

Dvoudveřový Obousměrný přístup  
**Ovladač**

Uživatelský manuál






**V1.0.1**

## Všeobecné

Tento dokument se zabývá strukturou, instalací a zapojením dvoudveřového dvoucestného přístupového ovladače.

## Bezpečnostní instrukce

V příručce se mohou objevit následující kategorizovaná signální slova s definovaným významem.

Signální slova	Význam
 <b>DANGER</b>	Označuje vysoké potenciální nebezpečí, které, pokud se mu nevyhnete, bude mít za následek smrt nebo vážné zranění.
 <b>WARNING</b>	Označuje střední nebo nízké potenciální nebezpečí, které, pokud se mu nevyhnete, může vést k lehkému nebo středně těžkému zranění.
 <b>CAUTION</b>	Označuje potenciální riziko, které, pokud se mu nevyhnete, může mít za následek poškození majetku, ztrátu dat, nižší výkon nebo nepředvídatelný výsledek.
 <b>TIPS</b>	Poskytuje metody, které vám pomohou vyřešit problém nebo vám ušetří čas.
 <b>NOTE</b>	Poskytuje doplňující informace jako zdůraznění a doplnění textu.

## Oznámení o ochraně soukromí

Jako uživatel zařízení nebo správce údajů můžete shromažďovat osobní údaje jiných osob, jako je obličej, otisky prstů, SPZ auta, e-mailová adresa, telefonní číslo, GPS a tak dále. Musíte být v souladu s místními zákony a předpisy na ochranu soukromí, abyste chránili legitimní práva a zájmy jiných lidí prováděním opatření, která zahrnují mimo jiné: poskytnutí jasně a viditelné identifikace za účelem informování subjektu údajů o existenci sledované oblasti a poskytování souvisejících Kontakt.

## O manuálu

- Manuál je pouze orientační. V případě rozporu mezi příručkou a skutečným produktem má přednost skutečný produkt.
- Neneseme odpovědnost za žádné ztráty způsobené operacemi, které nejsou v souladu s
- Manuálem. Manuál by byl aktualizován podle nejnovějších zákonů a nařízení souvisejících regionů. Podrobné informace naleznete v tištěné uživatelské příručce, CD-ROM, QR kódu nebo na našich oficiálních stránkách. V případě rozporu mezi tištěnou Uživatelskou příručkou a elektronickou verzí má přednost elektronická verze.

- Všechny návrhy a software se mohou změnit bez předchozího písemného upozornění. Aktualizace produktu mohou způsobit určité rozdíly mezi skutečným produktem a manuálem. Kontaktujte prosím zákaznický servis pro nejnovější program a doplňkovou dokumentaci. Stále se mohou vyskytovat odchylky v technických datech, popisu funkcí a operací nebo chyby v tisku. Pokud existují nějaké pochybnosti nebo spory, podívejte se prosím na naše konečné vysvětlení. Pokud průvodce (ve formátu PDF) nelze otevřít, upgradujte software čtečky nebo vyzkoušejte jiný standardní software pro čtení.
- Všechny ochranné známky, registrované ochranné známky a názvy společností v příručce jsou majetkem příslušných vlastníků.
- Navštivte prosím naši webovou stránku, kontaktujte dodavatele nebo zákaznický servis, pokud se při používání zařízení vyskytl nějaký problém.
- Pokud existuje nějaká nejistota nebo kontroverze, podívejte se prosím na naše konečné vysvětlení.

# Důležitá bezpečnostní opatření a varování

Následující popis je správný způsob aplikace zařízení. Před použitím si pozorně přečtěte návod, abyste předešli nebezpečí a ztrátě majetku. Při aplikaci přísně dodržujte návod a po přečtení jej řádně uschovejte.

## Provozní požadavek

- Neumísťujte a neinstalujte zařízení v oblasti vystavené přímému slunečnímu záření nebo v blízkosti zařízení generujícího teplo.
- Neinstalujte zařízení ve vlhkém, prašném nebo prašném prostředí.
- Udržujte jeho vodorovnou instalaci nebo jej nainstalujte na stabilní místa a zabraňte pádu.
- Zabraňte kapání nebo stříkání tekutin na zařízení; nepokládejte na zařízení nic naplněné tekutinou, aby se zabránilo vniknutí tekutin do zařízení.
- Instalujte prosím zařízení na dobře větraných místech; neblokuje jeho ventilační otvor.
- Používejte zařízení pouze v rámci jmenovitého vstupního a výstupního rozsahu.
- Nerozebírejte prosím zařízení svévolně.
- Přepravujte, používejte a skladujte zařízení v povoleném rozsahu vlhkosti a teploty.

## Požadavek napájení

- Ujistěte se, že používáte baterie podle požadavků; jinak může dojít k požáru, výbuchu nebo nebezpečí popálení baterií!
- Pro výměnu baterií lze použít pouze stejný typ baterií!
- Výrobek musí používat elektrické kabely (napájecí kabely) doporučené touto oblastí, které musí být použity v rámci své jmenovité specifikace!
- Použijte prosím standardní napájecí adaptér odpovídající zařízení. V opačném případě by uživatel způsobil zranění osob nebo poškození zařízení.
- Použijte prosím napájecí zdroj, který splňuje požadavky SELV (bezpečné extra nízké napětí) a napájejte jmenovitým napětím, které odpovídá omezenému zdroji napájení v IEC60950-1. Specifické požadavky na napájení naleznete na štítcích zařízení.
- Výrobky s konstrukcí kategorie I se připojují do síťové výstupní zásuvky, která je opatřena ochranným uzemněním.
- Spojka spotřebiče je odpojovací zařízení. Při běžném používání dodržujte úhel, který usnadňuje ovládání.

# Obsah

Úvodní slovo .....	I Důležitá
bezpečnostní opatření a varování .....	III
<b>1 Přehled .....</b>	<b>1</b>
1.1 Funkční funkce .....	1
1.2 Vnější rozměr .....	1
<b>2 Instalační příručka .....</b>	<b>3</b>
2.1 Struktura systému .....	3
2.2 Instalace zařízení .....	3
2.3 Demontáž .....	4
2.4 Schéma zapojení .....	5
2.4.1 Popis zapojení přístupového kontroléru .....	5
2.4.2 Popis zapojení výstupního tlačítka/dveřního kontaktu .....	6
2.4.3 Popis zapojení zámku .....	7
2.4.4 Popis zapojení čtečky.....	8
2.4.5 Popis zapojení externího poplachového vstupu.....	8
2.4.6 Popis zapojení externího poplachového výstupu.....	9
2.4.7 Popis zapojení interního poplachového výstupu .....	10
2.4.8 Popis pravidla pro vstup a výstup alarmu.....	11
2.5 DIP přepínač .....	11
2.6 Restartovat.....	12
<b>3 Smart PSS Config.....</b>	<b>13</b>
3.1 Přihlašovací klient .....	13
3.2 Přidat řadič přístupu.....	13
3.2.1 Automatické vyhledávání .....	13
3.2.2 Ruční přidání.....	15
3.3 Přidat uživatele .....	17
3.3.1 Typ karty .....	18
3.3.2 Jednorázové přidání.....	19
3.4 Přidat skupinu dveří .....	21
3.5 Autorizovat .....	23
3.5.1 Autorizace podle skupiny dveří.....	23
3.5.2 Autorizace podle uživatele .....	25
<b>4 FAQ .....</b>	<b>27</b>
1. Otázka: Po zapnutí se indikátor napájení nerozsvítí nebo bzučák nereaguje. ....	27
2. Otázka: Po připojení čtečky k zařízení se kontrolka přiložení karty nerozsvítí a po přiložení karty nereaguje. ....	27
3. Otázka: Klientský software nedokáže detekovat zařízení. ....	27
4. Otázka: Po přetažení karty se zobrazí výzva, že karta je neplatná.....	27
5. Otázka: Výchozí IP řadiče přístupu. ....	27
6. Otázka: Výchozí port, počáteční uživatelské jméno a heslo přístupového kontroléru. ....	27
7. Otázka: Online upgrade zařízení. ....	27

8. Otázka: Max. vzdálenost kabeláže a přenosová vzdálenost čtečky karet a ovladače. ....	27
<b>Dodatek 1 Doporučení pro kybernetickou bezpečnost .....</b>	<b>XXVIII</b>

Dvoudveřový obousměrný přístupový kontrolér je ovládací zařízení, které kompenzuje video dohled a vizuální interkom. Má elegantní a moderní design se silnou funkčností, vhodný pro komerční budovy, firemní nemovitosti a inteligentní komunitu.

## 1.1 Funkční funkce

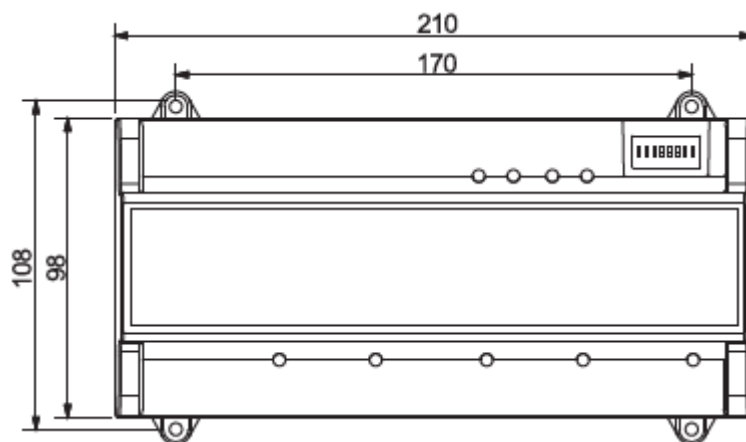
Jeho bohaté funkce jsou následující:

- Přijměte kluznou kolejnici a design ovládaný zámek, pohodlnou instalaci a údržbu.
- Integrujte alarm, kontrolu přístupu, video dohled a požární alarm.
- Podpora 4 sad čteček karet (které lze nastavit jako 2 jednodveřové dvoucestné čtečky). Podpora 8 skupin vstupních signálů (výstupní tlačítko\*2, dveřní kontakt\*2 a alarm narušení\*4). Podpora 6 skupin ovládacích výstupů (elektrický zámek \*2, externí alarmový výstup \*2 a interní alarmový výstup \*2).
- S portem RS485 se může rozšířit o připojení řídicího modulu.
- Kapacita úložiště FLASH je 16M (může se rozšířit až na 32M). Podpora max. 100 000 držitelů karet a 150 000 záznamů o čtení karet.
- Podpora alarmu proti nelegálnímu vniknutí, alarmu časového limitu odemknutí, nastavení nátlakové karty a nátlakového kódu. Podporujte také nastavení černé listiny a hlídkové karty.
- Podpora nastavení platného časového období, nastavení hesla a nastavení data expirace karet. U karty hosta lze nastavit dobu jejího použití.
- Podpora 128 skupin plánů a 128 skupin prázdninových plánů. Trvalé úložiště dat při výpadku, vestavěné RTC (podpora DST), online upgrade.

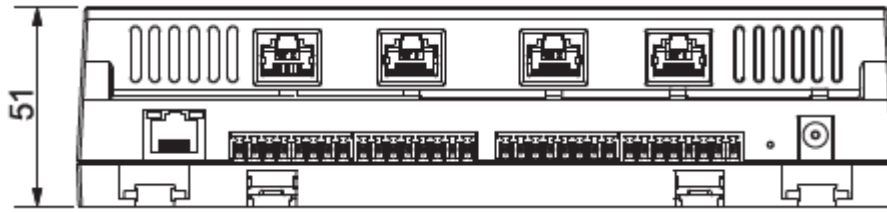
## 1.2 Vnější rozměr

Jeho vzhled a rozměry jsou znázorněny na obrázku 1-1 a obrázku 1-2. Jednotkou je mm.

