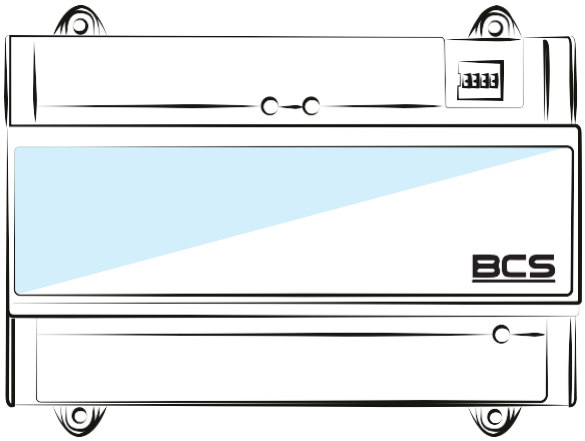
CZ

BCS-KKD-J222

Dvoudveřový jednosměrný přístupový ovladač

Uživatelská příručka



www.bcs.pl

NSS Sp. z o.o. Modularna 11 (hala IV), 02-238 Varšava tel. +48 22 846 25 31, fax. +48 22 846 23 31 linka 140
E-mail: info@bcscctv.pl, CÍN: 521-312-46-74

Aktualizovaný:

ÚVOD

OBECNÉ:

Dokument popisuje konstrukci, instalaci a zapojení dvoudveřového obousměrného přístupového ovladače.

BEZPEČNOSTNÍ POKYNY:

V instrukci se mohou objevit následující signální slova s definovaným významem.

Signální slova	Význam
VAROVÁNÍ !	Označuje nebezpečí s vysokým potenciálem, které pokud ignorujete může to mít za následek smrt nebo vážné zranění
VAROVÁNÍ !	Označuje střední nebo nízké potenciální nebezpečí, které může způsobit lehké až středně těžké zranění
POZNÁMKA !	Označuje potenciální rizika, která by mohla vést ke škodám na majetku, ztrátě dat, nižšímu výkonu nebo nepředvídanému výsledku.
VODÍTKO	Obsahuje rady , které vám pomohou problém vyřešit nebo vám ušetří čas
POZNÁMKA	Poskytuje další informace, které doplňují text.

OZNÁMENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ:

Jako uživatel zařízení nebo správce údajů můžete shromažďovat osobní údaje jiných lidí, jako je obličej, otisky prstů, registrační číslo vozidla, e-mailová adresa, telefonní číslo, GPS a tak dále. Musíte dodržovat místní zákony a předpisy o ochraně osobních údajů, abyste chránili práva a předpisy ostatních prostřednictvím exekutivních opatření která zahrnují ale nutnost: informování subjektu o existenci oblasti dohledu a zajištění kontaktu.

O POKYNECH

- Instrukce slouží pouze jako návod. Pokud existují rozdíly mezi skutečným produktem a příručkou, má přednost skutečný produkt.
- Nejsme zodpovědní za žádné ztráty způsobené jednáním v rozporu s pokyny.
- Příručka bude aktualizována v souladu s nejnovějšími zákony a předpisy platnými ve společnosti. Podrobnosti najdete v papírových uživatelských příručkách, CD ROM, QR kódu nebo na našich oficiálních webových stránkách. V případě rozporu mezi papírovým návodem k použití a elektronickou verzí má přednost elektronická verze.
- Všechny projekty a software se mohou změnit bez předchozího písemného upozornění. Aktualizace produktu mohou způsobit určité rozdíly mezi skutečným produktem a příručkou. Obraťte se na zákaznickou podporu pro nejnovější software a další dokumentaci.
- Mohou existovat odchylky v technických údajích, popisech funkcí a operacích nebo chyby v tisku. V případě pochybností si přečtěte naše vysvětlení.
- Pokud nemůžete otevřít uživatelskou příručku PDF, aktualizujte software pro čtení PDF nebo vyzkoušejte jiný software.
- Všechny ochranné známky, registrované ochranné známky a názvy společností v příručce jsou majetkem příslušných vlastníků.
- Pokud při používání zařízení narazíte na jakýkoli problém, navštivte naše webové stránky, obraťte se na svého dodavatele nebo zákaznický servis.
- Pokud máte pochybnosti, přečtěte si prosím naše vysvětlivky.

DŮLEŽITÉ UJIŠTĚNÍ A VAROVÁNÍ:

Následující popis je správný způsob aplikace zařízení. Před použitím byste si měli pečlivě přečíst pokyny, abyste se vyhnuli nebezpečí a ztrátě majetku. Při používání zařízení přísně dodržujte pokyny a dodržujte je po přečtení.

PROVOZNÍ POŽADAVKY

- Neumísťujte ani neinstalujte zařízení na místo vystavené přímému slunečnímu záření nebo v blízkosti zařízení, které vytváří teplo.
- Neinstalujte zařízení na vlhké, prašné nebo teplé místo.
- Instalujte zařízení vodorovně nebo na stabilní místa a chraňte před pádem.
- Nestříkejte na přístroj kapaliny, nepokládejte na přístroj nic naplněného kapalinami, abyste zabránili vniknutí kapalin do zařízení.
- Nainstalujte zařízení na dobře větraná místa. Neblokujte větrací otvor.
- Zařízení používejte pouze v nominálním rozsahu výstupu a vstupu.
- Zařízení libovolně nerozebírejte.
- Přepravujte, používejte a skladujte zařízení v přípustném rozsahu vlhkosti a teploty.

POŽADAVKY NA NAPÁJENÍ

- Ujistěte se, že používáte baterii podle požadavků, jinak může dojít k požáru baterie , výbuchu nebo popálení!
- K výměně baterie lze použít pouze stejný typ baterie.
- V produktu by měly být použity elektrické kabely (napájecí kabely) doporučené pro tento výrobek, použijte je podle jmenovité specifikace!
- Použijte standardní napájecí zdroj, který vyhovuje vašemu zařízení. V opačném případě se uživatel vystavuje zranění personálů nebo poškození zařízení.
- Použijte napájecí zdroj kompatibilní se STANDARDEM SELV (bezpečné velmi nízké napětí) a napájejte jej napětím kompatibilním s omezeným zdrojem energie v IEC60950-1. Podrobné požadavky na napájení naleznete na štítcích zařízení.
- Výrobky kategorie I musí být připojeny k elektrické zásuvce, která je vybavena ochranným uzemněním.
- Konektor zařízení je odpojovací zařízení. Během používání by měl být zachován úhel dostupnosti pro snadnou obsluhu.

OBSAH

Přístup II
Důležité zabezpečení a upozornění III
1 Přehled 1
1.1 Vlastnosti zařízení 1
1.2 Rozměry a vzhled 1
2 Instalační příručka 2
2.1 Struktura systému 2
2.2 Instalace zařízení 2
2.3 Demontáž 3
2.4 Schéma zapojení 4
2.4.1 Popis kabeláže přístupového řadiče 4
2.4.2 Popis kabeláže dveřního tlačítka ven/kontaktního tlačítka 5
2.4.3 Popis kabeláže zámku 5
2.4.4 Popis zapojení čtečky 7
2.4.5 Popis zapojení externího alarmového vstupu 7
2.4.6 Popis zapojení externího alarmového výstupu 8
2.4.7 Popis principu vstupu a výstupu alarmu 8
2.5 DIP přepínač 9
2.6 Restartovat 9
3 Konfigurace Smart PSS 10
3.1 Logováni klienta 10
3.2 Přidání řízení přístupu 10
3.2.1 Automatické vyhledávání 10
3.2.2 Ruční přidání 12
3.3 Přidání uživatele 14
3.3.1 Typ karty 14
3.3.2 Jednorázové přidání 15
3.4 Přidání skupiny dveří 17
3.5 Autorizace 18
3.5.1 Autorizace podle skupiny dveří 18
3.5.2 Autorizace uživatelem 19
4 Často kladené dotazy 21
Příloha 1 Doporučení pro kybernetickou bezpečnost 22

1. PŘEHLED

Dvoudveřový jednosměrný přístupový řadič je ovládací zařízení, které vyvažuje video dohled a vizuální interkom. Má elegantní a moderní design s vysokou funkčností, vhodný pro družstevní budovy, firemní nemovitosti a inteligentní komunitu.

1.1 VLASTNOSTI ZAŘÍZENÍ

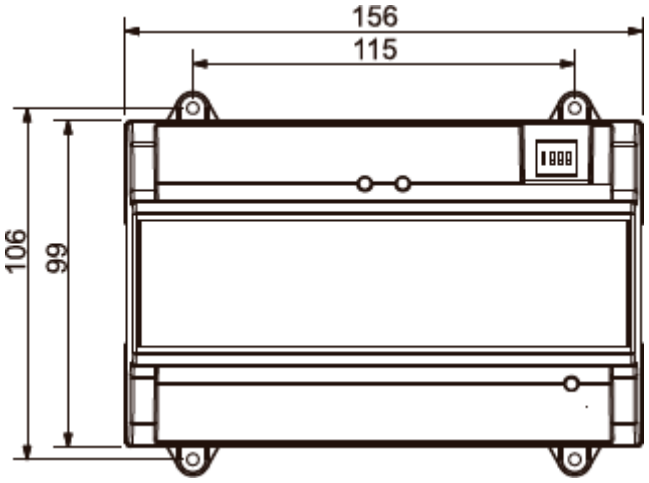
Jeho bohaté vlastnosti jsou následující:

- Použití posuvné kolejnice a konstrukce ovládané zámkem, pohodlná instalace a údržba.
- Integrovaný alarm, řízení přístupu, video dohled a požární poplach.
- Podpora 2 sad čteček karet .
- Podporuje 6 skupin vstupních signálů (výstupní tlačítko*2, dveřní kontakt*2 a alarm proti vloupání*2).
- Podporuje 4 skupiny řídicích výstupů (elektrický zámek *2 a alarmový výstup *2).
- S portem RS485 jej lze rozšířit o řídicí modul.
- Kapacita flash paměti je 16M (může se zvýšit na 32M). Podpora až 100 000 karet a 150 000 čtecích snímků karet.
- Obsluha alarmu proti nelegálnímu vloupání , odemykání alarmu časového limitu, karty donucerní a konfigurace kódu donucení. Podporuje také konfiguraci černé a bílé listiny a hlídkových karet.
- Podpora nastavení správného časového období, hesla a data vypršení platnosti karty. U karty hosta můžete nastavit dobu jejího používání.
- Podpora pro 128 skupin rozvrhů a 128 skupin harmonogramů svátků .
- Konstantní ukládání dat během selhání, vestavěná RTC (podpora letního času), online aktualizace.

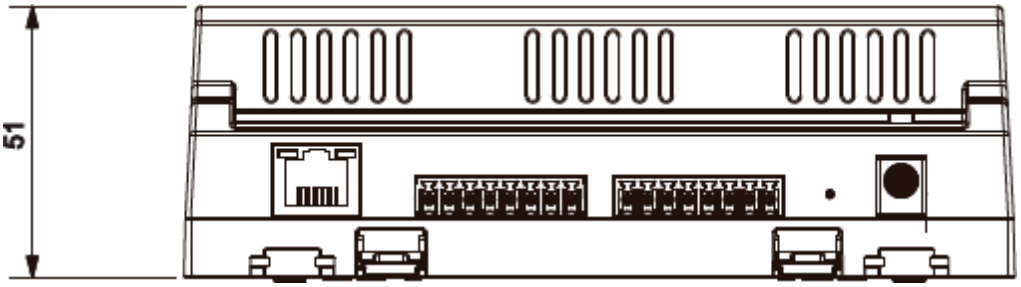
1.2 ROZMĚRY A VZHLED

Jeho vzhled a velikost jsou znázorněny na obrázku 1-1 a obrázku 1-2. Jednotkou délky jsou milimetry.

