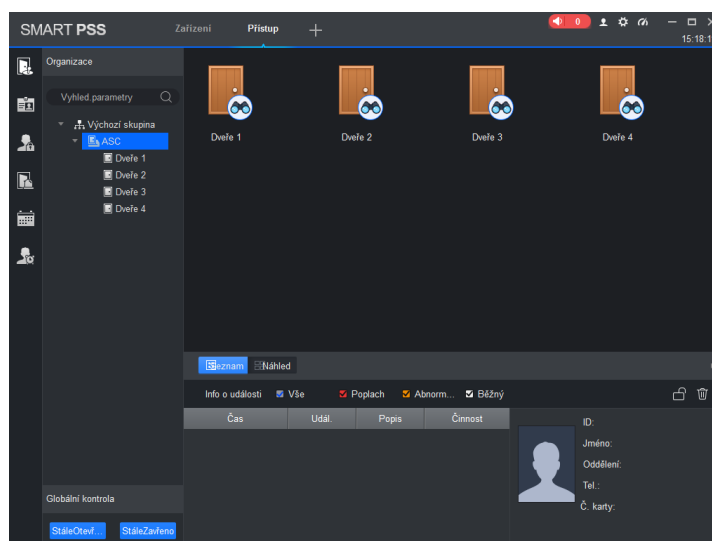


Instalační příručka pro přístupový systém Dahua



Bezpečnostní pokyny	3
1. Úvod.....	3
2. Komponenty a vzájemné propojení.....	3
2.1 Kontroléry.....	3
2.2 Čtečky vyžadující kontrolér.....	5
2.3 Autonomní čtečky.....	5
2.4 Software smartPSS	6
2.5 Software ACS Config	7
3. Základní IP konfigurace systému	7
3.1 Změna IP adres	7
3.2 Spárování zařízení se software smartPSS	7
3.3 Změna hesla pro přihlášení do zařízení (DŮLEŽITÉ PRO ZABEZPEČENÍ).....	8
3.4 Správa uživatelů přístupového systému.....	9
3.5 Základní oprávnění uživatelů	10
3.6 Hromadná změna oprávnění.	11
3.7 Plánovač.....	13
3.8 Export a Import.....	13
4. Základní lokální nastavení	14
4.1. Přihlášení (model ASI1212A).....	14
4.2. Přidání uživatele (model ASI1212A).....	14
4.3. Editace a smazání uživatele (model ASI1212A)	15
4.4. Přihlášení (model ASI1201A).....	15
4.5. Přidání uživatele (model ASI1201A).....	15
4.6 Smazání uživatele (model ASI1201A)	16
4.7 Doba přístupu (model ASI1201A).....	16
4.8 Systémová nastavení (model ASI1201A).....	16
4.9 Přidání karty správce (model ASI1201A).....	16
5. Pokročilé funkce oprávnění.....	17
5.1 Odemknutí první kartou.....	17
5.2 Odemknutí součinností	17
5.3 Vazba přístupu	17
5.4 Sekvenční zámek	17
5.5 Vzdálené ověření	17
6. Firmware, tovární nastavení	18
6.1 Aktualizace firmware.....	18
6.2 Návrat do továrních hodnot	18

Bezpečnostní pokyny

- Před použitím zařízení si pečlivě přečtěte uživatelský manuál.
- Uschovejte si tento manuál.
- Pokud zařízení prodáváte nebo dáváte jiné osobě, ujistěte se, že jste také předali tento návod.
- Používejte pouze nepoškozené přívodní kabely/napájecí adaptéry.
- Vaše elektrická síť musí odpovídat hodnotám uvedeným na výrobním štítku a elektrická zásuvka musí být uzemněna.
- Nepoužívejte k čištění abrazivní čisticí prostředky nebo kovové drátěnky. Zamezíte tak poškrábání povrchu. Před čištěním odpojte napájecí přívod.
- Zařízení nesmí obsluhovat osoby (včetně dětí) se sníženými fyzickými a smyslovými schopnostmi, nebo bez odpovídajících zkušeností, pokud nezajistíte dozor nebo přeškolení obsluhy osobou zodpovědnou za jejich bezpečnost.
- Zařízení používejte výhradně pro účely přístupového systému.
- Zařízení nesmí přijít do styku s ohněm.

1. Úvod

Přístupový systém Dahua **umožňuje uživatelům projít dveřmi na základě definovaných oprávnění a časových plánů**. Jako identifikační prvek uživatele může sloužit ID karta (přívěsek), biometrický otisk prstu, číselný kód, případně jejich kombinace.

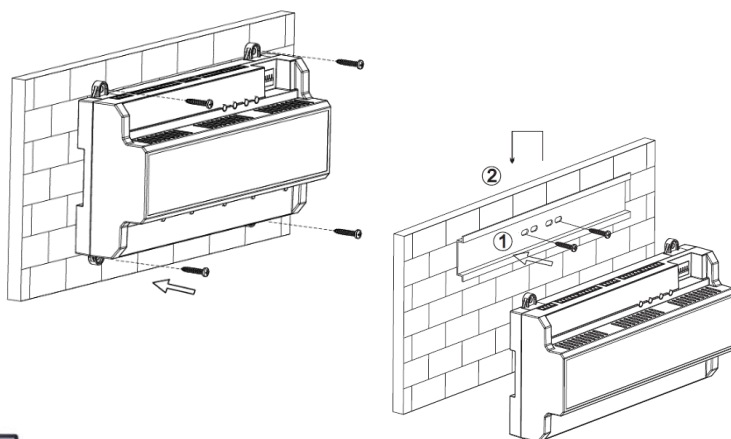
Systém se spravuje z centrálního místa pomocí software smartPSS vyžadující operační systém Windows.

