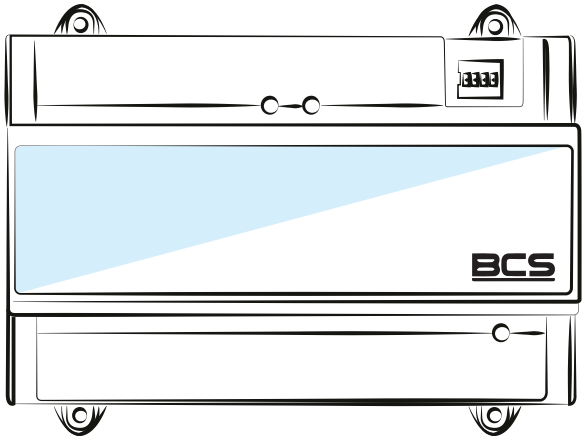
SK

BCS-KKD-J222

Dvojdverový jednosmerný prístupový ovládač

Používateľská príručka



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

Aktualizácia: 08.04.2022

ÚVOD

VŠEOBECNÉ:

Príručka popisuje konštrukciu, inštaláciu a kabeláž dvojdverového jednosmerného prístupového ovládača.

BEZPEČNOSTNÉ POKYNY:

príručke sa môžu objaviť nasledujúce signálne slová s definovaným významom.

Značky	Význam
DANGER!	Označuje vysoké potenciálne nebezpečenstvo, ktoré, ak sa mu nezabráni, bude mať za následok smrť alebo vážne zranenie
WARNING!	Označuje stredné alebo nízke potenciálne nebezpečenstvo, ktoré môže spôsobiť ľahké alebo stredne ťažké zranenie
CAUTION!	Označuje potenciálne riziko, ktoré môže viesť k poškodeniu majetku, strate údajov, spomaleniu výkonu alebo nepredvídateľnému výsledku
TIPS	Poskytuje rady, ktoré vám pomôžu vyriešiť problém alebo ušetriť čas
NOTE	Poskytuje dodatočné informácie na doplnenie textu

OZNÁMENIE O OCHRANE OSOBNÝCH ÚDAJOV:

Ako používateľ zariadenia alebo správca údajov môžete zhromažďovať osobné údaje iných ľudí, ako je tvár, odtlačky prstov, registračné číslo auta, e-mailová adresa, telefónne číslo, GPS atď. Musíte dodržiavať miestne zákony a nariadenia o ochrane súkromia, aby ste chránili práva a záujmy iných prostredníctvom vykonávania opatrení, ktoré zahŕňajú, ale nie sú obmedzené na: informovanie dotknutej osoby o existencii oblasti dohľadu a zabezpečenie kontaktu.

O PRÍRUČKE

- Príručka slúži len ako referencia. Ak existujú rozdiely medzi skutočným produktom a návodom, skutočný produkt má prednosť.
- Nezodpovedáme za žiadne straty spôsobené konaním, ktoré nie je v súlade s pokynmi.
- Príručka bude aktualizovaná podľa najnovších pravidiel a nariadení. Podrobnosti nájdete v papierovej používateľskej príručke, na disku CD-ROM, v kóde QR alebo na našej oficiálnej webovej stránke. V prípade rozporu medzi papierovou Používateľskou príručkou a elektronickou verziou má prednosť elektronická verzia.
- Všetok dizajn a softvér sa môže zmeniť bez predchádzajúceho písomného upozornenia. Aktualizácie produktu môžu spôsobiť určité rozdiely medzi skutočným produktom a manuálom. Ak chcete získať najnovší softvér a dodatočnú dokumentáciu, kontaktujte zákaznícky servis.
- Môžu sa vyskytnúť odchýlky v technických údajoch, popisoch funkcií a operácií alebo chyby tlače. Ak máte pochybnosti, pozrite si naše vysvetlenie.
- Ak nemôžete otvoriť Používateľskú príručku PDF, aktualizujte si softvér na čítanie súborov PDF alebo vyskúšajte iný softvér.
- Všetky ochranné známky, registrované ochranné známky a názvy spoločností v príručke sú majetkom príslušných vlastníkov.
- Ak sa pri používaní zariadenia vyskytne nejaký problém, navštívte našu webovú stránku, kontaktujte dodávateľa alebo zákaznícky servis.
- Ak máte pochybnosti, pozrite si naše vysvetlenie.

DÔLEŽITÉ BEZPEČNOSTNÉ OPATRENIA A UPOZORNENIA:

Nasledujúci popis je správny spôsob používania zariadenia. Pred použitím si pozorne prečítajte príručku, aby ste sa vyhli nebezpečenstvu a škode na majetku. Pri používaní zariadenia a po jej prečítaní prísne dodržiavajte pokyny.

PREVÁDZKOVÉ POŽIADAVKY

- Neumiestňujte a neinštalujte zariadenie na miesto vystavené priamemu slnečnému žiareniu alebo v blízkosti zariadenia, ktoré vytvára teplo.
- Zariadenie neinštalujte na vlhké, prašné alebo teplé miesto.
- Zariadenie nainštalujte vodorovne alebo na stabilné miesto a zaistite ho proti pádu.
- Na zariadenie nestriekajte tekutiny, neklaďte naň nič naplnené tekutinou, aby sa tekutiny nedostali do zariadenia.
- Zariadenie nainštalujte na dobre vetranom mieste. Neblokujte vetrací otvor.
- Zariadenie používajte iba v rámci menovitého výkonu a vstupného rozsahu.
- Zariadenie svojpomocne nerozoberajte.
- Zariadenie prepravujte, používajte a skladujte v rámci prípustného rozsahu vlhkosti a teploty.

POŽIADAVKY NA NAPÁJANIE

- Batériu používajte zhodne s požiadavkami , inak môže dôjsť k požiaru, výbuchu alebo popáleniu batériou.!
- Na výmenu batérie používajte iba rovnaký typ batérie!
- Používajte elektrické káble (napájacie káble) odporúčané pre tento druh produktu, používajte ich v súlade s menovitými špecifikáciami!
- Použite štandardný napájací adaptér, ktorý zodpovedá vášmu zariadeniu. Inak hrozí ohrozenie zdravia personálu alebo poškodenie zariadenia.
- Použite napájací adaptér, ktorý spĺňa požiadavky SELV (Safe Extra Low Voltage) a napájacie napätie, ktoré je v súlade s obmedzeným zdrojom napájania v IEC60950-1. Špecifické požiadavky na napájanie nájdete na štítkoch zariadenia.
- Výrobky kategórie I musia byť pripojené k sieťovej zásuvke vybavenej ochranným uzemňovacím systémom.
- Spojka zariadenia pre odpojenie zariadenia, musí zostať prístupné pre ľahkú manipuláciu.

OBSAH

1. OPIS

Dvojdverový jednosmerný prístupový ovládač je ovládacie zariadenie, ktoré môže nahradiť video interkom. Má elegantný a moderný dizajn so skvelou funkčnosťou, je vhodný do komerčných budov, firemných nehnuteľností a podobne.

1.1 VLASTNOSTI ZARIADENIA

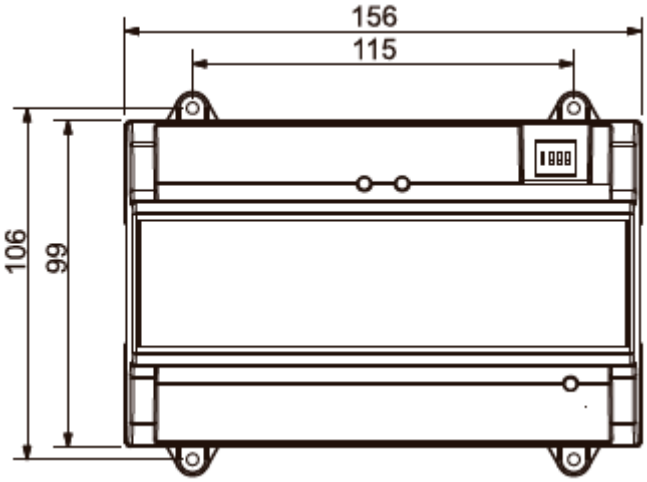
Jeho bohaté funkcie sú nasledovné:

- Použitie posuvnej koľajnice a konštrukcie ovládanej zámkom, pohodlná inštalácia a údržba.
- Integrovaný alarm, kontrola prístupu, video dohľad a požiarny alarm.
- Podpora 2 čítačiek kariet.
- Podpora 6 skupín vstupných signálov (2 výstupné tlačidlá, 2 dverové kontakty a 2 alarmy pri vniknutí.
- Podporuje 4 skupín ovládacích výstupov (2 elektrické zámky a 2 alarmové výstupy).
- S portom RS485, môže byť rozšírený o riadiaci modul.
- Kapacita pamäte FLASH je 16M (môže dosiahnuť až 32M). Podpora až 100 000 kariet a 150 000 záznamov.
- Podporuje alarm proti nelegálnemu vniknutiu, odblokovanie alarmu s časovým limitom, nastavenie nátlakovej karty a nátlakového kódu. Podporuje tiež konfigurácie čiernej a bielej listiny a karty hliadok
- Podpora nastavenia správneho časového obdobia, hesla a dátumu vypršania platnosti karty. V prípade karty hosťa je možné nastaviť dĺžku jej používania.
- Podpora 128 skupín harmonogramov a 128 skupín harmonogramov sviatkov.
- Trvalé ukladanie dát pri poruche, vstavané RTC (podpora DST), online aktualizácia.

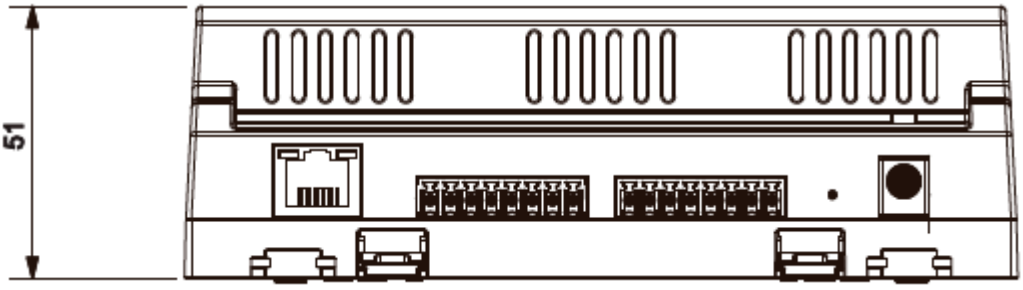
1.2 ROZMERY A VZHĽAD

Jeho vzhľad a rozmery sú znázornené na obrázku 1-1 a obrázku 1-2. Jednotkou dĺžky sú milimetre.

Obrázok 1-1



Obrázok 1-2

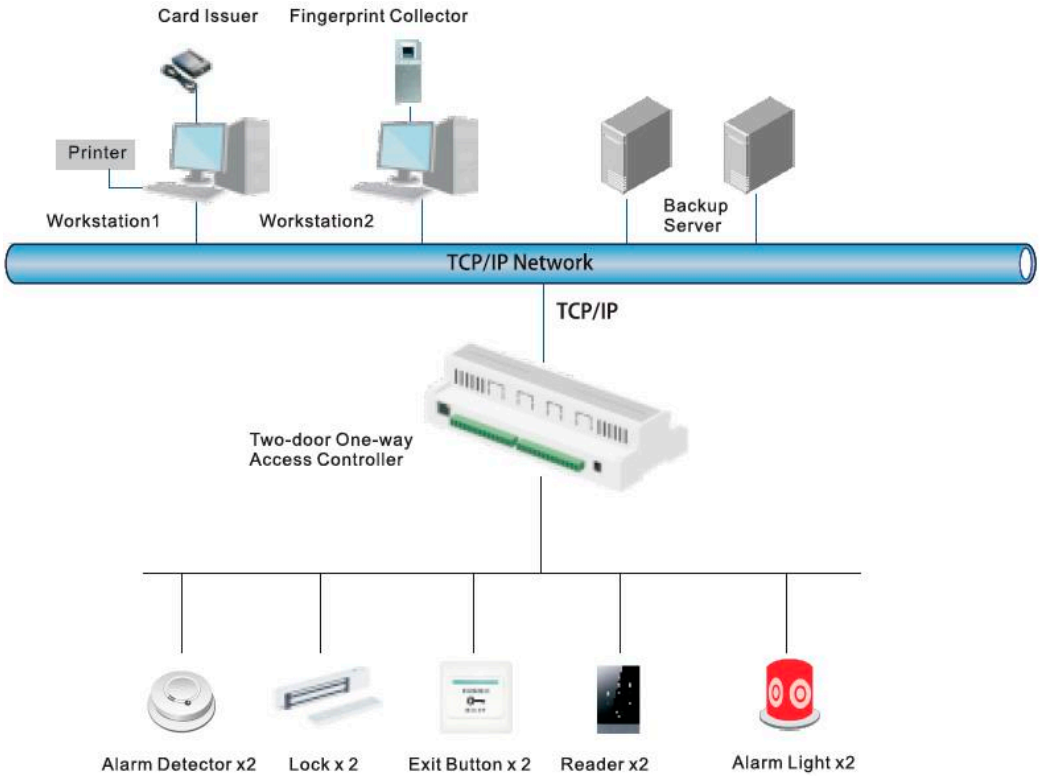


2. NÁVOD NA INŠTALÁCIU

2.1 ŠTRUKTÚRA SYSTÉMU

Systémová štruktúra dvojdverového jednosmerného prístupového ovládača, dverového zámku a čítačky je znázornená na Obrázku 2-1.