Obrázek 1-1



Obrázek 1-2

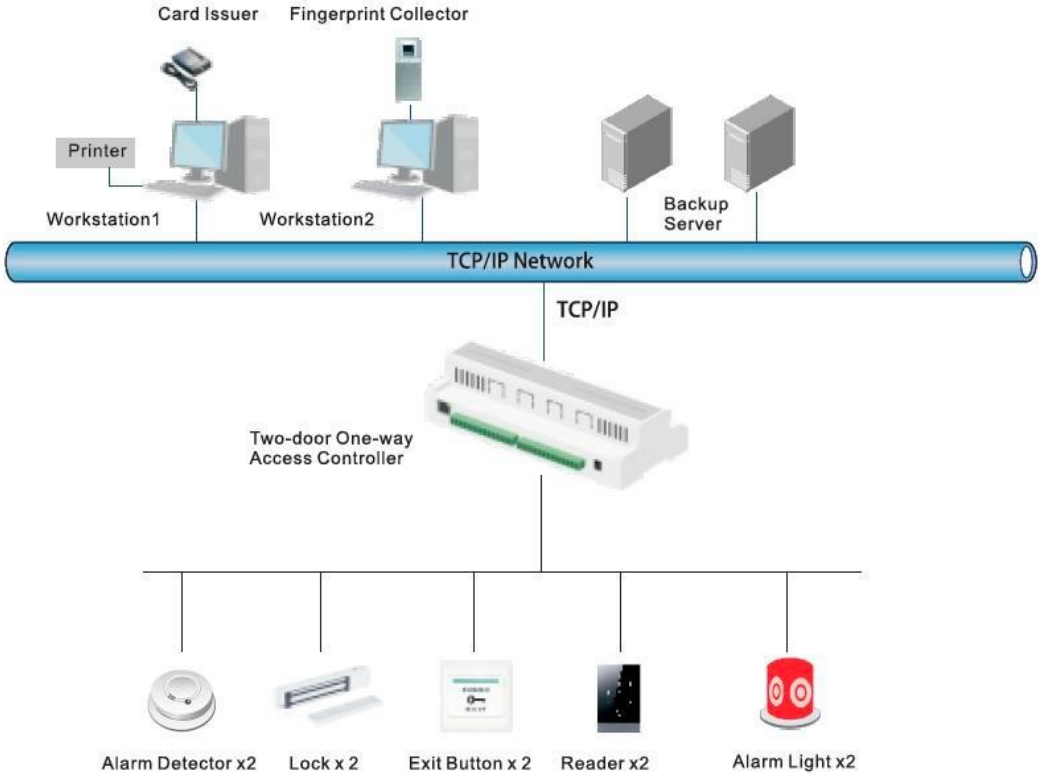


2. INSTALAČNÍ PŘÍRUČKA

2.1 STRUKTURA SYSTÉMU

Struktura dvoudveřového jednosměrného přístupového ovladače, dveřního zámku a čtecího systému je znázorněna na obrázku 2-1.

Obrázek 2-1



2.2 INSTALACE ZAŘÍZENÍ

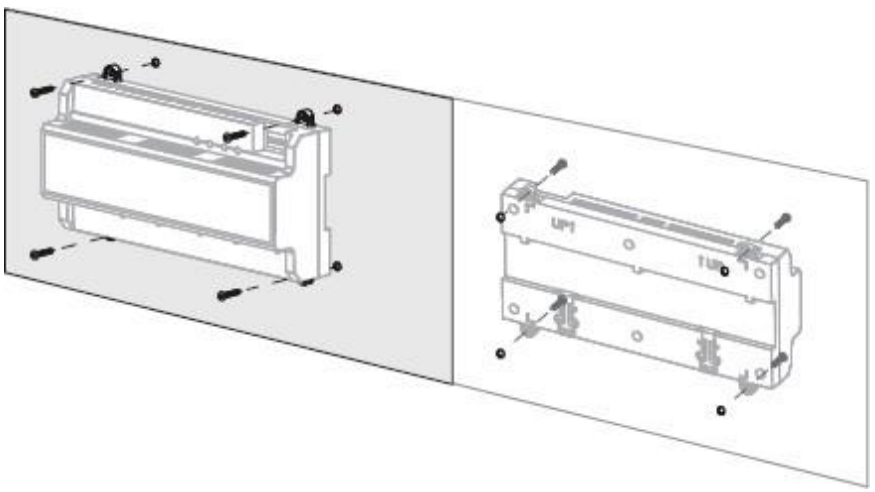
Existují dva způsoby instalace.

- Metoda 1: Připevněte celé zařízení ke stěně pomocí šroubů.
- Metoda 2: Pomocí vodicí lišty ve tvaru písmene U zavěste celé zařízení na stěnu (metoda 2 je volitelná montáž).

METODA 1

Instalační schéma je znázorněné na obrázku 2-2.

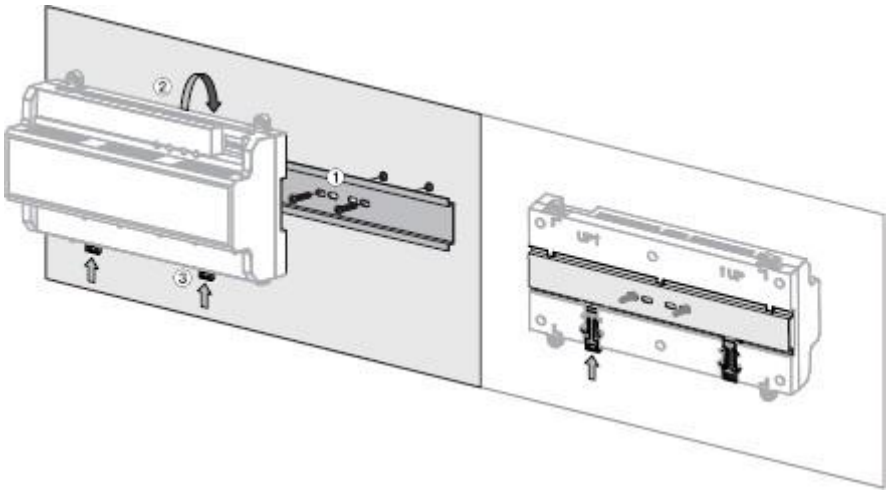
Obrázek 2-2



METODA 2

Instalační schéma je znázorněné na obrázku 2-3.

Obrázek 2-3

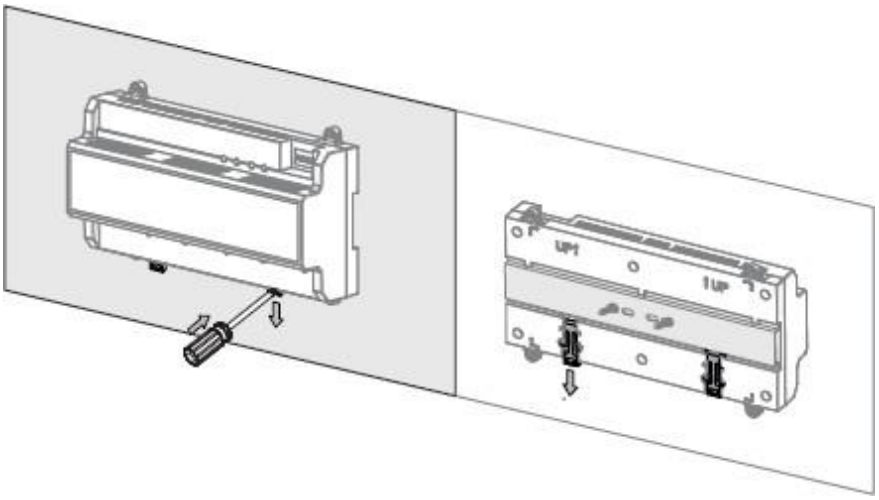


Krok 1 Připevněte vodicí lištu ve tvaru písmene U ke stěně pomocí šroubů.
Krok 2 Upevněte horní část zadní části zařízení v horním rohu vodicí lišty ve tvaru písmene U .
Krok 3 Stiskněte konektor snap v dolní části zařízení nahoru. Instalace je dokončena, když uslyšíte zvuk kliknutí.

2.3 ODSTRANĚNÍ

Pokud je zařízení nainstalováno v režimu 2, musí být demontováno podle obrázku 2-4. Přiložte šroubovák na snap konektor, stiskněte jej a konektor snap vyskočí, aby bylo možné celé zařízení hladce rozebrat.

Obrázek 2-4

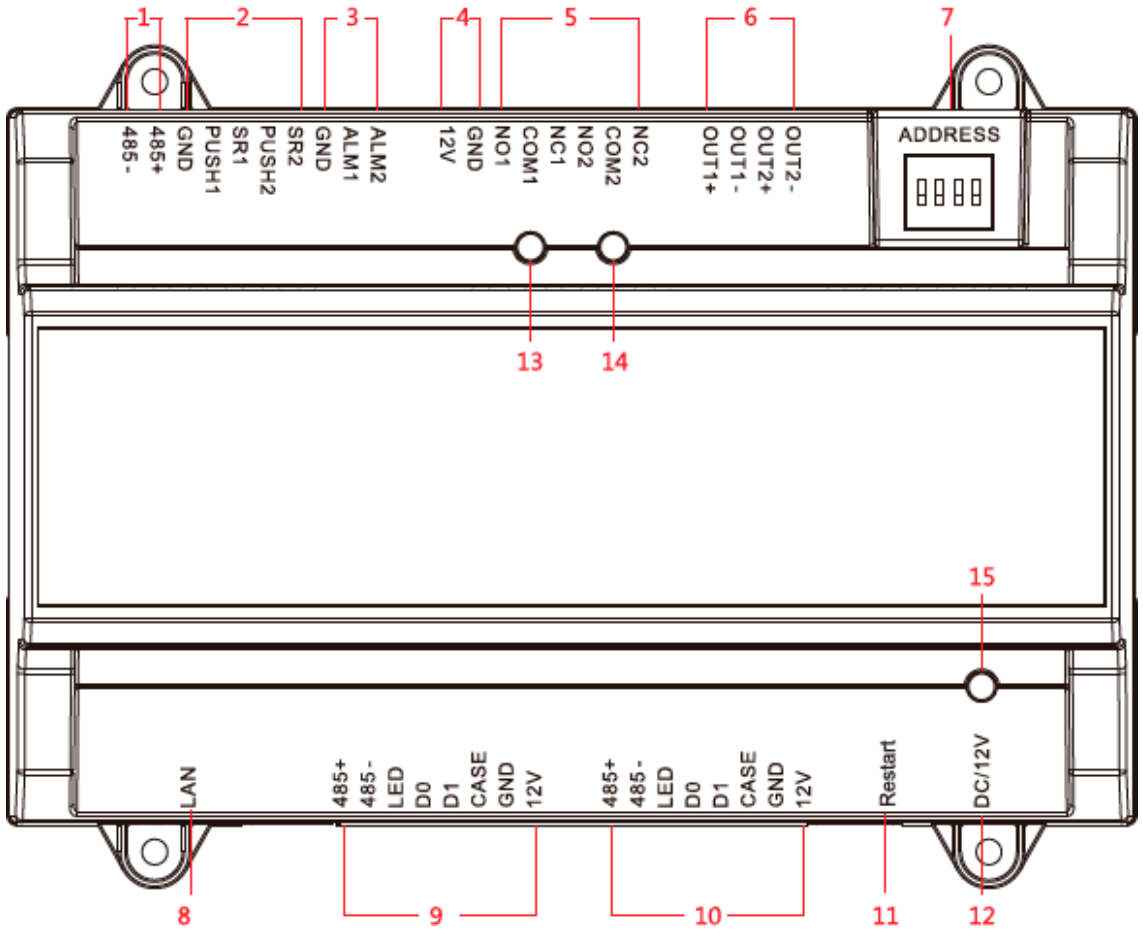


2.4 SCHÉMA ZAPOJENÍ

2.4.1 POPIS ZAPOJENÍ PŘÍSTUPOVÉHO ŘADIČE

Toto zařízení podporuje dvoudveřový jednosměrný vstup nebo výstup. Pro vstup alarmu aktivujte externí výstupní zařízení, aby se alarm rozezněl. Schéma zapojení zařízení je znázorněno na obrázku 2-5.

Obrázek 2-5



Rozhraní jsou popsána v tabulce 2-1.