2. Komponenty a vzájemné propojení

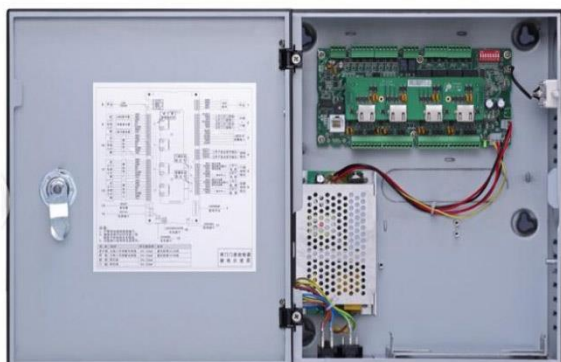
2.1 Kontroléry

Modely

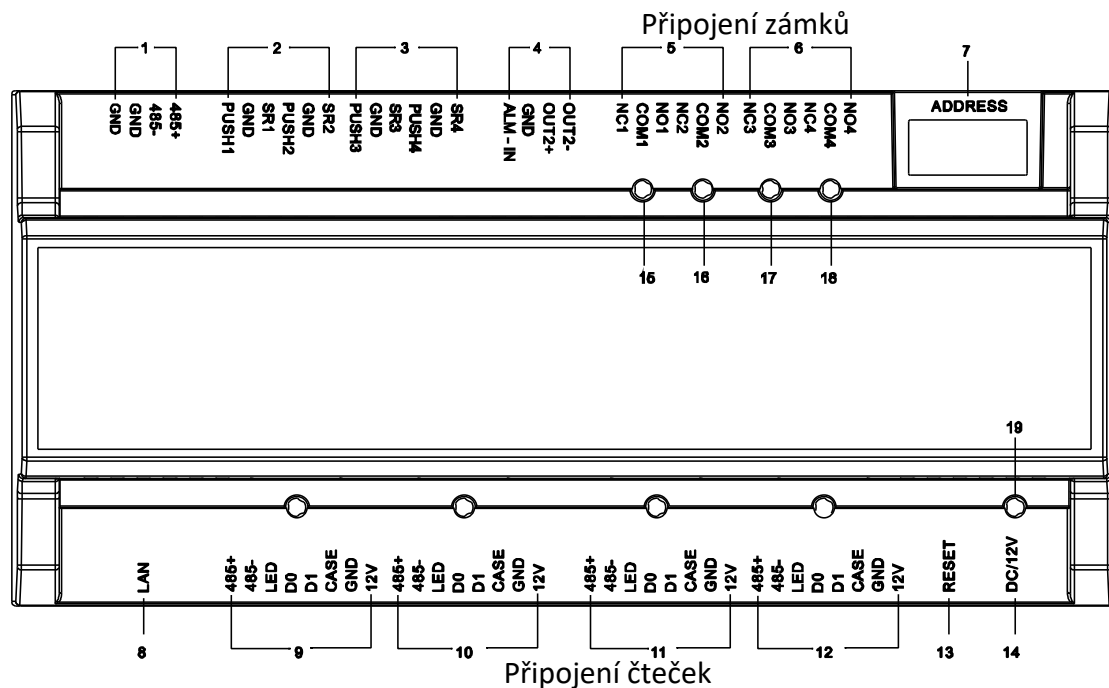
- ASC1204B na DIN lištu.



- ASC1204C v instalační skříni



Popis rozhraní



Č.	Port	Popis
1	GND GND 485- 485+	Připojení rozšiřujícího modulu, např. pro ovládání výtahu
2-3	PUSH1 GND, PUSH2 GND, PUSH3 GND, PUSH4 GND	Připojení odchodového tlačítka pro dveře1-4
	GND SR1, GND SR2, GND SR3, GND SR4	Připojení dveřního senzoru pro dveře1-4
4	ALM-IN GND, OUT+ OUT-	Alarmový vstup, alarmový výstup
5-6	NC1 COM1, NC2 COM2, NC3 COM3, NC4 COM4	Připojení zámku (NC – spínán odebráním napětí) pro dveře1-4; na COM přiveďte 12VDC
	COM1 NO1, COM2 NO2, COM3 NO3, COM4 NO4	Připojení zámku (NO – spínán přivedením napětí) pro dveře1-4; na COM přiveďte 12VDC
7	Address	DIP přepínače pro návrat do továrního nastavení Piny 1357 přepněte do polohy ON, restartujte zařízení a piny vraťte do polohy off
8	LAN	Připojení do sítě LAN pro správu přes smartPSS v počítači
9-12	485+ 485-	Připojení datových vodičů RS485 čtečky, max. 1000 m
	LED	Odezva Wiegand čtečky
	D0 D1	Připojení datových vodičů Wiegand čtečky, max. 40 m
	CASE	tamper kontakt
	GND 12V	Připojení napájecích vodičů čtečky, max. 100 m
13	Reset	Skryté tlačítko pro návrat do továrních hodnot
14	DC/12V	Připojení napájení 12 VDC do kontroléru
15-19		Signalizace odemknutí dveří 1-4 a napájení kontroléru

- Pokud mají dvě čtečky otevírat stejný zámek, můžete propojit výstup pro zámek druhé čtečky s odchodovým tlačítkem první čtečky. Další možností je připojit dvě RS485 čtečky na jeden vstup kontroléru (pro jednu raději přiveďte extra napájení).
- Pokud budou čtečky od sebe do vzdálenosti 20 cm, může docházet k vzájemnému rušení a čtečky nemusí správně reagovat na ID kartu.

2.2 Čtečky vyžadující kontrolér

Druhy čteček

- Rozdělení podle účelu
čtečka RFID / čtečka otisků prstů / čtečka RFID + klávesnice / čtečka RFID + čtečka otisků prstů
- Rozdělení podle frekvence RFID (nelze kombinovat různé frekvence v jednom systému)
13,56 MHz / 125 kHz (označení „-D“)
- Rozdělení podle technologie připojení
RS485 (max. 400 m) / Wiegand (max. 60 m) / USB (k počítači)

Připojení čtečky do kontroléru

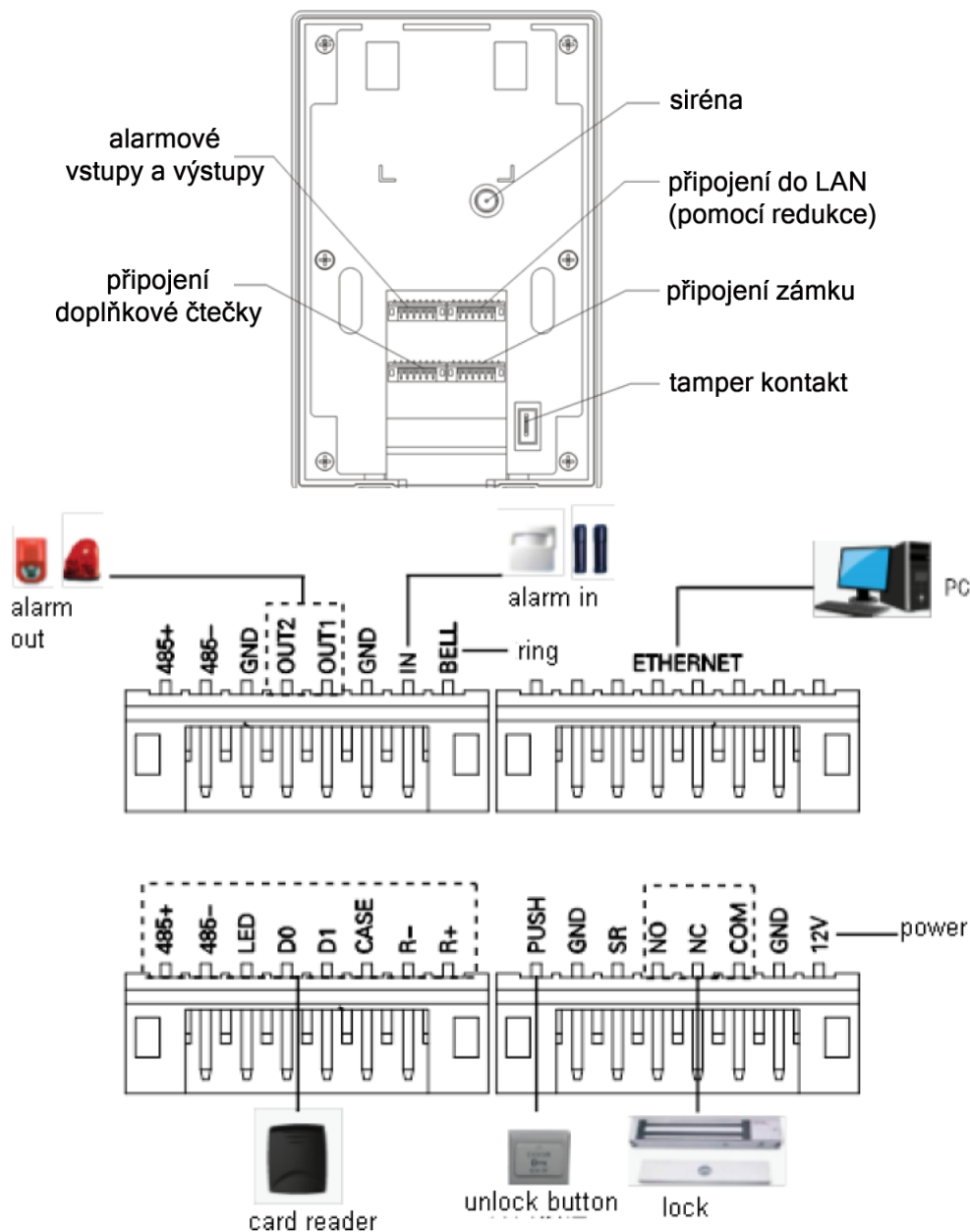
Čtečky mají vyvedeny barevné vodiče, které se nainstalují do svorkovnice kontroléru.