Obrázek 1-1



Obrázek 1-2



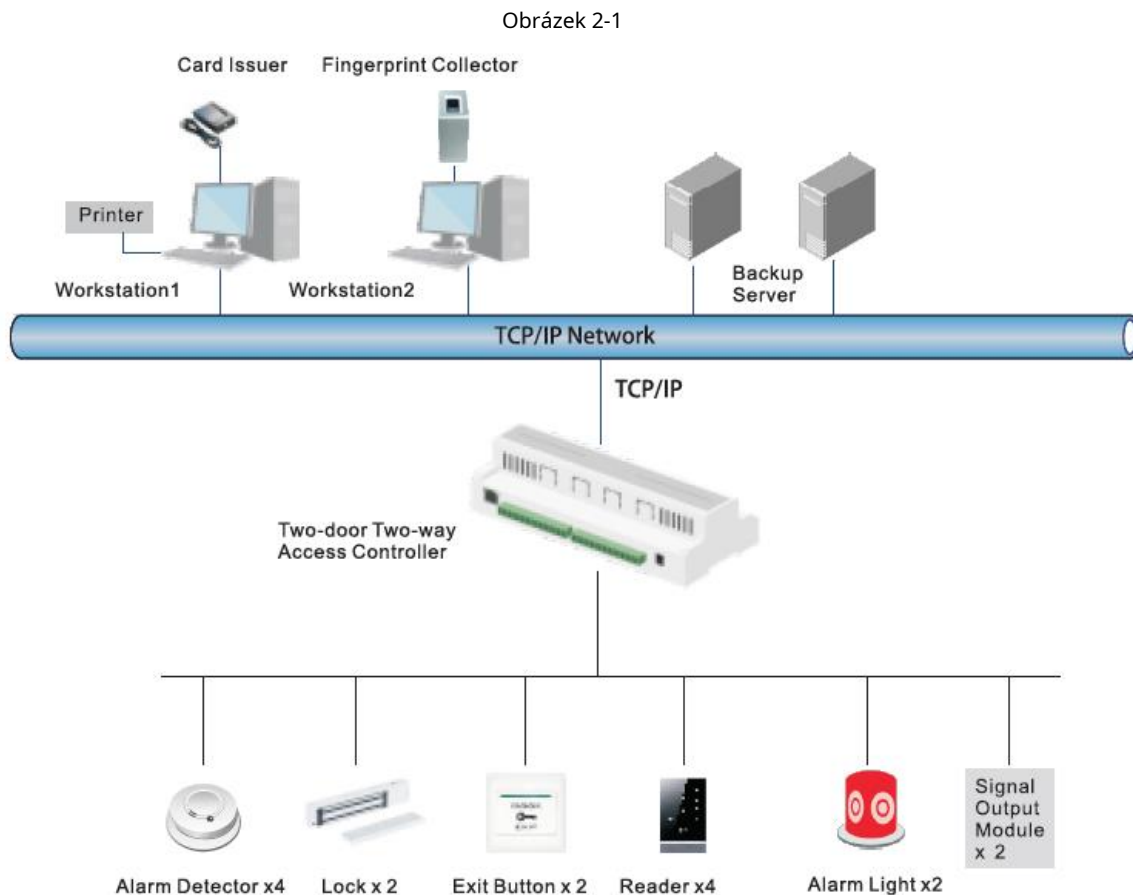


# 2

## Průvodce instalací

### 2.1 Struktura systému

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



### 2.2 Instalace zařízení

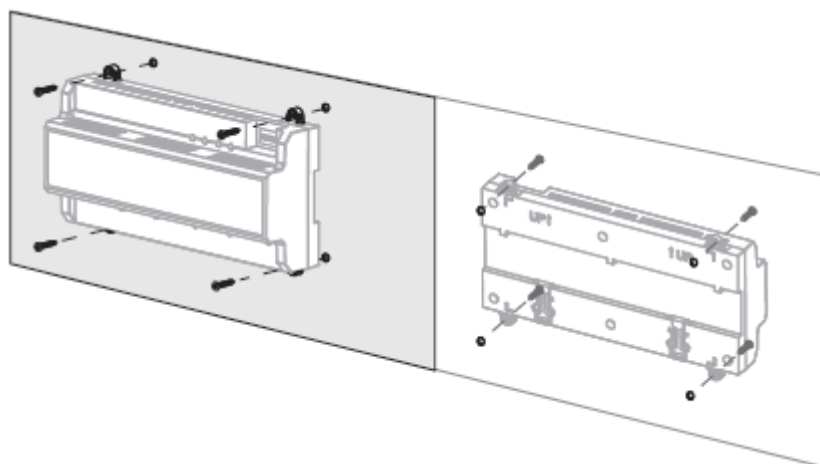
Existují dva režimy instalace.

- Režim 1: připevněte celé zařízení na zeď pomocí šroubů.
- Režim 2: s vodicí lištou ve tvaru U zavěste celé zařízení na stěnu (vodicí lišta ve tvaru U je volitelné příslušenství).

#### Režim 1

Schéma instalace je znázorněno na obrázku 2-2.

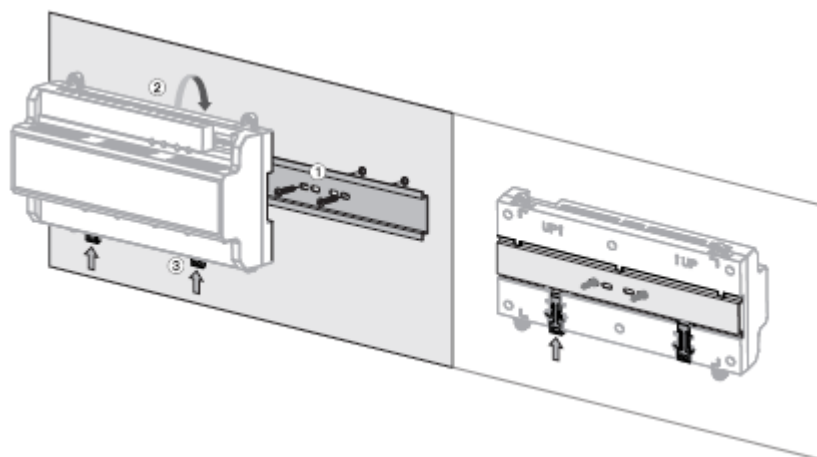
Obrázek 2-2



## Režim 2

Schéma instalace je znázorněno na obrázku 2-3.

Obrázek 2-3



**Krok 1** Připevněte vodící lištu ve tvaru U na stěnu pomocí šroubů.

**Krok 2** Zavěste horní zadní část zařízení do horní drážky vodící lišty ve tvaru U. Zatlačte

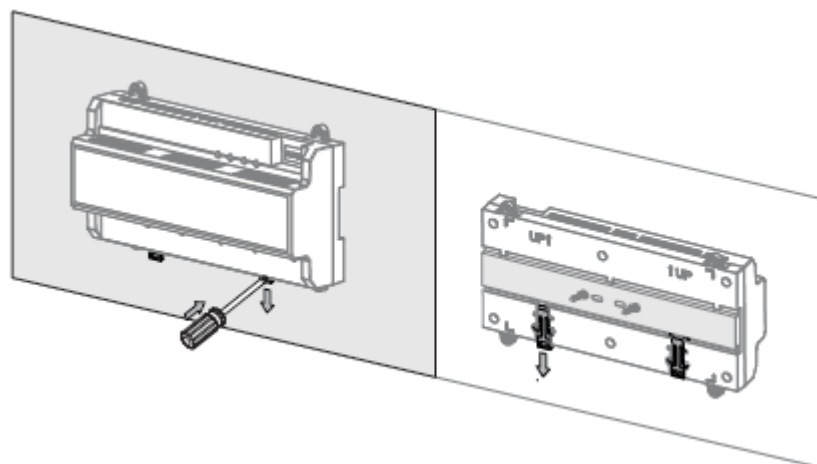
**Krok 3** západku na spodní straně zařízení směrem nahoru. Instalace je dokončena, když uslyšíte zvuk montáže.

## 2.3 Demontáž

Pokud je zařízení instalováno s režimem 2, rozeberte jej podle obrázku 2-4.

Zarovnejte šroubovák se zaklapávacím spojem, zatlačte jej dolů a zaklapávací spoj vyskočí, takže lze celé zařízení hladce rozebrat.

Obrázek 2-4

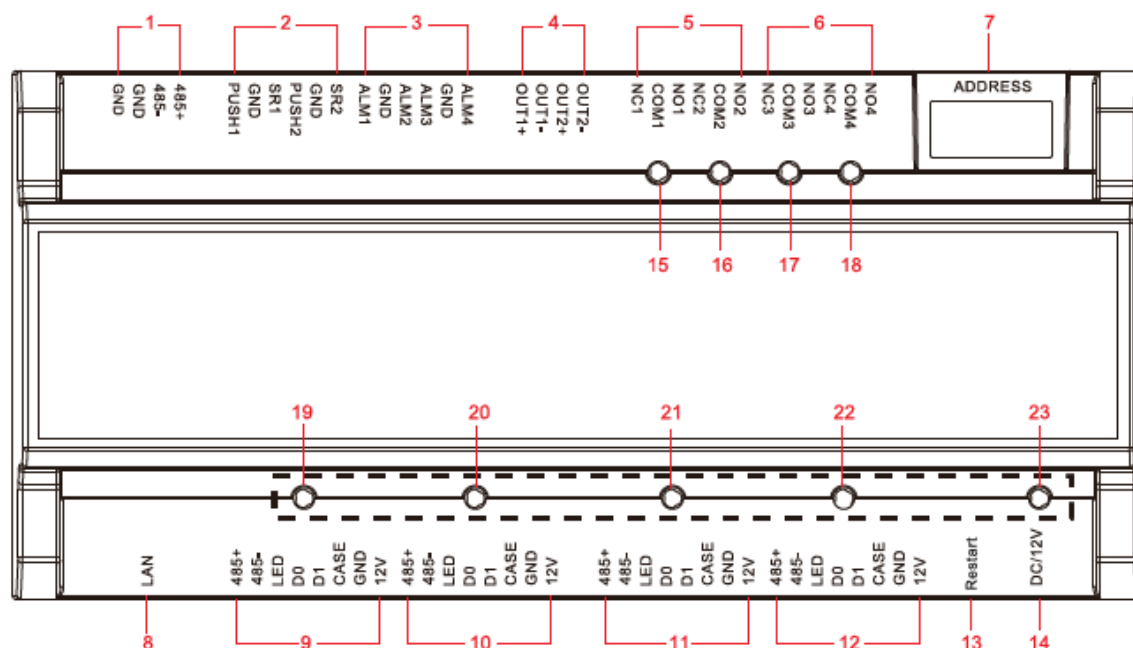


## 2.4 Schéma zapojení

### 2.4.1 Popis zapojení Access Controlleru

Toto zařízení podporuje dvoudveřový obousměrný vstup nebo výstup. V případě poplachového vstupu spustte externí poplachové výstupní zařízení, aby došlo k poplachu. Schéma zapojení zařízení je uvedeno na obrázku 2-5.

Obrázek 2-5



Rozhraní jsou popsána v tabulce 2-1.

Tabulka 2-1

Ne.	Popis portu	Ne.	Popis portu
1	Komunikace RS485	8	TCP/IP, port softwarové platformy
2	Tlačítko pro odchod a dveřní kontakt	9	Vstupní čtečka dveří 1
3	Externí alarmový vstup	10	Výstupní čtečka dveří 1
4	Externí alarmový výstup	11	Vstupní čtečka dveří 2
5	Uzamknout výkon	12	Výstupní čtečka dveří 2
6	Interní alarmový výstup	13	Restartujte

Ne.	Popis portu	Ne.	Popis portu
7	DIP přepínač	14	Napájecí port DC 12V

Kontrolky jsou popsány v tabulce 2-2.