Obrázok 2-1



2.2 INŠTALÁCIA ZARIADENIA

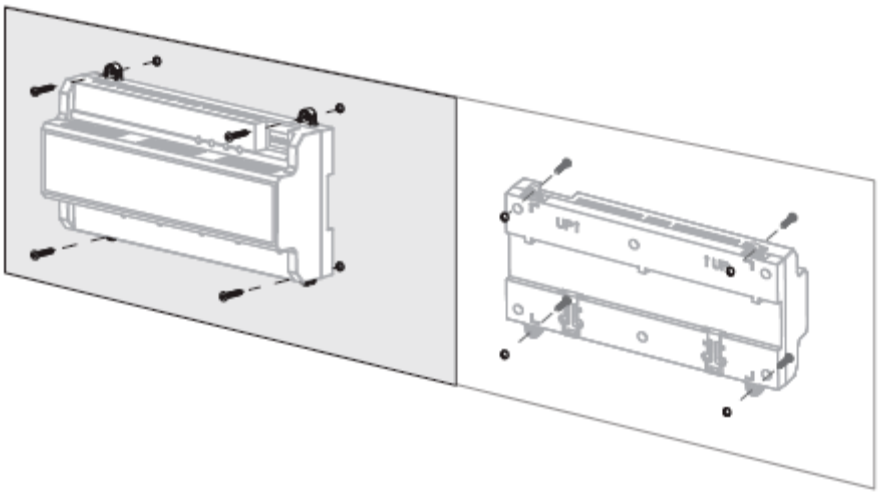
Existujú dva spôsoby inštalácie.

- 1. spôsob: Pripevnite celé zariadenie jednotku k stene pomocou skrutiek.
- 2. spôsob: Pomocou U-lišty zaveste celé zariadenie na stenu (2. spôsob je voliteľná montáž).

1. SPÔSOB

Schéma inštalácie je znázornená na Obrázku 2-2.

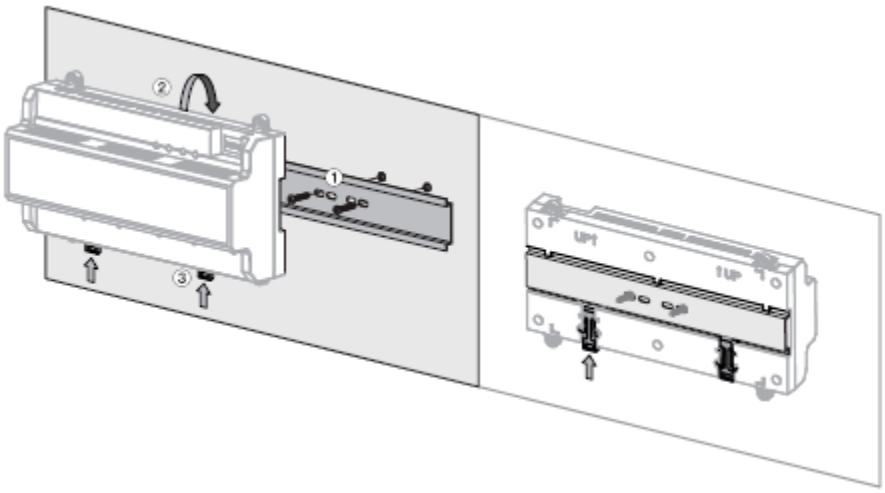
Obrázok 2-2



2. SPÔSOB

Schéma inštalácie je znázornená na Obrázku 2-3.

Obrázok 2-3

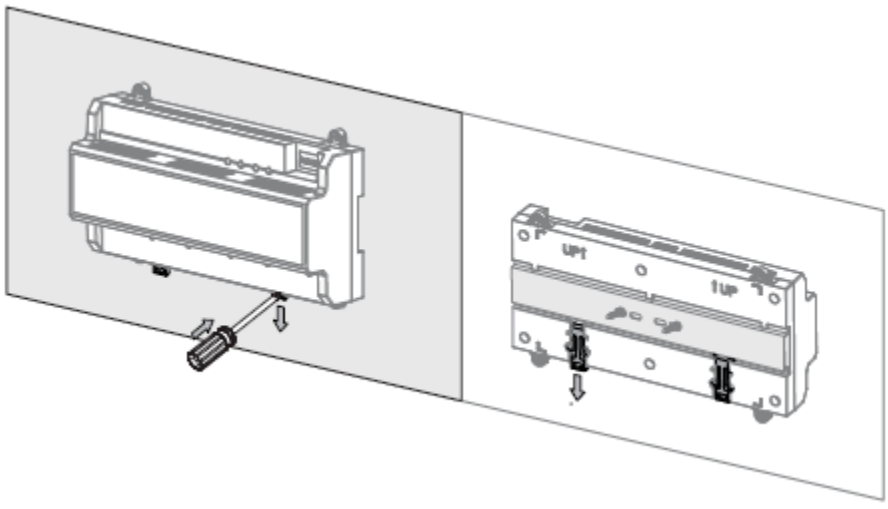


1. krok: Pripevnite U-lištu k stene pomocou skrutiek.
2. krok: Pripevnite hornú zadnú časť zariadenia k hornej časti U-lišty.
3. krok: Stlačte západkový konektor na spodnej strane zariadenia smerom nahor. Inštalácia je dokončená, keď budete počuť zvuk zapadnutia.

2.3 DEMONTÁŽ

Ak je zariadenie inštalované 2. spôsobom, demontujte ho podľa obrázku 2-4. Vložte skrutkovač so západkové konektora, zatlačte ho nadol a západkový konektor sa vysunie, aby bolo možné celé zariadenie hladko rozobrať.

Obrázok 2-4

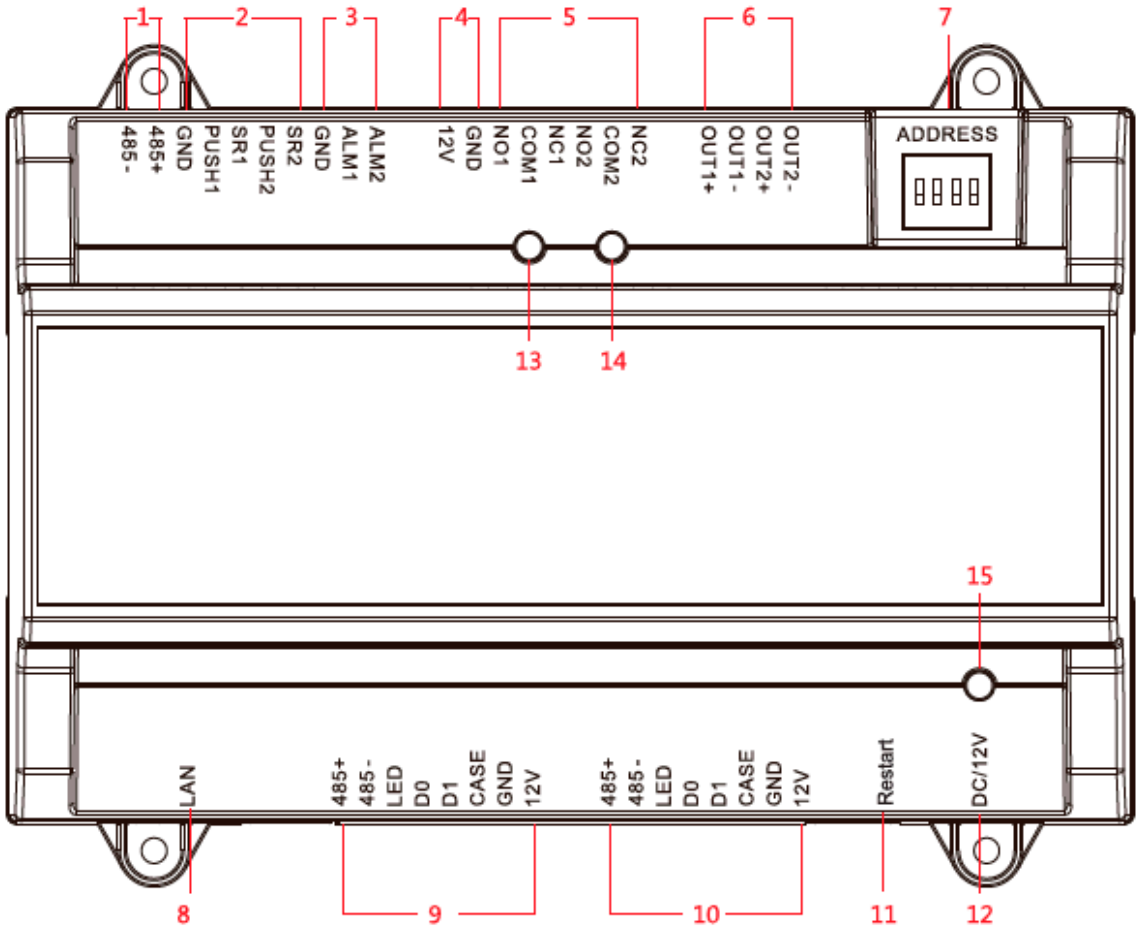


2.4 SCHÉMA ZAPOJENIA

2.4.1 POPIS ZAPOJENIA PRÍSTUPOVÉHO OVLÁDAČA

Toto zariadenie podporuje dvojdverový jednojsmerný vstup alebo výstup. Pre alarmový vstup aktivujte externé výstupné zariadenie, aby sa alarm zapol. Schéma zapojenia zariadenia je znázornená na Obrázku 2-5.

Obrázok 2-5



Rozhrania sú popísané v Tabuľke2-1.

Tabuľka 2-1

Číslo	Opis portu	Číslo	Opis portu
1	Výstupné tlačidlo a dverový kontakt	7	Przełącznik DIP
2	Externý alarmový vstup	8	TCP/IP
3	External alarm input	9	Čítačka dverí 1
4	Výstupný výkon zámku	10	Čítačka dverí 2
5	Výstup ovládania zámku	11	Reštart
6	Výstup alarmu	12	DC 12V

Ovládacie prvky sú popísané v Tabuľke 2-2.

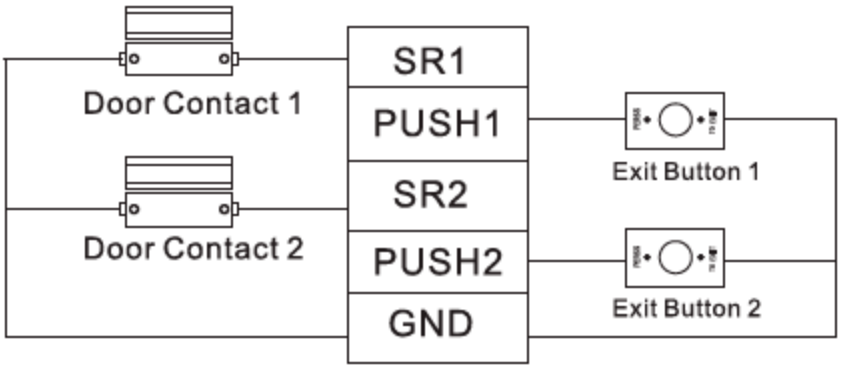
Tabuľka 2-2

Číslo	Opis portu
13	Stav indikátora zámku dverí
14	
15	LED indikátor napájania

2.4.2 POŽIADAVKA NA VÝSTUP / POPIS ZAPOJENIA DVERNÉHO KONTAKTU

Správne zapojenie výstupného tlačidla a dverného kontaktu je znázornené na obrázku 2-6. Popis káblového pripojenia nájdete v Tabuľke 2-3.