Tabulka 2-1

Číslo	Popis portu	Číslo	Popis portu
1	Komunikace RS485	7	Přepínač DIP
2	Tlačítko Výstup a dveřní kontakt	8	Protokol TCP/IP
3	Externí alarmový vstup	9	Čtečka dveří 1
4	Uzamknout výstup napájecího zdroje	10	Dveřní čtečka 2
5	Výstup ovládání zámku	11	Restartovat
6	Výstup alarmu	12	12VDC

Ovládací prvky jsou popsány v tabulce 2-2.

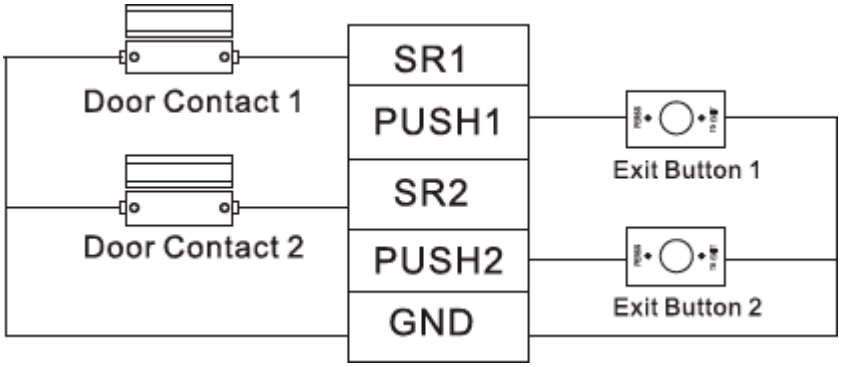
Tabulka 2-2

Číslo	Popis portu
13	Stav indikátoru zámku dveří
14	
15	LED indikátor napájení

2.4.2 POPIS ZAPOJENÍ DVEŘNÍHO TLAČÍTKA VEN/KONTAKTNÍHO TLAČÍTKA

Odpovídající připojení kabeláže výstupního tlačítka a dveřního kontaktu je znázorněno na obrázku 2-6. Popisy připojovacích vodičů jsou uvedeny v tabulce 2-3.

Obrázek 2-6



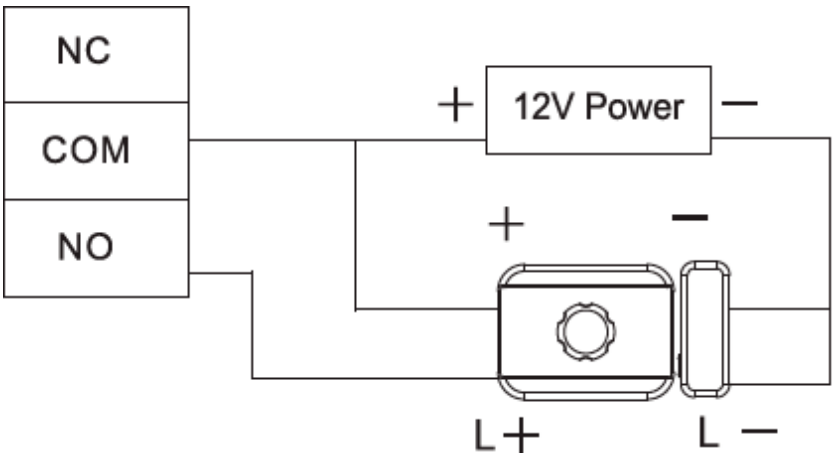
Tabulka 2-3

Port	Kabeláž	Popis
Tlačítko Výstup a dveřní kontakt	SR1	Kontaktní vstup pro dveře 1
	PUSH 1	Tlačítko pro výstup dveří 1
	SR2	Kontaktní vstup pro dveře 2
	PUSH2	Tlačítko výstupu dveří 2
	GND	Sdíleno výstupním tlačítkem , vstup dveřního kontaktu I RS485

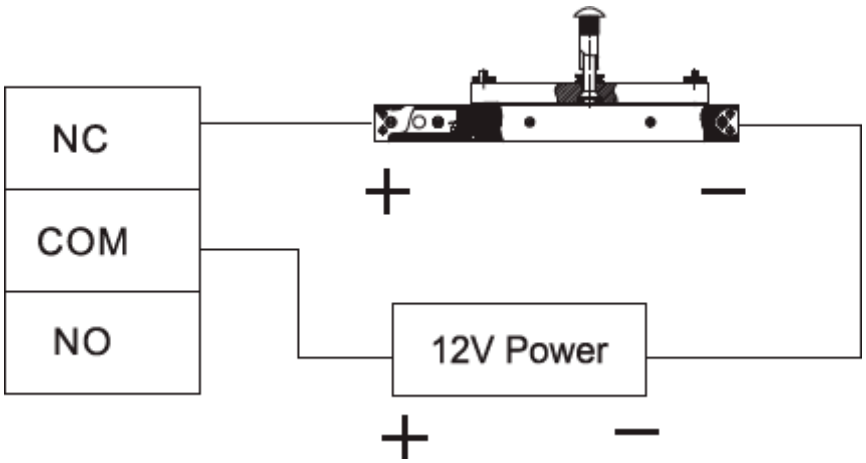
2.4.3 POPIS ZAPOJENÍ ZÁMKU

Podpora 2 skupin výstupů ovládání zámku, sériová čísla po připojení znamenají odpovídající dveře. Vezměte příslušný režim připojení podle typu zámku, jak je znázorněno na obrázku 2-7, obrázku 2-8 a obrázku 2-9. Popisy připojovacích vodičů naleznete v Tabulce 2-4.

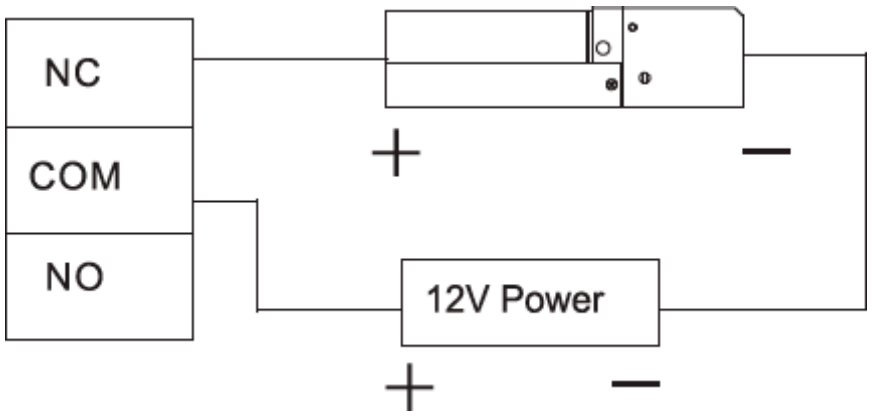
Obrázek 2-7



Obrázek 2-8



Obrázek 2-9



Tabulka 2-4

Port	Kabeláž	Popis
Řídicí port zámku výstupu	NC1	Kontrola zámku dveří 1
	COM1	
	NO. 1	
	NC2	Kontrola zámku dveří 2
	COM2	
	NO. 2	

2.4.4 POPIS ZAPOJENÍ ČTEČKY

Jedny dveře podporují pouze jeden typ čtečky – RS485 nebo Wiegand.

Popis zapojení čteček naleznete v tabulce 2-5. Vezměme si jako příklad dveře 1, ostatní čtečky jsou stejné. Popis specifikací a délky kabelu čtečky naleznete v tabulce 2-6.

Tabulka 2-5

Port	Kabeláž	Barva kabelu	Popis
Vstup dveřní čtečky 1	485+	Fialový	RS485
	485-	Žlutý	
	LED	Hnědý	Moderátor
	D0	Zelený	
	D1	Bílý	
	CASE	Modrý	
	GND	Černý	Napájecí zdroj čtečky
	12 voltů	Červený	

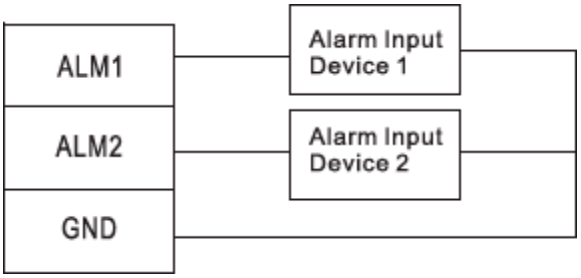
Tabulka 2-5

Druh	Typ připojení	Délka
RS485485	Síťový kabel CAT5e	100 m
Moderátor	Síťový kabel CAT5e	100 m

2.4.5 POPIS ZAPOJENÍ EXTERNÍHO ALARMOVÉHO VSTUPU

2 kanálový vstup externího alarmu je zobrazen na obrázku 2-10. Popisy připojovacích vodičů jsou uvedeny v tabulce 2-7.

Obrázek 2-10



Tabulka 2-7

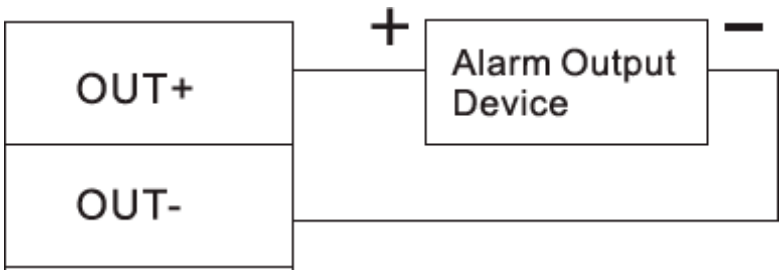
Port	Kabeláž		Popis
Externí alarmový vstup	ALM1	Vstupní port alarmu 1	Prostřednictvím externích vstupních portů alarmu můžeme připojit detektor kouře, infračervený detektor atd.
	ALM2	Vstupní port alarmu 2	
	GND	Sdíleno přes alarmový vstupní port 1 a 2	

Externí alarm může kombinovat stav otevírání a zavírání dveří.
- ALM1 spojuje všechny dveře pro normální otevírání.
- ALM2 spojuje všechny dveře pro normální zavírání.

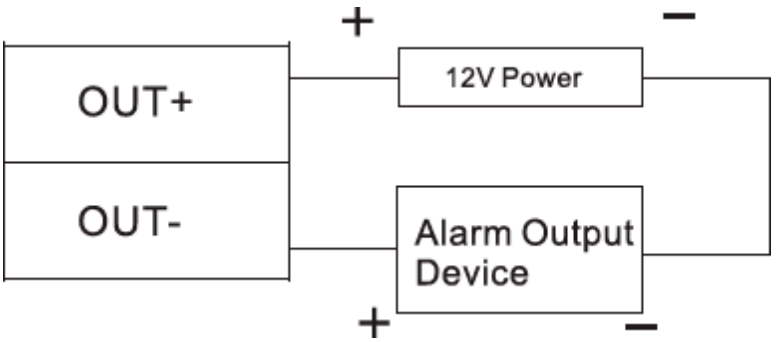
2.4.6 POPIS ZAPOJENÍ EXTERNÍHO ALARMOVÉHO VÝSTUPU

Existují dva způsoby, jak připojit externí alarmový výstup, v závislosti na poplašném zařízení. Například IPC může použít režim 1, zatímco zvuková a vizuální poplach může použít druhý způsob, jak je znázorněno na obrázcích 2-11 a 2-12. Popisy zapojení jsou uvedeny v tabulce 2-8.

Obrázek 2-11



Obrázek 2-12



Tabulka 2-8

Číslo	Popis portu		Popis portu
Externí alarmový výstup	OUT1+	ALM1 spustí alarmový výstup. • Výstup alarmu při překročení časového limitu dveří a signály vniknutí dveří 1. • Výstup alarmu neoprávněné manipulace dveřní čtečky 1.	Interní a externí výstupní porty alarmu mohou kombinovat zvukové a vizuální poplachy.
	OUT1-		
	OUT2+	ALM2 spustí alarmový výstup. • Výstup alarmu o překročení časového limitu dveří a signalizaci vloupání do dveří 2. • Výstup alarmu neoprávněné manipulace dveřní čtečky 2.	
	OUT2-		

2.4.7 POPIS PRINCIPU VSTUPU A VÝSTUPU ALARMU

V případě poplachu alarm trvá 15 sekund. Podrobné informace o alarmových vstupech a výstupech naleznete v tabulce 2-9.