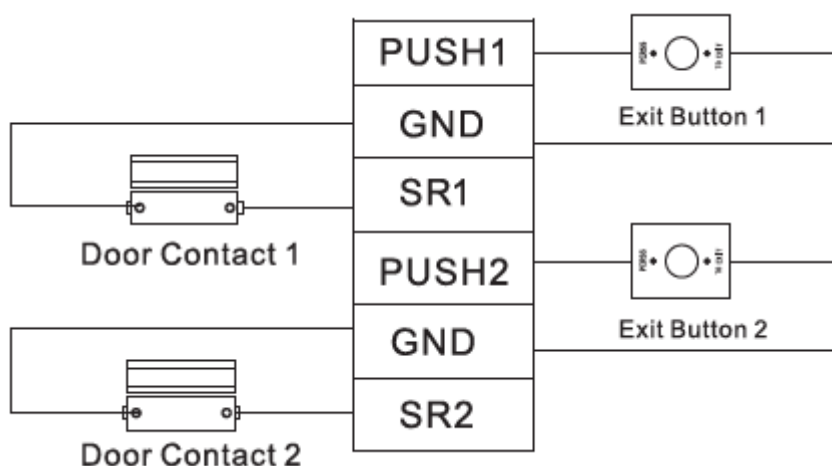
Tabulka 2-2

Ne.	Popis
15	Indikátor stavu zámku
16	
17	Indikátor stavu alarmu
18	
19	Detekční indikátor vstupní čtečky dveří 1
20	Detekční indikátor výstupní čtečky dveří 1
21	Detekční indikátor vstupní čtečky dveří 2
22	Detekční indikátor výstupní čtečky dveří 2
23	Signalizace napájení

## 2.4.2 Popis zapojení výstupního tlačítka/dveřního kontaktu

Odpovídající kabelové svorky výstupního tlačítka a dveřního kontaktu jsou znázorněny na obrázku 2-6. Popis svorek zapojení naleznete v tabulce 2-3.

Obrázek 2-6



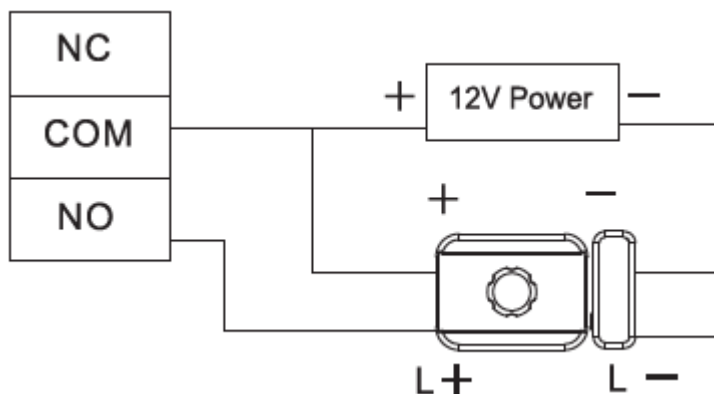
Tabulka 2-3

Přístav	Kabelový terminál	Popis
Tlačítko pro odchod + dveře Kontakt	PUSH1	Tlačítko pro odchod dveří 1
	GND	Sdíleno výstupním tlačítkem dveří 1 a vstupem dveřního kontaktu dveří 1
	SR1	Vstup dveřního kontaktu dveří 1
	PUSH2	Tlačítko pro odchod dveří 2
	GND	Sdíleno výstupním tlačítkem dveří 2 a vstupem dveřního kontaktu dveří 2
	SR2	Vstup dveřního kontaktu dveří 2

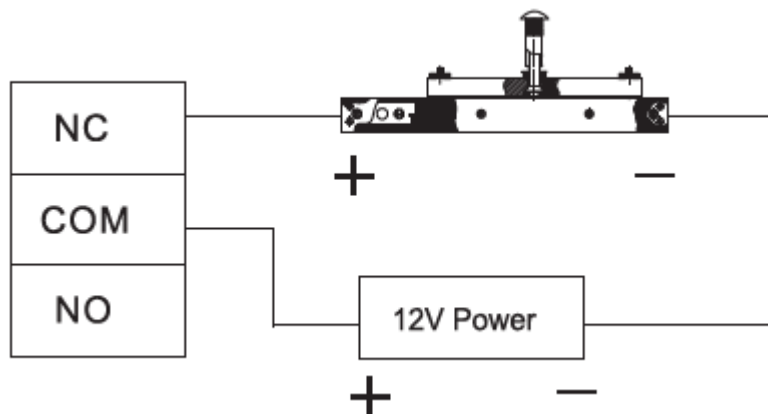
## 2.4.3 Zapojení Popis zámku

Podpora 4 skupin výstupů ovládání zámku; sériová čísla za svorkami představují odpovídající dveře. Vyberte prosím správný režim připojení podle typu zámku, jak je znázorněno na obrázku 2-7, obrázku 2-8 a obrázku 2-9. Popis svorek zapojení naleznete v tabulce 2-4.

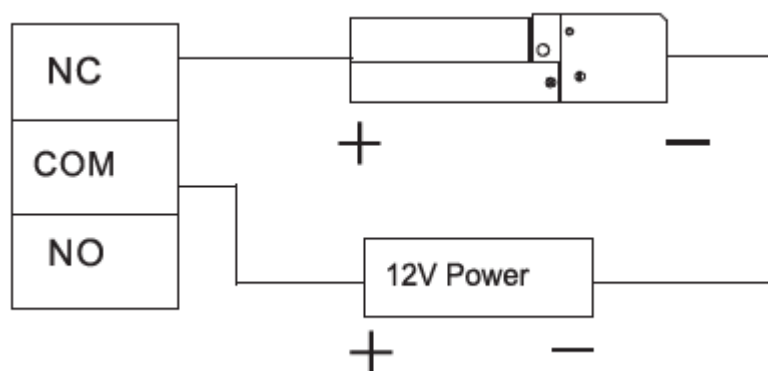
Obrázek 2-7



Obrázek 2-8



Obrázek 2-9



Tabulka 2-4

Přístav	Kabelový terminál	Popis
Výstup ovládání zámku přístav	NC1	Ovládání zámku dveří 1
	COM1	
	Č.1	
	NC2	Ovládání zámku dveří 2
COM2		

Přístav	Kabelový terminál	Popis
	NO2	

## 2.4.4 Popis zapojení čtečky

### NOTE

1 dveře podporují pouze připojení jednoho typu čtečky – 485 nebo Wiegand.

Popis svorek vodičů odpovídajících čtecím zařízením naleznete v tabulce 2-5. Vezměte si například dveře 1; ostatní čtenáři jsou na tom stejně. Popis specifikace a délky kabelu čtečky naleznete v tabulce 2-6.

Tabulka 2-5

Přístav	Kabelový terminál	Barva kabelu	Popis
Vstup čtenáře Dveře 1	485+	Nachový	485 čtenář
	485-	Žlutá	
	VEDENÝ	Hnědý	Čtečka Wiegand
	D0	Zelená	
	D1	Bílý	
	PŘÍPAD	Modrý	
	GND	Černá	Napájení čtečky
	12V	Červené	

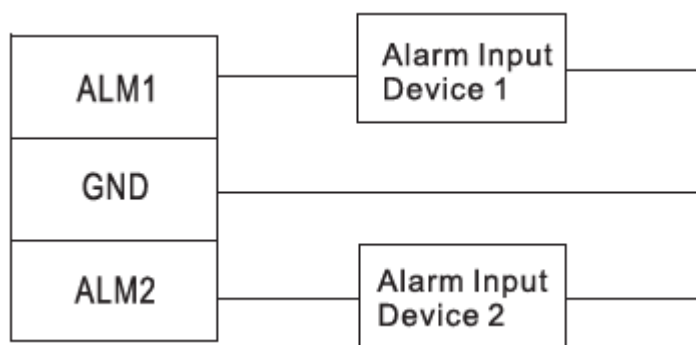
Tabulka 2-6

Typ čtečky	Režim připojení	Délka
485 Čtenář	Síťový kabel CAT5e, připojení 485	100 m
Wiegand Reader	Síťový kabel CAT5e, připojení Wiegand	100 m

## 2.4.5 Popis zapojení externího poplachového vstupu

Připojení 4kanálového vstupu externího alarmu je znázorněno na obrázku 2-10. Popis svorek zapojení naleznete v tabulce 2-7.

Obrázek 2-10



Tabulka 2-7

Přístav	Kabelový terminál	Popis
Externí poplach vstup	ALM1	Vstupní port alarmu 1
	GND	Sdíleno poplachovým vstupním portem 1 a 2
		Externí poplachové vstupní porty umožňují připojit detektor kouře a IR detektor atd.

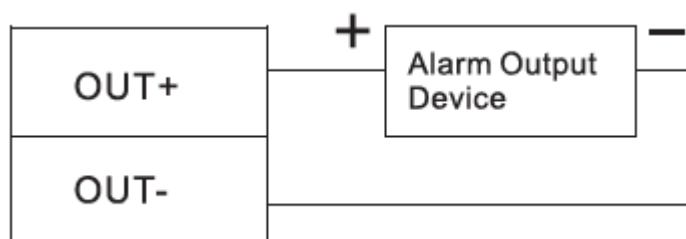
Přístav	Kabelový terminál		Popis
	ALM2	Vstupní port alarmu 2	<p> NOTE</p> <p>Externí alarm může propojit dveře otevřený a uzavřený stav.</p> <ul style="list-style-type: none"> <li>- ALARM1 ~ ALARM2 externí alarm spojí všechny dveře tak, aby byly normálně otevřené.</li> <li>- ALARM3 ~ ALARM4 externí alarm spojí všechny dveře tak, aby byly normálně zavřené.</li> </ul>
	ALM3	Vstupní port alarmu 3	
	GND	Sdíleno poplachovým vstupním portem 3 a 4	
	ALM4	Vstupní port alarmu 4	

## 2.4.6 Popis zapojení externího poplachového výstupu

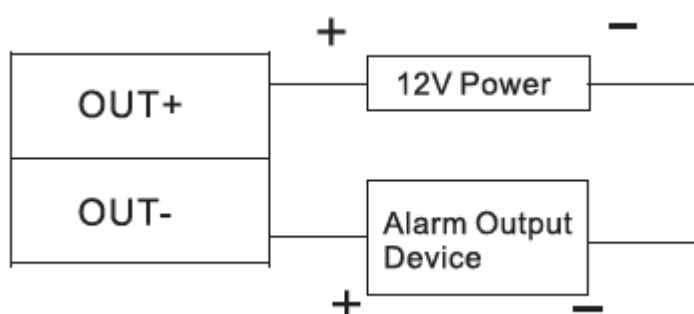
S 2kanálovým externím poplachovým výstupem po spuštění poplachu vydá poplachové výstupní zařízení poplach po dobu 15s.

Existují dva režimy připojení externího poplachového výstupu v závislosti na poplachovém zařízení. Například IPC může používat režim 1, zatímco zvuková a vizuální siréna může používat režim 2, jak je znázorněno na obrázku 2-11 a obrázku 2-12. Popis svorek zapojení naleznete v tabulce 2-8.

Obrázek 2-11



Obrázek 2-12



Tabulka 2-8

Přístav	Kabelový terminál		Popis
Externí alarmový výstup	OUT1+	ALM1/ALM2 spustí poplachový výstup.	Externí alarmový výstup porty jsou schopny připojit slyšitelné a vizuální sirény.
	OUT1-		
	OUT2+	ALM3/ALM4 spouští výstup alarmu.	
	OUT2-		

## 2.4.7 Popis zapojení interního alarmového výstupu

S 2kanálovým interním poplachovým výstupem poté, co vnitřní poplachový vstup (jako je časový limit dveří) spustí poplach, poplachové výstupní zařízení vydá poplach po dobu 15 sekund.

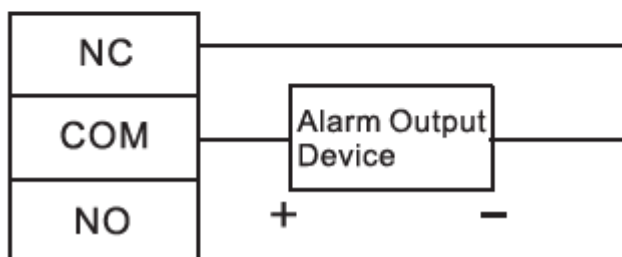
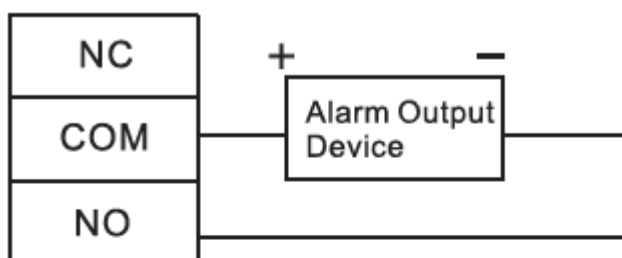
Během připojení výstupního zařízení alarmu vyberte NC/NO podle stavu normálně zavřeno nebo normálně otevřeno.