Obrázok 2-6



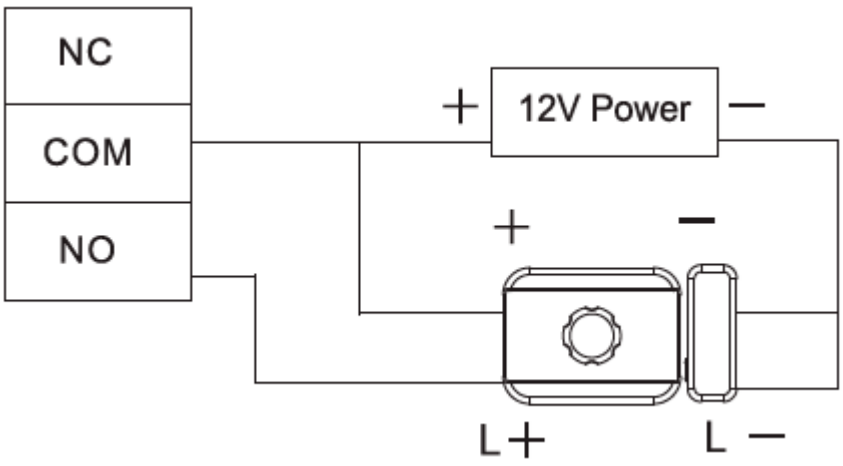
Tabuľka 2-3

Port	Odkaz na kabeláž	Opis
Výstupné tlačidlo a kontakt dverí	SR1	Vstupný kontakt dverí 1
	PUSH1	Tlačidlo východu z dverí 1
	SR2	Vstupný kontakt dverí 2
	PUSH2	Tlačidlo východu z dverí 2
	GND	Zdieľané výstupným tlačidlom, vstuponý kontakt dverí I RS485

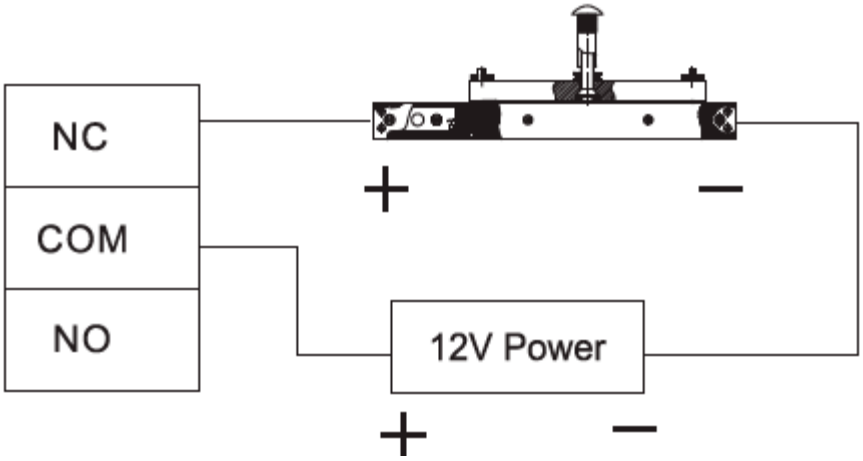
2.4.3 OPIS ELEKTROINŠTALÁCIE ZÁMKU

Podpora pre 2 skupiny výstupov ovládania zámku, sériové čísla po spojení znamenajú zodpovedajúce dvere. Vyberte vhodný režim pripojenia podľa typu zámku, ako je znázornené na Obrázku 2-7, Obrázku 2-8 a Obrázku 2-9. Popis pripojení vodičov nájdete v Tabuľke 2-4.

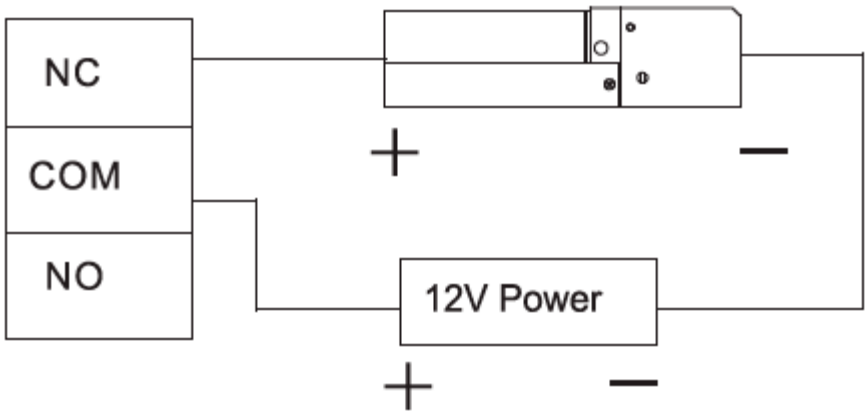
Obrázok 2-7



Obrázok 2-8



Obrázok 2-9



Tabuľka 2-4

Port	Odkaz na kabeláž	Opis
Výstupný ovládací port zámku	NC1	Kontrola zámku dverí 1
	COM1	
	NO1	
	NC2	Kontrola zámku dverí 2
	COM2	
	NO2	

2.4.4 POPIS ZAPOJENIA ČÍTAČKY

Jedny dvere podporujú iba jeden typ čítačky - RS485 alebo Wiegand.

Pozrite si Tabuľku 2-5, kde nájdete popis zapojenia káblov čítačky. Vezmite si ako príklad dvere 1, ostatné čítačky sú rovnaké. Špecifikácie a dĺžky káblov čítačky nájdete v Tabuľke 2-6.

Tabuľka 2-5

Port	Odkaz na kabeláž	Farba kábla	Opis
Vstup čítačky dverí 1	485+	Fialová	RS485
	485-	Žltá	
	LED	Hnedá	Wiegand
	D0	Zelená	
	D1	Biela	
	CASE	Modrá	
	GND	Čierna	Napájanie čítačky
	12V	Červená	

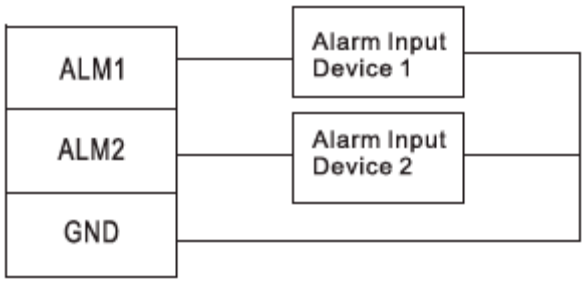
Tabuľka 2-5

Typ	Typ pripojenia	Dĺžka
RS485485	Sieťový kábel CAT5e	100 m
Wiegand	Sieťový kábel CAT5e	100 m

2.4.5 POPIS ZAPOJENIA EXTERNÉHO ALARMOVÉHO VSTUPU

2-kanálový externý alarmový vstup je znázornený na obrázku 2-10. Popis pripojení káblov nájdete v Tabuľke 2-7.

Obrázok 2-10



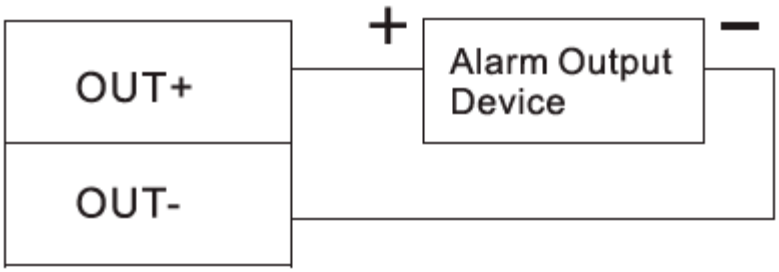
Tabuľka 2-7

Port	Odkaz na kabeláž		Opis
Externý alarmový vstup	ALM1	Vstupný port alarmu 1	Cez externé vstupné porty alarmu môžeme pripojiť detektor dymu, infračervený detektor atď.
	ALM2	Vstupný port alarmu 2	
	GND	Zdieľané vstupným portom alarmu 1 a 2	Externý alarm môže kombinovať stav otvárania a zatvárania dverí. • ALM1 spája všetky dvere pre normálne otváranie. • ALM2 spája všetky dvere pre normálne zatváranie.

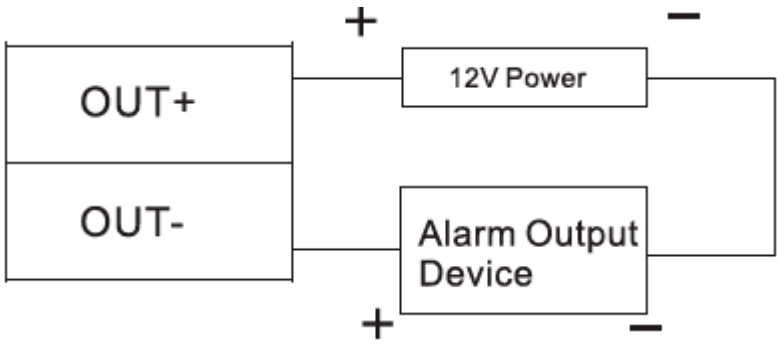
2.4.6 POPIS ZAPOJENIA EXTERNÉHO ALARMOVÉHO VÝSTUPU

Existujú dva spôsoby pripojenia externého alarmového výstupu v závislosti od alarmového zariadenia. Napríklad IPC môže použiť metódu 1, zatiaľ čo zvuková a vizuálna siréna môže použiť metódu dva, ako je znázornené na Obrázku 2-11 a Obrázok 2-12. Popis zapojenia pozri v Tabuľke 2-8.

Obrázok 2-11



Obrázok 2-12



Tabuľka 2-8

Port	Odkaz na kabeláž		Opis
Externý alarmový výstup	OUT1+	ALM1 spúšťa alarmový výstup. • Výstup alarmu o prekročení limitu času dverí 1 a signalizácia vlámania do dverí 1. • Výstup alarmu sabotáže čítačky dverí 1.	Interné a externé výstupné porty alarmu môžu kombinovať zvukové a vizuálne sirény.
	OUT1-		
	OUT2+	ALM2 spúšťa alarmový výstup. • Výstup alarmu o prekročení limitu času dverí 2 a signalizácia vlámania do dverí 2. • Výstup alarmu sabotáže čítačky dverí 2.	
	OUT2-		

2.4.7 POPIS PRINCÍPU VSTUPU A VÝSTUPU ALARMU

V prípade alarmovej udalosti bude alarm trvať 15 sekúnd. Podrobnosti o alarmových vstupoch a výstupoch nájdete v Tabuľke 2-9.

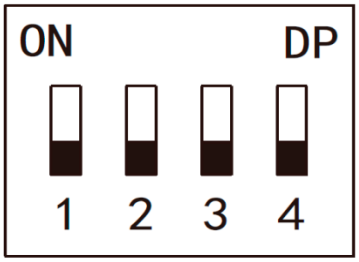
Tabuľka 2-9

Typ alarmu	Port vstupu alarmového signálu	Port výstupu alarmového signálu	Status alarmu
Externý alarmový vstup	ALM1	OUT1	Spája všetky dvere, aby zostali normálne otvorené.
	ALM2	OUT2	Spája všetky dvere, aby zostali normálne zatvorené.
Interný alarmový vstup	SR1	OUT1	Časový limit dverí a alarm vlámania spustí externý alarm.
	SR2	OUT2	
	RS-485/CASE	OUT1	Alarm sabotáže čítačky spustí externý alarm.
	RS-485/CASE	OUT2	

2.5 DIP PREPÍNAČ

Ovládanie pomocou prepínača DIP.

