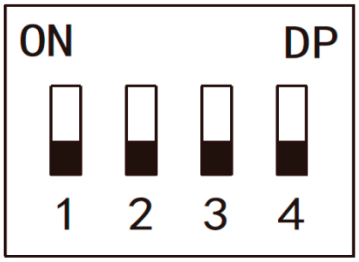
Tabela 2-9

Typ alarmu	Port wejściowy sygnału alarmowego	Port wyjściowy sygnału alarmowego	Status alarmu
Zewnętrzne wejście alarmowe	ALM1	OUT1	Łączy wszystkie drzwi, aby były normalnie otwarte.
	ALM2	OUT2	Łączy wszystkie drzwi, aby były normalnie zamknięte.
Wewnętrzne wejście alarmowe	SR1	OUT1	Alarm przekroczenia czasu drzwi i włamania wyzwala alarm zewnętrzny.
	SR2	OUT2	
	RS-485/CASE	OUT1	Alarm sabotażowy czytnika wyzwala alarm zewnętrzny.
	RS-485/CASE	OUT2	

2.5 PRZEŁĄCZNIK DIP

Obsługa za pomocą przełącznika DIP.

Obraz 2-13



- Przełącznik znajduje się w pozycji ON, co oznacza 1.
- Przełącznik znajduje się w pozycji OFF, co oznacza 0.
- 1~ 4 wszystkie są ustawione na 0. System jest uruchamiany normalnie.
- 1~4 wszystkie są ustawione na 1. System przechodzi w tryb BOOT po uruchomieniu.
- 1, 3 są ustawione na 1, gdy reszta ustawiona jest na 0. Po restarcie system przywróci ustawienia fabryczne.
- 2, 4 są ustawione na 1, gdy reszta ustawiona jest na 0. Po ponownym uruchomieniu system przywraca ustawienia fabryczne, ale informacje o użytkowniku zostają zachowane.

2.6 RESTART

Włóż igłę do otworu restartu, naciśnij raz, aby ponownie uruchomić urządzenie.

Przycisk Restart służy do ponownego uruchomienia urządzenia, a nie do modyfikacji konfiguracji.

3. KONFIGURACJA SMART PSS

Żeby zapewnić kontrolę i właściwą konfiguracje jednych drzwi lub grup drzwi, kontrolerem dostępu zarządza się za pomocą klienta Smart PSS. W tym rozdziale opisano głównie szybką konfigurację. Szczegółowe informacje na temat operacji można znaleźć w instrukcji obsługi klienta Smart PSS.

Klient Smart PSS oferuje różne porty dla różnych wersji. Proszę odnieść się do faktycznego portu.

3.1 LOGOWANIE KLIENTA

Zainstaluj pasującego klienta Smart PSS i kliknij dwukrotnie , aby uruchomić. Wykonaj konfigurację inicjalizacji zgodnie z podpowiedziami interfejsu i zakończ logowanie.

3.2 DODANIE KONTROLI DOSTĘPU

Dodaj kontroler dostępu w Smart PSS. Wybierz „Automatycznie wyszukiwanie” i „Dodaj”.

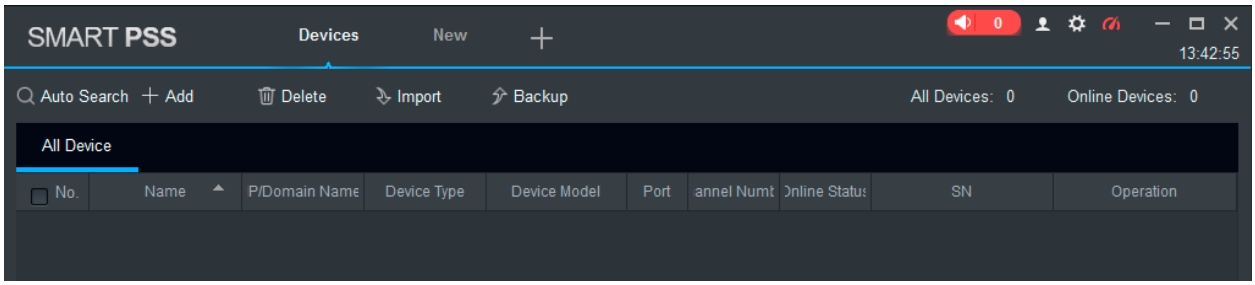
3.2.1 AUTOMATYCZNE WYSZUKIWANIE

Urządzenia muszą znajdować się w tym samym segmencie sieci.

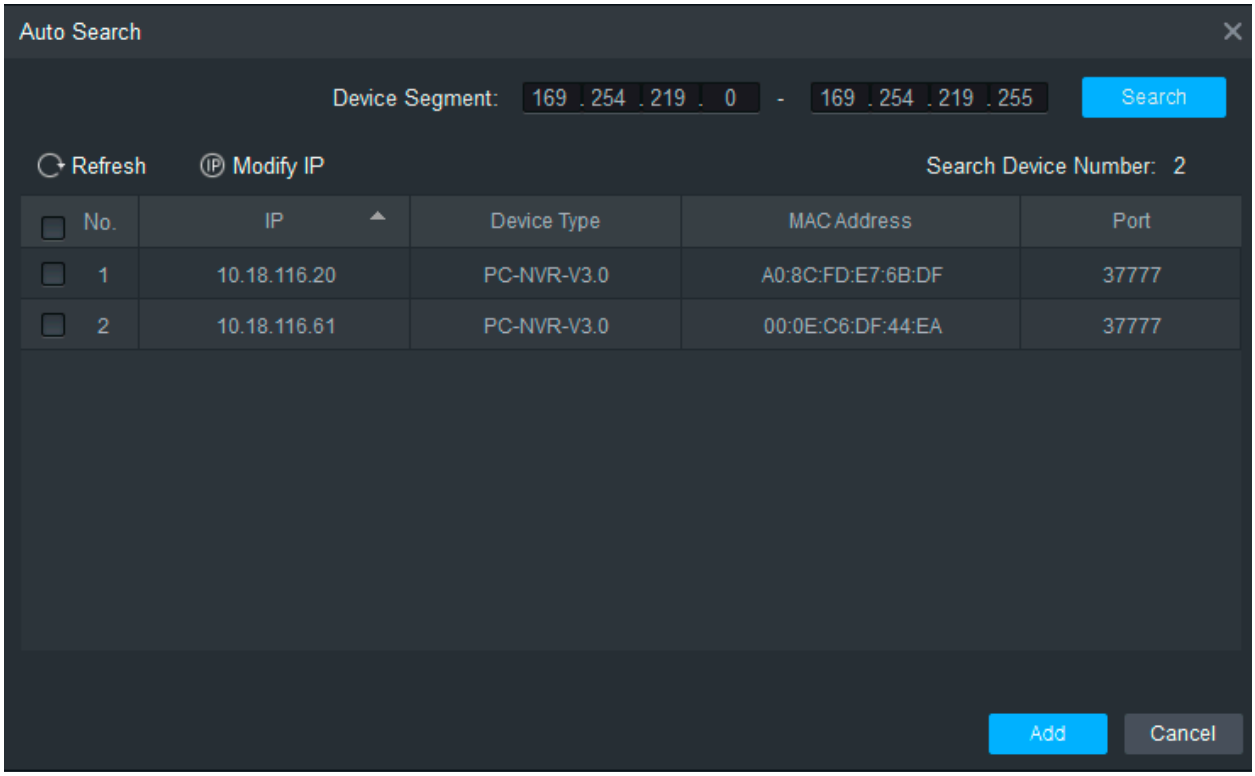
Krok 1 W interfejsie „Urządzenia”, kliknij „Automatyczne wyszukiwanie”, jak pokazano na Obrazie 3-1.

System wyświetla interfejs „Auto Wyszukiwanie”, jak pokazano na Obrazie 3-2.

Obraz 3-1



Obraz 3-2



Krok 2 Wpisz segment w którym znajduje się urządzenie i kliknij „Wyszukaj”.