- NC představuje normálně uzavřený stav. NO
- představuje normálně otevřený stav.

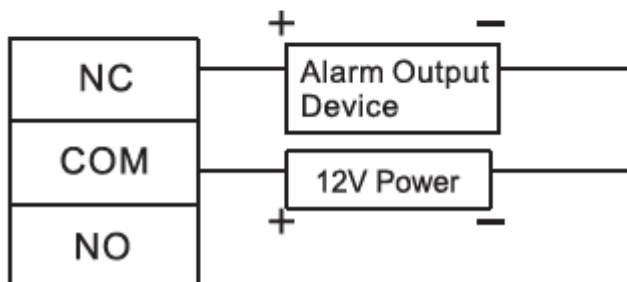
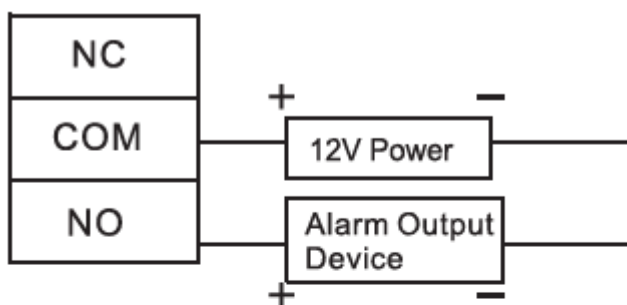
Existují dva režimy připojení vnitřního alarmového výstupu v závislosti na alarmovém zařízení.

Například IPC může používat režim 1, zatímco zvuková a vizuální siréna může používat režim 2, jak je znázorněno na obrázku 2-13 a obrázku 2-14. Popis svorek zapojení naleznete v tabulce 2-9.

Obrázek 2-13



Obrázek 2-14





Tabulka 2-9

Přístav	Kabelový terminál		Popis
Vnitřní alarmový výstup	NC3	-	Výstup alarmu sabotáže vstupní a výstupní čtečky dveří 1 Timeout a výstup alarmu narušení dveří 1
	COM3		
	NO3		
	NC4	-	Výstup alarmu sabotáže vstupní a výstupní čtečky dveří 2 Timeout a výstup alarmu narušení dveří 2
	COM4		
	NO4		
			Vnitřní alarm výstupní porty jsou schopny se připojit slyšitelné a vizuální sirény.

## 2.4.8 Popis pravidla pro vstup a výstup alarmu

V případě poplachové události poplach trvá 15s. Podrobná pravidla pro vstup a výstup alarmu naleznete v tabulce 2-10.

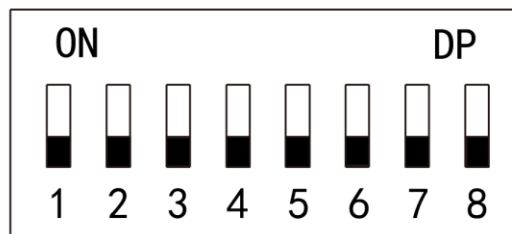
Tabulka 2-10



Typ alarmu	Vstup poplachového signálu Přístav	Alarmový signál Výstupní port	Stav alarmu
Externí poplachový vstup	ALM1	OUT1	Propojte všechny dveře, aby byly normálně otevřené.
	ALM2		
	ALM3	OUT2	Spojte všechny dveře, aby byly normálně zavřené.
	ALM4		
Vnitřní alarm vstup	SR1	OUT1	Časový limit dveří a alarm vloupání spustí externí alarm a spustí alarm.
	SR2	OUT2	
	RS-485/CASE	OUT1	Tamper alarm čtečky spustí externí alarm, který vydá alarm.
	RS-485/CASE	OUT2	

## 2.5 DIP přepínač

Ovládání pomocí DIP přepínače.

Obrázek 2-15



-  přepínač je v poloze ON, což znamená 1.
-  přepínač je dole, což znamená 0.

- 1~8 jsou všechny 0; systém se normálně spustí.
- 1~8 jsou všechny 1; systém po startu přejde do režimu BOOT.
- 1, 3, 5 a 7 jsou 1, zatímco ostatní jsou 0. Po restartu systém obnoví výchozí tovární nastavení.
- 2, 4, 6 a 8 jsou 1, zatímco ostatní jsou 0. Po restartu systém obnoví výchozí tovární nastavení, ale informace o uživateli zůstanou zachovány.

## 2.6 Restartujte

Vložte jehlu do otvoru pro restart, stiskněte ji jednou pro restart zařízení.



**NOTE**

Tlačítko Restart slouží k restartování zařízení, nikoli k úpravě konfigurace.

# 3

## Inteligentní konfigurace PSS



Přístupový kontrolér je řízen pomocí klienta Smart PSS, aby bylo možné realizovat ovládání a správnou konfiguraci jedné dveří a skupin dveří.

Tato kapitola představuje především rychlou konfiguraci. Konkrétní operace naleznete v uživatelské příručce Smart PSS Client.

 NOTE

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

### 3.1 Přihlašovací klient

Nainstalujte odpovídajícího klienta Smart PSS a dvakrát klikněte na  a přejděte na . Proveďte inicializaci konfiguraci podle pokynů rozhraní a dokončete přihlášení.

### 3.2 Přidat řadič přístupu

Přidejte do Smart PSS kontrolér přístupu; vyberte „Automatické vyhledávání“ a „Přidat“.

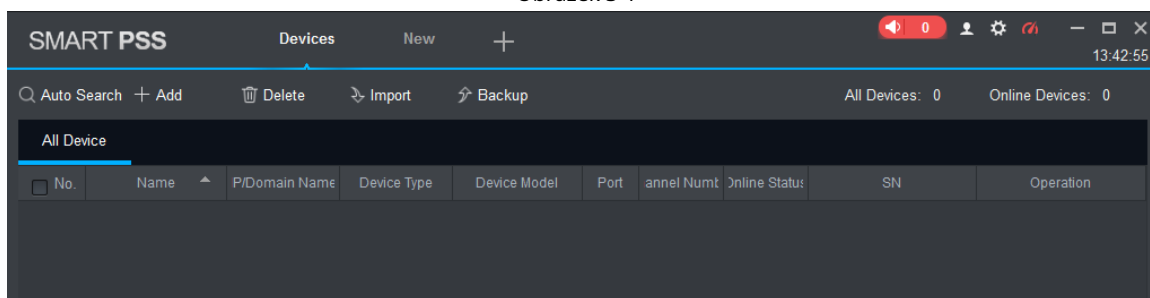
#### 3.2.1 Automatické vyhledávání

Zařízení musí být ve stejném segmentu sítě. Krok 1

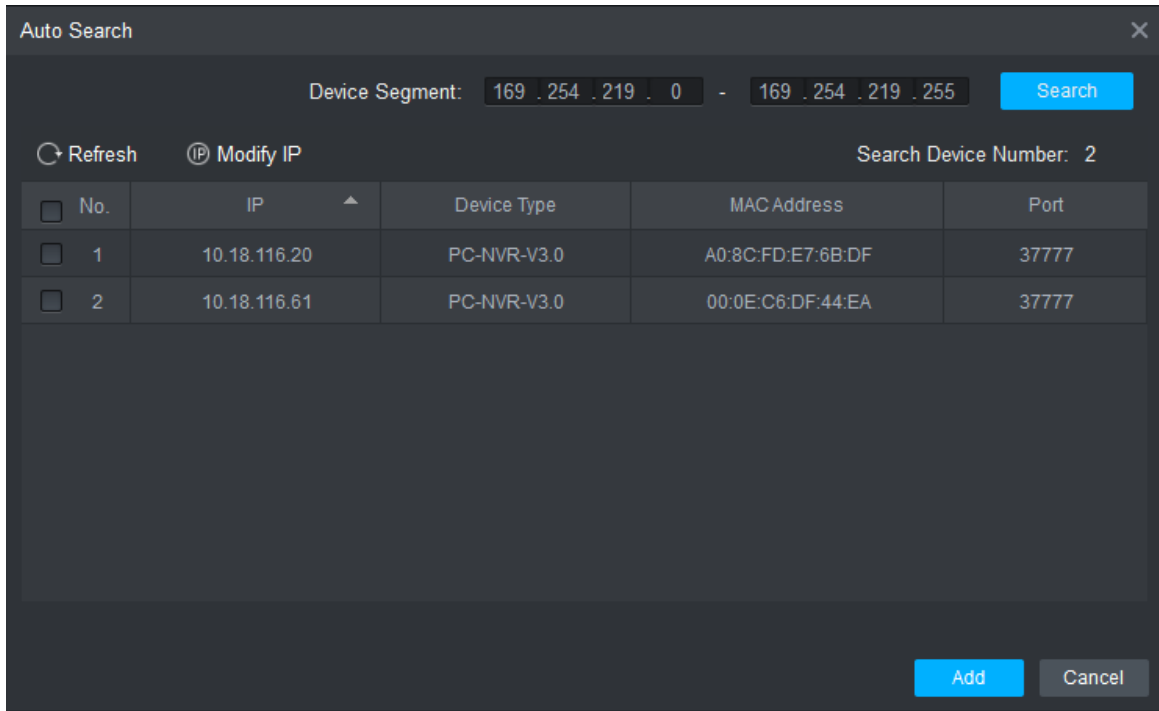
V rozhraní „Devices“ klikněte na „Auto Search“, jak je znázorněno na obrázku 3-1.

System zobrazí rozhraní „Auto Search“, jak je znázorněno na obrázku 3-2.

Obrázek 3-1



Obrázek 3-2



**Krok 2** Zadejte segment zařízení a klikněte na „Hledat“.

System zobrazí výsledky vyhledávání.



**NOTE**

- Kliknutím na „Obnovit“ aktualizujete informace o zařízení.
- Vyberte zařízení, klikněte na „Upravit IP“ pro úpravu IP adresy zařízení. Pro konkrétní operace, nahlédněte do uživatelské příručky klienta Smart PSS.

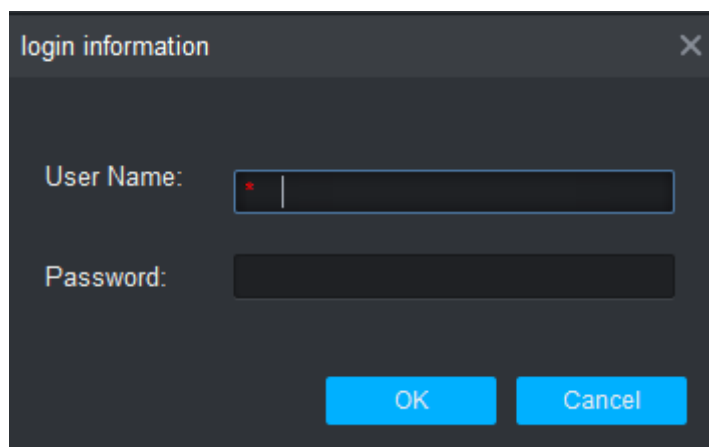
**Krok 3** Vyberte zařízení, které je třeba přidat, a klikněte na „Přidat“.

System vyskočí „Prompt“.

**Krok 4** Klikněte na „OK“.

System zobrazí dialogové okno „Přihlašovací údaje“, jak je znázorněno na obrázku 3-3.

Obrázek 3-3



**Krok 5** Pro přihlášení k zařízení zadejte „User Name“ a „Password“ a klikněte na „OK“.

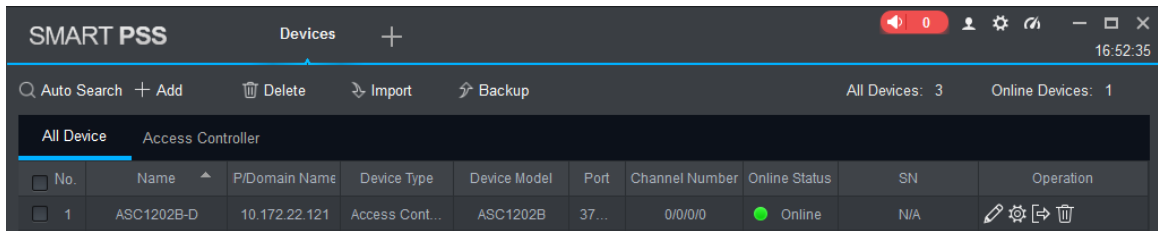
System zobrazí seznam přidávaných zařízení, jak je znázorněno na obrázku 3-4. Podrobnosti naleznete v tabulce 3-1.