Obrázok 2-13



- Prepínač je v polohe ON, čo znamená 1.
- Prepínač je v polohe OFF, čo znamená 0.
- 1~4 sú všetky nastavené na 0. Systém sa spustí normálne.
- 1~4 sú všetky nastavené na 1. Systém po spustení prejde do režimu BOOT.
- 1, 3 sú nastavené na 1, ostatné sú nastavené na 0. Po reštarte systém obnoví výrobné nastaveni.
- 2, 4 sú nastavené na 1, zatiaľ čo ostatné sú nastavené na 0. Po reštarte systém obnoví výrobné nastavenia, ale informácie o používateľovi sa zachovajú.

2.6 REŠTART

Vložte ihlu do otvoru na reštartovanie a jedným stlačením reštartujte zariadenie.

Tlačidlo Reštart sa používa na reštartovanie zariadenia, nie na úpravu konfigurácie.

3. KONFIGURÁCIA SMART PSS

Aby sa zabezpečilo ovládanie a správna konfigurácia jedných dverí alebo skupiny dverí, prístupový kontrolér je riadený klientom Smart PSS. Táto kapitola popisuje hlavne rýchle nastavenie. Podrobnosti o prevádzke nájdete v užívateľskej príručke Smart PSS.

Klient Smart PSS ponúka rôzne porty pre rôzne verzie. Pozrite si skutočný port.

3.1 LOGOVANIE KLIENTA

Nainštalujte zodpovedajúceho klienta Smart PSS a spustite ho dvojitým kliknutím na , Podľa pokynov na rozhraní nakonfigurujte inicializáciu a dokončite prihlásenie.

3.2 PRIDANIE KONTROLY PRÍSTUPU

Pridajte ovládač prístupu do Smart PSS. Vyberte „Automatické vyhľadávanie" a „Pridať".

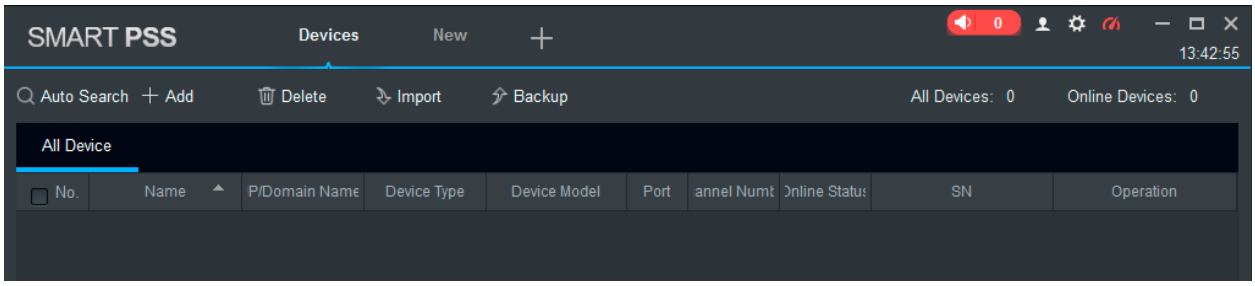
3.2.1 AUTOMATICKÉ VYHĽADÁVANIE

Zariadenia musia byť v rovnakom segmente siete.

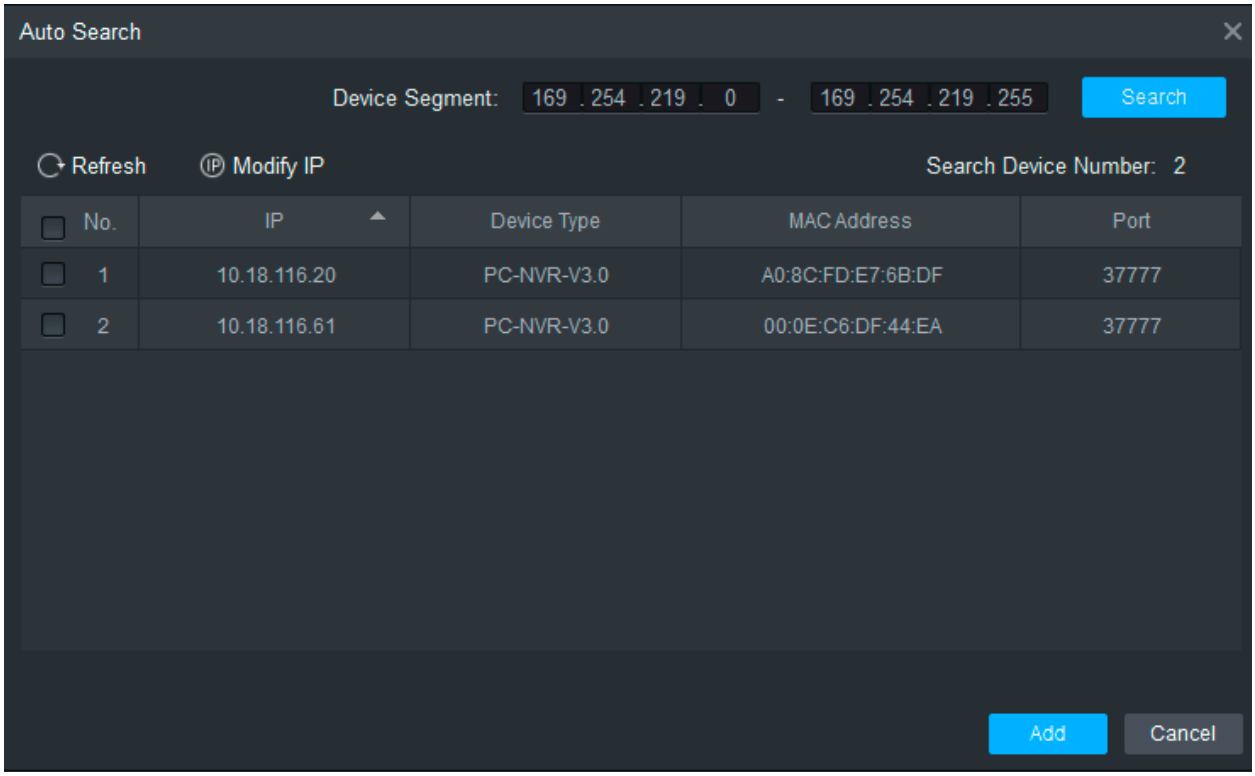
Krok 1: V rozhraní „Zariadenia" kliknite na „Automatické vyhľadávanie", ako je znázornené na obrázku 3-1.

Systém zobrazí rozhranie „Automatické vyhľadávanie" ako na obrázku 3-2.

Obrázok 3-1



Obrázok 3-2



Krok 2: Zadajte segment, v ktorom sa zariadenie nachádza, a kliknite na „Hľadať“.

Systém zobrazí výsledky vyhľadávania.

- Kliknutím na „Obnoviť“ aktualizujte informácie o zariadení.
- Vyberte zariadenie a kliknutím na „Upraviť IP“ upravte IP adresu zariadenia. Podrobnosti o prevádzke nájdete v užívateľskej príručke Smart PSS

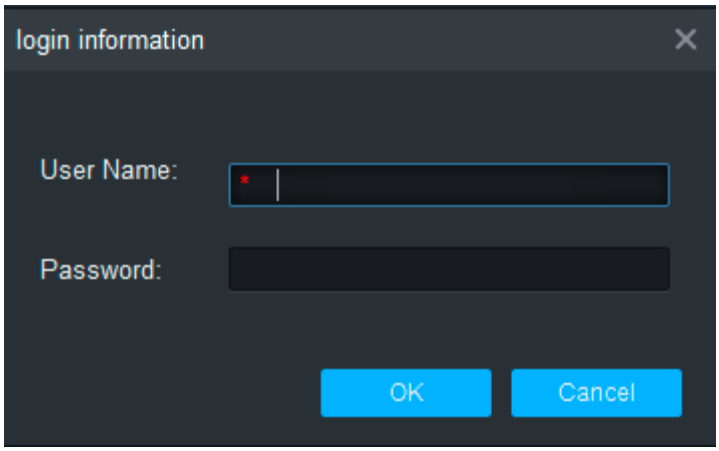
Vyberte zariadenie, ktoré chcete pridať, a kliknite na „Pridať“.

Systém zobrazí „Výzva“

Kliknite na „OK“.

Systém zobrazí dialógové okno „Prihlasovacie údaje” ako na obrázku 3-3.

Obrázok 3-3

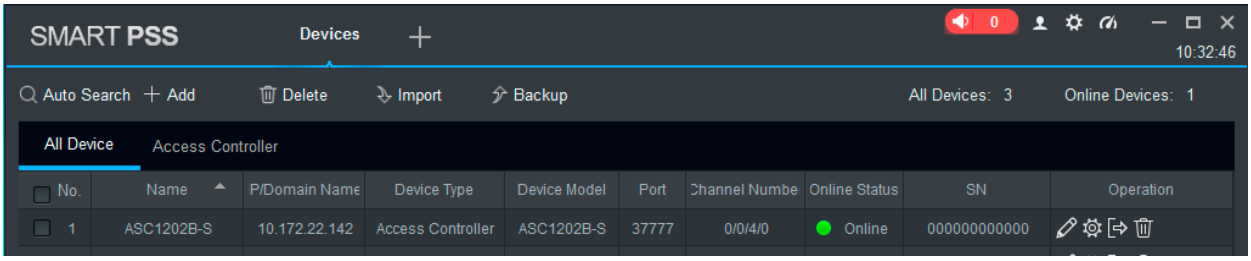


Krok 5: Zadajte „User name“ a „Password“ na prihlásenie do zariadenia a kliknite na „OK”.

Systém zobrazí zoznam pridaných zariadení, ako je znázornené na obrázku 3-4. Podrobnosti nájdete v Tabuľke 3-1.

- Po dokončení pridávania systém stále zostáva v rozhraní „Automatické vyhľadávanie“. Môžete pokračovať v pridávaní ďalších zariadení alebo kliknutím na tlačidlo „Zrušiť“ opustíte rozhranie „Automatické vyhľadávanie“.
- Po dokončení pridávania sa Smart PSS automaticky prihlási do zariadenia. Ak je prihlásenie úspešné, stav zariadenia sa zmení na „Online“. V opačnom prípade sa zobrazí „Offline”.

Obrázok 3-1



Tabuľka 3-1

Ikona	Opis
	Kliknutím na túto ikonu vstúpite do rozhrania „Upraviť zariadenie“ a upravíte informácie o zariadení vrátane názvu zariadenia, adresy IP / názvu domény, portu, používateľského mena a hesla. Alebo dvakrát kliknite na zariadenie, aby ste vstúpili do rozhrania „Upraviť zariadenie”
	Kliknutím na túto ikonu vstúpite do rozhrania „Konfigurácia zariadenia“ a nakonfigurujete kameru zariadenia, sieť, udalosť, pamäť a systémové informácie.
	• Keď je zariadenie online, ikona je  . Kliknutím na túto ikonu ukončíte prihlásenie a ikona sa zmení na  . • Keď je zariadenie offline, ikona je  . Kliknutím na túto ikonu sa prihláste (so správnymi informáciami o zariadení) a ikona sa zmení na  .
	Kliknutím na túto ikonu zariadenie odstránite.

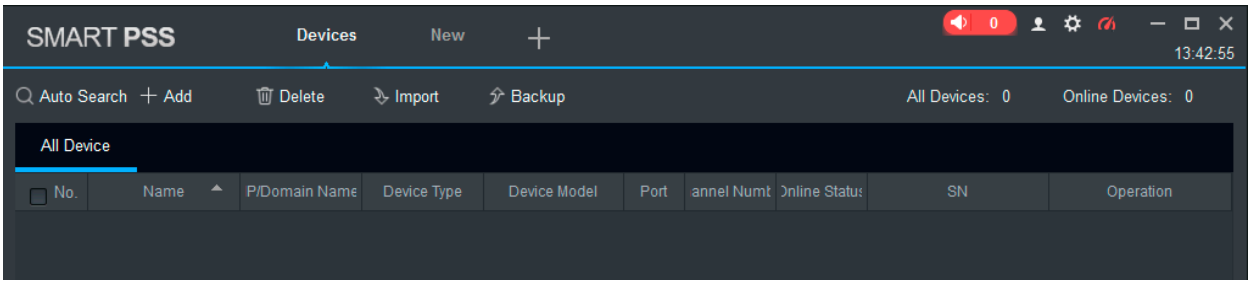
3.2.2 RUČNÉ DODÁVANIE

Ak chcete pridať zariadenia, musíte najprv poznať IP adresu zariadenia alebo názov domény.