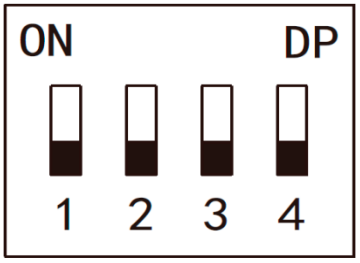
Tabulka 2-9

Typ alarmu	Vstupní port alarmu	Výstupní port alarmového signálu	Stav alarmu
Externí alarmový vstup	ALM1	VÝST UP1	Spojuje všechny dveře tak, aby byly normálně otevřené.
	ALM2	VÝST UP2	Spojuje všechny dveře tak, aby byly normálně zavřené.
Interní alarmový vstup	SR1	VÝST UP1	Alarm časového limitu dveří a vloupání spustí externí poplach.
	SR2	VÝST UP2	
	RS-485/POUZDRO	VÝST UP1	Alarm neoprávněné manipulace čtečkou spustí externí alarm.
	RS-485/POUZDRO	VÝST UP2	

2.5 DIP SPÍNAČ

Ovládání pomocí DIP spínače.

Obrázek 2-13



- Spínač je v poloze ON, což znamená 1.
- Spínač je v poloze OFF, což znamená 0.
- 1 ~ 4 všechny jsou nastaveny na 0. Systém se spustí normálně.
- 1 ~ 4 jsou nastaveny na 1. Systém po zavedení přejde do režimu BOOT.
- 1, 3 jsou nastaveny na 1, zatímco zbytek je nastaven na 0. Po restartu se systém obnoví na tovární nastavení.
- 2.4 jsou nastaveny na 1, zatímco zbytek je nastaven na 0. Po restartování systém obnoví tovární nastavení, ale informace o uživatelích jsou zachovány.

2.6 RESTARTOVAT

Zasuňte jehlu do otvoru pro restartování a jedním stisknutím zařízení restartujte.

Tlačítko Restartovat se používá k restartování zařízení, nikoli ke změně konfigurace.

3. KONFIGURACE SMART PSS

Pro zajištění kontroly a správné konfigurace jedněch dveří nebo skupiny dveří je přístupový řadič spravován prostřednictvím klienta Smart PSS. Tato kapitola popisuje především rychlé nastavení. Podrobné informace o provozu naleznete v zákaznické příručce Smart PSS.

Klient Smart PSS nabízí různé porty pro různé verze. Podívejte se prosím na skutečný port.

3.1 LOGOVÁNÍ KLIENTA

Nainstalujte odpovídajícího klienta PSS Smart Client a dvojitým kliknutím jej spusťte. Proveďte konfiguraci inicializace podle výzev rozhraní a dokončete přihlášení.

3.2 PŘIDÁNÍ ŘÍZENÍ PŘÍSTUPU

Přidejte do systému Smart PSS řadič přístupu. Vyberte "Automatické vyhledávání" a "Přidat".

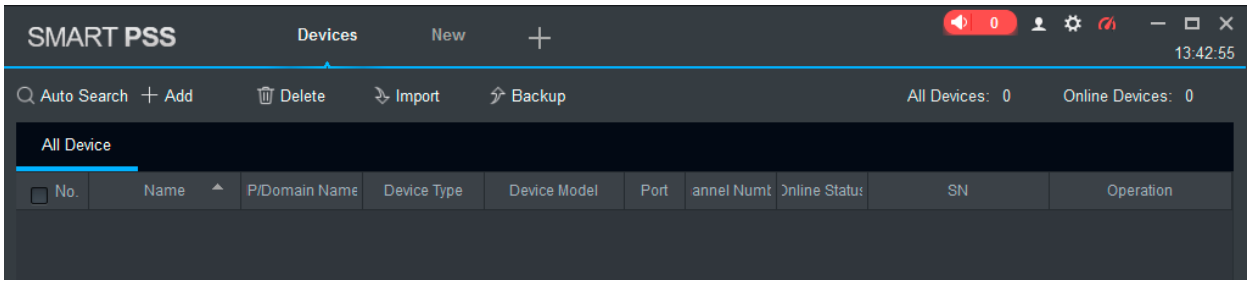
3.2.1 AUTOMATICKÉ VYHLEDÁVÁNÍ

Zařízení musí být ve stejném segmentu sítě .

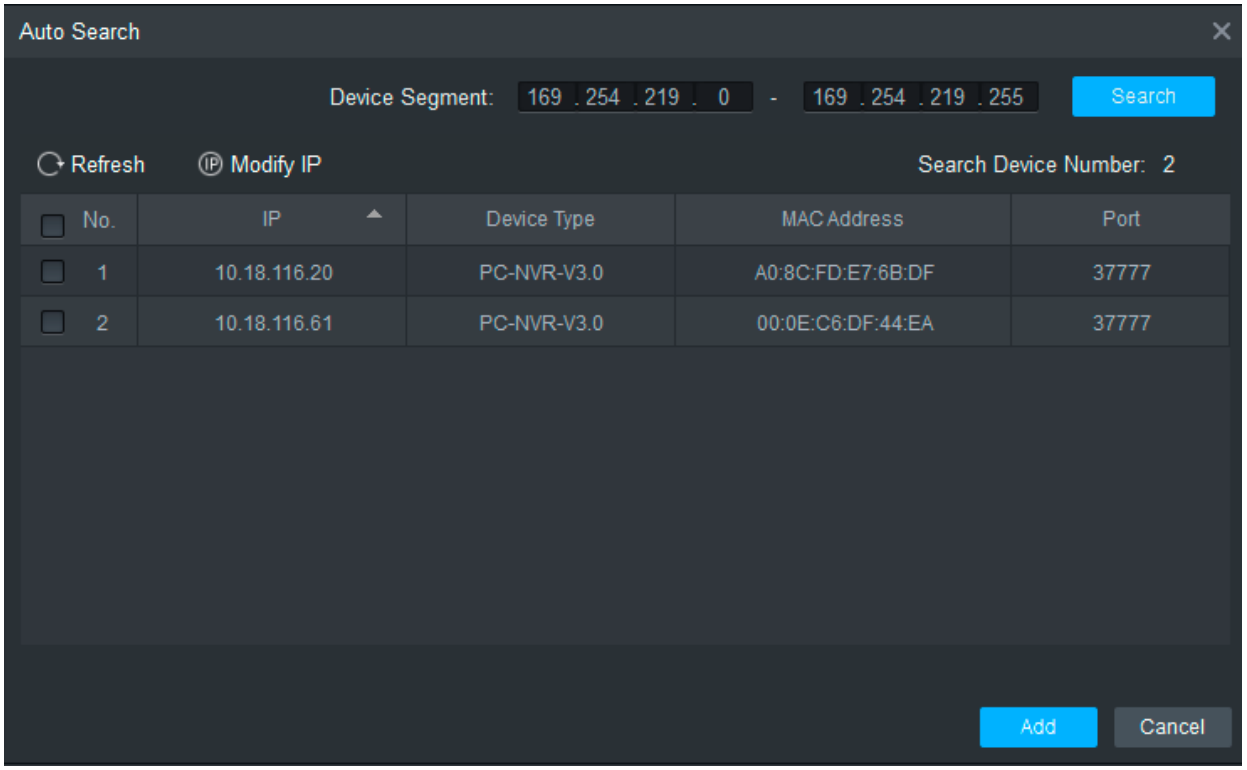
Krok 1. V rozhraní "Zařízení" klikněte na "Automatické vyhledávání", jak je znázorněno na obrázku 3-1.

Systém zobrazí rozhraní "Automatické vyhledávání", jak je znázorněno na obrázku 3-2.

Obrázek 3-1



Obrázek 3-2



Krok 2. Zadejte segment, ve kterém se zařízení nachází, a klikněte na "Hledat".

Systém zobrazí výsledky vyhledávání.

- Kliknutím na tlačítko "Obnovit" aktualizujete informace o zařízení.
- Vyberte zařízení, klikněte na "Upravit IP" a upravte IP adresu zařízení. Podrobné informace o provozu naleznete v zákaznické příručce Smart PSS

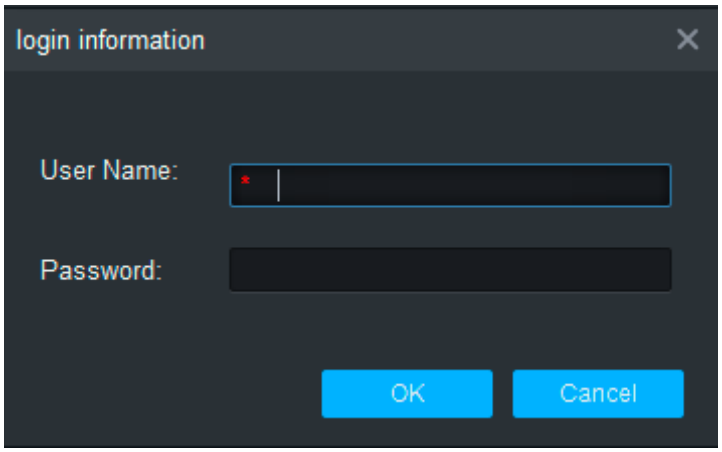
Krok 3. Vyberte zařízení, které chcete přidat, a klikněte na "Přidat".

Systém zobrazí "Monitoruj"

Krok 4. Klikněte na "OK".

Systém zobrazí dialogové okno "Přihlašovací údaje", jak je znázorněno na obrázku 3-3.

Obrázek 3-3

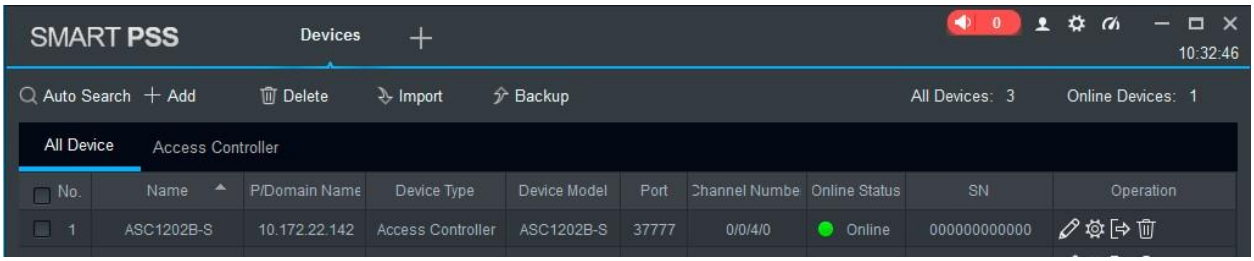


Krok 5 Zadejte "Uživatelské jméno" a "Heslo", přihlaste se do zařízení a klikněte na "OK".

Systém zobrazí seznam přidaných zařízení, jak je znázorněno na obrázku 3-4. Podrobnosti viz tabulka 3-1 .

- Po dokončení přidání zůstává systém stále v rozhraní "Automatické vyhledávání". Můžete pokračovat v přidávání dalších zařízení nebo kliknutím na "Zrušit" ukončit rozhraní "Automatické vyhledávání".
- Po dokončení přidání se Smart PSS automaticky přihlásí k zařízení. V případě úspěšného přihlášení se stav zařízení změní na "Online". V opačném případě se zobrazí "Offline".

Obrázek 3-4



Tabulka 3-1

Ikona	Popis
	Kliknutím na tuto ikonu přejdete do rozhraní "Upravit zařízení" a upravíte informace o zařízení, včetně názvu zařízení, IP adresy / názvu domény, portu, uživatelského jména a hesla. Nebo dvojitým kliknutím na zařízení přejděte do rozhraní "Upravit zařízení"
	Kliknutím na tuto ikonu přejdete do rozhraní "Konfigurace zařízení" a nakonfigurujete kameru zařízení, síť, událost, paměť a systémové informace.
	• Když je zařízení online, ikona je . Kliknutím na tuto ikonu ukončíte přihlášení a ikona se změní na . • Když je zařízení offline, ikona je . Kliknutím na tuto ikonu se přihlaste (s platnými informacemi o zařízení) a ikona se změní na .
	Kliknutím na tuto ikonu odeberete zařízení.