**NOTE**

- Po dokončení přidávání systém nadále zůstává v rozhraní „Automatické vyhledávání“.  
Můžete pokračovat v přidávání dalších zařízení, nebo kliknutím na „Storno“ ukončit „Automatické vyhledávání“ rozhraní.
- Po dokončení přidávání se Smart PSS automaticky přihlásí do zařízení. V případě úspěšné přihlášení, stav online zobrazí „Online“. Jinak se zobrazí „Offline“.

Obrázek 3-4



Tabulka 3-1

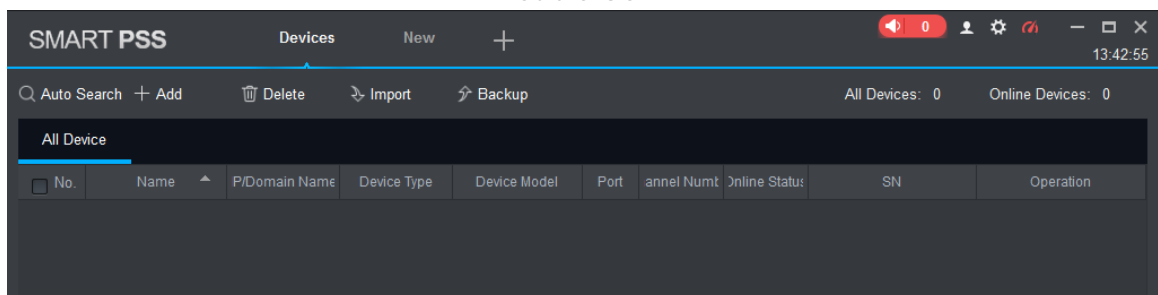
Ikona	Popis
	Kliknutím na tuto ikonu vstoupíte do rozhraní „Upravit zařízení“ a upravíte informace o zařízení, včetně názvu zařízení, názvu IP/domény, portu, uživatelského jména a hesla. Případně poklepejte na zařízení pro vstup do rozhraní „Upravit zařízení“.
	Klepnutím na tuto ikonu vstoupíte do rozhraní „Device Config“ a nakonfigurujete kameru zařízení, síť, událost, úložiště a systémové informace.
 a 	<ul style="list-style-type: none"> <li>- Když je zařízení online, ikona je  Klepnutím na tuto ikonu ukončíte přihlášení a tato ikona se změní na .</li> <li>- Když je zařízení offline, ikona je  Kliknutím na tuto ikonu se přihlaste (se správnými informacemi o zařízení) a tato ikona se změní na .</li> </ul>
	Klepnutím na tuto ikonu zařízení odstraní.

## 3.2.2 Ruční přidání

Pro přidání zařízení musí být nejprve známa IP adresa zařízení nebo název domény. Krok

- 1 V rozhraní „Devices“ klikněte na „Add“, jak je znázorněno na obrázku 3-5.  
Systém zobrazí rozhraní „Manual Add“, jak je znázorněno na obrázku 3-6.

Obrázek 3-5



Obrázek 3-6

**Krok 2** Nastavte parametry zařízení. Popis konkrétních parametrů naleznete v tabulce 3-2.

Tabulka 3-2

Parametr	Popis
Název zařízení	Navrhuje se, aby název zařízení byl pojmenován podle monitorovací zóny, aby se usnadnila údržba.
Metoda přidat	Vyberte „Název IP/domény“. Přidejte zařízení podle IP adresy zařízení nebo názvu domény.
Název IP/domény	IP adresa nebo název domény zařízení.
Přístav	Číslo portu zařízení. Výchozí číslo portu je 37777. Vyplňte prosím podle aktuálních podmínek.
Skupinové jméno	Vyberte skupinu zařízení.
Uživatelské jméno a heslo	Uživatelské jméno a heslo zařízení.

**Krok 3** Kliknutím na „Přidat“ přidáte zařízení.

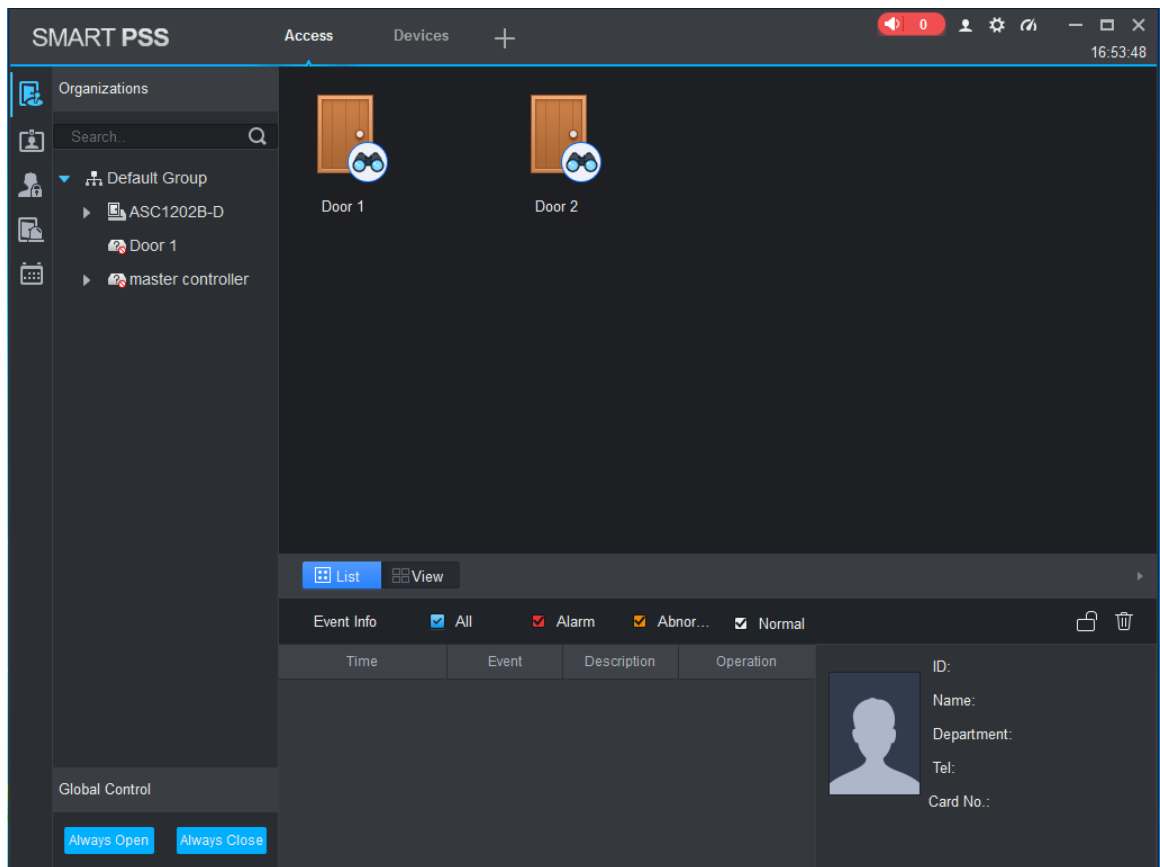
System zobrazí seznam přidanych zařízení, jak je znázorněno na obrázku 3-4. Podrobnosti naleznete v tabulce 3-1. Dveře přidaného ovladače se zobrazí na kartě „Přístup“, jak je znázorněno na obrázku 3-7.



#### NOTE

- Chcete-li přidat další zařízení, klikněte na „Uložit a pokračovat“, přidejte zařízení a zůstaňte na „Ručně. Add“ rozhraní.
- Chcete-li přidání zrušit, klikněte na „Zrušit“ a opusťte rozhraní „Ruční přidání“.
- Po dokončení přidávání se Smart PSS automaticky přihlásí do zařízení. V případě úspěšné přihlášení, stav online zobrazí „Online“. Jinak se zobrazí „Offline“.

Obrázek 3-7

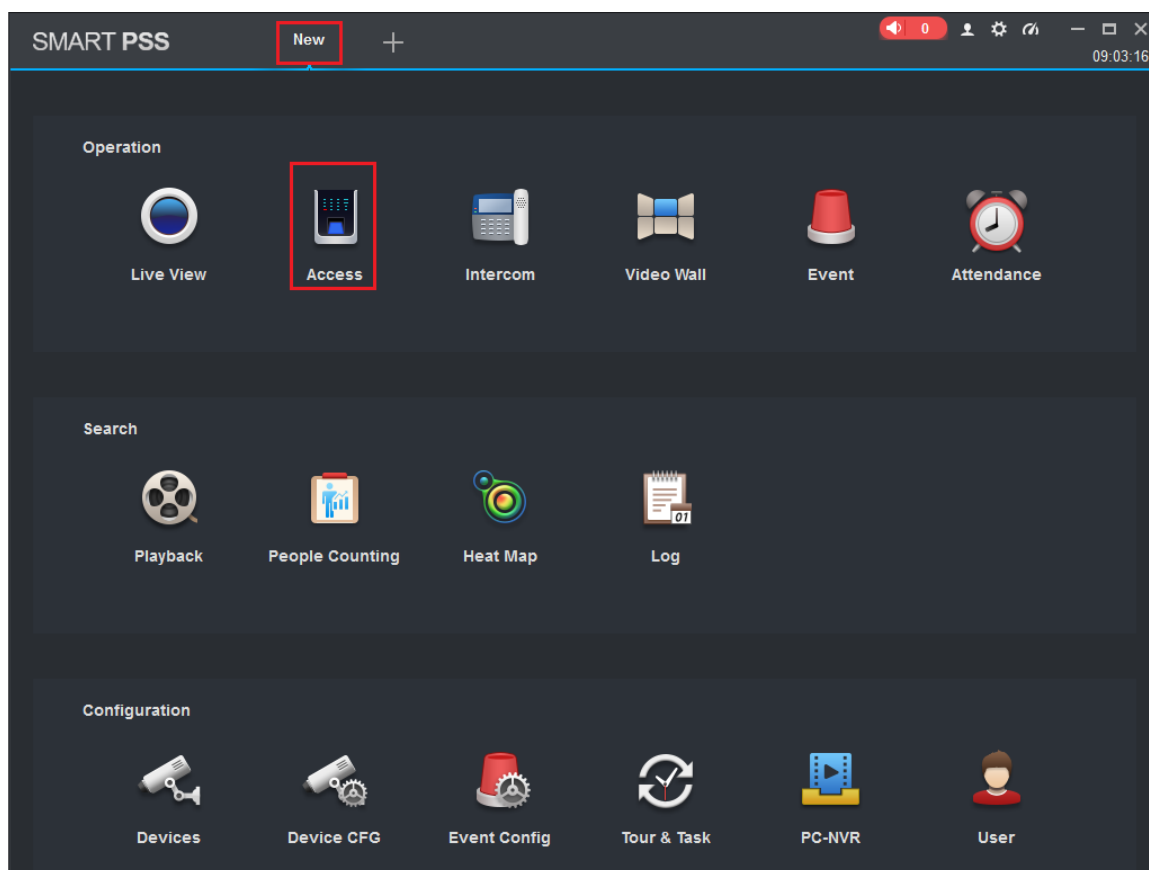


### 3.3 Přidat uživatele

Přidejte uživatele a svažte je pomocí karet, abyste rozdělili autoritu.

V „Novém“ rozhraní klikněte na „Přístup“ pro vstup do rozhraní „Přístup“ a zde dokončete konfiguraci přístupu.