- Fialová -> 485+
- Žlutá -> 485-
- Hnědá -> LED
- Zelená -> D0
- Bílá -> D1
- Modrá -> Case
- Černá -> GND
- Červená -> 12V



2.3 Autonomní čtečky

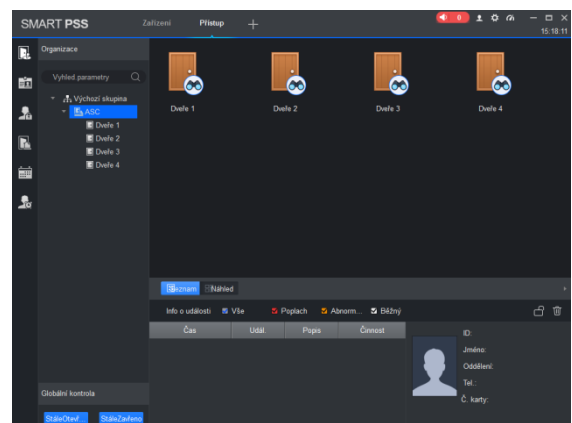
Autonomní čtečky **nevyžadují kontrolér**. Vše potřebné pro připojení mají již na sobě. Správa oprávnění přes **interní menu nebo přes aplikaci smartPSS** v počítači.



2.4 Software smartPSS

Software smartPSS umožňuje **uživatelsky přívětivou správu uživatelů a oprávnění** všech připojených kontrolerů a autonomních čteček. Doporučujeme **spravovat jen z jednoho počítače**, software nemá integrovanou funkci synchronizace, nicméně aktuální stav otevření dveří a záznamy událostí lze prohlížet i z vícero počítačů současně.

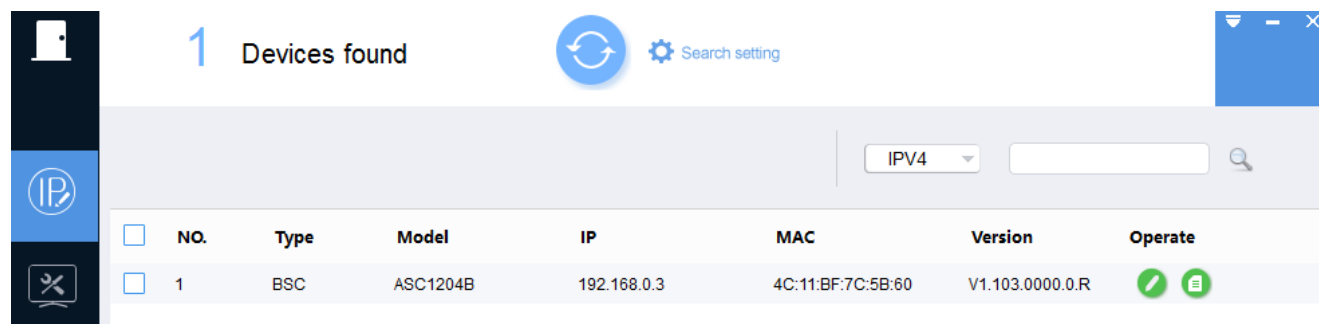
Stahujte pomocí utility [Dahua Toolbox](#)



2.5 Software ACS Config

Software slouží k vyhledání zařízení v síti, změnu IP adres, nahrání nového firmware, návrat do továrních hodnot.

Stahujte pomocí utility [Dahua ToolBox](#)

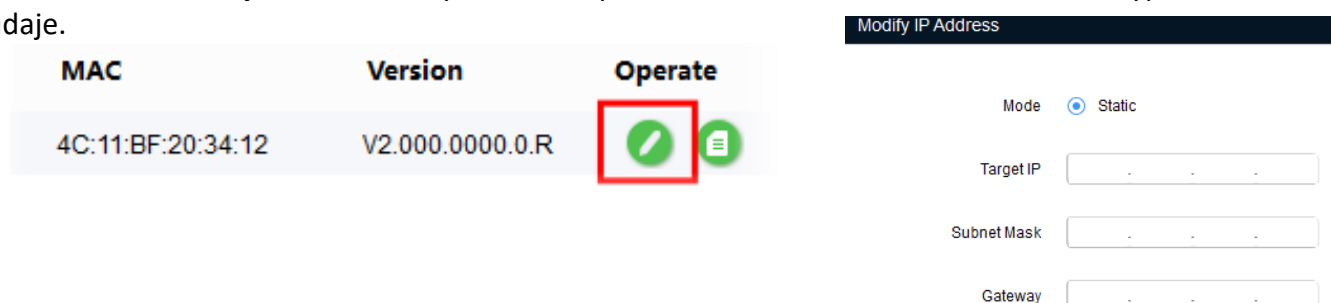


3. Základní IP konfigurace systému

3.1 Změna IP adres

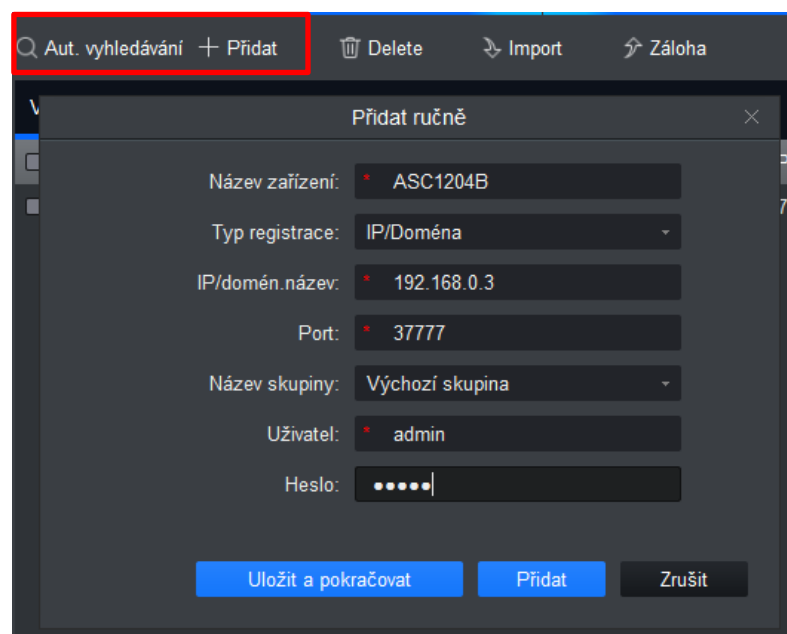
Spustíme software **ACS Config** (viz kapitola 2.5). Software nám automaticky nalezne připojená zařízení, ať jsou v kterémkoliv síťovém rozsahu. Tovární IP adresa je **192.168.0.2**.

Pro změnu IP adresy klikneme na symbol „tužky“ na konci řádku nalezeného zařízení a vyplníme nové údaje.



3.2 Spárování zařízení se software smartPSS

Spustíme aplikaci **smartPSS** (viz kapitola 2.4) a přejdeme do sekce „**Zařízení**“.



Pokud nám software automaticky nevyhledá zařízení, přiřadíme jej ručním zadáním – klikneme na „**Přidat**“.