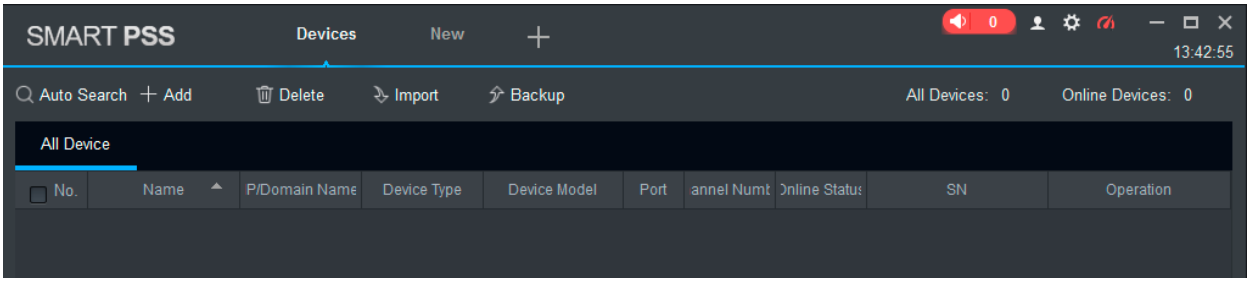
3.2.2 PŘIDAT RUČNĚ

Chcete-li přidat zařízení, musíte nejprve znát IP adresu zařízení nebo název domény.

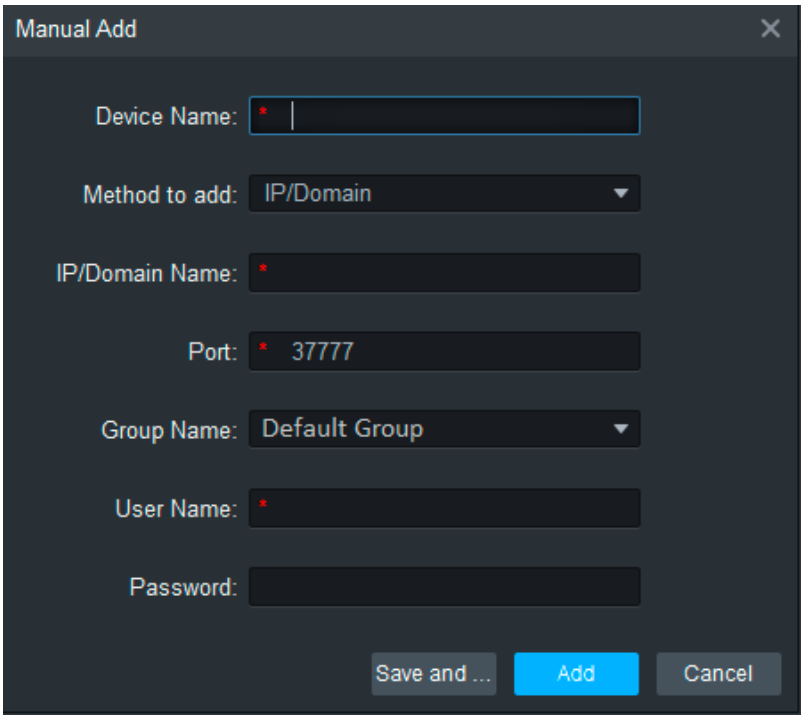
Krok 1. V rozhraní "Zařízení" klikněte na "Přidat", jak je znázorněno na obrázku 3-5.

Systém zobrazí rozhraní "Ruční přidání", jak je znázorněno na obrázku 3-6.

Obojek 3-5



Obrázek 3-6



Krok 2 Nastavte parametry zařízení. Podrobné popisy parametrů jsou uvedeny v tabulce 3-2.

Tabulka 3-2

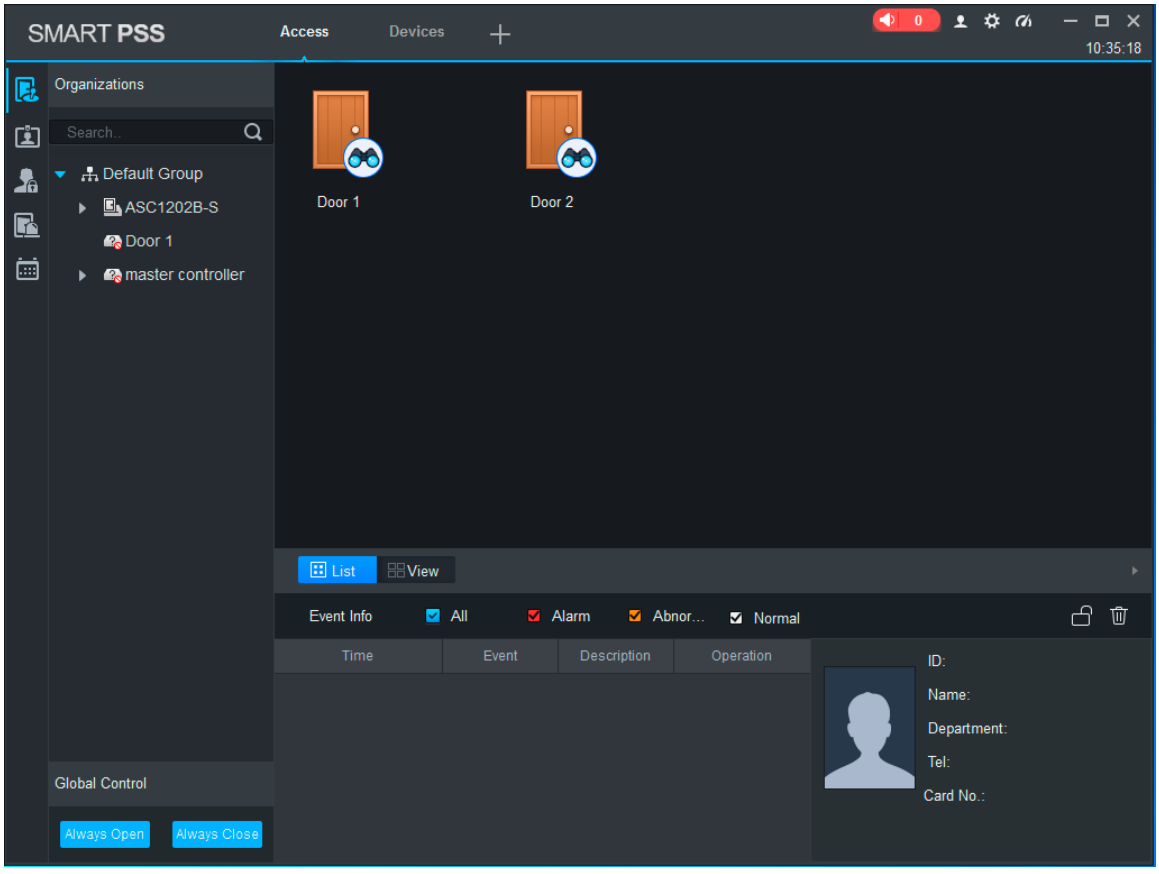
Parametr	Popis
Název zařízení	Doporučuje se, aby se název zařízení nazýval monitorovací zónu pro usnadnění údržby.
Způsob přidání	Vyberte "IP/Domain Name". Přidejte zařízení podle IP adresy nebo názvu domény zařízení.
IP/ název domény	IP adresa nebo název domény zařízení.
Port	Číslo portu zařízení. Výchozí číslo portu je 37777. Vyplňte prosím dle aktuálních podmínek.
Název skupiny	Vyberte skupinu zařízení .
Uživatelské jméno a heslo	Uživatelské jméno a heslo zařízení.

Krok 3. Kliknutím na "Přidat" přidáte zařízení.

Systém zobrazí seznam přidaných zařízení, jak je znázorněno na obrázku 3-7. Podrobnosti viz tabulka 3-2. Přidané dveře do ovladače se zobrazí na kartě "Přístup", jak je znázorněno na obrázku 3-8.

- Chcete-li přidat další zařízení, klikněte na "Uložit a pokračovat", přidejte zařízení a zůstaňte v rozhraní "Ruční nahrávání".
- Chcete-li zrušit přidávání, klikněte na "Zrušit" a ukončete rozhraní "Ruční přidání".
- Po dokončení přidání se Smart PSS automaticky přihlásí do zařízení v případě úspěšného přihlášení, stav se zobrazí "Online". V opačném případě se zobrazí "Offline".

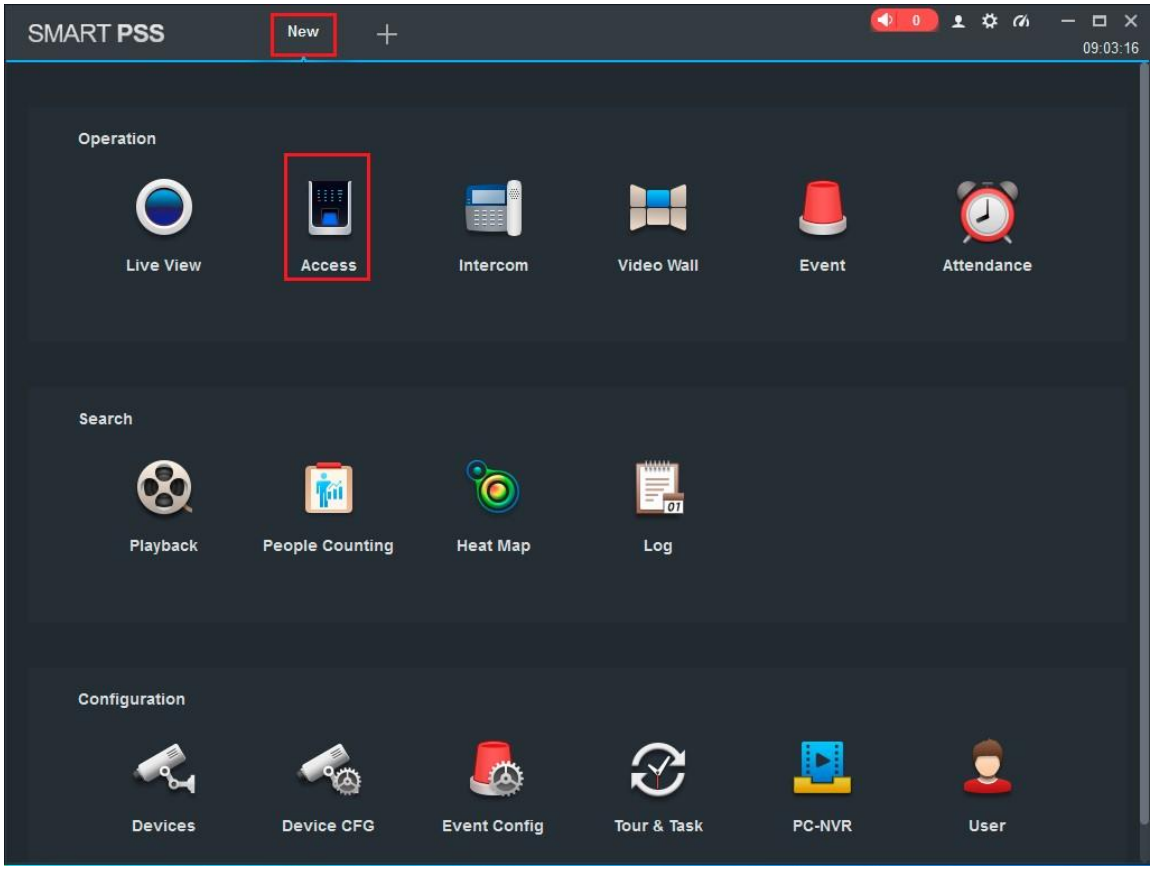
Obrázek 3-7



3.3 PŘIDÁNÍ UŽIVATELE

Přidejte uživatele a odkaz na karty pro distribuci oprávnění .
V rozhraní "Nový" klikněte na "Přístup" a přejděte do rozhraní "Přístup" a dokončete nastavení přístupu zde.