System wyświetli wyniki wyszukiwania.

- Kliknij „Odśwież”, aby zaktualizować informacje o urządzeniach.
- Wybierz urządzenie, kliknij „Zmodyfikuj IP”, aby zmodyfikować adres IP urządzenia. Szczegółowe informacje na temat operacji można znaleźć w instrukcji obsługi klienta Smart PSS

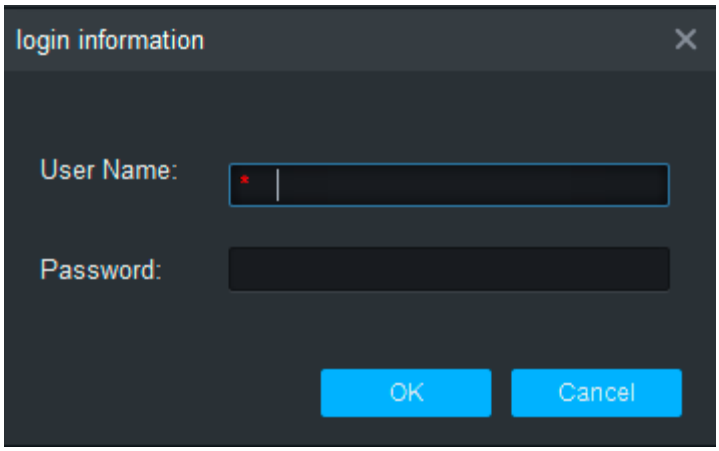
Krok 3 Wybierz urządzenie, które chcesz dodać i kliknij „Dodaj”.

System wyświetli „Monituj”

Krok 4 Kliknij „OK”.

System wyświetli okno dialogowe „Informacje logowania”, jak pokazano na Obrazie 3-3.

Obraz 3-3



Krok 5 Wpisz „Nazwa użytkownika” i „Hasło”, aby zalogować się do urządzenia i kliknij „OK”.

System wyświetli listę dodanych urządzeń, jak pokazano na Obrazie 3-4. Szczegóły znajdują się w Tabeli 3-1.

- Po zakończeniu dodawania system nadal pozostaje w interfejsie „Automatyczne wyszukiwanie”. Możesz kontynuować dodawanie kolejnych urządzeń lub kliknąć „Anuluj”, aby wyjść z interfejsu „Automatyczne wyszukiwanie”.
- Po zakończeniu dodawania Smart PSS automatycznie loguje się do urządzenia. W przypadku pomyślnego logowania status urządzenia zmieni się na „Online”. W przeciwnym razie wyświetli się „Offline”.

Obraz 3-4

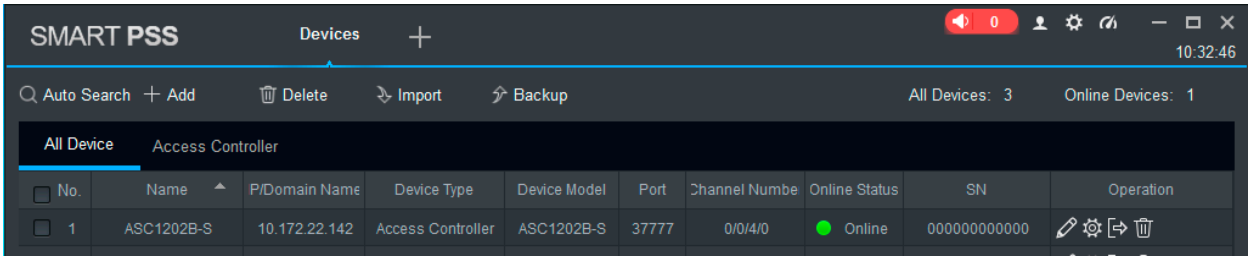


Tabela 3-1

Ikona	Opis
	Kliknij tę ikonę, aby przejść do interfejsu „Modyfikuj urządzenie” i zmodyfikować informacje o urządzeniu, w tym nazwę urządzenia, adres IP/nazwę domeny, port, nazwę użytkownika, hasło. Lub kliknij dwukrotnie urządzenie, aby przejść do interfejsu „Modyfikuj urządzenie”
	Kliknij tę ikonę, aby przejść do interfejsu „Konfiguracja urządzenia” i skonfigurować kamerę urządzenia, sieć, zdarzenie, pamięć i informacje o systemie.
	• Gdy urządzenie jest w trybie online, ikona to  . Kliknij tę ikonę, aby wyjść z logowania, a ikona zmieni się w  . • Gdy urządzenie jest offline, ikona to  . Kliknij tę ikonę, aby zalogować się (z prawidłowymi informacjami o urządzeniu), a ikona zmieni się w  .
	Kliknij tę ikonę, aby usunąć urządzenie.

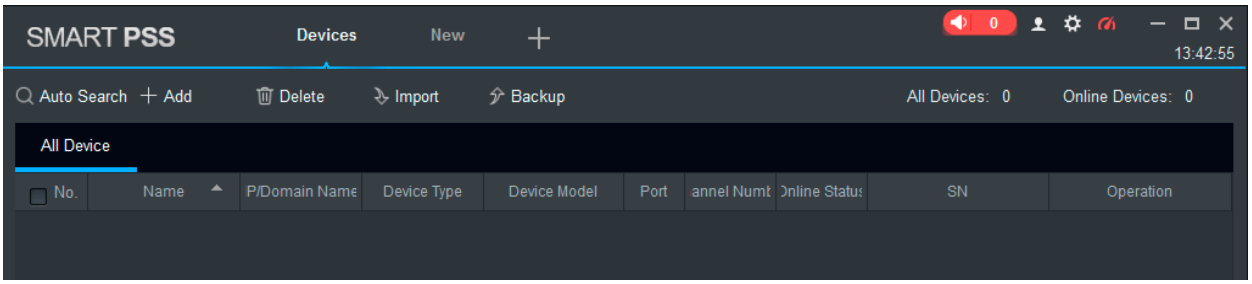
3.2.2 RĘCZNE DODAWANIE

Aby dodać urządzenia, najpierw należy znać adres IP urządzenia lub nazwę domeny.

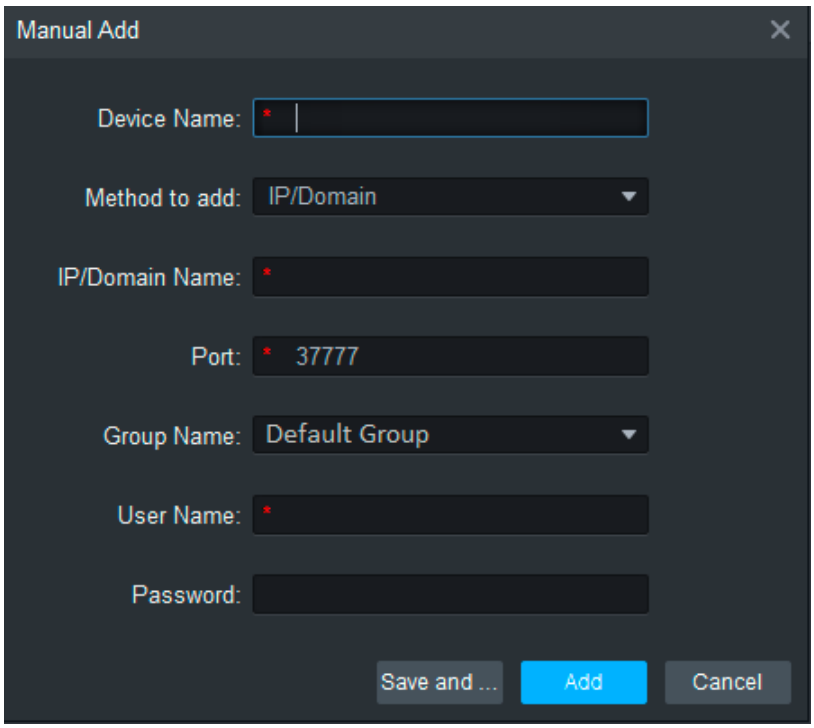
Krok 1 W interfejsie „Urządzenia” kliknij „Dodaj”, jak pokazano na Obrazie 3-5.