Obrázek 3-8



### 3.3.1 Typ karty



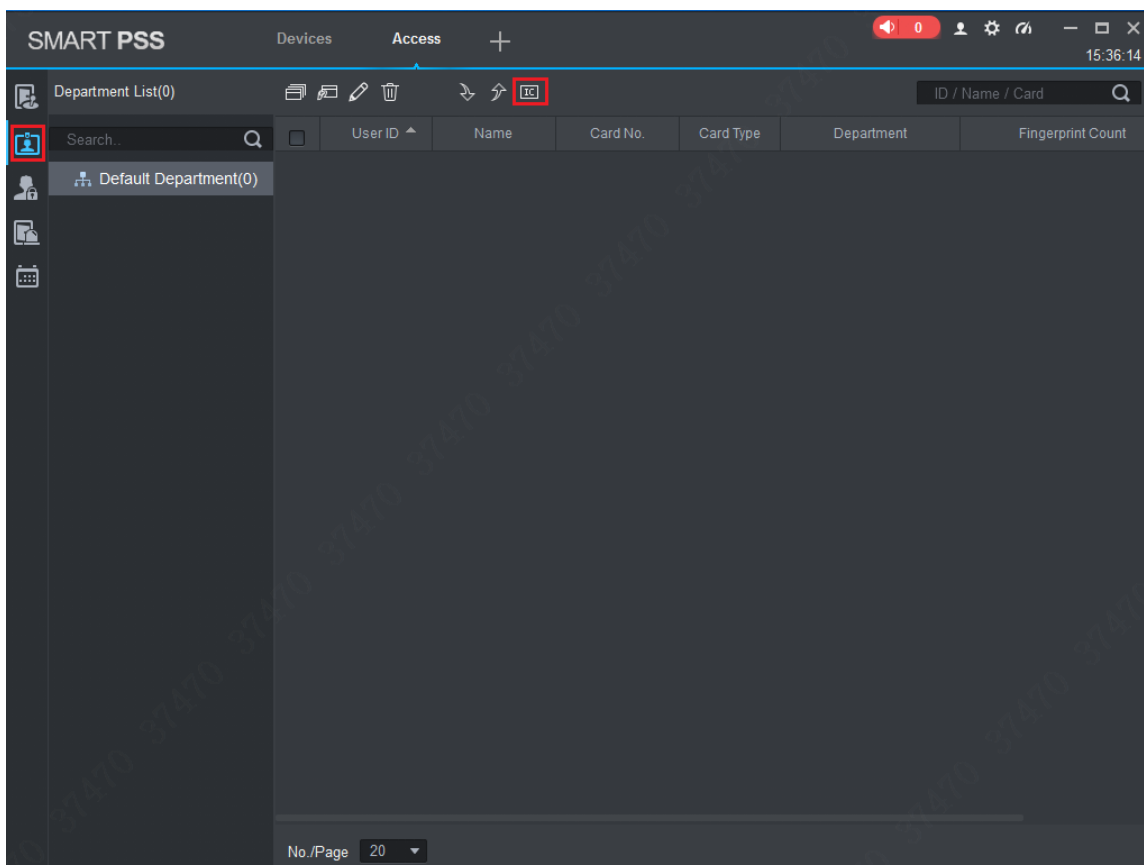
**CAUTION**

Typ karty musí být stejný jako u vydavatele karty; jinak nepřechte číslo karty.

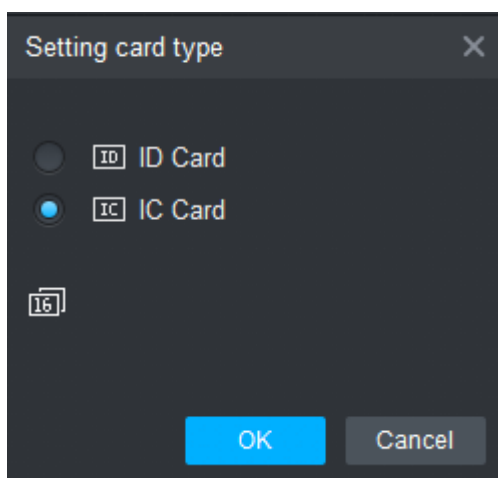
V rozhraní „Přístup“ klikněte na  a poté klikněte  pro nastavení typu karty, jak je znázorněno na obrázku 3-9 a Obrázek 3-10.



Obrázek 3-9





Obrázek 3-10



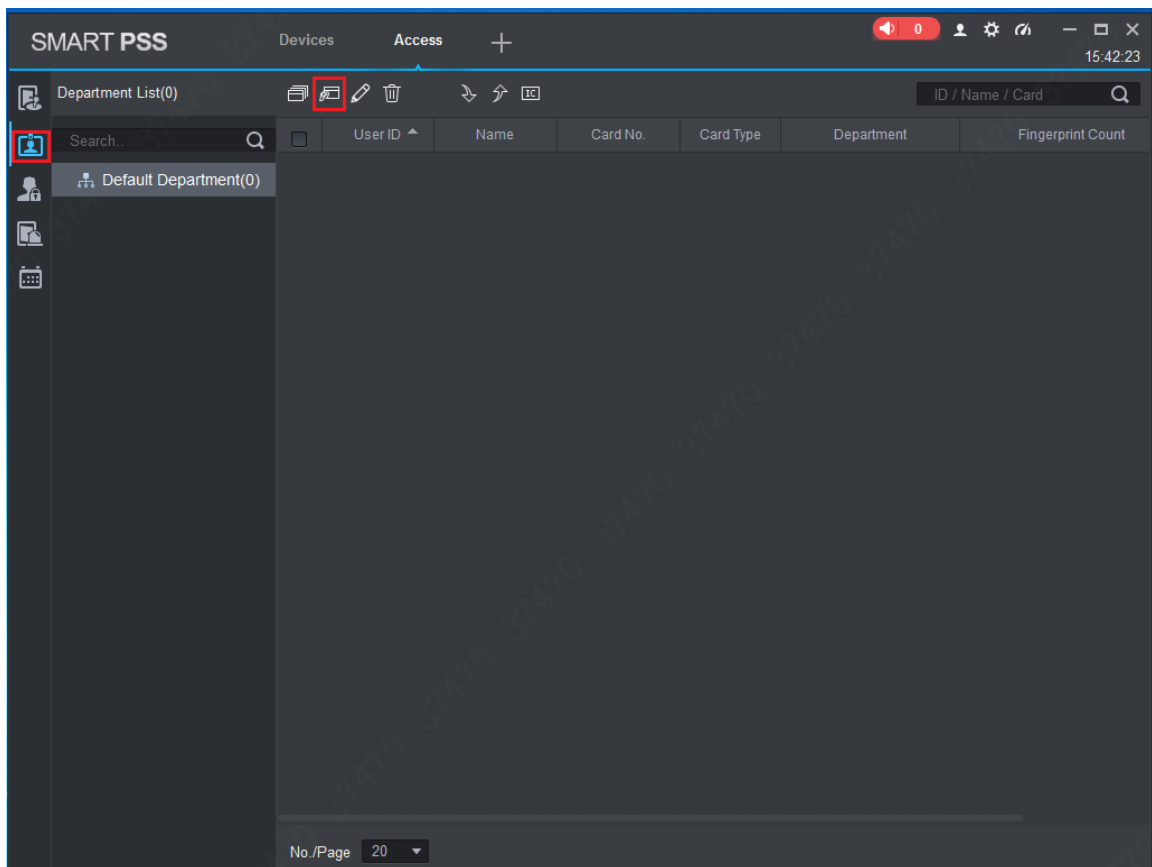
### 3.3.2 Single Add

Přidejte jednoho uživatele, odešlete kartu a zadejte informace o uživateli.

**Krok 1** V rozhraní „Přístup“ klikněte na  a poté klepněte na , jak je znázorněno na obrázku 3-11.

System zobrazí dialogové okno „Přidat uživatele“, jak je znázorněno na obrázku 3-12.

Obrázek 3-11



Obrázek 3-12


The screenshot shows the 'Add User' form in the SMART PSS web interface. The form has three tabs: 'Basic Info', 'Fingerprint Info', and 'Details'. The 'Basic Info' tab is active. The form contains the following fields:

- User ID: \* [text input]
- Name: \* [text input]
- Department: Default Department [dropdown]
- Card No.: Card Reader not ready! [text input]
- Card issuer: [dropdown]
- Card Type: General Card [dropdown]
- Card Password: [password input]
- Unlock Password: [password input]
- Number of Use: 200 [text input]
- Valid Time: 2018/7/11 0:00:00 [calendar icon] 2028/7/11 23:59:59 [calendar icon] 3654 Days

On the right side, there is a placeholder for a user profile picture with the text 'Image Size:0 ~ 120KB' and an 'Upload Picture' button. At the bottom right, there are three buttons: 'Continue t...', 'Finish', and 'Cancel'.

**Krok 2** Ručně přidejte informace o uživateli, včetně základních informací, informací o otiscích prstů a podrobnosti. Podrobnosti naleznete v tabulce 3-3.


Tabulka 3-3

Parametr	Popis
Základní informace	<ul style="list-style-type: none"> <li>- ID uživatele (povinné).</li> <li>- Jméno (povinné).</li> <li>- Oddělení (autosdružení).</li> <li>- Číslo karty: zadání pomocí čtečky karet nebo ruční zadání.</li> <li>- Typ karty: obecná karta, VIP karta, karta hosta, karta hlídky, karta černé listiny a karta nátlaku.</li> <li>- Heslo karty: slouží k otevření dveří kartou + heslem.</li> <li>- Odemknout heslo: používá se k otevření dveří pomocí hesla.</li> <li>- Počet použití: platí pouze pro kartu hosta.</li> <li>- Platnost: nastavte dobu platnosti karty, která je standardně 10 let.</li> <li>- Obrázek: uživatelský obrázek, max. 120 tis.</li> </ul> <p> <b>NOTE</b> Číslo karty. a ID uživatele nelze opakovat.</p>
Informace o otisku prstu	<p>Sbírejte otisky prstů pomocí čtečky otisků prstů a čtečky přístupu.</p> <ul style="list-style-type: none"> <li>- Max. 2 otisky prstů pro každého.</li> <li>- Podpora pro zadání názvu otisku prstu.</li> </ul>
Podrobnosti	Vyplňte podrobné informace o uživateli podle parametrů rozhraní.

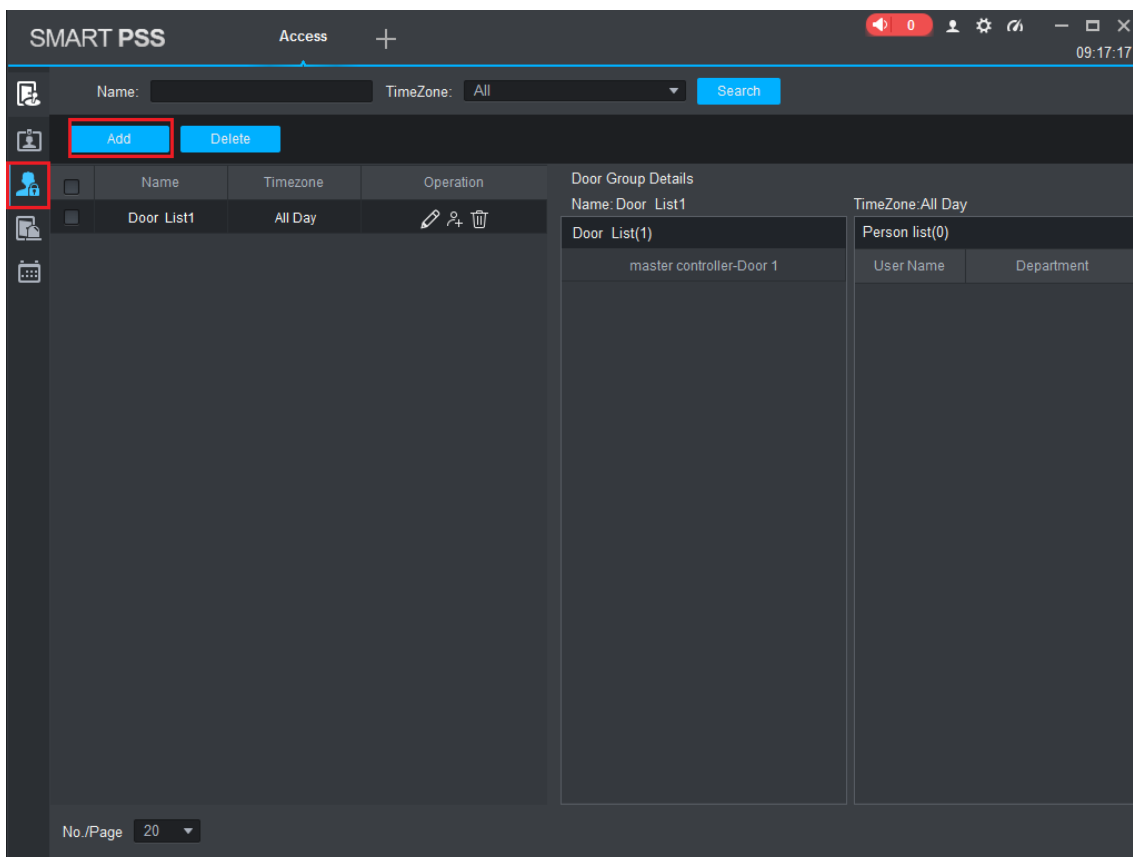
Krok 3 Kliknutím na „Dokončit“ dokončíte přidávání uživatelů.