Obrázek 3-8

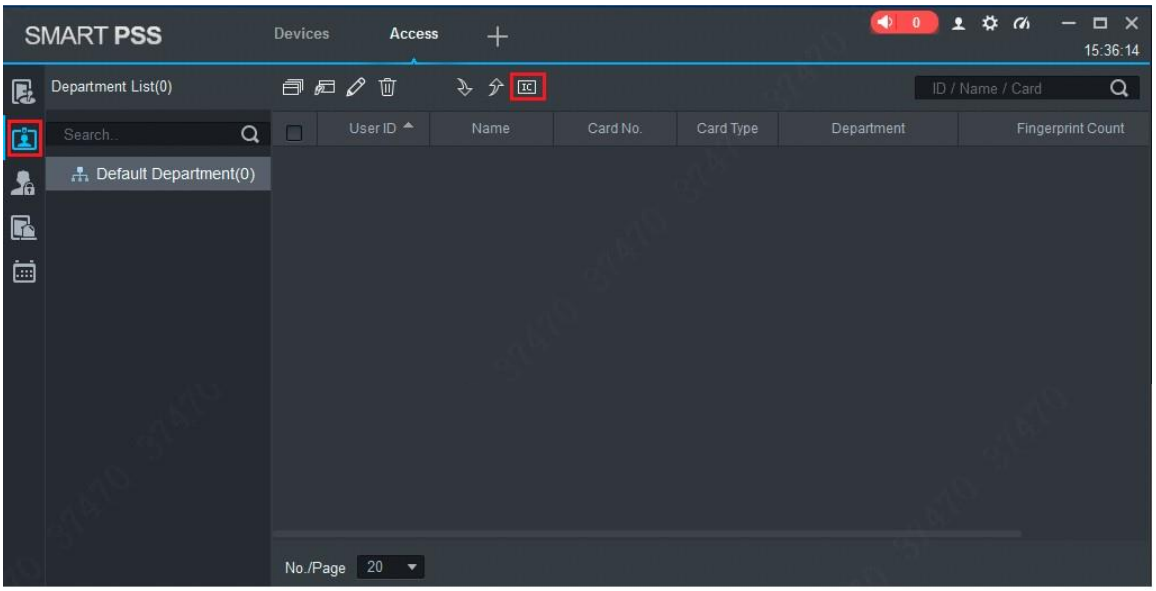


3.3.1 TYP KARTY

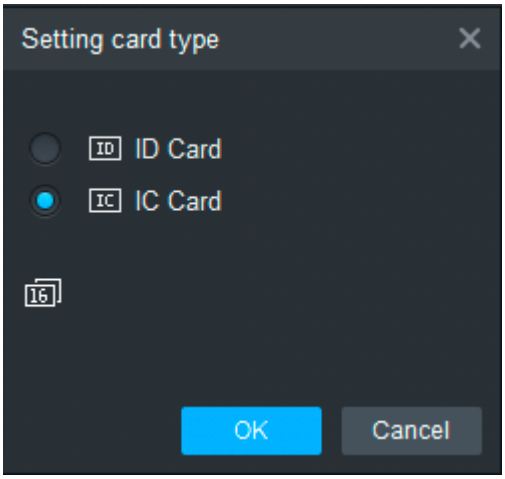
POZNÁMKA!
Typ karty je stejný jako u vydavatele karty, jinak nebude číst číslo karty.

V rozhraní "Přístup" klikněte a poté kliknutím nastavte typ karty, jak je znázorněno na obrázku 3-9 a obrázku 3-10.

Obrázek 3-9



Obrázek 3-10

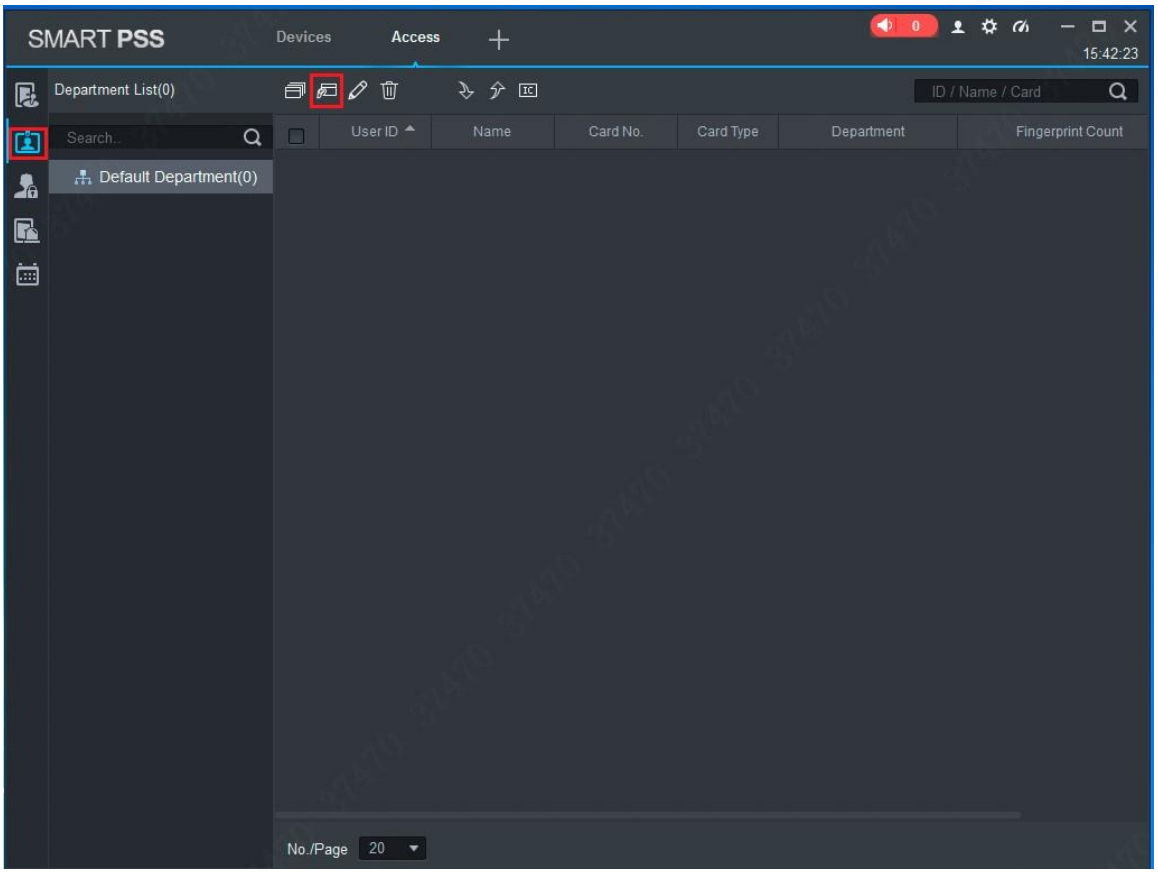


3.3.2 JEDNORÁZOVĚ PŘÍDÁNÍ

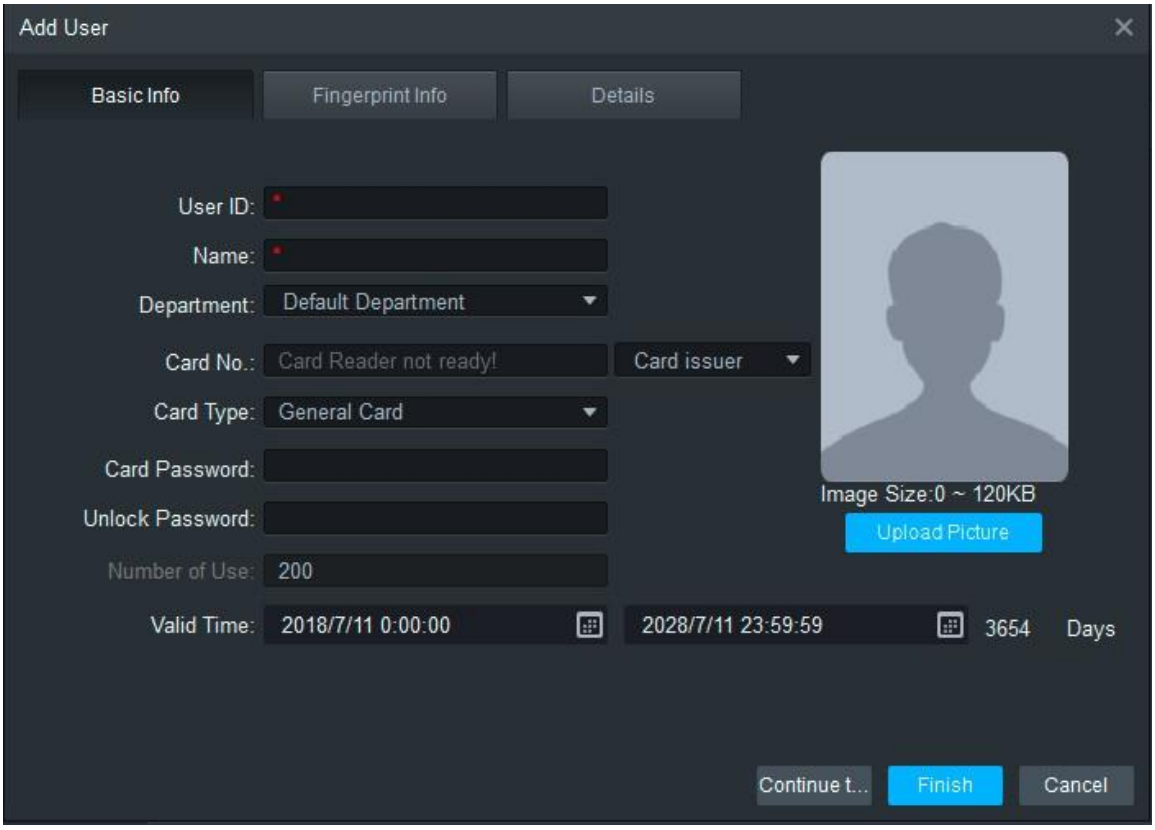
Přidejte jednoho uživatele, zadejte kartu a informace o uživateli .

Krok 1 V rozhraní "Přístup" klikněte na , poté klikněte na , jak je znázorněno na obrázku 3-11. Systém zobrazí dialogové okno "Přidat uživatele", jak je znázorněno na obrázku 3-12.

Obrázek 3-11



Obrázek 3-12



Krok 2 Přidejte informace o uživateli ručně, včetně základních informací o otiscích prstů a podrobností. Podrobnosti viz tabulka 3-3.

Tabulka 3-3

Parametr	Popis
Základní informace	ID uživatele (povinné). • Jméno a příjmení (povinné). • Oddělení (automatické párování). • Číslo karty: Zadáno čtečkou karet nebo zadáno ručně. • Typ karty: Obecná karta, VIP karta, karta hosta, hlídková karta, karta černé listiny a karta donucení. • Heslo karty: Používá se k otevření dveří kartou + heslem. • Odemknout heslo: Používá se k otevření dveří heslem. • Počet použití: Platí pouze pro kartu hosta. • Důležitý čas: Nastavte dobu trvání přístupu, která je ve výchozím nastavení 10 let. • Fotografie: Uživatelská fotografie, maximálně 120K. Číslo karty a ID uživatele nelze opakovat.
Informace o otiscích prstů	Sbírejte otisky prstů pomocí čtečky otisků prstů a přístupové čtečky. • Maximálně 2 otisky prstů na osobu. • Pomoc se zadáním názvu otisku prstu.
Podrobnosti	Poskytněte podrobné informace o uživateli podle parametrů rozhraní.