System wyświetli interfejs „Ręczne dodawanie”, jak pokazano na Obrazie 3-6.

Obraz 3-5



Obraz 3-6



Krok 2 Ustaw parametry urządzenia. Szczegółowe opisy parametrów znajdują się w Tabeli 3-2.

Tabela 3-2

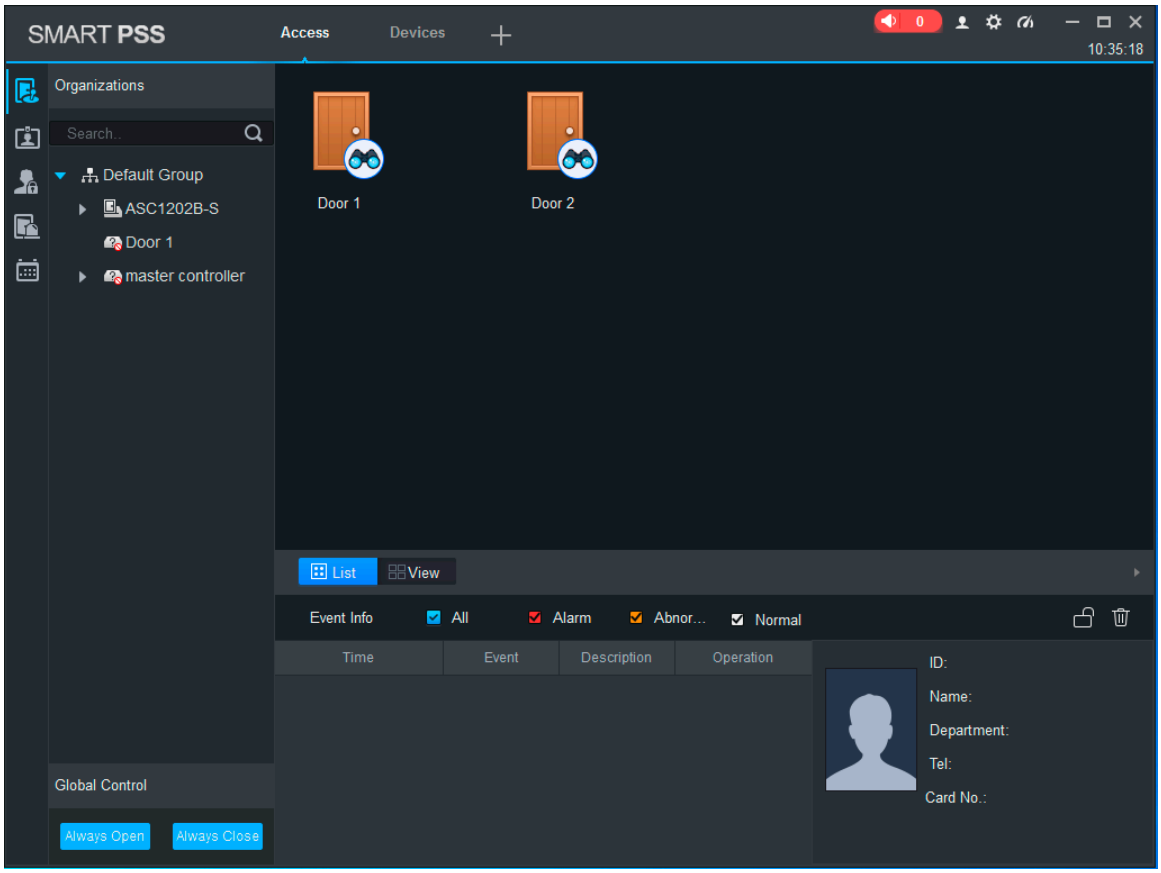
Parametr	Opis
Nazwa urządzenia	Zaleca się, aby nazwa urządzenia była nazywana strefą monitorowania, żeby ułatwić konserwację.
Metoda dodania	Wybierz „IP/Nazwa Domeny”. Dodaj urządzenia zgodnie z adresem IP urządzenia lub nazwą domeny.
IP/Nazwa domeny	Adres IP lub nazwa domeny urządzenia.
Port	Numer portu urządzenia. Domyślny numer portu to 37777. Proszę wypełnić zgodnie z aktualnymi warunkami.
Nazwa grupy	Wybierz grupę urządzenia.
Nazwa użytkownika i hasło	Nazwa użytkownika i hasło urządzenia.

Krok 3 Kliknij „Dodaj”, aby dodać urządzenie.

System wyświetli listę dodanych urządzeń, jak pokazano na Obrazie 3-7. Szczegóły znajdują się w Tabeli 3-2. Drzwi dodanego kontrolera są wyświetlane w zakładce „Dostęp”, jak pokazano na Obrazie 3-8.

- Aby dodać więcej urządzeń, kliknij „Zapisz i kontynuuj”, dodaj urządzenia i pozostań w interfejsie „Ręczne dodawanie”.
- Aby anulować dodawanie, kliknij „Anuluj” i wyjdź z interfejsu „Ręczne dodawanie”.
- Po zakończeniu dodawania Smart PSS automatycznie loguje się do urządzenia przypadku pomyślnego logowania status wyświetli „Online”. W przeciwnym razie wyświetli się „Offline”.

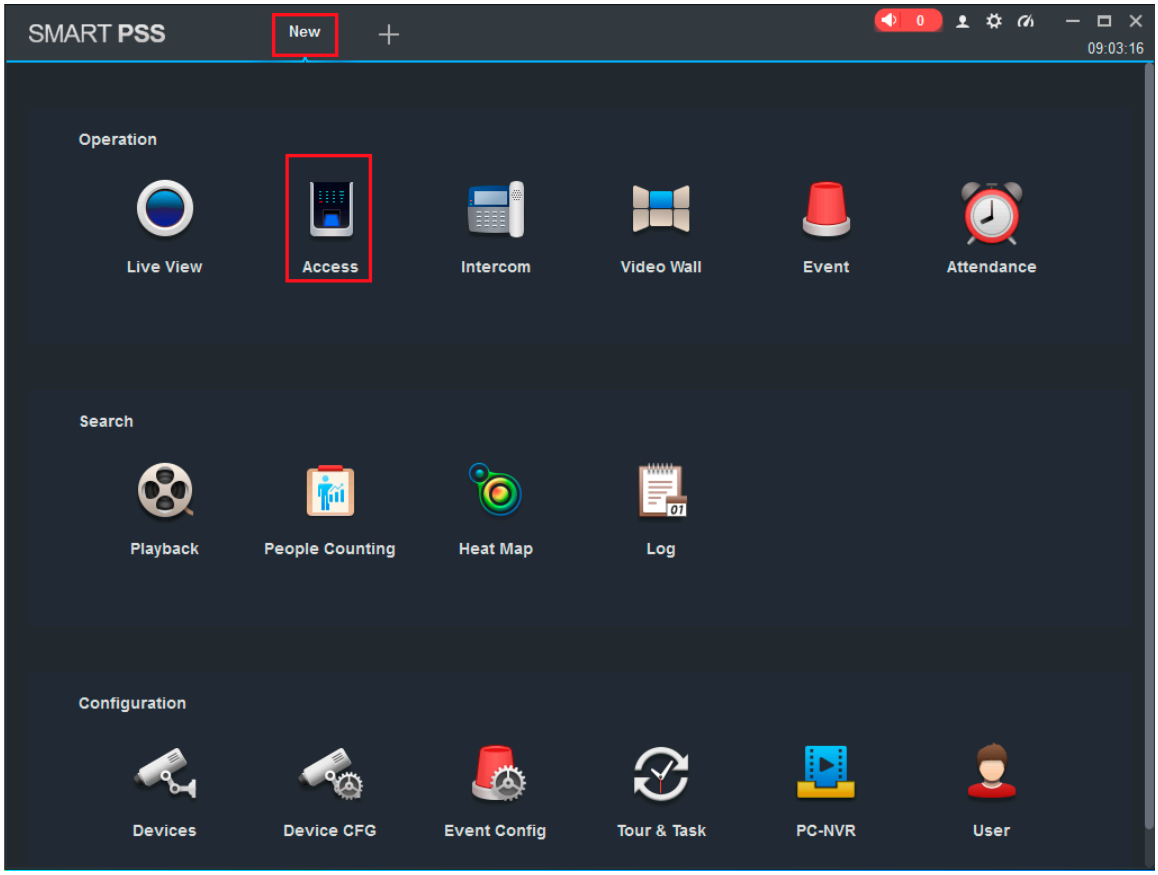
Obraz 3-7



3.3 DODAWANIE UŻYTKOWNIKA

Dodaj użytkowników i połącz z kartami, aby rozdzielić uprawnienia.
W interfejsie „Nowy” kliknij „Dostęp”, aby przejść do interfejsu „Dostęp” i tutaj zakończ konfigurację dostępu.