### 3.4 Přidat skupinu dveří

Rozdělte dveře do skupin a spravujte je společně.

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

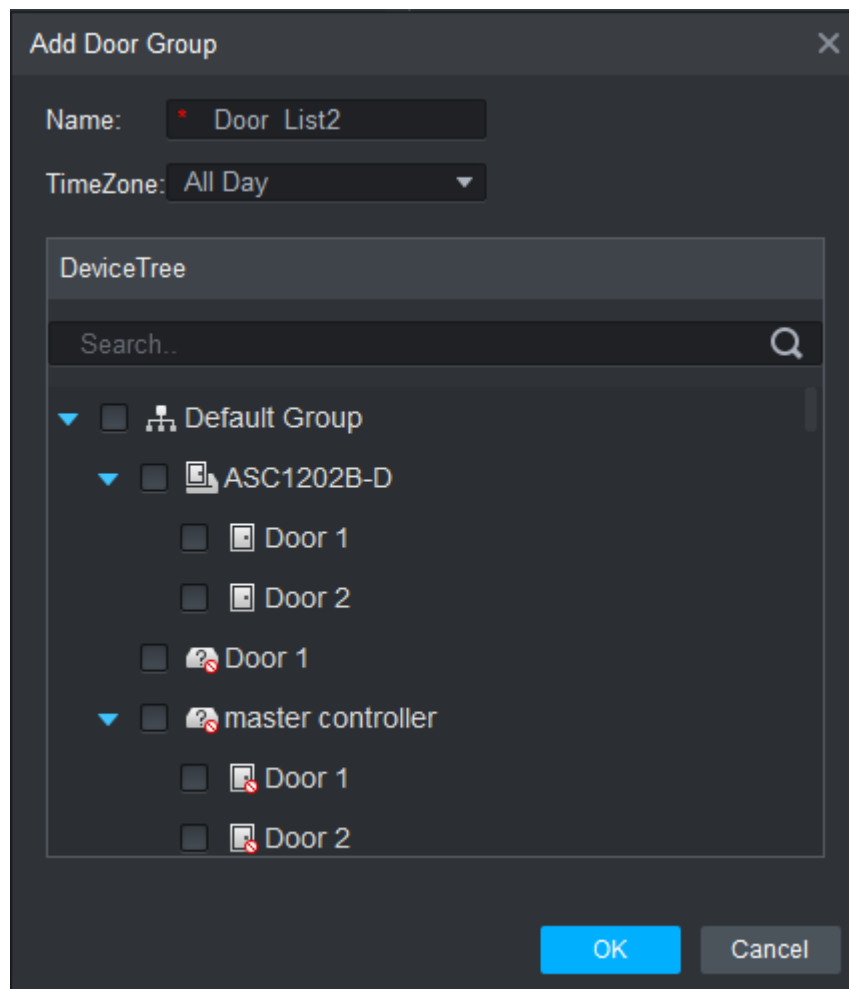
Obrázek 3-13



**Krok 2** Klikněte na „Přidat“.

System zobrazí dialogové okno „Přidat skupinu dveří“, jak je znázorněno na obrázku 3-14.

Obrázek 3-14



**Krok 3** Napište jméno"; vyberte „Časové pásmo“ a dveře, které chcete spravovat.


**Krok 4** Kliknutím na „OK“ dokončíte přidávání.

## 3.5 Autorizovat

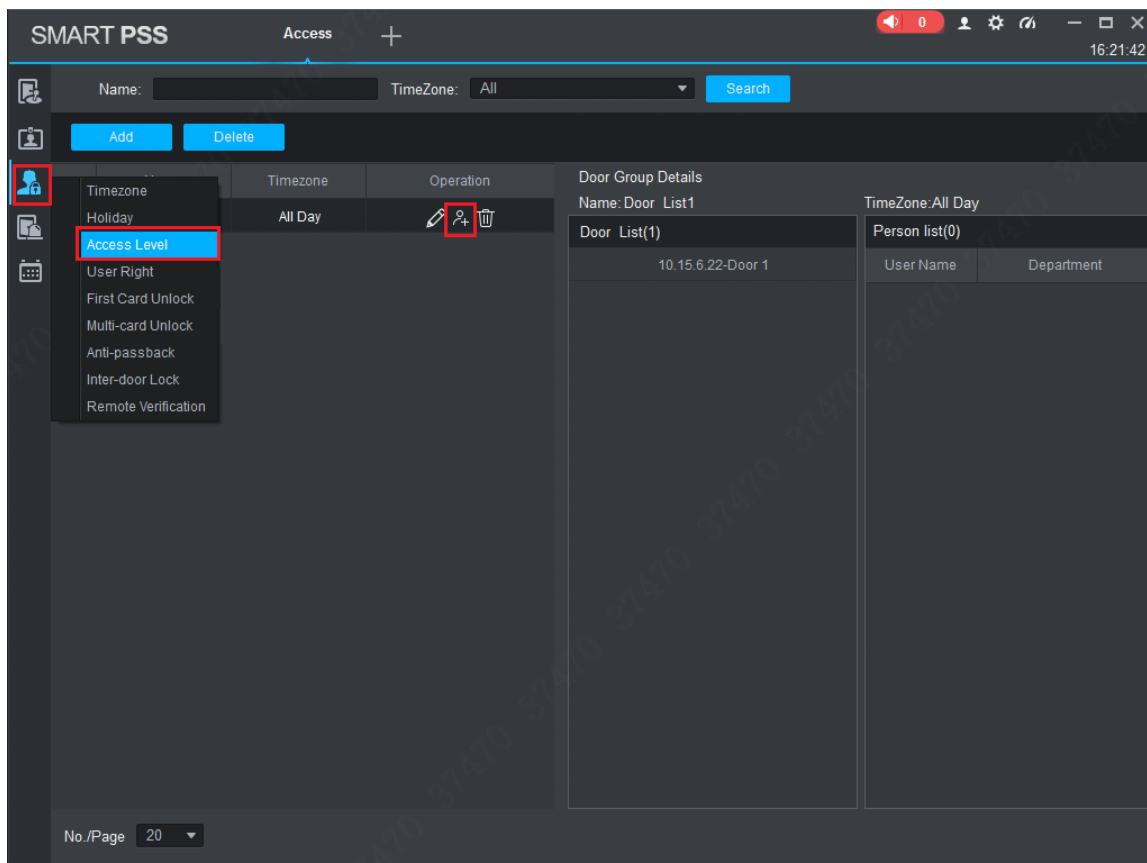
Udělte uživatelům oprávnění podle skupiny dveří a uživatele.


### 3.5.1 Autorizovat podle skupiny dveří

Vyberte skupinu dveří, přidejte do skupiny odpovídající uživatele, aby všichni uživatelé ve skupině získali oprávnění ke všem dveřím ve skupině.

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

Obrázek 3-15

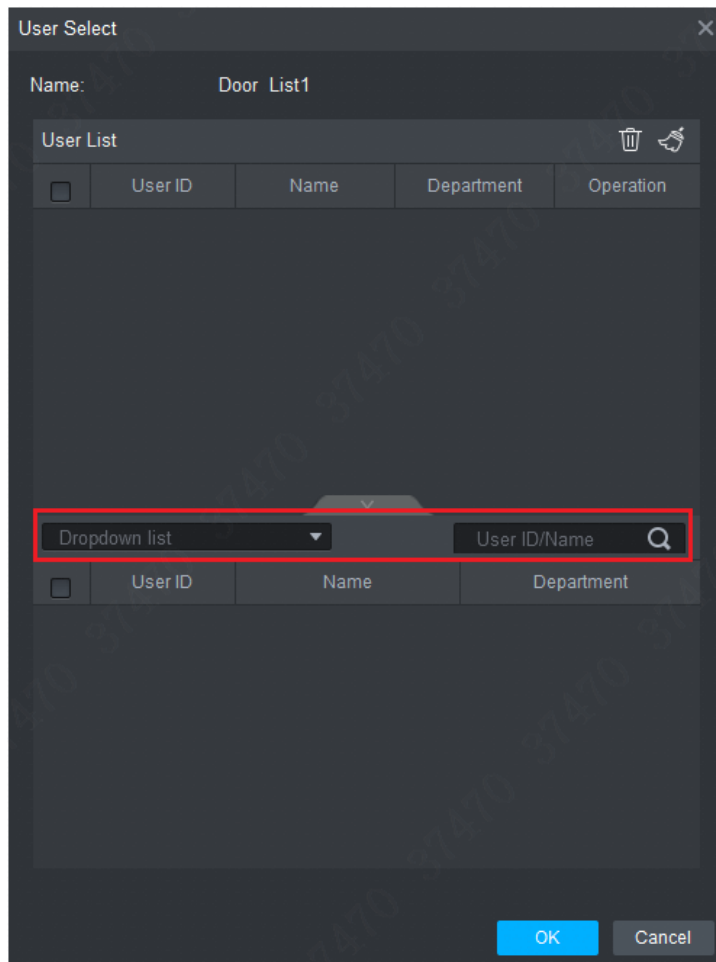


**Krok 2** Klikněte .

System zobrazí dialogové okno „Výběr uživatele“.

**Krok 3** Vyberte oddělení uživatele z rozevřacího seznamu nebo zadejte přímo ID nebo jméno uživatele, jak je znázorněno na obrázku 3-16.

Obrázek 3-16



**Krok 4** V seznamu hledání vyberte uživatele a přidejte jej do seznamu uživatelů.

**Krok 5** Klikněte na „OK“ pro dokončení autorizace.

 **NOTE**

- Seznam vyhledávání filtruje informace o uživateli bez čísla karty.
- V seznamu uživatelů zrušte přidaného uživatele a odstraňte oprávnění uživatele.