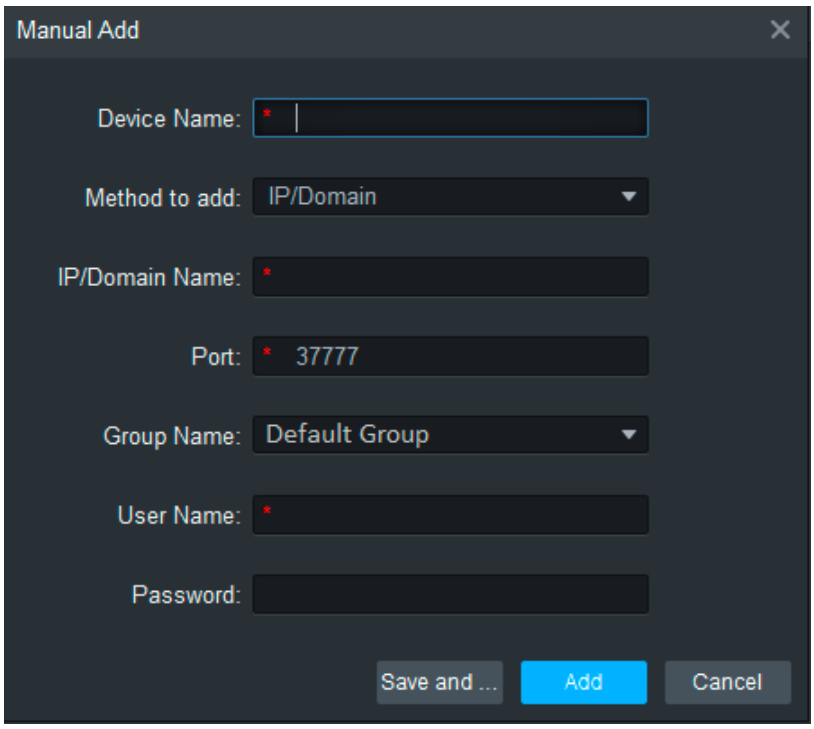
Krok 1: V rozhraní „Zariadenia“ kliknite na „Pridať“, ako je znázornené na Obrázku 3-5.

Systém zobrazí rozhranie „Manuálne pridanie“, ako je znázornené na obrázku Obrázku 3-6.

Obrázok 3-5



Obrázok 3-6



Krok 2: Nastavte parametre zariadenia. Podrobné popisy parametrov nájdete v Tabuľke 3-2.

Tabuľka 3-2

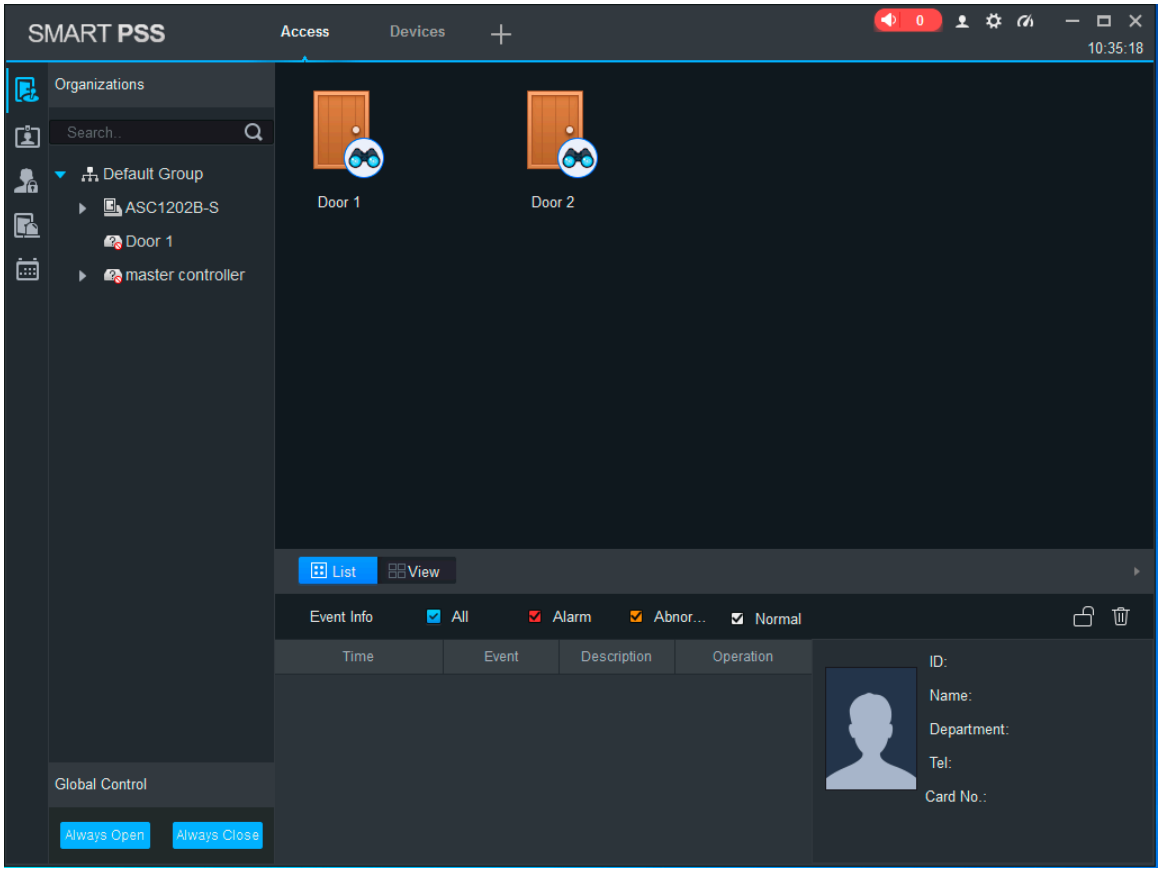
Parametr	Opis
Nazwa urządzenia	Zaleca się, aby nazwa urządzenia była nazywana strefą monitorowania, żeby ułatwić konserwację.
Metoda dodania	Wybierz „IP/Nazwa Domeny”. Dodaj urządzenia zgodnie z adresem IP urządzenia lub nazwą domeny.
IP/Nazwa domeny	Adres IP lub nazwa domeny urządzenia.
Port	Numer portu 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: Kliknutím na „Pridať“ pridáte zariadenie.

Systém zobrazí zoznam pridaných zariadení, ako je znázornené na obrázku 3-7. Podrobnosti nájdete v Tabuľke 3-2. Pridané dvierka ovládača sa zobrazia na karte „Prístup“ ako na obrázku 3-8.

- Ak chcete pridať ďalšie zariadenia, kliknite na „Uložiť a pokračovať“, pridajte zariadenia a zostaňte v rozhraní „Manuálne pridávanie“.
- Ak chcete zrušiť pridávanie, kliknite na „Zrušiť“ a opustite rozhranie „Manuálne pridávanie“.
- Po dokončení pridávania sa Smart PSS automaticky prihlási do zariadenia, ak je prihlásenie úspešné, stav zobrazí „Online“. V opačnom prípade sa zobrazí „Offline”.

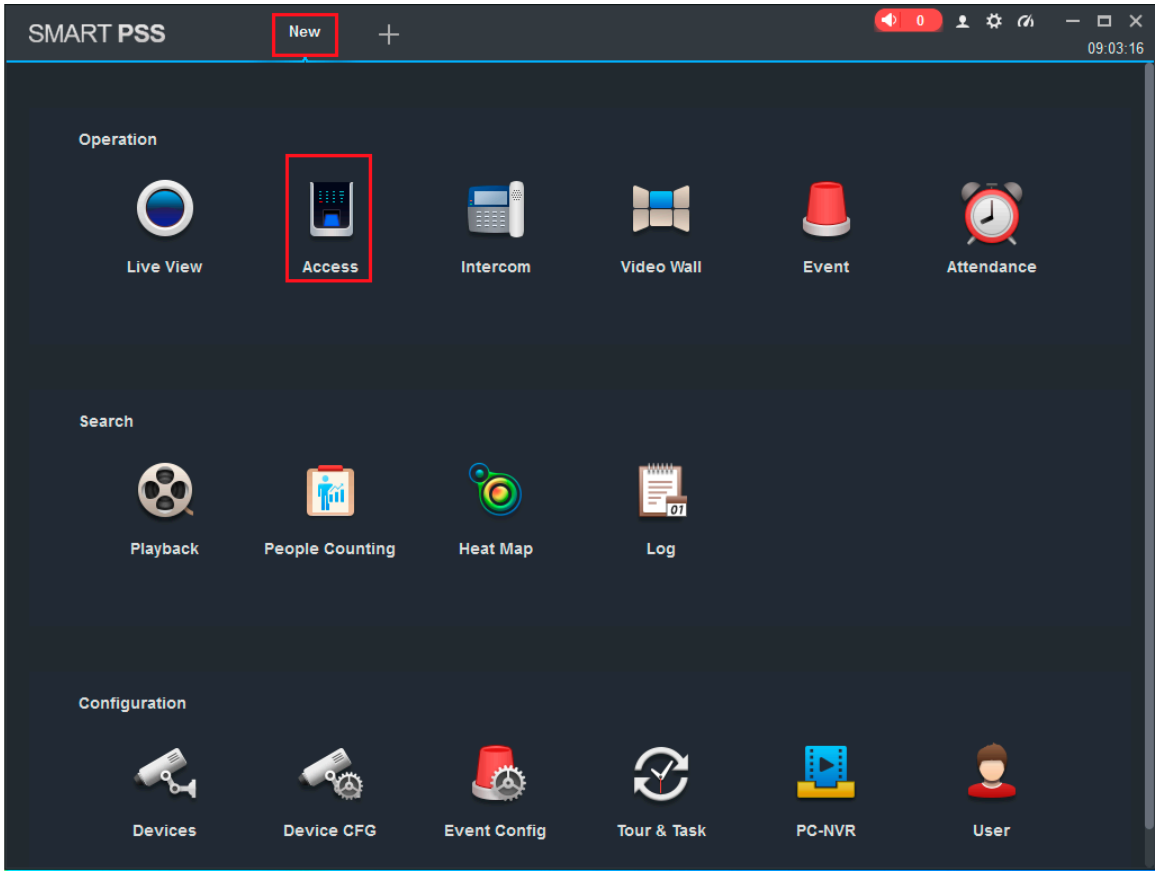
Obrázok 3-7



3.3 PRIDANIE POUŽÍVATEĽA

Pridajte používateľov a vytvorte prepojenie na karty na distribúciu povolení.
V rozhraní „Nové“ kliknite na „Prístup“ pre vstup do rozhrania „Prístup“ a tu dokončite konfiguráciu prístupu.