Obraz 3-8

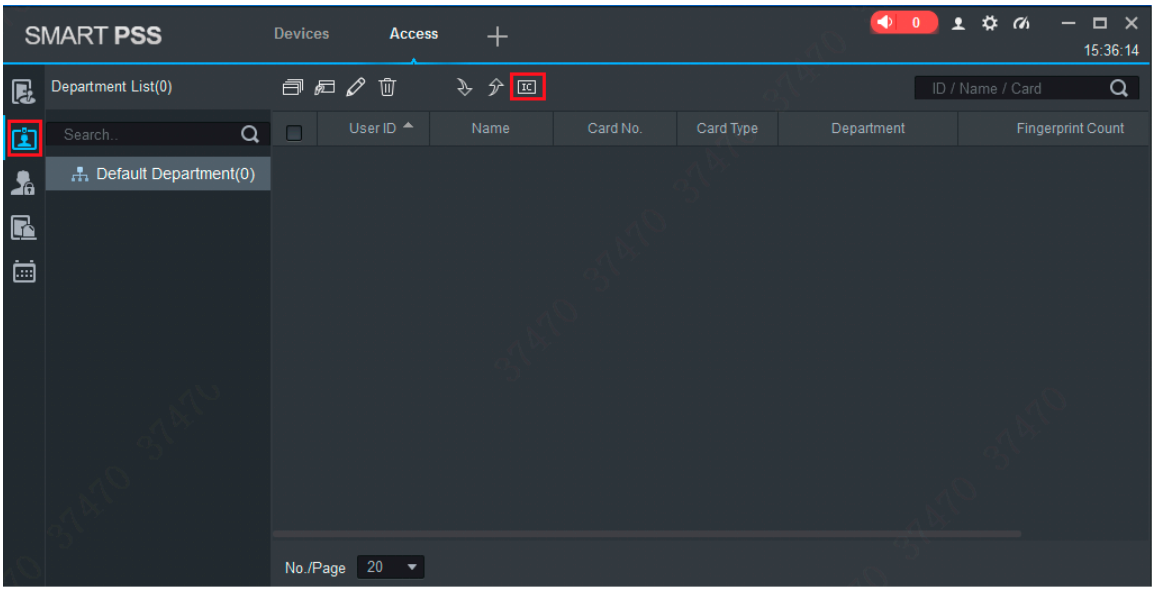


3.3.1 RODZAJ KARTY

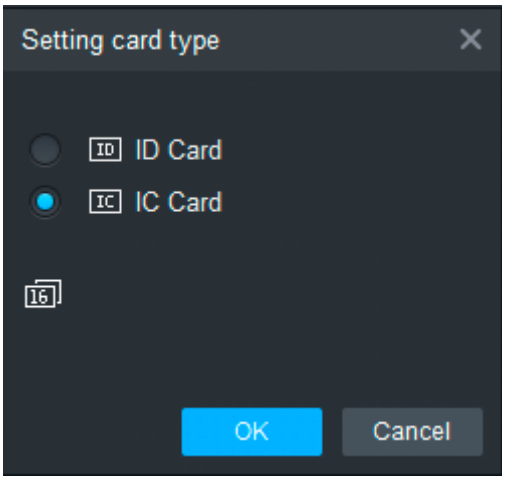
UWAGA!
Rodzaj karty jest taki sam jak w przypadku wystawcy karty, w przeciwnym razie nie odczyta numeru karty.

W interfejsie „Dostęp” kliknij  , a następnie kliknij  , aby ustawić typ karty, jak pokazano na Obrazie 3-9 i Obrazie 3-10.

Obraz 3-9



Obraz 3-10



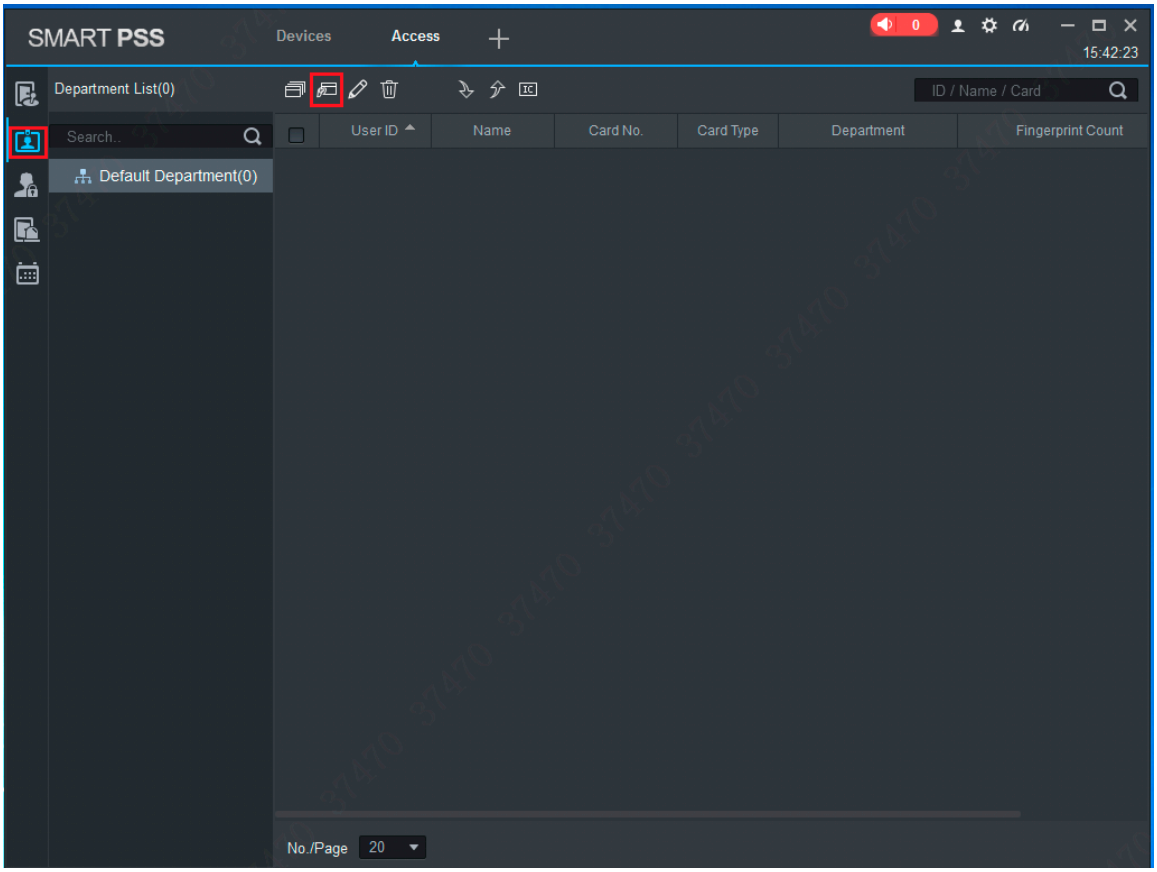
3.3.2 POJEDYNCZE DODANIE

Dodaj pojedynczego użytkownika, wprowadź kartę i informacje o użytkowniku.