Název zařízení ... libovolné označení

Typ registrace ... nechte „IP/Doména“

IP/domén.název ... **aktuální IP adresu** (továrně 192.168.0.2)

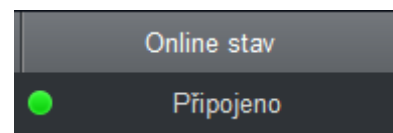
Port ... zadejte **37777**

Název skupiny ... přiřazení do organizační struktury

Uživatel ... zadejte **admin**

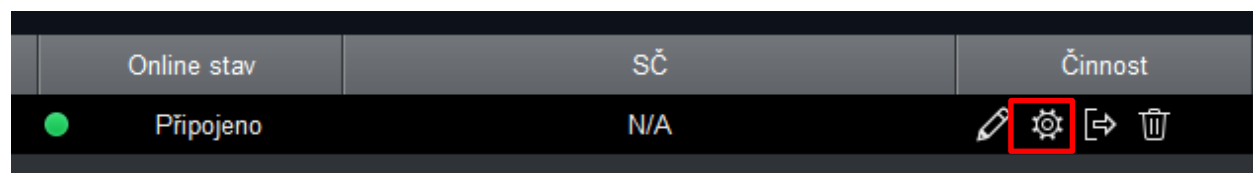
Heslo ... zadejte **123456**, popř. admin

Potvrdíme modrou volbou „Přidat“ a zkontrolujeme, že zařízení je připojeno.

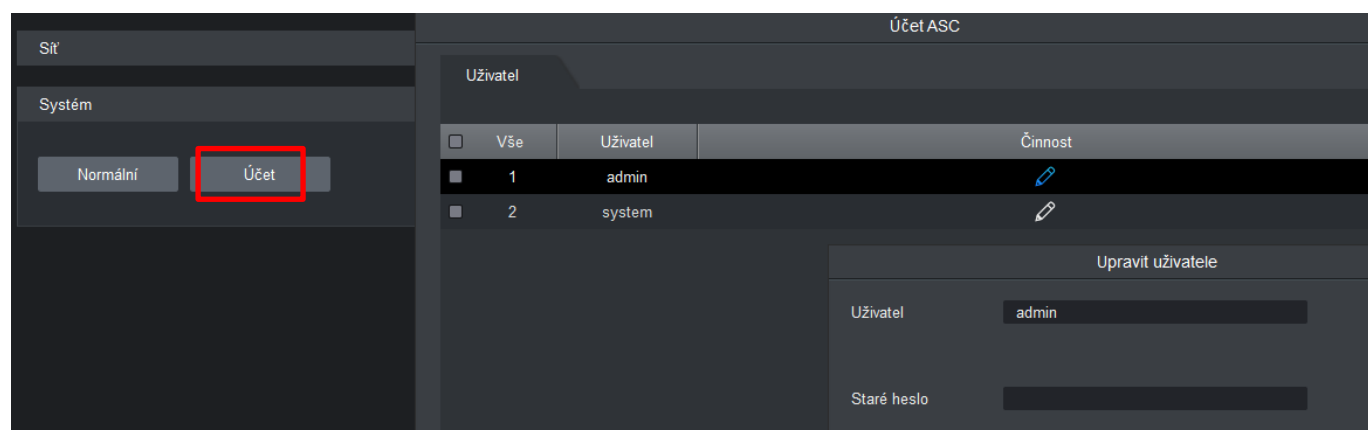


3.3 Změna hesla pro přihlášení do zařízení (DŮLEŽITÉ PRO ZABEZPEČENÍ)

V aplikaci **smartPSS** v sekci „**Zařízení**“ (viz předchozí kapitola) klikneme na symbol ozubeného kola v řádku daného zařízení.

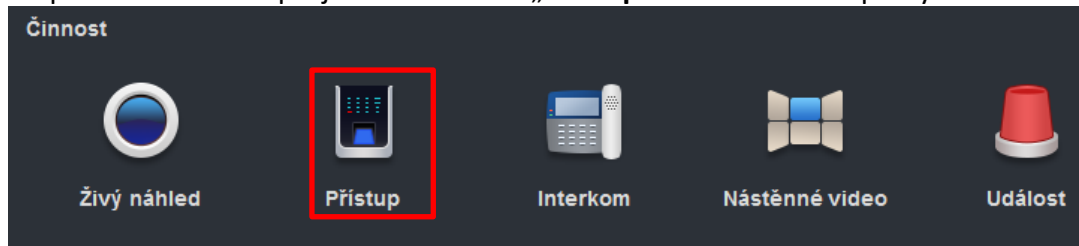


Následně přejdeme do sekce „**Systém**“ - „**Účet**“.

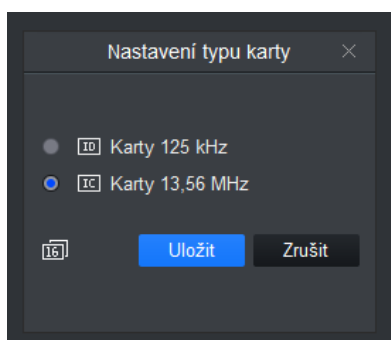
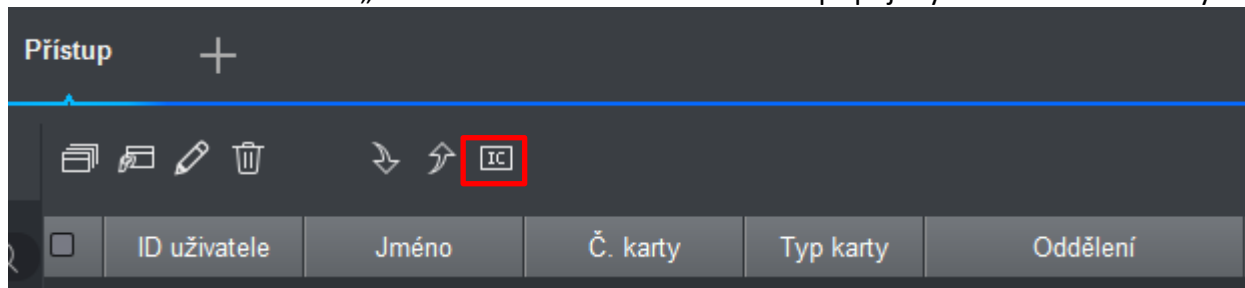


3.4 Správa uživatelů přístupového systému

V aplikaci **smartPSS** přejdeme do sekce „**Přístup**“ a následně do správy uživatelů



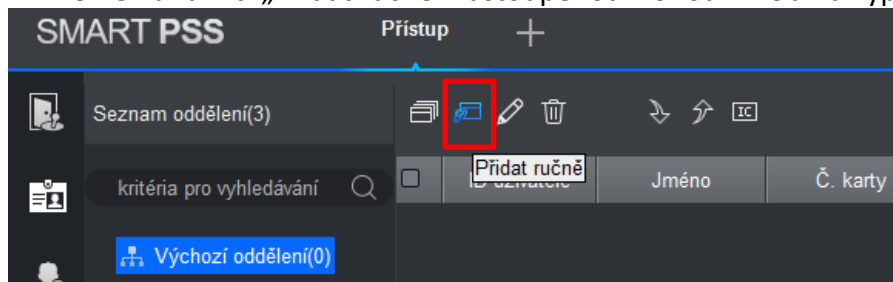
Klikneme na tlačítko „IC“ a nastavíme frekvenci připojených čteček a styl zadávání.



ID Card – zvolíme pro 125 kHz
IC Card – zvolíme pro 13,56 MHz

16/10 – styl zadávání čísel karet (hexa/decimální kód)

Klikneme na funkci „Přidat ručně“ zastoupenou ikonou viz obr. a vyplníme údaje.