Obrázok 3-8

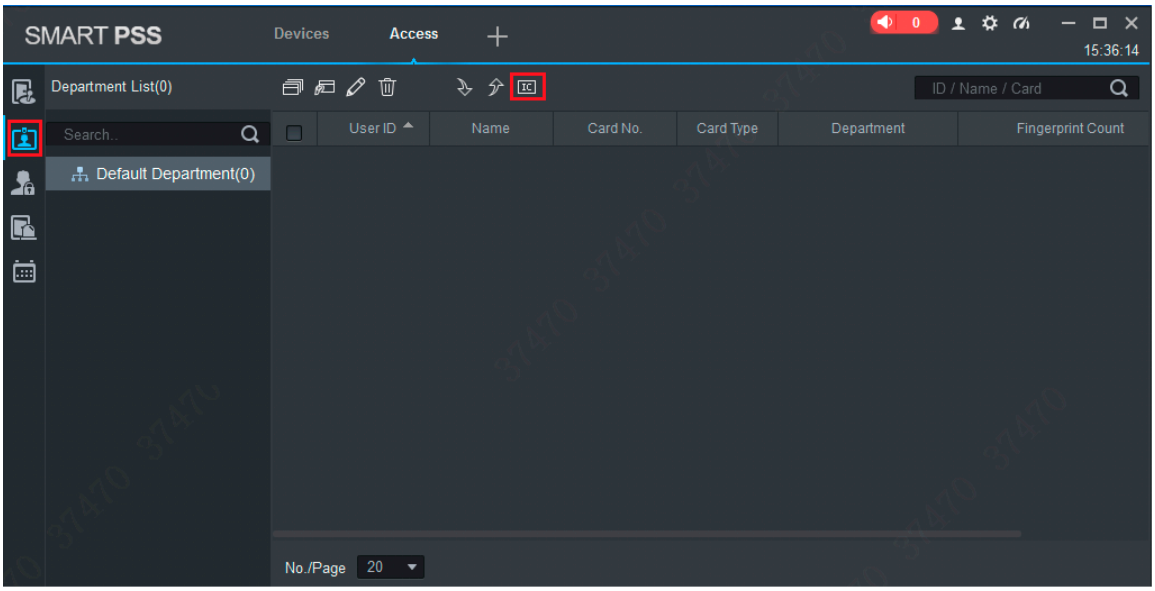


3.3.1 TYP KARTY

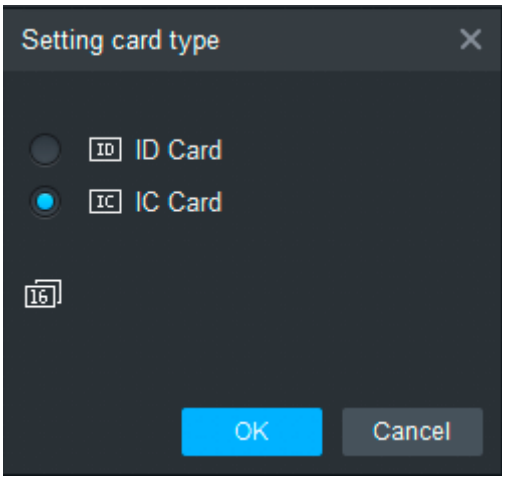
CAUTION!
Typ karty je rovnaký ako u vydavateľa karty, inak neprečíta číslo karty.

V rozhraní „Prístup” kliknite na  , a potom kliknite na  , na nastavenie typu karty ako na Obrázku 3-9 a Obrázku 3-10.

Obrázok 3-9



Obrázok 3-10



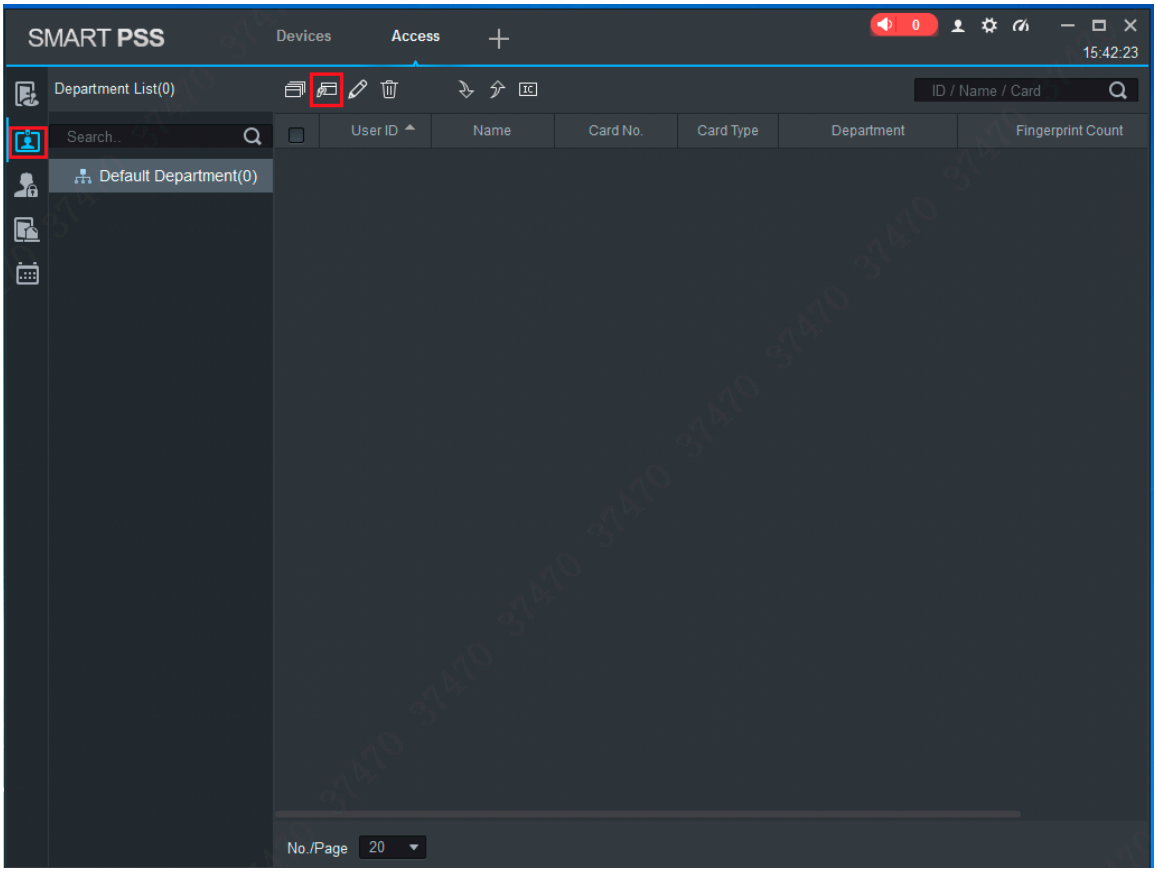
3.3.2 JEDNORAZOVÉ PRIDANIE

Pridajte jedného používateľa, zadajte informácie o karte a používateľovi.

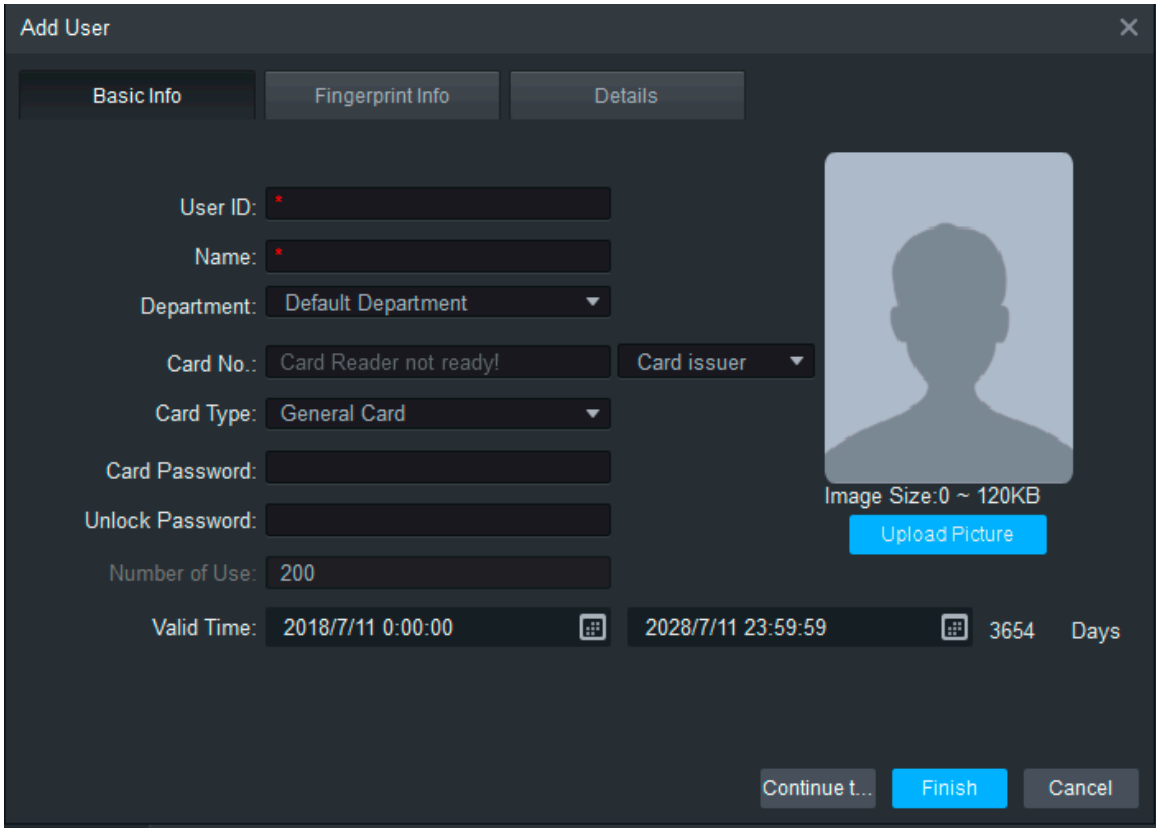
Krok 1: V rozhraní „Prístup“ kliknite na , potom kliknite na , ako je ukázané na Obrázku 3-11.

Systém zobrazí dialógové okno „Pridať používateľa“ ako na obrázku 3-12.

Obrázok 3-11



Obrázok 3-12



Krok 2: Manuálne pridajte informácie o používateľovi vrátane základných informácií o odtlačkoch prstov a podrobnosti. Detaily nájdete v Tabuľke3-3.

Tabuľka 3-3

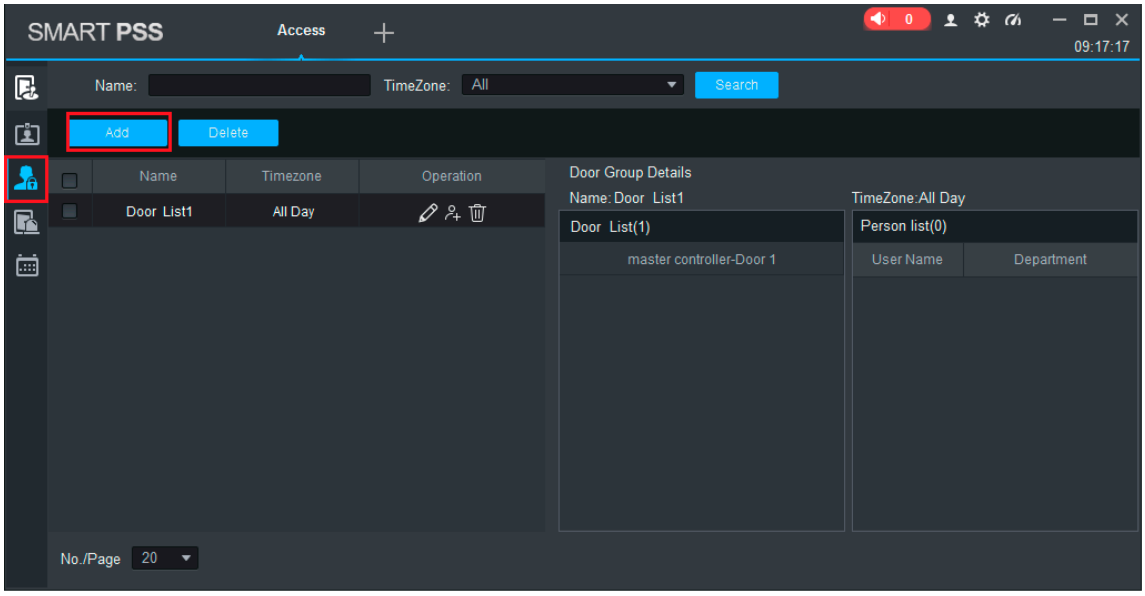
Parametr	Opis
Základné informácie	ID používateľa (povinné). • Meno a priezvisko (povinné). • Oddelenie (Automatické doplnenie). • Číslo karty: zadanie pomocou čítačky kariet alebo manuálne zadanie. • Typ karty: všeobecná karta, VIP karta, návštevnícka karta, hliadková karta, blacklist či nátlaková karta. • Heslo karty: Používa sa na otvorenie dverí kartou + heslom. • Heslo na odomknutie: Používa sa na odomknutie dverí pomocou hesla. • Počet použití: Platí len pre kartu hosťa. • Platný čas: nastavte dĺžku trvania prístupu, ktorá je štandardne 10 rokov. • Fotografia: Používateľská fotografia, maximálne 120 kB. Číslo karty a ID používateľa nemožno opakovať.
Informácie o odtlačkoch prstov	Zbierajte odtlačky prstov pomocou čítačky odtlačkov prstov a čítačky prístupu. • Maximálne 2 odtlačky prstov pre každú osobu. • Pomoc pri zadávaní názvu odtlačku prsta.
Podrobnosti	Poskytnite podrobnosti o používateľovi podľa parametrov rozhrania.