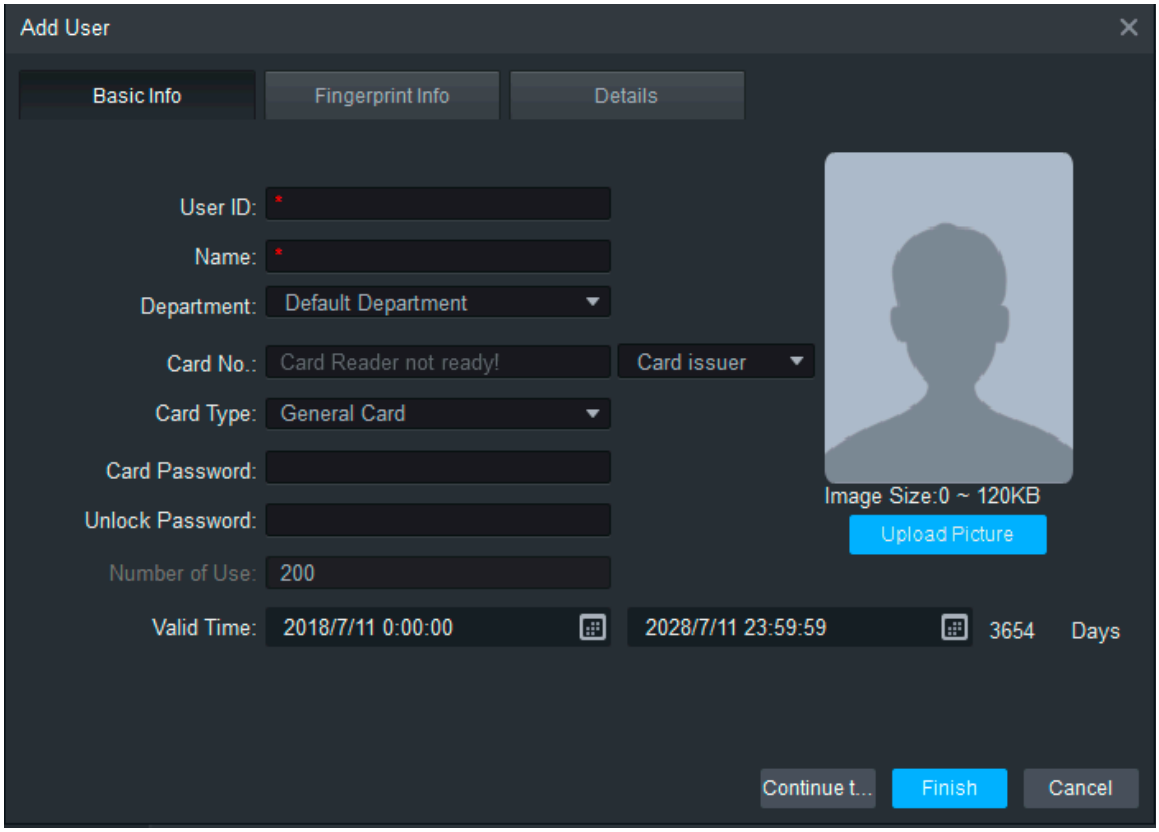
Krok 1 W interfejsie „Dostęp” kliknij , następnie kliknij , jak pokazano na Obrazie 3-11.

System wyświetli okno dialogowe „Dodaj użytkownika”, jak pokazano na Obrazie 3-12.

Obraz 3-11



Obraz 3-12



Krok 2 Dodaj informacje o użytkowniku ręcznie, w tym podstawowe informacje o odciskach palców i szczegóły. Szczegółowe informacje znajdują się w Tabeli 3-3.

Tabela 3-3

Parametr	Opis
Podstawowe informacje	ID użytkownika (obowiązkowy). • Imię i Nazwisko (obowiązkowy). • Dział (Automatyczne dopasowanie). • Numer karty: wprowadzany przez czytnik kart lub wprowadzany ręcznie. • Rodzaj karty: karta ogólna, karta VIP, karta gościa, karta patrol, karta z czarnej listy i karta przymusu. • Hasło karty: służy do otwierania drzwi za pomocą karta + hasło. • Odblokuj hasło: służy do otwierania drzwi za pomocą hasła. • Liczba użyć: dotyczy tylko karty gościa. • Ważny czas: ustaw czas trwania dostępu, który domyslnie wynosi 10 lat. • Zdjęcie: zdjęcie użytkownika, maksymalnie 120K. Numer karty i identyfikator użytkownika, nie może być powtórzony.
Informacja o odciskach palców	Zbieraj odciski palców za pomocą czytnika linii papilarnych i czytnika dostępu. • Maksymalnie 2 odciski palców na każdą osobę. • Pomoc przy wprowadzeniu nazwy odcisku palca.
Detale	Podaj szczegółowe informacje o użytkowniku zgodnie z parametrami interfejsu.

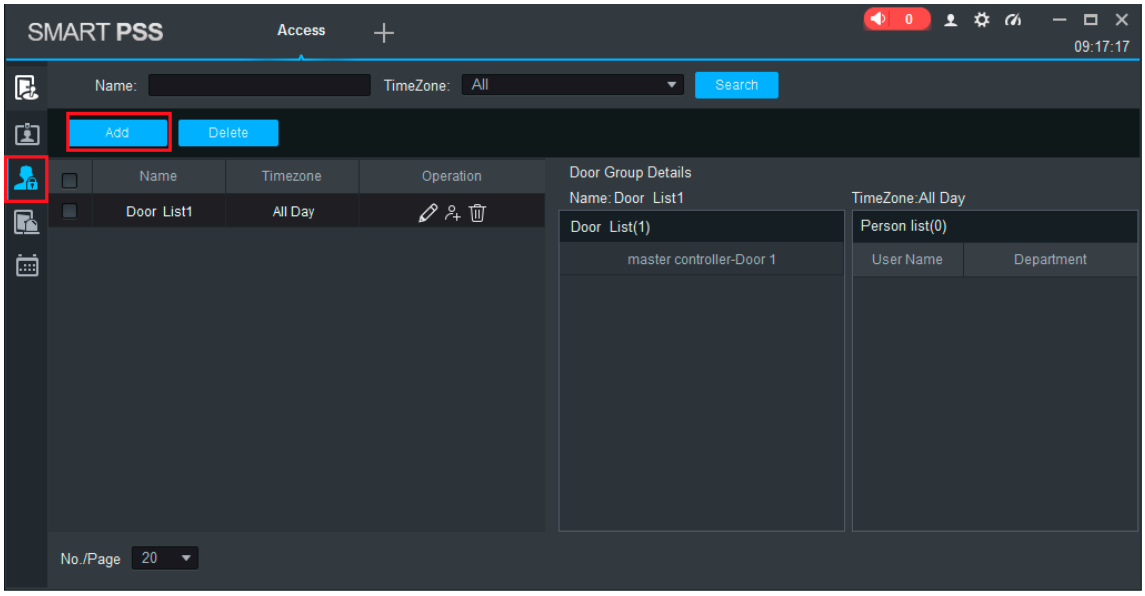
Krok 3 Kliknij „Zakończ”, aby zakończyć dodawanie użytkowników.

3.4 DODAWANIE GRUPY DRZWI

Podziel drzwi na grupy i zarządzaj nimi razem.

Krok 1 W interfejsie „Dostęp” kliknij , a następnie kliknij „Poziom dostępu”, jak pokazano na Obrazie 3-13.