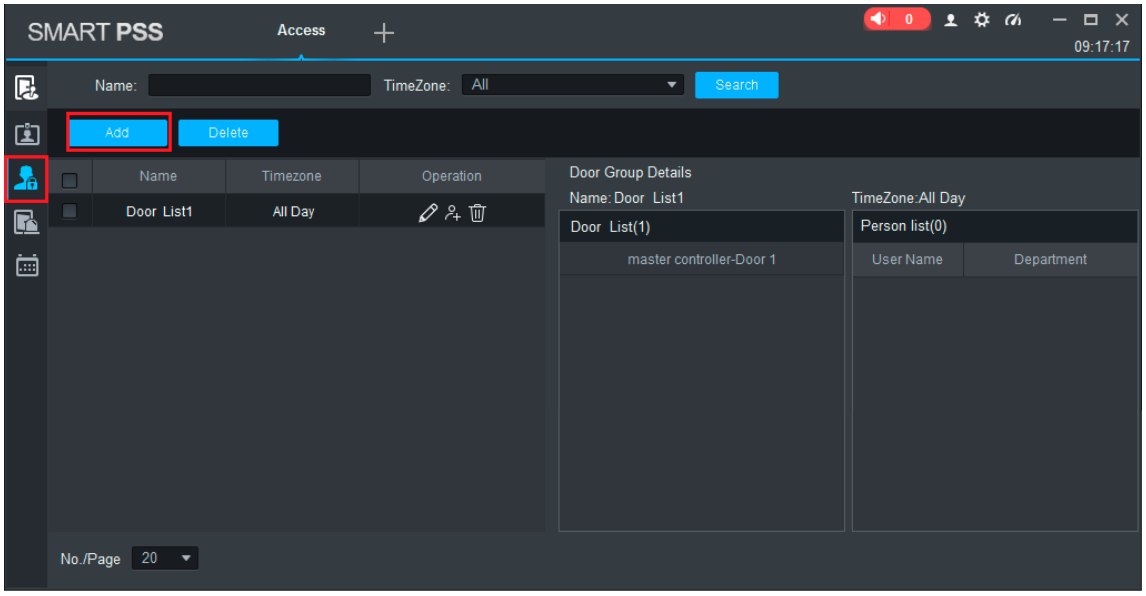
Krok 3. Kliknutím na "Dokončit" dokončíte přidávání uživatelů.

3.4 PŘIDÁNÍ SKUPINY DVEŘÍ

Rozdělte dveře do skupin a spravujte je společně.

Krok 1. V rozhraní "Přístup" klikněte a poté klikněte na "Úroveň přístupu", jak je znázorněno na obrázku 3-13.

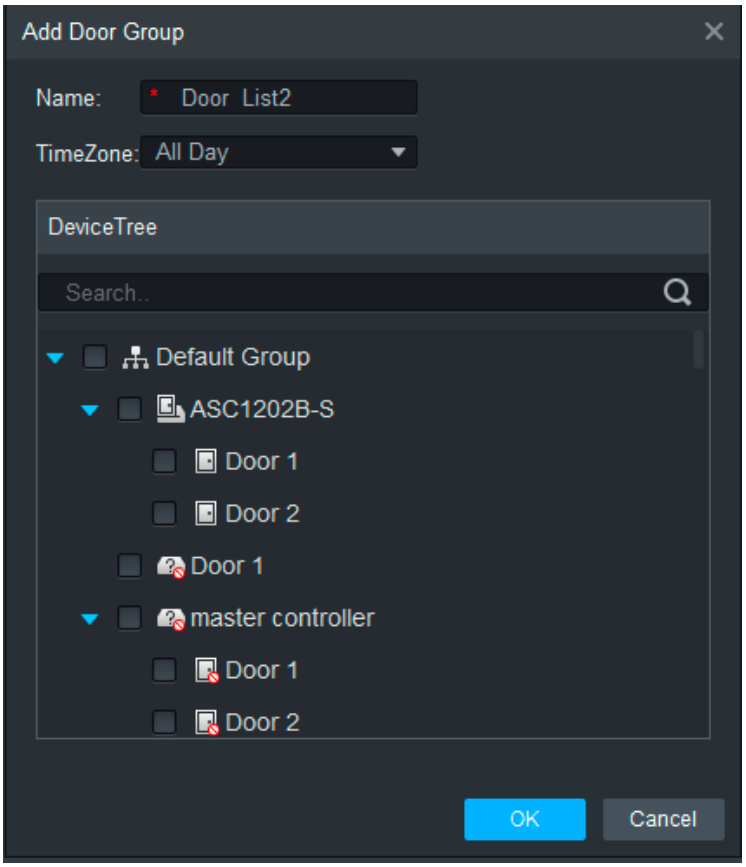
Obrázek 3-13



Krok 2 Klikněte na "Přidat".

Systém zobrazí dialogové okno "Přidat skupinu dveří", jak je znázorněno na obrázku 3-14.

Obrázek 3-14



Krok 3 Zadejte "Název", vyberte "Časové pásmo" a dveře, které chcete spravovat.

Krok 4 Kliknutím na "OK" dokončete přidávání.

3.5 OPRÁVNĚNÍ

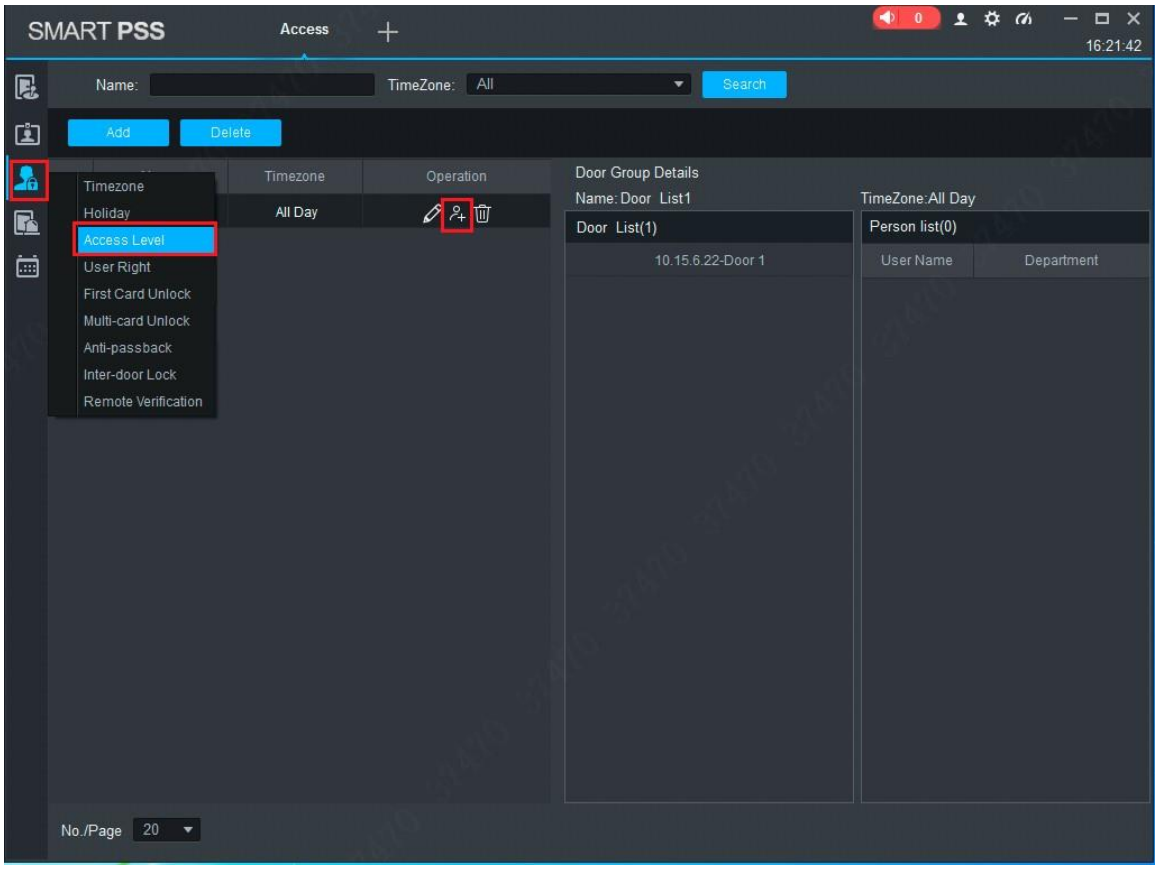
Udělte oprávnění uživatelům podle skupiny dveří a uživatele.

3.5.1 AUTORIZACE PODLE SKUPINY DVEŘÍ

Vyberte skupinu dveří a přidejte do skupiny příslušné uživatele, aby všichni uživatelé ve skupině měli oprávnění ke všem dveřím ve skupině.

Krok 1. V rozhraní "Přístup" klikněte a poté klikněte na "Úroveň přístupu", jak je znázorněno na obrázku 3-15.

Obrázek 3-15

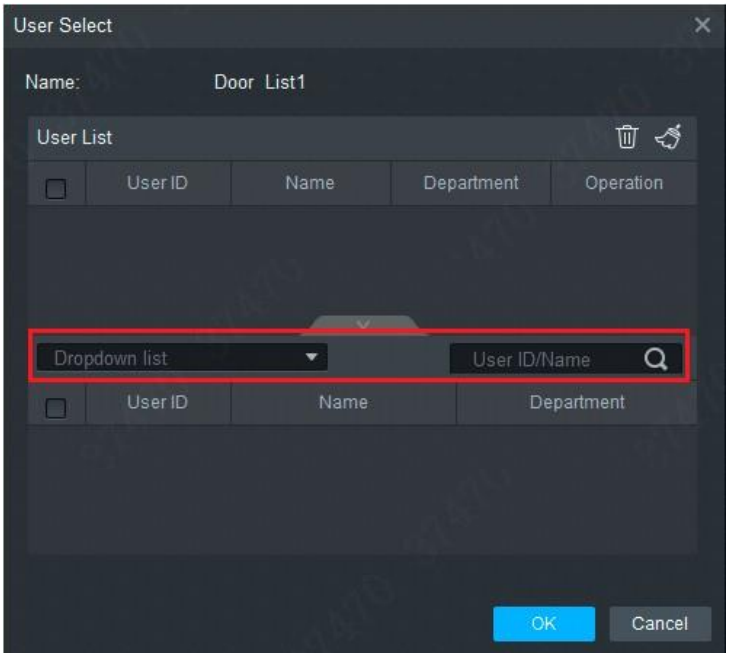


Krok 2. Klepněte na tlačítko .

Systém zobrazí dialogové okno "Výběr uživatele".

Krok 3. Z rozevíracího seznamu vyberte uživatelské oddělení nebo zadejte ID uživatele nebo jméno přímo, jak je znázorněno na obrázku 3-16.

Obrázek 3-16



Krok 4. Ze seznamu vyhledávání vyberte uživatele a přidejte jej do seznamu uživatelů.

Krok 5. Kliknutím na tlačítko: OK." dokončete autorizaci.

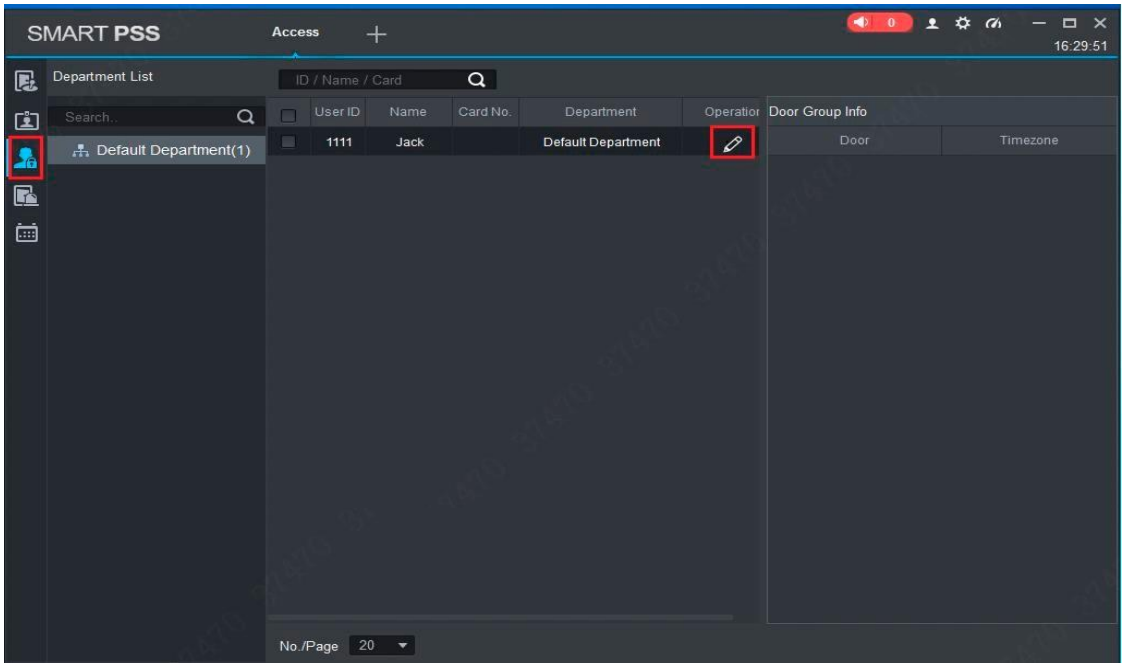
- Seznam hledání filtruje informace o uživateli bez čísla karty.
- V seznamu uživatelů zrušte uživatele, kterého jste přidali a odeberte jeho oprávnění.