Krok 3: Kliknutím na „Dokončiť“ dokončíte pridávanie používateľov.

3.4 PRIDANIE SKUPINY DVERÍ

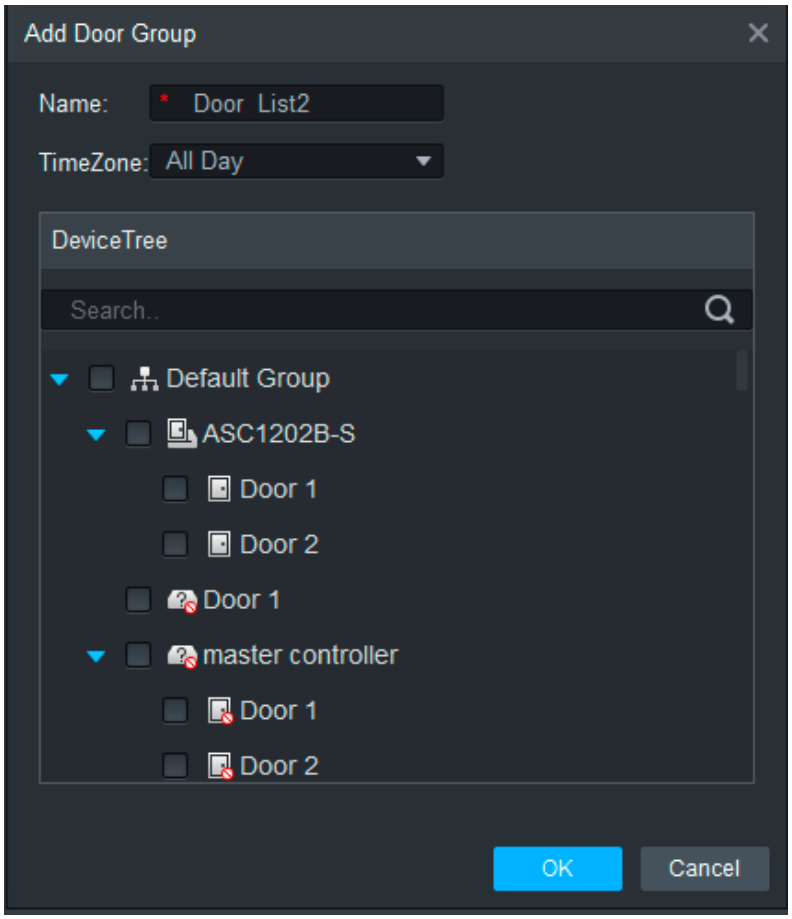
Rozdeľte dvere do skupín a spravujte ich spoločne.
Krok 1: V rozhraní „Prístup" kliknite na , a potom kliknite na „Úroveň prístupu" ako je znázornené na Obrázku 3-13.

Obrázok 3-13



Krok 2: Kliknite na „Pridať".
Systém zobrazí dialógové okno „Pridať skupinu dverí" ako na obrázku 3-14.

Obrázok 3-14



Krok 3: Zadajte „Názov", vyberte „Časové pásmo" a dvere, ktoré chcete spravovať.
Krok 4: Kliknutím na „OK" dokončite pridávanie.

3.5 AUTORIZÁCIA

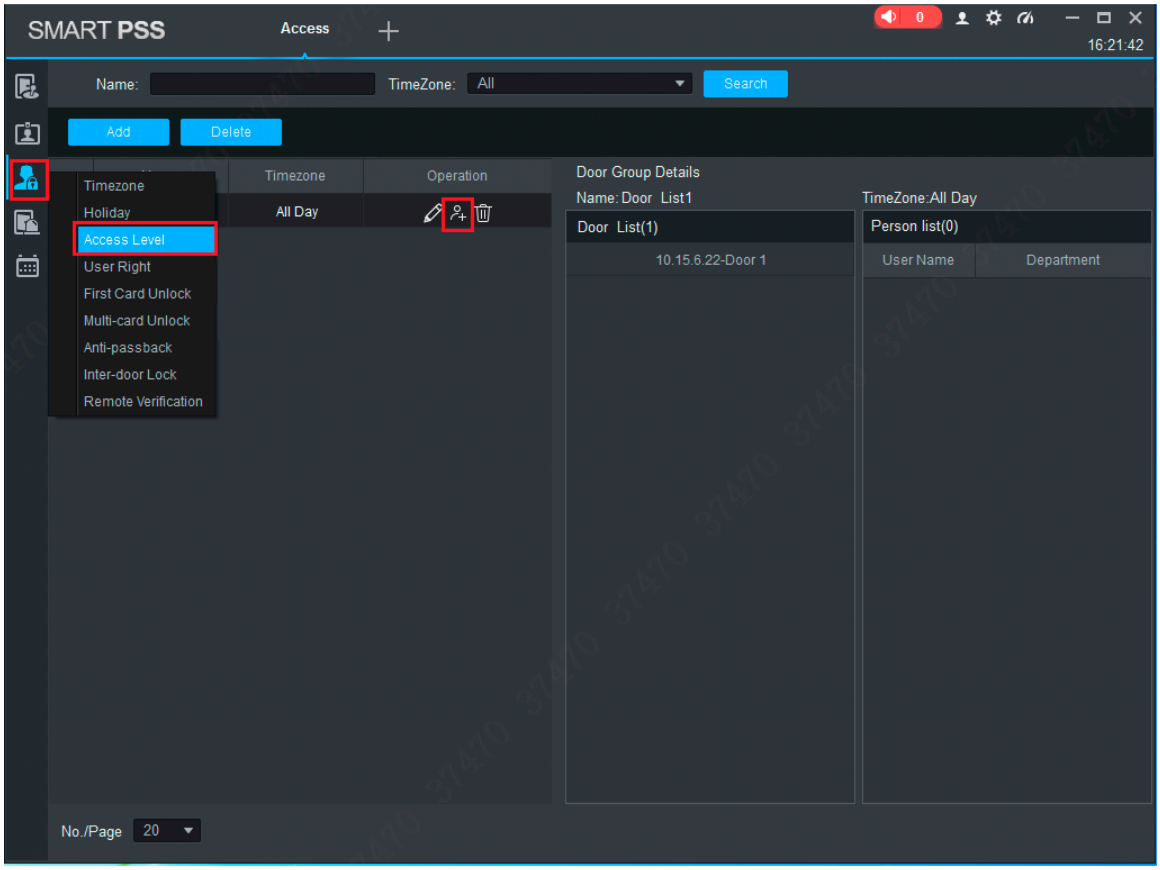
Udeľte povolenia používateľom podľa skupiny dverí a používateľa.

3.5.1 AUTORIZÁCIA PODĽA SKUPINY DVERÍ

Vyberte skupinu dverí, pridajte príslušných používateľov do skupiny, aby všetci používatelia v skupine získali povolenia pre všetky dvere v skupine.

Krok 1: V rozhraní „Prístup" kliknite na , a potom kliknite na „Úroveň prístupu" ako je znázornené na Obrázku 3-15.

Obrázok 3-15

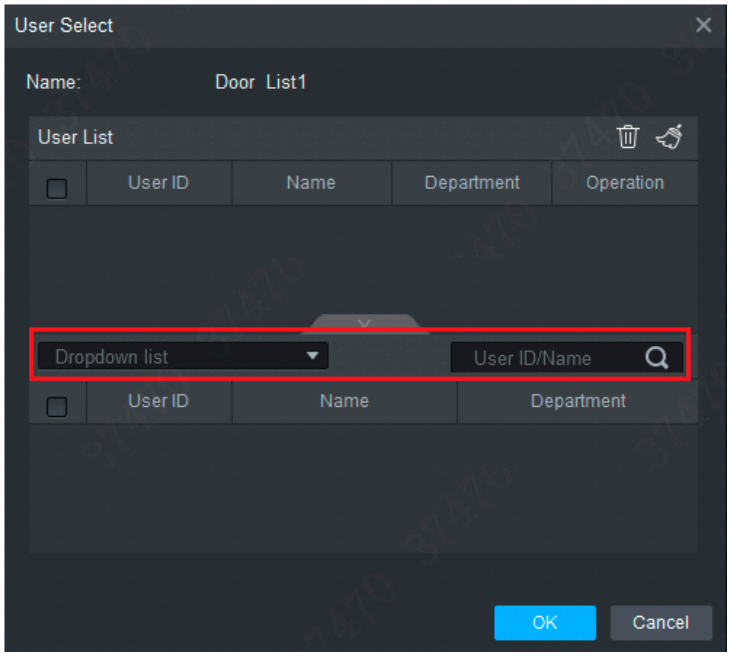


Krok 2: Kliknite na .

Systém zobrazí dialógové okno „Výber používateľa".

Krok 3: Vyberte používateľské oddelenie z rozbaľovacieho zoznamu alebo zadajte ID používateľa alebo meno používateľa priamo, ako je uvedené na Obrázku 3-16.

Obrázok 3-16



Krok 4: Z Vyberte používateľa zo zoznamu vyhľadávania a pridajte ho do zoznamu používateľov.

Krok 5: Kliknutím na „OK“ dokončíte autorizáciu.

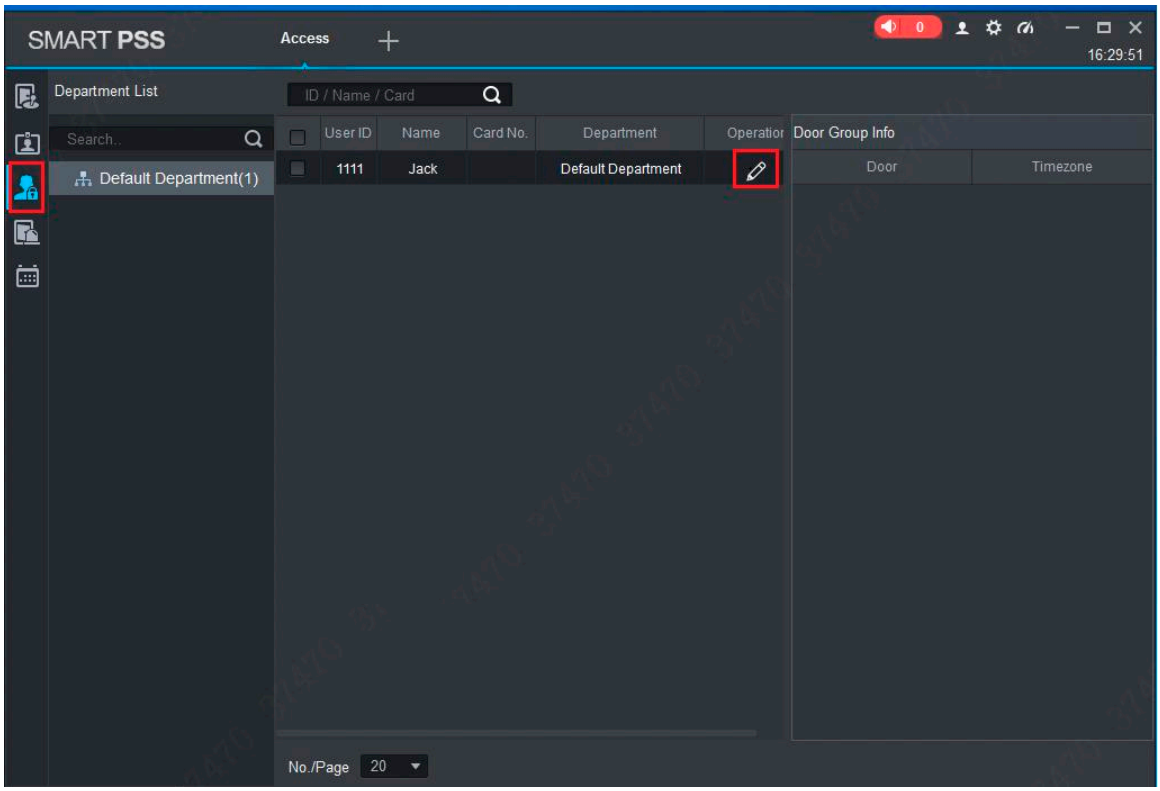
• Zoznam vyhľadávania filtruje informácie o používateľovi bez čísla karty.
• V zozname používateľov zrušte pridaného používateľa a odstráňte jeho povolenia.