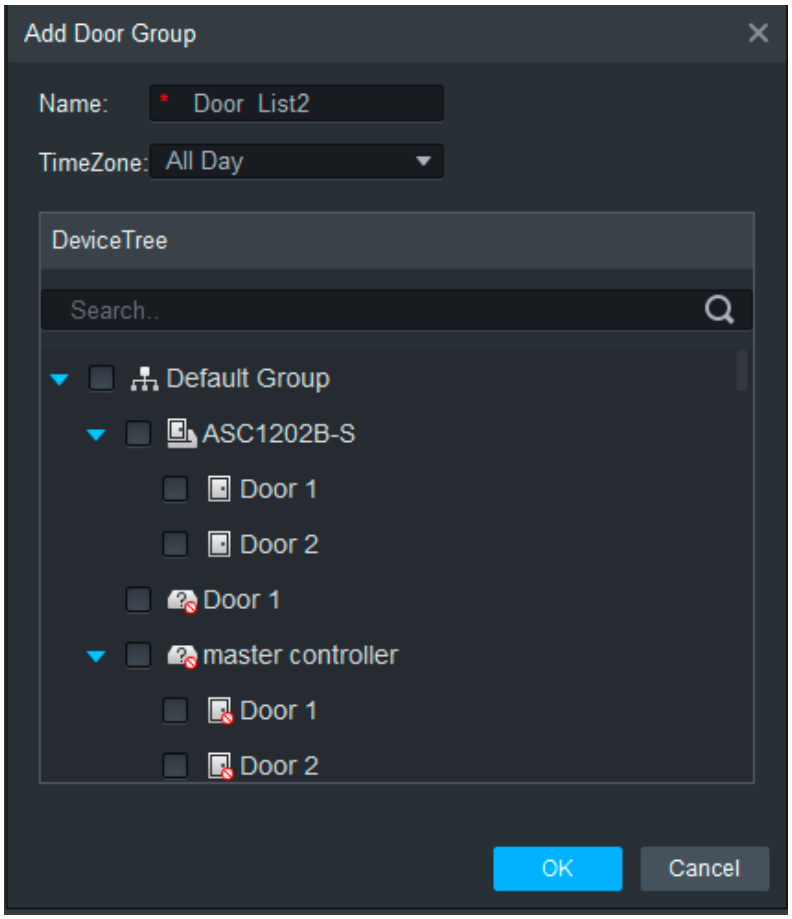
Obraz 3-13



Krok 2 Kliknij „Dodaj”.

System wyświetli okno dialogowe „Dodaj grupę drzwi”, jak pokazano na Obrazie 3-14.

Obraz 3-14



Krok 3 Wpisz „Nazwa”, wybierz „Strefa czasowa” i drzwi, którymi chcesz zarządzać.

Krok 4 Kliknij „OK.”, aby zakończyć dodawanie.

3.5 AUTORYZACJA

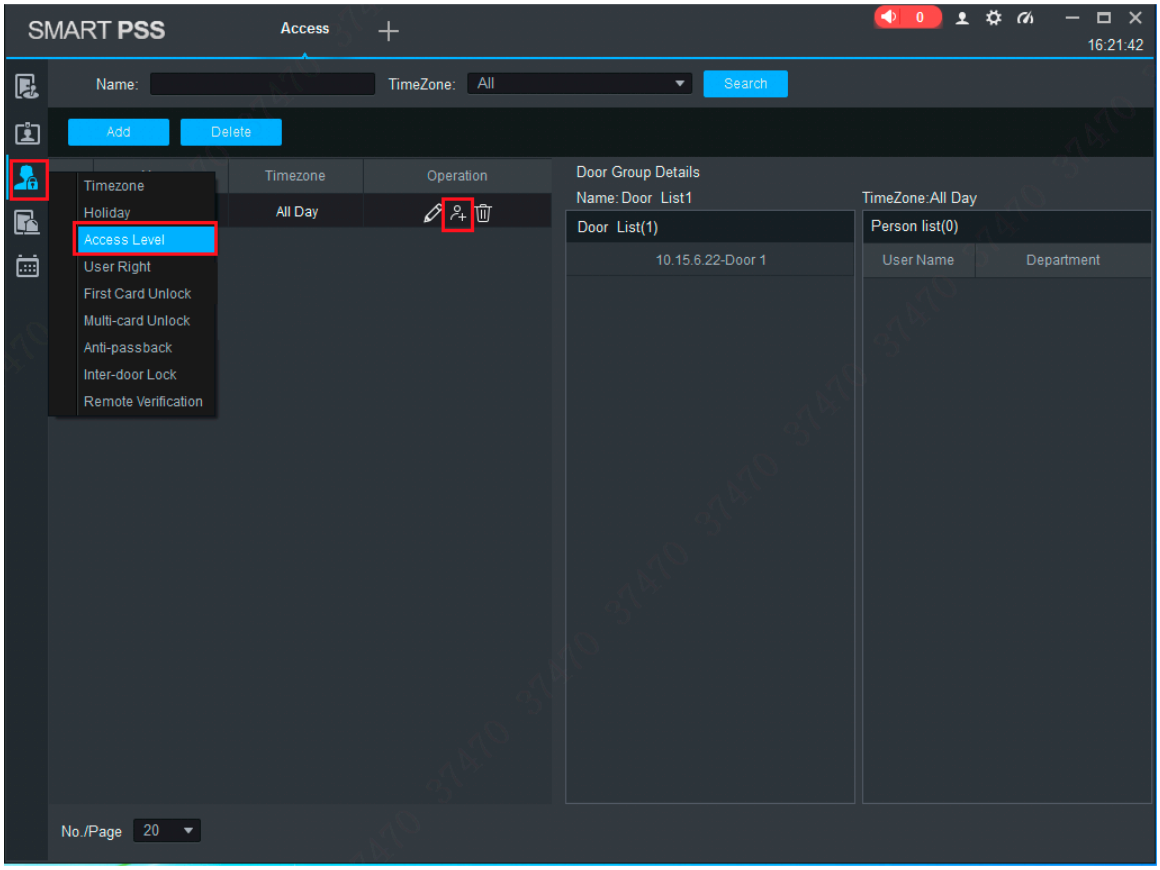
Przyznaj uprawnienia użytkownikom zgodnie z grupą drzwi i użytkownikiem.

3.5.1 AUTORYZACJA WEDŁUG GRUPY DRZWI

Wybierz grupę drzwi, dodaj odpowiednich użytkowników do grupy, aby wszyscy użytkownicy w grupie uzyskali uprawnienia do wszystkich drzwi w grupie.

Krok 1 W interfejsie „Dostęp” kliknij , a następnie kliknij „Poziom dostępu”, jak pokazano na rysunku Obrazie 3-15.

Obraz 3-15

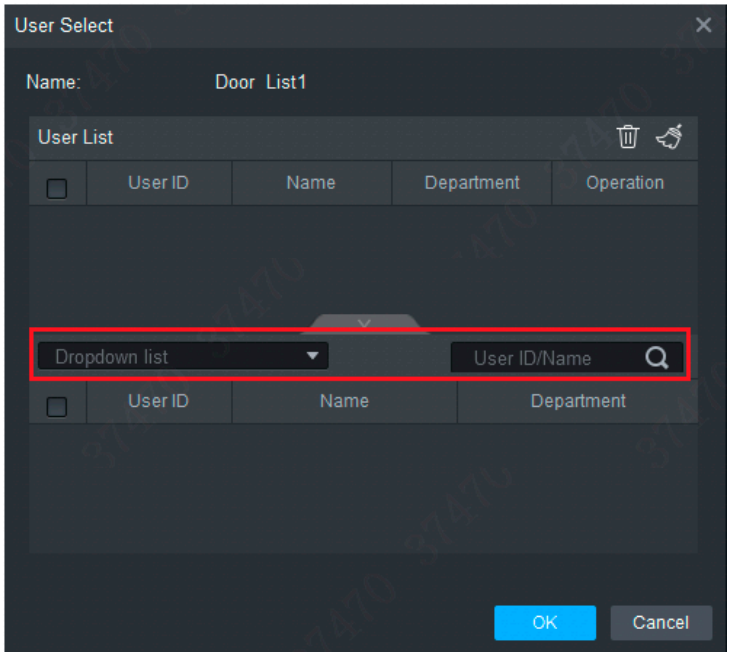


Krok 2 Kliknij .