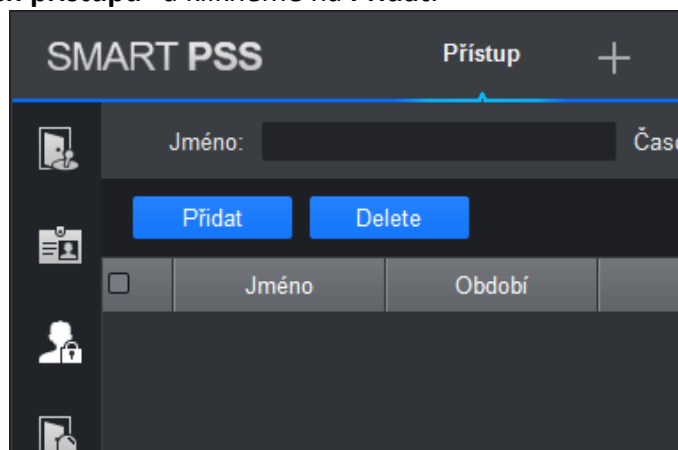
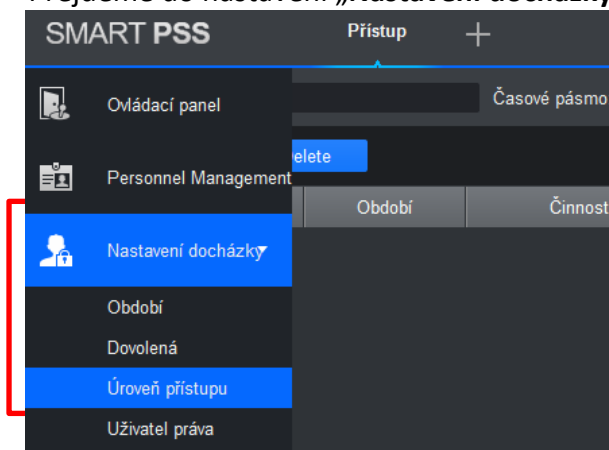


Číslo karty můžeme vyplnit ručně nebo využít čtečku karet. Máme-li USB čtečku ASM100, přepneme doplňující volbu na možnost „Karta vydána“ či „ASM100“ (dle revize překladu). Pro načtení karty přes pracovní čtečku ASRxxxx či ASlxxxx přepneme doplňující volbu na „Kontrolér“ a zvolíme danou pozici.

Pro vytvoření dalšího uživatele klikneme na „**Pokračovat v přidávání**“, jinak klikneme na „**Konec**“.

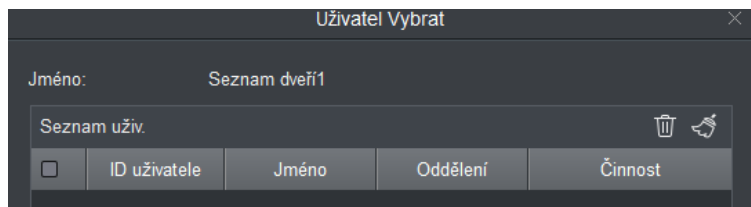
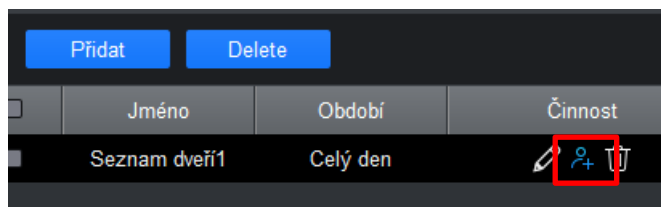
3.5 Základní oprávnění uživatelů

Přejdeme do nastavení „**Nastavení docházky**“ - „**Úroveň přístupu**“ a klikneme na **Přidat**.



Vytvoříme zde skupinu/skupiny dveří, do kterých budou moci uživatelé vstoupit. Můžeme zvolit jedny dveře i všechny dveře. Máme-li vytvořen časový plán přístupu (viz kapitola 3.5), můžeme jej zvolit pod položkou *Časová zóna*.

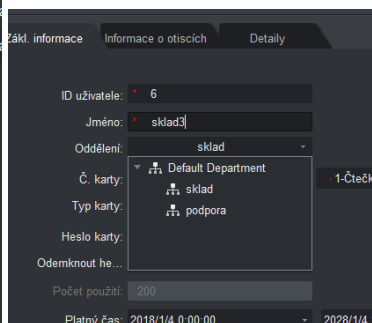
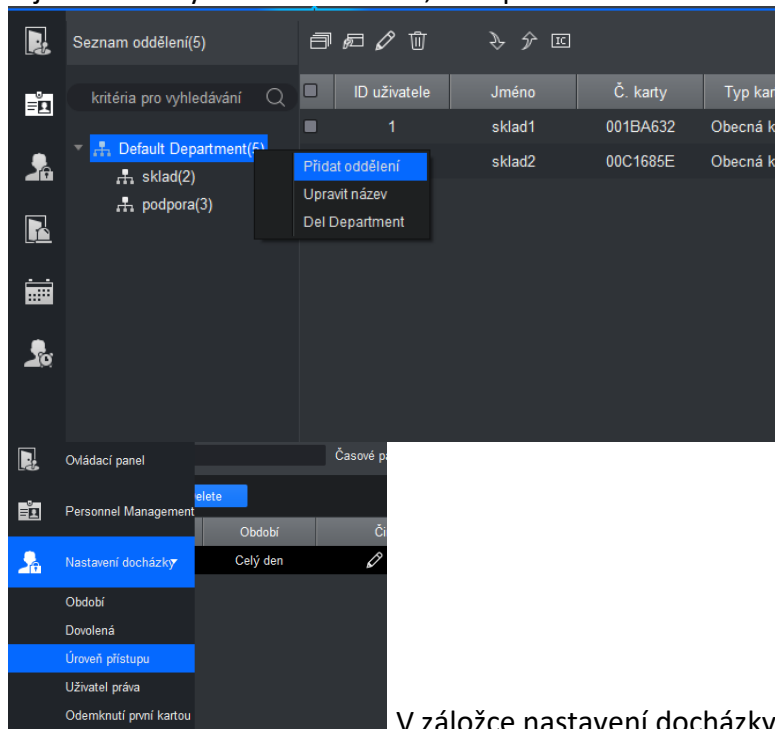
Po uložení klikneme na ikonu zvýrazněnou níže, poté ve spodní části **zvolíme oddělení**, které obsahuje uživatele, kterým chceme přidat oprávnění. Ukáží se zde jen ti **uživatelé, kteří mají přiřazenu ID kartu**. Vybereme požadované uživatele a klikneme na **Uložit**.



V tuto chvíli budou moci přidání uživatelé přiložením ID karty projít přes čtečku. Pokud smartPSS hlásí „chyba platnosti karty“ a používáte autonomní čtečku **ASlxxxx**, ověřte přes její interní menu, že je zde **správně nastaveno datum a čas**.