3.5.2 AUTORIZÁCIA PODĽA POUŽÍVATEĽA

Vyberte užívateľa, rozdeľte skupinu dverí a udeľte skupine užívateľov oprávnenie.

Krok 1: V rozhraní „Prístup“ kliknite na  , a potom kliknite na „Práva používateľa“, ako je znázornené na obrázku 3-17.

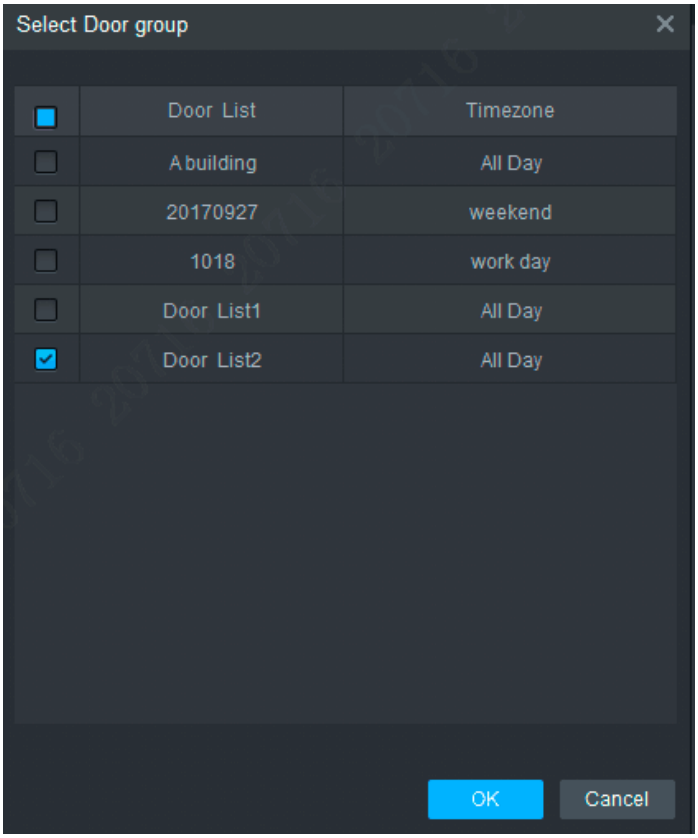
Obrázok 3-17



Krok 2: Kliknite na  .

Systém zobrazí dialógové okno „Výber skupiny dverí“ ako na obrázku 3-18.

Obrázok 3-18



Krok 3: Vyberte skupinu dverí a kliknutím na „OK“ dokončite autorizáciu.

4. FAQ

V prípade problémov, ktoré nie sú uvedené nižšie, kontaktujte miestny zákaznícky servis alebo zákaznícky servis ústredia. Vždy Vám budeme k dispozícii.

1. Otázka: Po zapnutí napájania sa indikátor napájania nerozsvieti alebo bzučiak nereaguje.

Odpoveď: Skontrolujte, či je zástrčka správne zasunutá. Vytiahnite ju a znova vložte.

2. Otázka: Po použití čítačky so zariadením kontrolka posunu karty nesvieti a po potiahnutí kartou nie je žiadna odozva.

Odpoveď: Skontrolujte, či je konektor čítačky zasunutý na správnom mieste. Vytiahnite a znova vložte, skontrolujte, či svieti kontaktná kontrolka čítačky.

3. Otázka: Softvér nerozpoznal zariadenie.

Odpoveď: Skontrolujte, či je kabeláž správne pripojená a či je IP adresa zariadenia v rovnakom segmente siete.

4. Otázka: Po zobrazení karty sa zobrazí hlásenie, že karta nie je platná.

Odpoveď: Skontrolujte, či bolo toto číslo karty pridané do ovládača.

5. Otázka: Aká je predvolená adresa IP kontroléra prístupu?

Odpoveď: Predvolená IP adresa je 192.168.0.2.

6. Otázka: Aký je predvolený port, používateľské meno a heslo kontroléra prístupu?

Odpoveď: Predvolený port je 37777, počiatočné používateľské meno je admin a heslo je 123456.

7. Otázka: Ako urobiť online aktualizáciu zariadenia?

Odpoveď: Pripojte zariadenie a počítač cez sieť a aktualizujte ho na platforme.

8. Otázka: Aká je maximálna vzdialenosť vedenia a prenosová vzdialenosť čítačky, kariet a ovládača?

Odpoveď: Závisí to od typu sieťového kábla a od toho, či potrebuje napájanie ovládacieho relé.

Pri pripojení sieťovým káblom CAT5E je typická hodnota:

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

DODATOK 1 ODPORÚČANIA PRE KYBERNETICKÚ BEZPEČNOSŤ

Kybernetická bezpečnosť je viac než len módne slovo: je to niečo, čo platí pre akékoľvek zariadenie pripojené k internetu. Video dohľad nie je imúnny voči kybernetickým hrozbám, no ak podniknete základné kroky na ochranu a posilnenie vašich sietí a zariadení, budú menej zraniteľné voči útokom. Nižšie je niekoľko tipov a odporúčaní od BCS, ako vytvoriť bezpečnejší systém.

POVINNÉ OPATRENIA, KTORÉ JE POTREBNÉ PRIJAŤ NA ZABEZPEČENIE ZÁKLADNÉHO ZABEZPEČENIA SIETE ZARIADENÍ:

1. Používajte silné heslá

Pozrite si nasledujúce návrhy na nastavenie hesiel:

- Dĺžka by nemala byť kratšia ako 8 znakov;
- Zahrňte aspoň dva typy znakov; typy znakov zahŕňajúce veľké a malé písmená, čísla a symboly;
- Nezadávajte ako heslo názov účtu alebo názov účtu naopak;
- Nepoužívajte po sebe idúce znaky ako 123, abc atď.;
- Nepoužívajte rovnaké znaky ako 111, aaa atď.;

2. Aktualizujte firmvér a klientský softvér včas

- Podľa priemyselného štandardného postupu vám odporúčame aktualizovať firmvér vášho hardvéru (ako je NVR, DVR, IP kamera atď.), aby ste sa uistili, že váš systém je vybavený najnovšími bezpečnostnými opravami. Keď je zariadenie pripojené k verejnej sieti, odporúča sa zapnúť funkciu „automatická kontrola aktualizácií“, aby ste získali najnovšie informácie o aktualizáciách firmvéru vydaných výrobcom.
- Odporúčame vám stiahnuť a používať najnovšiu verziu klientskeho softvéru.

UŽITOČNÉ ODPORÚČANIA NA ZLEPŠENIE ZABEZPEČENIA SIETE ZARIADENÍ:

1. Fyzická ochrana

Odporúčame vám fyzicky chrániť váš hardvér, najmä úložné zariadenia. Napríklad umiestnite zariadenie do špeciálnej počítačovej miestnosti a skrinky a aplikujte dobre vykonanú kontrolu prístupu a správu kľúčov, aby ste zabránili neoprávnenému personálu vykonávať fyzické činnosti, ako je poškodenie zariadenia, neoprávnené pripojenie vymeniteľného zariadenia (ako je USB flash disk , sériový port) atď.

2. Pravidelne meňte heslá

Odporúčame vám, aby ste si heslá pravidelne menili, aby ste znížili riziko uhádnutia alebo prelomenia.

3. Nastavte a aktualizujte heslá, resetujte informácie včas

Zariadenie podporuje funkciu obnovenia hesla. Včas nastavte súvisiace informácie o obnovení hesla, vrátane emailu koncového používateľa a otázok o ochrane hesla. Ak sa informácie zmenia, musia byť včas revidované. Pri nastavovaní otázok na ochranu hesla sa odporúča nepoužívať tie, ktoré sa dajú ľahko uhádnuť.

4. Zapnite blokovanie účtu konta

Funkcia uzamknutia účtu je predvolene zapnutá a odporúčame vám ju nechať zapnutú, aby ste sa uistili, že je váš účet bezpečný. Ak sa útočník pokúsi prihlásiť viackrát s nesprávnym heslom, príslušný účet a zdrojová IP adresa budú zablokované.

5. Zmeňte predvolené porty HTTP a porty inných služieb

Odporúčame zmeniť predvolené porty HTTP a porty iných služieb na ľubovoľnú sadu čísel medzi 1024 - 65535, čím sa zníži riziko, že okoloidúci budú môcť uhádnuť, ktoré porty používate.

6. Povoľte HTTPS

Odporúčame vám povoliť protokol HTTPS na návštevu webovej služby cez zabezpečený komunikačný kanál.

7. Povoľte Whitelist

Odporúčame vám povoliť funkciu whitelistu, aby ste zabránili komukoľvek okrem ľudí s konkrétnymi IP adresami v prístupe k vášmu systému.

8. Naviazanie MAC adresy

Odporúčame vám prepojiť IP a MAC adresu brány so zariadením, čím sa zníži riziko spoofingu ARP.

9. Priraďte účty a povolenia rozumným spôsoboma

Podľa vašich obchodných a manažérskych požiadaviek pridávajte používateľov rozumne a priraďte im minimálny súbor povolení.

10. Vypnite nepotrebné služby a vyberte bezpečné režimy

Ak to nie je potrebné, odporúča sa vypnúť niektoré služby ako SNMP, SMTP, UPnP atď., aby sa znížilo riziko. Dôrazne sa odporúča, aby ste v prípade potreby používali núdzové režimy vrátane, ale nie výlučne, nasledujúcich služieb:

- SNMP: Vyberte SNMP v3 a nakonfigurujte silné šifrovacie a autentifikačné heslá.
- SMTP: Zvoľte TLS pre prístup k poštovému serveru.
- FTP: Vyberte SFTP a nastavte silné heslá.
- Prístupový bod AP: Vyberte režim šifrovania WPA2 PSK a nastavte silné heslá.

11. Šifrovaný prenos audia a videa

Ak je obsah audio a video dát veľmi dôležitý alebo citlivý, odporúčame použiť funkciu šifrovaného prenosu, aby ste znížili riziko krádeže audio a video dát počas prenosu.
Poznámka: šifrovaný prenos spôsobí určité zníženie výkonu.

12. Bezpečný audit

- Kontrola online používateľov: Odporúčame vám pravidelne sledovať online používateľov, aby ste skontrolovali, či nie je zariadenie prihlásené neoprávnene.
- Skontrolujte protokol hardvéru: zobrazením protokolov môžete zistiť adresy IP, ktoré boli použité na prihlásenie do zariadení, a ich kľúčové operácie.

13. Sieťový denník

V dôsledku obmedzenej úložnej kapacity hardvéru je uchovávaný protokol obmedzený. Ak potrebujete uchovávať protokolovanie dlhší čas, odporúča sa zapnúť funkciu sieťového denníka, aby ste sa uistili, že vaše kritické denníky sú synchronizované so serverom sieťových denníkov na účely sledovania.

14. Vytvorte bezpečné sieťové prostredie

Ak chcete lepšie chrániť svoj hardvér a znížiť potenciálne kybernetické hrozby, odporúčame:

- Vypnite funkciu mapovania portov smerovača, aby ste zabránili priamemu prístupu k intranetovým zariadeniam z externej siete.
- Sieť by mala byť rozdelená a izolovaná podľa skutočných potrieb siete. Ak neexistujú žiadne komunikačné požiadavky medzi týmito dvoma podsieťami, odporúča sa použiť VLAN, sieť GAP a ďalšie technológie na rozdelenie siete, aby sa dosiahol efekt izolácie siete.
- Nakonfigurujte prístupový autentifikačný systém 802.1x a znížite riziko neoprávneného prístupu do súkromných sietí.

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

Aktualizácia: 08.04.2022