System wyświetli okno dialogowe „Wybór użytkownika”.

Krok 3 Wybierz dział użytkownika z rozwijanej listy lub wprowadź bezpośrednio identyfikator lub nazwę użytkownika, jak pokazano na Obrazie 3-16.

Obraz 3-16



Krok 4 Z listy wyszukiwania wybierz użytkownika i dodaj do listy użytkowników.

Krok 5 Kliknij: OK.", aby zakończyć autoryzację.

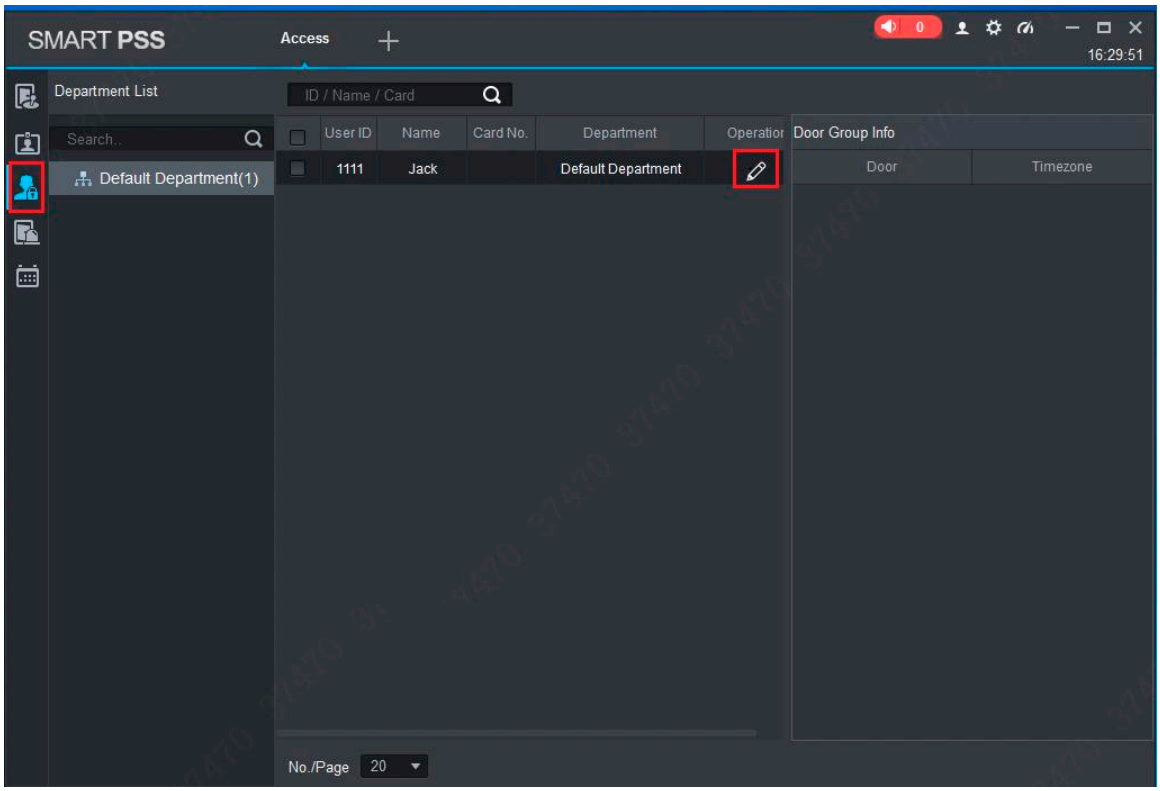
- Lista wyszukiwania filtruje informacje o użytkowniku bez numeru karty.
- Na liście użytkowników anuluj dodanego użytkownika i usuń jego uprawnienia.

3.5.2 AUTORYZACJA WEDŁUG UŻYTKOWNIKA

Wybierz użytkownika, rozdziel grupę drzwi i nadaj użytkownikowi uprawnienia grupy drzwi.

Krok 1 W interfejsie „Dostęp" kliknij  , a następnie kliknij „Prawa użytkownika", jak pokazano na Obrazie 3-17.

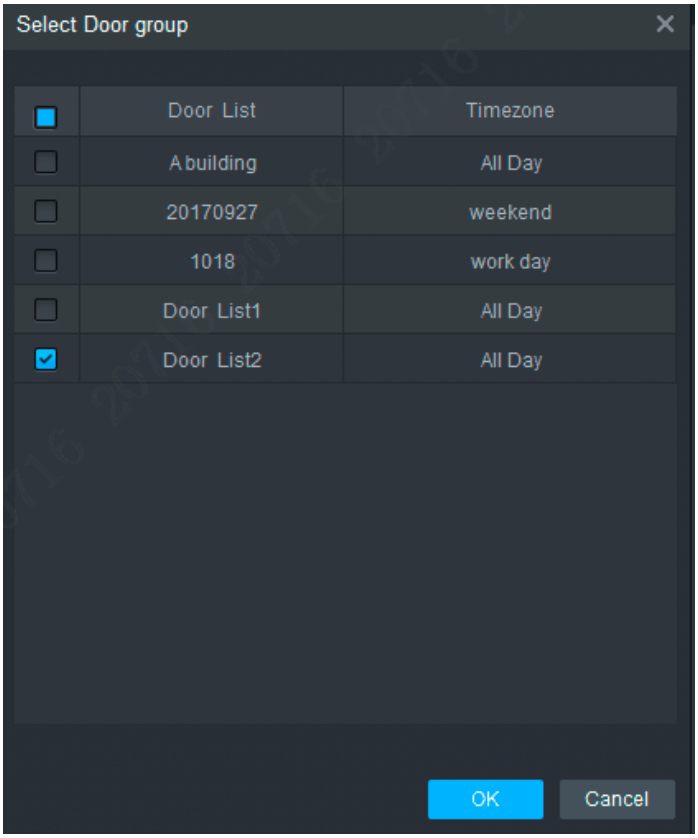
Obraz 3-17



Krok 2 Kliknij  .

System wyświetli okno dialogowe „Wybierz grupę drzwi”, jak pokazano na Obrazie 3-18.

Obraz 3-18



Krok 3 Wybierz grupę drzwi i kliknij „OK.”, aby zakończyć autoryzację.

4. FAQ

W przypadku problemów nieuwzględnionych w dalszej części należy skontaktować się z lokalnym personelem obsługi klienta lub z personelem obsługi klienta z centrali. Będziemy zawsze do Twojej dyspozycji.

1. Pytanie: Po włączeniu zasilania wskaźnik zasilania nie włącza się lub brzęczyk nie reaguje.

Odpowiedź: Sprawdź czy wtyczka jest włożona właściwie. Wyciągnij ją i włóż ponownie.

2. Pytanie: Po użyciu czytnika z urządzeniem lampka przesuwania karty nie świeci się i nie reaguje po przeciągnięciu karty.

Odpowiedź: Sprawdź czy złącze czytnika jest włożone we właściwe miejsce. Proszę wyciągnąć i włożyć ponownie, sprawdź czy lampka kontaktu czytnika świeci.

3. Pytanie: Oprogramowanie nie wykrywa urządzenia.

Odpowiedź: Sprawdź czy okablowanie jest prawidłowo podłączone i czy IP urządzenia znajduje się w tym samym segmencie sieci.

4. Pytanie: Po wyświetleniu karty wyświetla się komunikat, że karta jest nieprawidłowa.

Odpowiedź: Sprawdź czy ten numer karty został dodany do kontrolera.

5. Pytanie: Domyślny adres IP kontrolera dostępu.

Odpowiedź: Domyślny adres IP to 192.168.0.2.

6. Pytanie: Domyślny port, nazwa użytkownika i hasło kontrolera dostępu.

Odpowiedź: Domyślny port to 37777, początkowa nazwa użytkownika to admin, a hasło to 123456.

7. Pytanie: Aktualizacja online urządzenia.

Odpowiedź: Połącz urządzenie i komputer przez sieć i zaktualizuj ją na platformie.