3.5.2 AUTORIZACE UŽIVATELEM

Vyberte uživatele, oddělte skupinu dveří a udělte skupině dveří uživatele oprávnění .

Krok 1. V rozhraní "Přístup" klikněte a poté klikněte na "Uživatelská práva", jak je znázorněno na obrázku 3-17.

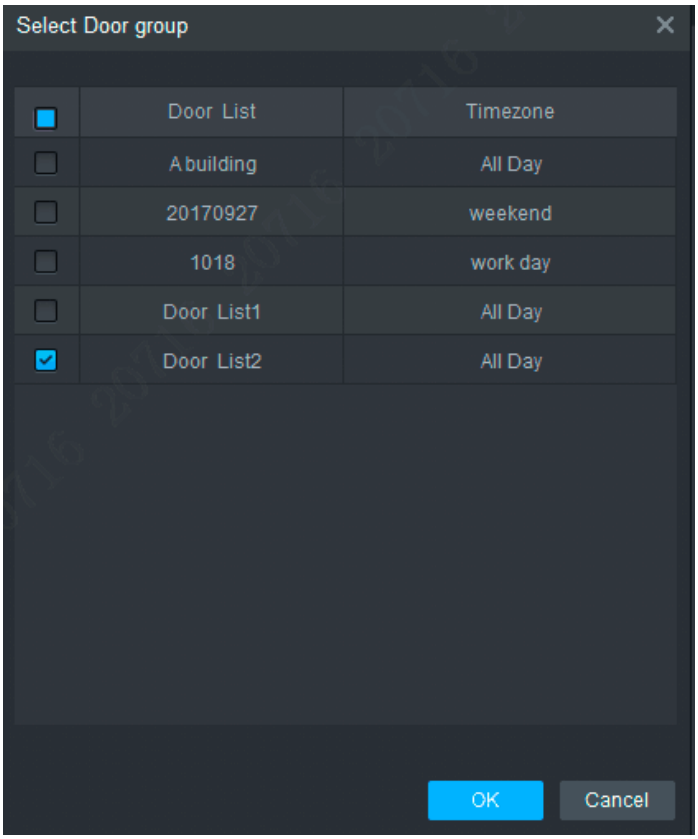
Obrázek 3-17



Krok 2 Kliknět .

Systém zobrazí dialogové okno "Vybrat skupinu dveří", jak je znázorněno na obrázku 3-18.

Obrázek 3-18



Krok 3 Vyberte skupinu dveří a kliknutím na "OK" dokončete autorizaci.

4. Často kladené dotazy

Pokud se na vás nevztahují problémy, které nejsou zahrnuty níže, obraťte se na místní pracovníky zákaznického servisu nebo zákaznického servisu v ústředí. Budeme vám vždy k dispozici.

1. **Otázka: Když je napájení zapnuto, indikátor napájení se nezapne nebo bzučák nereaguje.**

   Odpověď: Zkontrolujte, zda je zástrčka správně vložena. Vytáhněte ji a znovu vložte.

2. **Otázka: Při použití čtečky se zařízením se kontrolka přejetí karty nerozsvítí a nereaguje při přejetí karty.**

   Odpověď: Zkontrolujte, zda je konektor čtečky vložen na správném místě. Vytáhněte a znovu vložte, zkontrolujte, zda svítí kontrolka kontaktu čtenáře.

3. **Otázka: Software nerozpozná zařízení.**

   Odpověď: Zkontrolujte, zda je kabeláž správně připojena a zda je IP adresa zařízení ve stejném segmentu sítě.

4. **Otázka: Když je karta zobrazena, zobrazí se zpráva, že karta je neplatná.**

   Odpověď: Zkontrolujte, zda bylo toto číslo karty přidáno do ovladače.

5. **Otázka: Výchozí IP adresa řadiče přístupu.**

   Odpověď: Výchozí adresa IP je 192.168.0.2.

6. **Otázka: Výchozí port, uživatelské jméno a heslo řadiče přístupu .**

   Odpověď: Výchozí port je 37777, počáteční uživatelské jméno je admin a heslo je 123456.

7. **Otázka: Online aktualizace zařízení.**

   Odpověď: Připojte zařízení a počítač přes síť a aktualizujte jej na platformě .

8. **Otázka: Maximální vzdálenost zapojení a přenosová vzdálenost čtečky, karty a řadiče.**

   Odpověď : Záleží na typu síťového kabelu a na tom, zda vyžaduje napájení řídicího relé.

Připojeno síťovým kabelem CAT5E, typická hodnota je:

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

PŘÍLOHA 1 DOPORUČENÍ PRO KYBERNETICKOU BEZPEČNOST

Kybernetická bezpečnost je více než jen módní slovo: je to něco, co platí pro jakékoli zařízení připojené k internetu. Video dohled není imunní vůči kybernetickým hrozbám, ale přijetí základních kroků k ochraně a posílení sítí a síťových zařízení je učiní méně zranitelnými vůči útokům. Níže jsou uvedeny některé tipy a doporučení od BCS, jak vytvořit bezpečnější systém.

Povinná opatření, která mají být přijata k zajištění bezpečnosti základního síťového vybavení:

1. Používejte silná hesla

Podívejte se na následující návrhy pro nastavení hesla:

- Délka by neměla být kratší než 8 znaků;
- Zahrňte alespoň dva typy znaků, které zahrnují velká a malá písmena, čísla a symboly;
- Neobsahují název účtu ani název účtu v opačném pořadí;
- Nepoužívejte souvislé znaky, například 123, abc atd.;
- Nepoužívejte překrývající se znaky, jako je 111, aaa atd.;

2. Aktualizujte firmware a klientský software včas

- V souladu se standardním postupem doporučujeme aktualizovat hardwarový software (například NVR, DVR, IP kamera atd.), Aby bylo zajištěno, že váš systém je vybaven nejnovějšími bezpečnostními záplatami. Pokud je zařízení připojeno k veřejné síti, doporučujeme povolit "Automatická kontrola aktualizací" pro získání aktuálních informací o aktualizacích firmwaru vydaných výrobcem.
- Doporučujeme stáhnout a používat nejnovější verzi klientského softwaru.

Doporučení , která je třeba dodržovat , abyste zlepšili zabezpečení sítě vašeho zařízení:

1. Fyzická ochrana

Doporučujeme fyzicky chránit hardware, zejména paměťová zařízení. Umístěte například zařízení do speciální počítačové místnosti a skříně a implementujte dobře provedená oprávnění k řízení přístupu a správu klíčů, abyste zabránili neoprávněným osobám v navazování fyzických kontaktů, jako je poškození hardwaru, neoprávněné připojení vyměnitelných zařízení (jako je USB flash disk, sériový port) atd.

2. Pravidelně měňte své heslo

Doporučujeme pravidelně měnit hesla, abyste snížili riziko prolomení hesla.

3. Nastavení a aktualizace hesel , resetování informací včas

Zařízení podporuje funkci resetování hesla. Nakonfigurujte související informace pro čas resetování hesla, včetně poštovní schránky uživatele a otázek týkajících se ochrany heslem. Pokud se informace změní, upravte je prosím včas.

Při nastavování otázek týkajících se ochrany heslem se doporučuje nepoužívat ty, které lze snadno uhodnout.

4. Povolení uzamčení účtu

Funkce uzamčení účtu je ve výchozím nastavení povolena a doporučujeme ji povolit, aby bylo zaručeno zabezpečení vašeho účtu. Pokud se útočník pokusí přihlásit několikrát pomocí nesprávného hesla, odpovídající účet a zdrojová adresa IP budou zablokovány.

5. Změna výchozích portů HTTP a dalších portů služby

Doporučujeme změnit výchozí porty HTTP a další porty služeb na libovolnou sadu čísel od 1024 do 65535, což snižuje riziko, že vetřelci budou moci hádat, které porty používáte.

6. Povolení protokolu HTTPS

Doporučujeme povolit protokol HTTPS, abyste mohli navštívit internetovou službu prostřednictvím zabezpečeného komunikačního kanálu.

7. Povolit seznam povolených

Doporučujeme povolit funkci seznamu povolených, abyste zabránili všem kromě těch, kteří mají konkrétní IP adresy, v přístupu k vašemu systému. Proto nezapomeňte přidat IP adresu vašeho počítače a IP adresu doprovodného zařízení na seznam povolených.

8. Vazba MAC adresy

Doporučujeme přidružit IP adresu a MAC adresu hardwaru, což snižuje riziko falšování identity ARP.

9. Přiměřené přiřazení účtů a oprávnění

V souladu s obchodními požadavky a požadavky na správu přiměřeně přidejte uživatele a přiřaďte jim minimální sadu oprávnění.

10. Zakažte nepotřebné služby a vyberte možnost Nouzové režimy

V případě potřeby se doporučuje zakázat určité služby, jako jsou SNMP, SMTP, UPnP atd., Aby se snížilo riziko.

V případě potřeby se důrazně doporučuje používat bezpečné režimy, mimo jiné včetně následujících služeb:

- SNMP: Vyberte SNMP v3 a nakonfigurujte silná šifrovací hesla a ověřovací hesla.
- SMTP: Vyberte TLS pro přístup k poštovnímu serveru.
- FTP: Vyberte SFTP a nastavte silná hesla.
- AP: Vyberte režim šifrování WPA2-PSK a nakonfigurujte silná hesla.

11. Šifrovaný přenos zvuku a videa

Pokud je obsah zvukových a obrazových dat velmi důležitý nebo citlivý, doporučujeme použít funkci šifrovaného přenosu, aby se snížilo riziko krádeže dat během přenosu.
Připomenutí: Šifrovaný přenos bude mít za následek určitou ztrátu výkonu přenosu.

12. Bezpečné ovládání

- Kontrola uživatelů online: Doporučujeme pravidelně kontrolovat uživatele online, abyste zjistili, zda je na vaše zařízení nějaké přihlášení bez autorizace.
- Zkontrolujte protokol zařízení: Zobrazením protokolů můžete znát IP adresy, které byly použity k přihlášení k vašim zařízením a jejich klíčovým operacím.

13. Síťový protokol

Vzhledem k omezené kapacitě zařízení je uložený protokol omezen. Chcete-li zapisovat protokol po dlouhou dobu, doporučujeme povolit funkci síťového protokolu, abyste zajistili synchronizaci důležitých protokolů se serverem síťových protokolů pro trasování.

14. Vytvoření zabezpečeného síťového prostředí

Chcete-li lépe zajistit bezpečnost vašeho zařízení a snížit potenciální kybernetická rizika, doporučujeme:

- Zakažte funkci mapování portů směrovače, abyste zabránili přímému přístupu k intranálním zařízením z externí sítě.
- Síť by měla být rozdělena na části a izolována podle skutečných potřeb sítě. Pokud mezi těmito dvěma podsítěmi nejsou žádné požadavky na komunikaci, navrhuje použít VLAN, síť GAP a další technologie k rozdělení sítě, aby se dosáhlo účinku izolace sítě.
- Vytvořte systém ověřování přístupu 802.1x, abyste snížili riziko neoprávněného přístupu k privátním sítím.

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

Aktualizovaný: 08.04.2022