## 3.5.2 Autorizovat podle uživatele

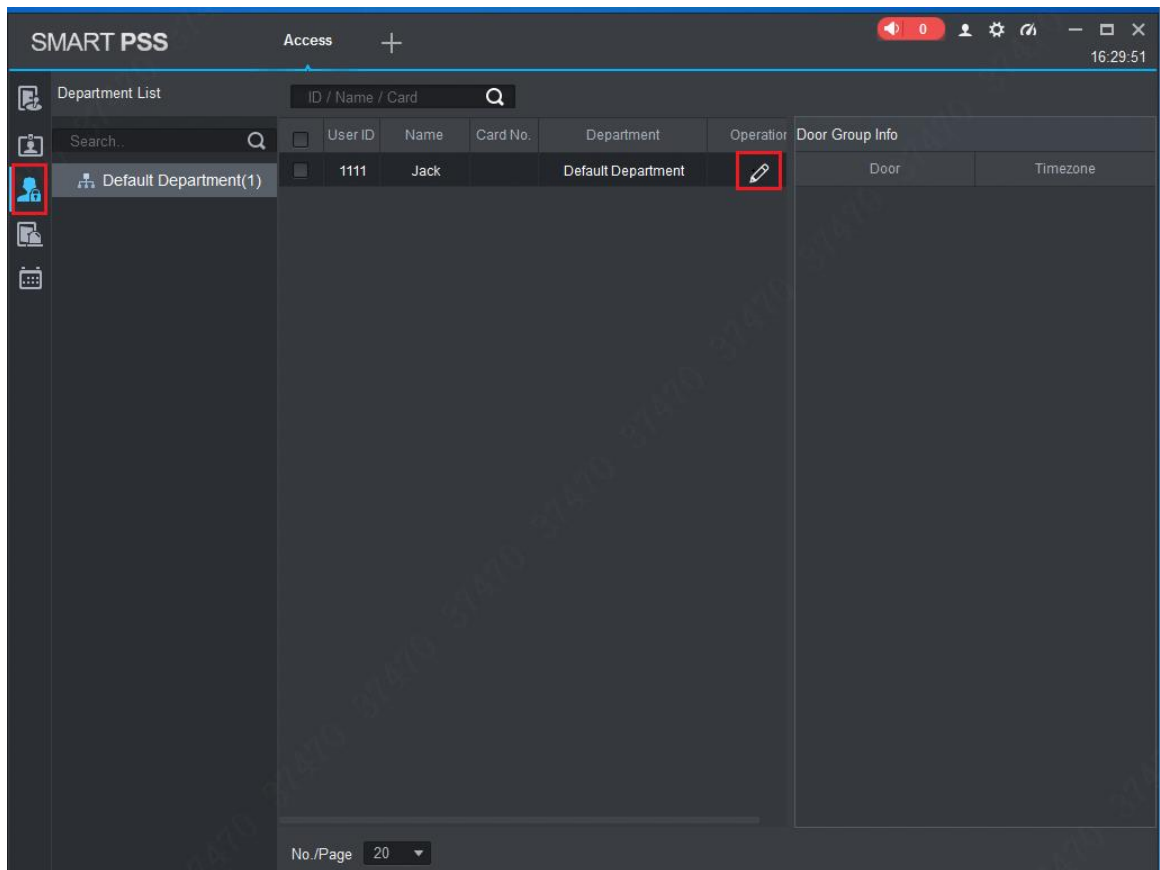
Vyberte uživatele, rozdělte skupinu dveří a udělte uživateli oprávnění ke skupině dveří.


**Krok 1** V rozhraní „Přístup“ klikněte na



a poté klikněte na „Uživatelské právo“, jak ukazuje Obrázek 3-17.

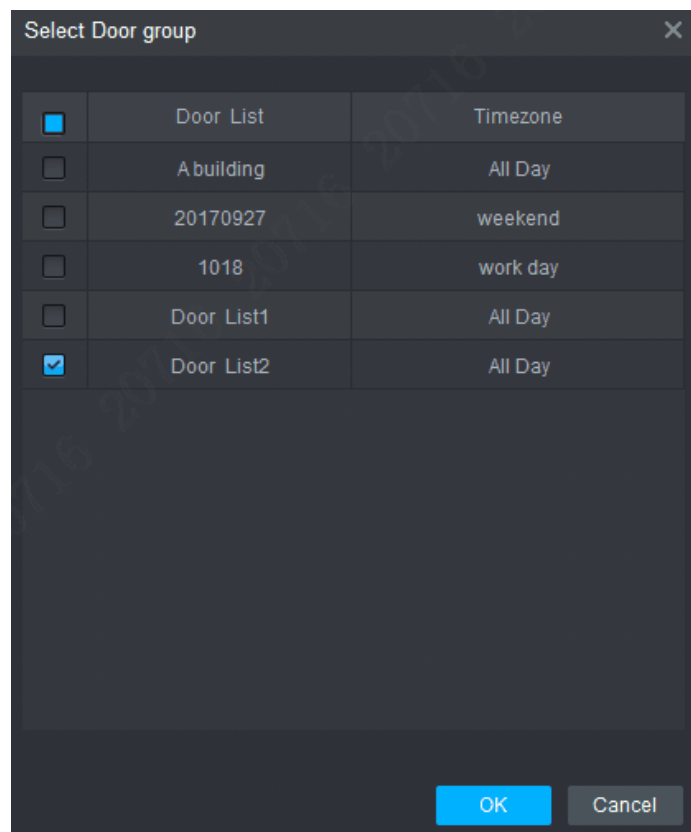
Obrázek 3-17



**Krok 2**  Klikněte

System zobrazí dialogové okno „Select Door Group“, jak je znázorněno na obrázku 3-18.

Obrázek 3-18



**Krok 3** Vyberte skupinu dveří a kliknutím na „OK“ dokončete autorizaci.



V případě problémů, které zde nejsou uvedeny, kontaktujte místní pracovníky zákaznického servisu nebo se obraťte na pracovníky zákaznických služeb ústředí. Budeme vám vždy k službám.

**1. Otázka: Po zapnutí se indikátor napájení nerozsvítí nebo bzučák nereaguje.**

Odpověď: Zkontrolujte, zda je zástrčka zasunuta na svém místě. Vytáhněte jej a znovu vložte.

**2. Otázka: Po připojení čtečky k zařízení se kontrolka přiložení karty nerozsvítí a po přiložení karty nereaguje.**

Odpověď: Zkontrolujte, zda je konektor čtečky zasunut na svém místě. Vytáhněte jej a znovu vložte; zkontrolujte, zda se rozsvítí kontrolka kontaktu čtečky.

**3. Otázka: Klientský software nedokáže detekovat zařízení.**

Odpověď: Zkontrolujte, zda je správně připojen konektor TCP/IP a zda je IP zařízení ve stejném segmentu sítě.

**4. Otázka: Po přiložení karty se zobrazí výzva, že karta je neplatná.**

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

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

Odpověď: Výchozí IP adresa je 192.168.0.2.

**6. Otázka: Výchozí port, počáteční uživatelské jméno a heslo přístupového kontroléru.**

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

**7. Otázka: Online upgrade zařízení.**

Odpověď: Připojte zařízení a platformu prostřednictvím sítě a upgradujte je na platformě.

**8. Otázka: Max. vzdálenost kabeláže a přenosová vzdálenost čtečky karet a ovladače.**

Odpověď: Záleží na typu síťového kabelu a zda potřebuje napájení ovládacího relé. Připojeno síťovým kabelem CAT5E, typická hodnota je:

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

# Dodatek 1 Doporučení pro kybernetickou bezpečnost

Kybernetická bezpečnost je víc než jen módní slovo: je to něco, co se týká každého zařízení připojeného k internetu. IP video dohled není imunní vůči kybernetickým rizikům, ale podniknutím základních kroků k ochraně a posílení sítí a síťových zařízení budou méně náchylné k útokům. Níže je několik tipů a doporučení od společnosti Dahua, jak vytvořit bezpečnější bezpečnostní systém.

## **Povinná opatření pro zabezpečení sítě základního vybavení: 1.**

### **Používejte silná hesla**

Pro nastavení hesel se řiďte následujícími návrhy:

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

### **2. Aktualizujte firmware a klientský software včas**

- Podle standardního postupu v Tech-industry doporučujeme udržovat firmware vašeho zařízení (jako je NVR, DVR, IP kamera atd.) aktuální, abyste zajistili, že systém bude vybaven nejnovějšími bezpečnostními záplatami a opravami. Když je zařízení připojeno k veřejné síti, doporučuje se povolit funkci „automatická kontrola aktualizací“, abyste získali včasné informace o aktualizacích firmwaru vydaných výrobcem.
- Doporučujeme, abyste si stáhli a používali nejnovější verzi klientského softwaru.

## **Doporučení pro zlepšení zabezpečení sítě vašeho zařízení: 1. Fyzická ochrana**

Doporučujeme provádět fyzickou ochranu zařízení, zejména úložných zařízení. Umístěte zařízení například do speciální počítačové místnosti a skříně a zaveďte dobře provedenou kontrolu přístupu a správu klíčů, abyste zabránili neoprávněným osobám ve fyzickém kontaktu, jako je poškození hardwaru, neoprávněné připojení vyměnitelného zařízení (jako je USB flash disk), sériový port) atd.

### **2. Pravidelně měňte hesla**

Doporučujeme vám, abyste hesla pravidelně měnili, abyste snížili riziko uhodnutí nebo prolomení.

### **3. Nastavte a aktualizujte hesla Resetujte informace včas**

Zařízení podporuje funkci resetování hesla. Nastavte související informace pro resetování hesla včas, včetně poštovní schránky koncového uživatele a otázek ochrany heslem. Pokud se informace změní, včas je upravte. Při nastavování otázek ochrany heslem se doporučuje nepoužívat ty, které lze snadno uhodnout.

### **4. Povolte zámek účtu**

Funkce uzamčení účtu je ve výchozím nastavení povolena a doporučujeme vám ji ponechat, aby byla zaručena bezpečnost účtu. Pokud se útočník několikrát pokusí přihlásit se špatným heslem, příslušný účet a zdrojová IP adresa budou uzamčeny.

## 5. Změňte výchozí porty HTTP a další služby

Doporučujeme vám změnit výchozí porty HTTP a dalších služeb na libovolnou sadu čísel mezi 1024~65535, čímž se sníží riziko, že lidé zvenčí budou schopni uhodnout, které porty používáte.

## 6. Povolte HTTPS

Doporučujeme vám povolit HTTPS, abyste navštívili webovou službu prostřednictvím zabezpečeného komunikačního kanálu.

## 7. Povolte seznam povolených

Doporučujeme vám povolit funkci whitelistu, abyste zabránili všem, kromě těch, kteří mají zadané IP adresy, v přístupu do systému. Proto prosím nezapomeňte přidat IP adresu vašeho počítače a IP adresu doprovodného zařízení na bílou listinu.

## 8. Vazba MAC adresy

Doporučujeme vám svázat IP a MAC adresu brány se zařízením, čímž se sníží riziko falšování ARP.

## 9. Přidělte účty a oprávnění přiměřeně

Podle obchodních a manažerských požadavků přiměřeně přidejte uživatele a přidělte jim minimální sadu oprávnění.

## 10. Vypněte nepotřebné služby a zvolte zabezpečené režimy

Pokud to není potřeba, doporučuje se vypnout některé služby, jako je SNMP, SMTP, UPnP atd., abyste snížili rizika.

Je-li to nutné, důrazně se doporučuje používat nouzové režimy, mimo jiné včetně následujících služeb:

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

## 11. Šifrovaný přenos zvuku a videa

Pokud je obsah vašich zvukových a obrazových dat velmi důležitý nebo citlivý, doporučujeme použít funkci šifrovaného přenosu, abyste snížili riziko odcizení zvukových a obrazových dat během přenosu.

Připomenutí: šifrovaný přenos způsobí určitou ztrátu účinnosti přenosu.

## 12. Zabezpečený audit

- Kontrola online uživatelů: doporučujeme pravidelně kontrolovat online uživatele, abyste zjistili, zda není zařízení přihlášeno neoprávněně.
- Kontrola protokolu zařízení: Zobrazením protokolů můžete zjistit adresy IP, které byly použity k přihlášení k vašim zařízením, a jejich klíčové operace.

## 13. Protokol sítě

Vzhledem k omezené skladovací kapacitě zařízení je uložená kláda omezena. Pokud potřebujete uložit protokol na dlouhou dobu, doporučuje se povolit funkci síťového protokolu, abyste zajistili synchronizaci kritických protokolů se serverem síťového protokolu pro trasování.

## 14. Vytvořte bezpečné síťové prostředí

Pro lepší zajištění bezpečnosti zařízení a snížení potenciálních kybernetických rizik doporučujeme:

- Vypněte funkci mapování portů routeru, abyste zabránili přímému přístupu k intranetovým zařízením z externí sítě.

- Sít' by měla být rozdělena a izolována podle skutečných potřeb sítě. Pokud neexistují žádné komunikační požadavky mezi dvěma podsítěmi, doporučuje se použít VLAN, síťový GAP a další technologie k rozdělení sítě, aby se dosáhlo efektu izolace sítě.
- Zaveďte systém ověřování přístupu 802.1x, abyste snížili riziko neoprávněného přístupu do privátních sítí.