8. Pytanie: Maksymalna odległość okablowania i odległość transmisji czytnika, kart i kontrolera.

Odpowiedź: Zależy to od rodzaju kabla sieciowego i tego, czy wymaga on zasilania przekaźnika sterującego.

Podłączona kablem sieciowym CAT5E, typowa wartość to:

- RS485, 100 m.
- Wiegand, 100 m.

DODATEK 1 ZALECENIA DOTYCZĄCE CYBERBEZPIECZEŃSTWA

Cyberbezpieczeństwo to coś więcej niż tylko modne hasło: to coś co dotyczy każdego urządzenia podłączonego do Internetu. Nadzór wideo nie jest odporny na zagrożenia cybernetyczne, ale podjęcie podstawowych kroków w celu ochrony i wzmocnienia sieci i urządzeń sieciowych sprawi, że będą mniej podatne na ataki. Poniżej znajduje się kilka wskazówek i zaleceń od BCS, jak stworzyć bardziej bezpieczny system.

Obowiązkowe działania, które należy podjąć w celu zapewnienia bezpieczeństwa podstawowego sprzętu sieciowego:

1. Używaj silnych haseł

Zapoznaj się z następującymi sugestiami dotyczących ustawienia hasła:

- Długość nie powinna być mniejsza niż 8 znaków;
- Uwzględnij co najmniej dwa rodzaje znaków, które obejmują wielkie i małe litery, cyfry i symbole;
- Nie zawierają nazwy konta ani nazwy konta w odwrotnej kolejności;
- Nie używaj ciągłych znaków, takich jak 123, abc itp.;
- Nie używaj nakładających się znaków, takich jak 111, aaa itp.;

2. Zaktualizuj firmware i oprogramowanie klienckie na czas

- Zgodnie ze standardową procedurą w branży technicznej zalecamy aktualizację oprogramowania sprzętowego (takiego jak NVR, DVR, kamera IP itp.), aby upewnić się, że system jest wyposażony w najnowsze poprawki bezpieczeństwa. Gdy urządzenie jest podłączone do sieci publicznej, zaleca się włączenie funkcji „automatycznego sprawdzania aktualizacji", aby uzyskać aktualne informacje o aktualizacjach firmware wydanych przez producenta.
- Zalecamy pobranie najnowszej wersji oprogramowania klienckiego i korzystanie z niej.

Zalecenia, które warto stosować, aby poprawić bezpieczeństwo sieciowe sprzętu:

1. Fizyczna ochrona

Zalecamy fizyczną ochronę sprzętu, zwłaszcza urządzeń pamięci masowej. Na przykład umieść sprzęt w specjalnym pomieszczeniu komputerowym i szafie oraz zaimplementuj dobrze wykonane pozwolenie kontroli dostępu i zarządzanie kluczami, aby uniemożliwić nieupoważnionemu personelowi nawiązania kontaktów fizycznych, takich jak uszkodzenie sprzętu, nieautoryzowane podłączenie urządzeń wymiennych (takich jak dysk flash USB, port szeregowy) itp.

2. Regularnie zmieniaj hasło

Zalecamy regularną zmianę haseł, aby zmniejszyć ryzyko złamania hasła.

3. Ustaw i aktualizuj hasła, resetuj informacje na czas

Urządzenie obsługuje funkcję resetowania hasła. Skonfiguruj powiązane informacje na czas resetowania hasła, w tym skrzynkę pocztową użytkownika i pytania dotyczące ochrony hasłem. Jeśli informacje ulegną zmianie, proszę zmodyfikować je na czas.
Podczas ustawiania pytań dotyczących ochrony hasłem zaleca się, aby nie używać tych, które można łatwo odgadnąć.

4. Włącz blokadę konta

Funkcja blokady konta jest domyślnie włączona i zalecamy, żeby była włączona, aby zagwarantować bezpieczeństwo konta. Jeśli atakujący spróbuje kilka razy zalogować się przy użyciu niewłaściwego hasła, odpowiednie konto i źródłowy adres IP zostaną zablokowane.

5. Zmień domyślne porty HTTP I inne porty usług

Sugerujemy, aby zmienić domyślne porty HTTP I inne porty usług na dowolny zestaw liczb od 1024~65535, co zmniejsza ryzyko, że osoby postronne będą w stanie odgadnąć, których portów używasz.

6. Włącz HTTPS

Zalecamy włączenie HTTPS, abyś mógł odwiedzić serwis internetowy za pośrednictwem bezpiecznego kanału komunikacji.

7. Włącz Białą listę

Zalecamy włączenie funkcji białej listy, aby uniemożliwić wszystkim, z wyjątkiem tych o określonych adresach IP, dostęp do systemu. Dlatego pamiętaj, aby dodać adres IP komputera I adres IP urządzenia towarzyszącego do białej listy.

8. Wiązanie adresu MAC

Zalecamy powiązanie adresu IP i MAC sprzętu, co zmniejsza ryzyko fałszowania ARP.

9. Rozsądnie przypisz konta i uprawnienia

Zgodnie z wymogami biznesowymi i zarządczymi racjonalnie dodaj użytkowników i przypisz im minimalny zestaw uprawnień.

10. Wyłącz niepotrzebne usługi i wybierz Bezpieczne tryby

W razie potrzeby zaleca się wyłączenie niektórych usług, takich jak SNMP, SMTP, UPnP itp., aby zmniejszyć ryzyko.
W razie potrzeby zdecydowanie zaleca się korzystanie z trybów awaryjnych, w tym między innymi następujących usług:

- SNMP: Wybierz SNMP v3 i skonfiguruj silne hasła szyfrowania i hasła uwierzytelniania.
- SMTP: Wybierz TLS, aby uzyskać dostęp do serwera skrzynki pocztowej.
- FTP: Wybierz SFTP i skonfiguruj silne hasła.
- AP: Wybierz tryb szyfrowania WPA2-PSK i skonfiguruj silne hasła.

11. Szyfrowana transmisja audio I wideo

Jeśli zawartość danych audio i wideo jest bardzo ważna lub wrażliwa, zalecamy użycie funkcji szyfrowanej transmisji, aby zmniejszyć ryzyko kradzieży danych podczas transmisji.
Przypomnienie: szyfrowana transmisja spowoduje pewną utratę wydajności transmisji.

12. Bezpieczna kontrola

- Sprawdź użytkowników online: zalecamy regularne sprawdzanie użytkowników online, aby sprawdzić czy urządzenie jest zalogowane bez autoryzacji.
- Sprawdź dziennik urządzenia: przeglądając dzienniki, możesz poznać adresy IP, które zostały użyte do zalogowania się na twoich urządzeniach i ich kluczowe operacje.

13. Dziennik sieci

Ze względu na ograniczoną pojemność urządzenia, przechowywany dziennik jest ograniczony. Jeśli konieczne jest zapisywanie dziennika przez długi czas, zaleca się włączenie funkcji dziennika sieci, aby zapewnić synchronizację dzienników krytycznych z serwerem dziennika sieci w celu śledzenia.

14. Zbuduj bezpieczne środowisko sieciowe

Aby lepiej zapewnić bezpieczeństwo sprzętu i zmniejszyć potencjalne ryzyko cybernetyczne, zalecamy:

- Wyłączyć funkcję mapowania portów routera, aby uniknąć bezpośredniego dostępu do urządzeń intranetowych z sieci zewnętrznej.
- Sieć powinna być podzielona na części i odizolowana zgodnie z rzeczywistymi potrzebami sieci. Jeśli nie ma żadnych wymagań komunikacyjnych między dwiema podsieciami, sugeruje użycie VLAN, GAP sieci i innych technologii do podziału sieci, aby uzyskać efekt izolacji sieci.
- Ustanowienie systemu uwierzytelniania dostępu 802.1x, aby zmniejszyć ryzyko nieautoryzowanego dostępu do sieci prywatnych.

NSS Sp. z o.o.
ul. Modularna 11 (hala IV)
02-238 Warszawa

Aktualizacja: 08.04.2022