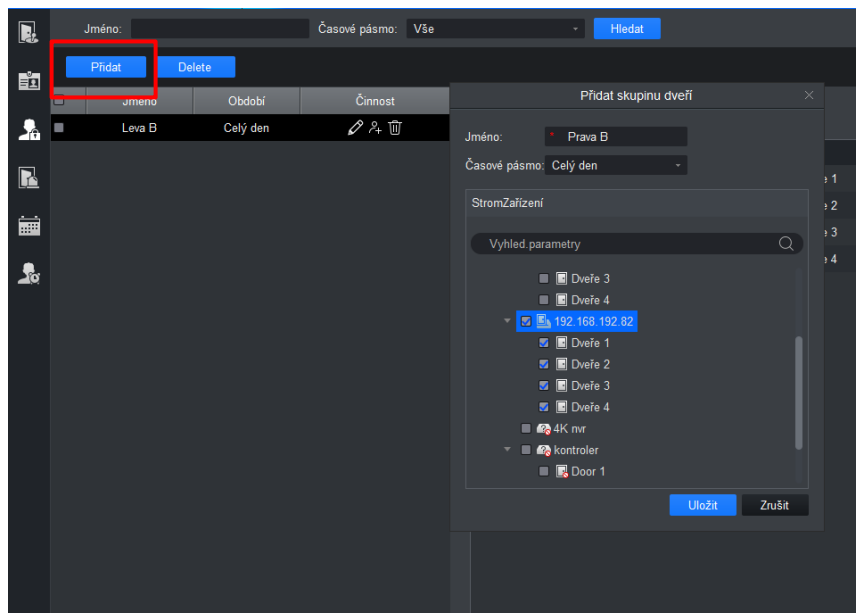
3.6 Hromadná změna oprávnění.


V záložce Personal management vytvoříme skupiny uživatelů. Nabídka se zobrazí po kliknutí pravým tlačítkem myši na Default Department. Když jsou skupiny vytvořené můžeme začít vytvářet uživatele. V jeho kartě vybereme oddělení, kam patří.

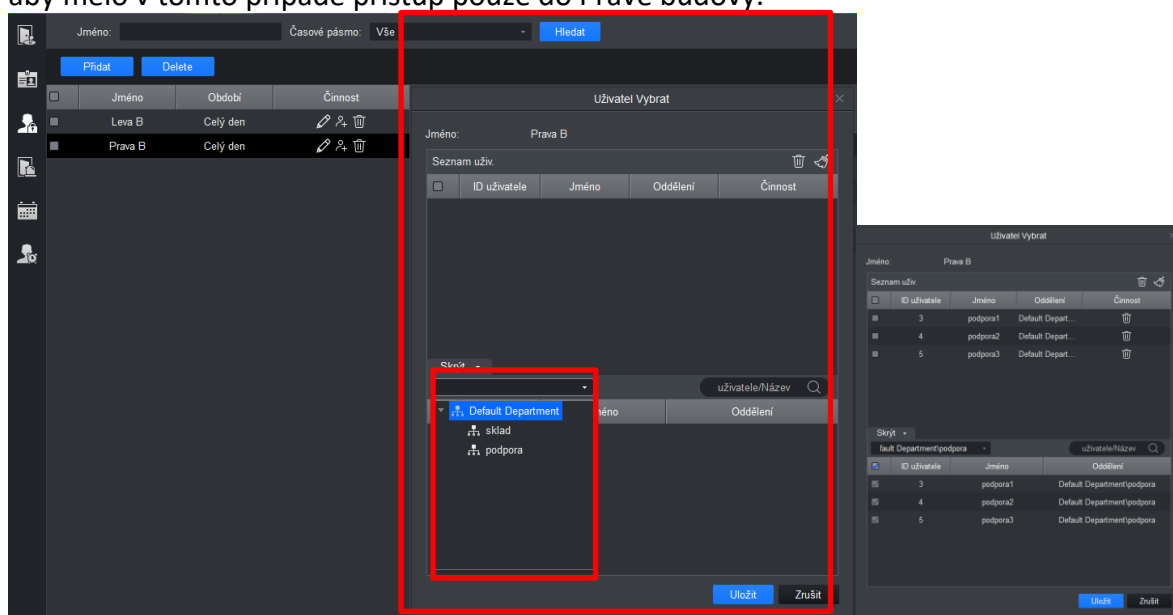


V záložce nastavení docházky vybereme možnost Úroveň přístupu

Zde vytvoříme seznamy dveří pro jednotlivá místa, kde jsou kontroléry např.: Pravá budova, Levá budova atd... a přiřadíme k nim požadované kontroléry.

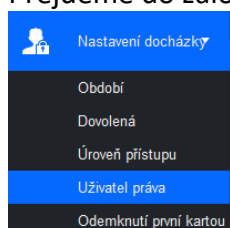


Kliknutím na ikonu  přidáme oddělení s uživateli do kontroléru kam budou mít přístup. Otevře se tabulka a ve spodní části, kde otevřeme rozvíjecí nabídku. Vybereme oddělení, které chceme aby mělo v tomto případě přístup pouze do Pravé budovy.




Vybereme všechny uživatele a dáme uložit.

Přejdeme do záložky Uživatelská práva a vybereme skupinu uživatelů.

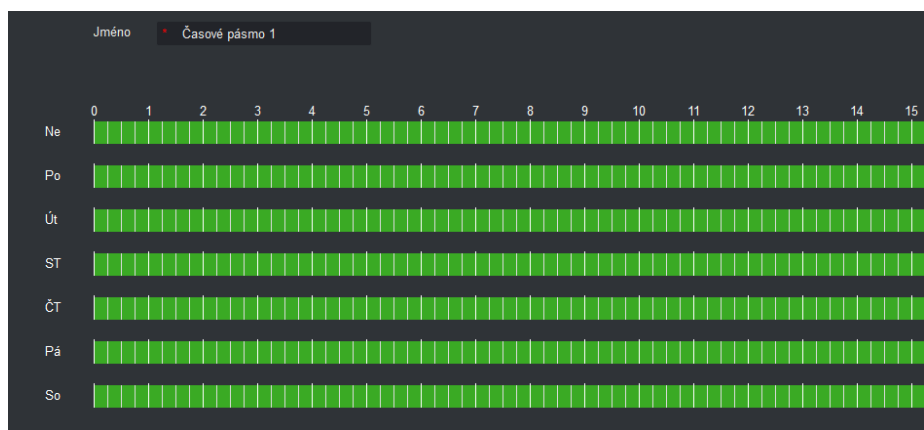
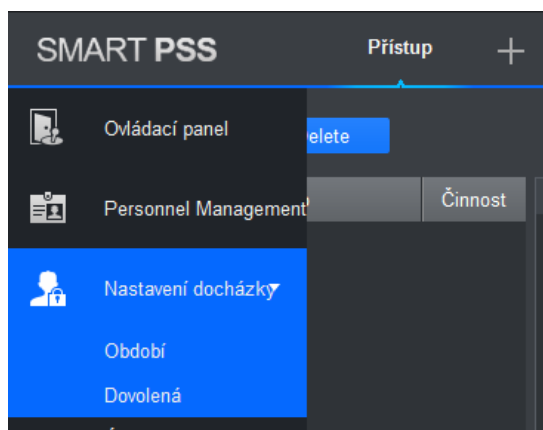


ID / Jméno / Karta	ID uživatele	Jméno	Č. karty	Oddělení	Činnost
Default Department(5)	3	podpora1	0030CAF2	Default Depar...	
uMaad(2)	4	podpora2	0030C582	Default Depar...	
podpora(3)	5	podpora3	0034481A	Default Depar...	

Označíme všechny uživatele a klikneme na ikonu , zde vybereme Dveře, respektive budovu kam mají přístup.

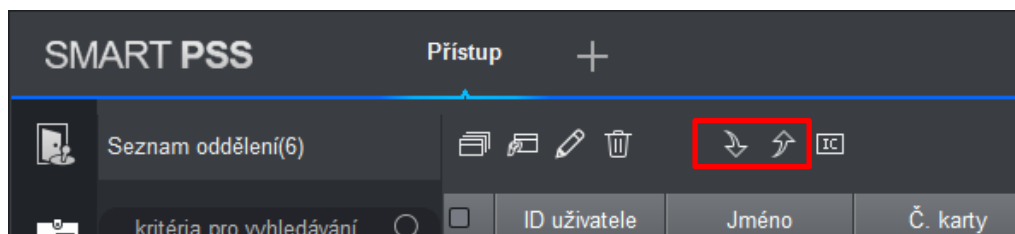
3.7 Plánovač

Můžeme nastavit časový plán, podle kterého se bude mít uživatel přístup pouze v předdefinované časové rozmezí. Přejdeme do nastavení „Nastavení docházky“ - „Plán“ či „Období“ (dle revize překladu) a vytvoříme zde týdenní časové schéma přístupu. Následně přejdeme do nastavení „Dovolená“ či „Platnost plánu“ (dle revize překladu), kde vytvoříme období, ve kterém má být vytvořený Plán platný.



3.8 Export a Import

SmartPSS umožňuje provést export a import uživatelů přes příslušnou funkci software, příp. zálohu a obnovení všech položek pomocí přenosu určitých souborů z C:\Users\Public\SmartPSS\ viz níže



Název	Přípona
AccessControl	db
ACSEventInfo	db
ACSManagerDbFile	db
ACSRightDeviceDbFile	db

4. Základní lokální nastavení

Lokální nastavení slouží pro přímé základní nastavení, jako je přidání a odebrání uživatele.

4.1. Přihlášení (model ASI1212A)

Stiskněte OK pro vyvolání rozhraní přihlášení, kde zadejte administrátorské jméno „000000“ a heslo „123456“ (obojí bez uvozovek). Pokud je definována karta nebo otisk prstu administrátora, lze k nastavení přistupovat přímo danou osobou.

Pro pohyb v menu použijte následující prvky:

- **【↑】** pohyb nahoru
- **【↓】** pohyb dolů
- **【OK】** potvrzení volby
- **【↶】** návrat nebo odchod
- **【←】** smazat
- **【🔔】** zvonek

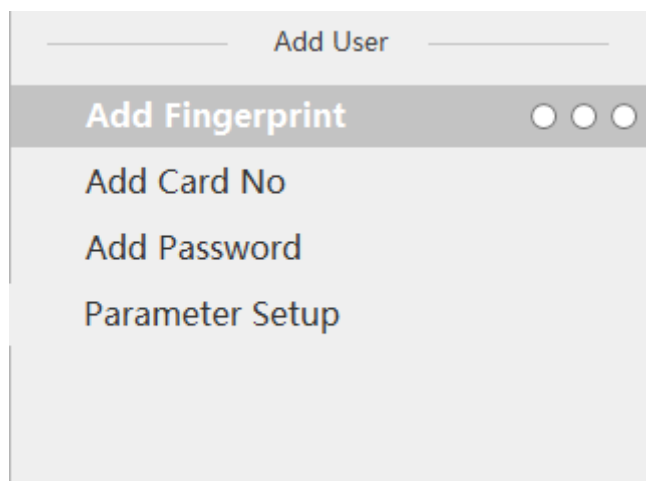


4.2. Přidání uživatele (model ASI1212A)

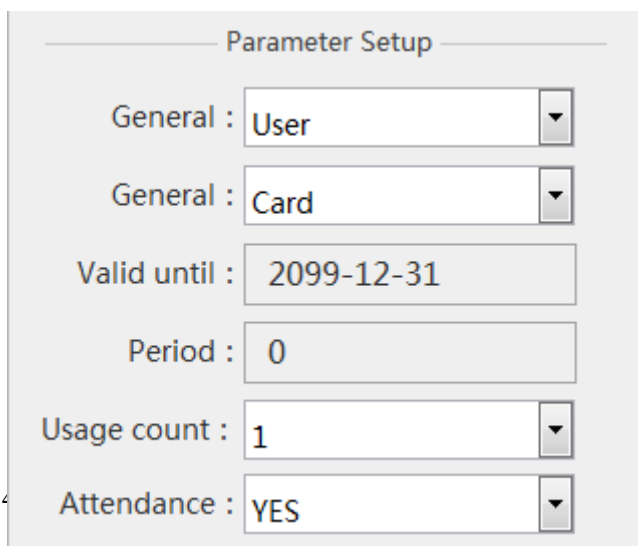
Na základní obrazovce stiskněte **【↑】** nebo **【↓】**, vyberte položku uživatele „user“, potom vyberte přidat uživatele „add user“, potvrďte OK.

Stiskněte **【↑】** nebo **【↓】** pro editaci uživatele, potom potvrďte OK.

Lokální nastavení umožňuje zadat pouze uživatele s 5-ti místným ID.



V menu přidání uživatele „add user“ lze definovat patřičný otisk prstu „fingerprint“, číslo karty „card no“, zadat heslo uživatele „add password“ a změnit parametry „set parameter“.



Parametry uživatele:

- úroveň „level“: general- obecná, manager-pro náhled na všechny záznamy, admin-správce
- typy karty „card type“: general, VIP, guest, patrol, blacklist, duress
- platnost uživatele „validity“
- délka trvání „period“
- doba používání „times of use“
- s obsluhou „attendance“

4.3. Editace a smazání uživatele (model ASI1212A)

Na základní obrazovce stiskněte **【↑】** nebo **【↓】** , vyberte položku uživatele „user“, potom vyberte editovat uživatele „edit user“, potvrďte OK.

Při editaci můžete změnit příslušný otisk prstu, přístupovou kartu a další parametry uživatele.

V menu uživatele „user“, potom vyberte smazat uživatele „delete user“, pro odebrání uživatele ze systému.

4.4. Přihlášení (model ASI1201A)

Stiskněte # a zadejte heslo (standardně 88888888), bude možné měnit nastavení uživatelů, odemknutí, času a systému.

Pro pohyb v menu užíjte následující prvky:

- **【2】** pohyb nahoru
- **【8】** pohyb dolů
- **【#】** potvrzení volby
- **【*】** návrat nebo odchod

4.5. Přidání uživatele (model ASI1201A)

Na základní obrazovce stiskněte **【2】** nebo **【8】** , vyberte položku nastavení uživatelů „user management“, potom vyberte přidat uživatele „add user“, dále přidat kartu „add card“, jednotlivě „single card“, běžnou „normal card“, potvrďte **【#】** .

Pomocí **【2】** nebo **【8】** definujte číslo karty a tu pak přiložte ke čtečce, nově přidaná karta bude zobrazena na displeji, potvrďte **【#】** , systém se vás dotáže, zda spárovat kartu s heslem (6-místné). Dále zvolte periodu denního užívání karty, její platnost, potvrďte **【#】** pro uložení.

Pro přidání více uživatelů a jejich karet zvolte v menu „continuous card“ a typ karet „normal“, potom lze přidat více karet najednou, potom se způsob přidávání opakuje dle výše zmíněného.



4.6 Smazání uživatele (model ASI1201A)

Lze smazat jednotlivé karty a uživatele, nebo postupně nebo všechny najednou.

V menu vyberte smazat uživatele „delete user“, zadejte číslo karty nebo kartu přiložte ke čtečce pro její smazání, volbu potvrďte **【#】** .

Pro mázání více karet zvolte v menu „continuous“, pro smazání všech karet zvolte v menu „all“.

Pro smazání hesla uživatele zvolte v menu „delete password“, pak zadejte číslo uživatele.

4.7 Doba přístupu (model ASI1201A)

Dobou přístupu se rozumí perioda, kdy bude umožněno uživateli vstoupit do objektu. Lze definovat až 128 period, pro každou periodu je nutné nastavit pro jaký den v týdnu bude platná, například pracovní dny pondělí až pátek od 8hod do 18hod.

V hlavním menu vyberte volbu definice periody doby přístupu „time period“, vyberte patřičnou periodu a zadejte její číslo (0~127), potom ji definujte a potvrďte **【#】**.

Standardní periodou je veškerý čas, kdy bude přístup umožněn vždy.

Pokud karta nebo heslo spadají do prázdninové „holiday“ periody, nebude jim umožněn přístup.

4.8 Systémová nastavení (model ASI1201A)

V systémovém nastavení lze definovat IP adresu autonomního zařízení, typ komunikace, datum a čas, nastavení poplachu.

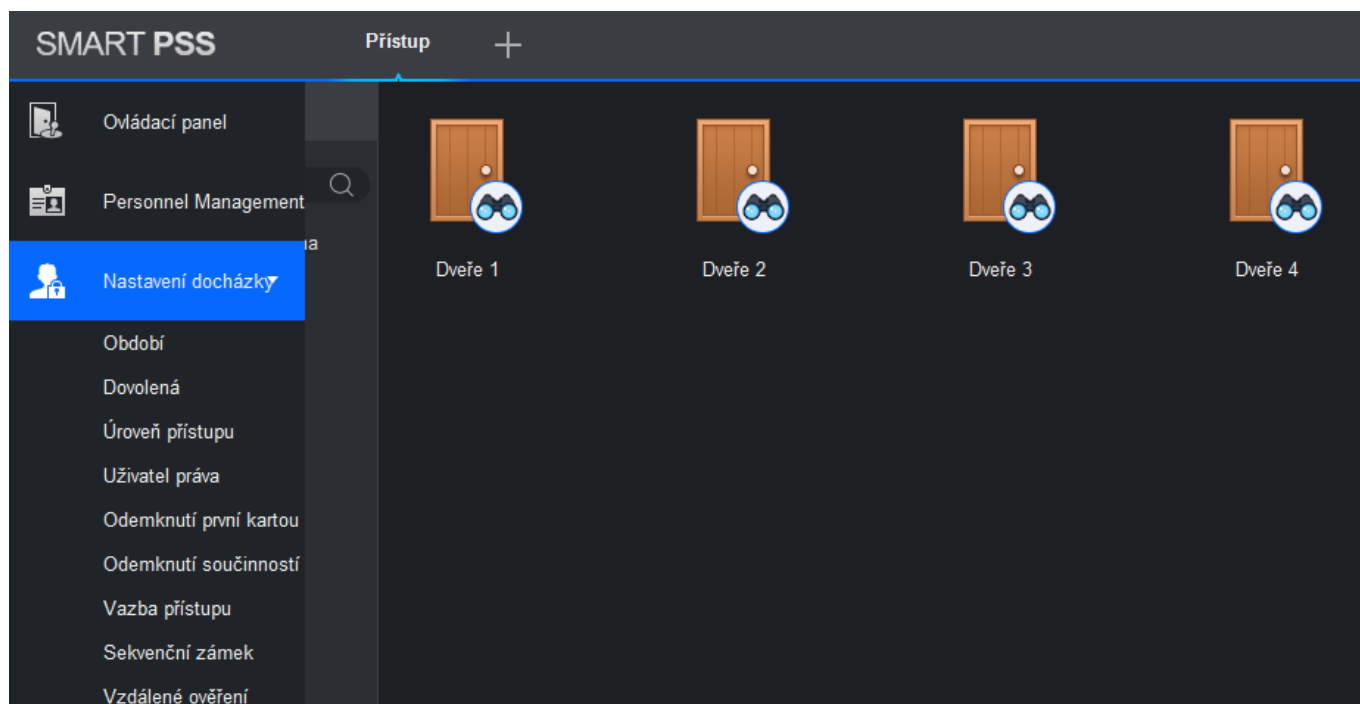
Poplachy se mohou vztahovat na dlouho otevřené dveře „overtime“, násilné otevření „intrusion“, zlomyslné „forced“ otevření kartou nebo heslem (je nutné definovat předem), poničení zařízení „vandal-proof alarm“. Pro aktivaci zvolte v menu položku „alarm“.

4.9 Přidání karty správce (model ASI1201A)

Karta správce umožňuje přidat uživatele, pro její přidání zvolte v menu „master card“ a její změnu „modify“, potom zadejte číslo karty nebo ji přiložte ke čtečce.

Pro přidání karty běžného uživatele zvolte v menu možnost přidání uživatele master kartou „add card with master card“, vyberte obecnou kartu a zda budete definovat hesla. Potom zvolte příslušnou periodu ke kartám. Systém vás vyžádá přiložit master kartu ke čtečce.

5. Pokročilé funkce oprávnění



5.1 Odemknutí první kartou

Nadefinujeme uživatele, kteří musí přiložit kartu jako první, aby mohli další uživatelé vstoupit.

5.2 Odemknutí součinností

Tato funkce vyžádá přiložení více karet, než je umožněn vstup.

5.3 Vazba přístupu

Uživatel zde zařazený nemůže dvakrát po sobě přijít stejnými dveřmi. Jakmile přiloží kartu na vstupní čtečku, musí poté přiložit na odchodovou (musí odejít), aby mohl opět vstoupit do objektu.

5.4 Sekvenční zámek


Uživatel nemůže otevřít více dveří současně.


5.5 Vzdálené ověření

Jakmile uživatel přiloží kartu na čtečku, objeví se v software smartPSS výzva k povolení nebo zamítnutí žádosti o vstup. Vyžaduje tedy součinnost operátora smartPSS.

6. Firmware, tovární nastavení

6.1 Aktualizace firmware


Spustíme software **ACS Config** a přepneme se do aktualizací sekce kliknutím na , zadáme umístění nového firmware a spustíme aktualizaci kliknutím na „Upgrade“.

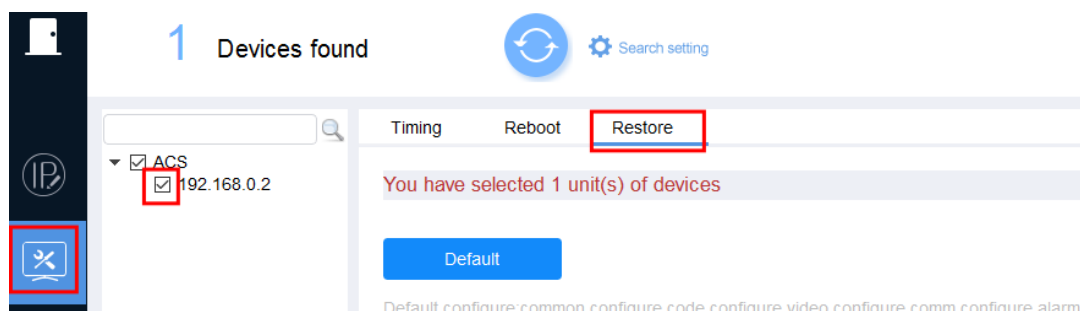


<input type="checkbox"/>	NO.	Type	IP	Version	Upgrade File Path	Browse	Operate
<input type="checkbox"/>	1	BSC	192.168.0.3	V1.103.0000.0.R		<button>Browse</button>	<button>Upgrade</button>

6.2 Návrat do továrních hodnot

a) Známe přihlašovací heslo

Spustíme software **ACS Config** a přepneme se do konfigurační sekce kliknutím na , zatrhneme zařízení, kterému chceme vrátit tovární nastavení, přepneme se do záložky „Restore“ a klikneme na „Default“.



b) Neznáme přihlašovací heslo

Pouze pro kontrolér. Nastavte adresu na 1357, poté restartujte kontroler. V tu chvíli by mělo být obnoveno tovární nastavení a přepínače můžete vrátit do původní polohy.

