2N Access Commander

Uživatelský manuál

2N TELEKOMUNIKACE a.s.
Modřanská 621 | Prague 4 | 143 01

2N.com

Abstrakt

Firmware 3.1

Obsah

Použité symboly a termíny

V manuálu jsou použity následující symboly a piktogramy:

NEBEZPEČÍ
Vždy dodržujte tyto pokyny, abyste se vyhnuli nebezpečí úrazu.

VAROVÁNÍ
Vždy dodržujte tyto pokyny, abyste se vyvarovali poškození zařízení.

VÝSTRAHA
Důležité upozornění. Nedodržení pokynů může vést k nesprávné funkci zařízení.

TIP
Užitečné informace pro snazší a rychlejší používání nebo nastavení.

POZNÁMKA
Postupy a rady pro efektivní využití vlastností zařízení.

Obecné informace

2N Access Commander je softwarový nástroj pro hromadnou správu přístupového systému. Rozhraní **Access Commanderu** je přístupné prostřednictvím webového prohlížeče.

V rámci jedné instalace lze nastavení **Access Commanderu** rozdělit do **Společností**, jejichž správa se provádí odděleně. Tento způsob umožňuje rozdělit správu mezi správce v jednotlivých společnostech. Správce z jedné společnosti tak nemá přístup k informacím o jiné společnosti. Správci z jedné společnosti neuvidí uživatele jiné společnosti.

Pro správu přístupů je nutné přidat do **Access Commanderu Zařízení**. Zařízení jsou fyzické jednotky v objektu ovládající vstupy (2N interkomy nebo 2N přístupové jednotky) nebo umožňující komunikaci (2N odpovídací jednotky). Zařízení se seskupují do **Zón**. Každé zařízení může být pouze v jedné zóně.

Zóny nebo zařízení lze sdílet napříč společnostmi, což umožňuje správu přístupu společnosti do společných prostor (vstupy, restaurace, konferenční sály...).

Uživatelé jsou jednotliví lidé, jejichž pohyb po objektu je nutné spravovat, případně kterým lze z připojených zařízení volat. Uživatelé se seskupují do **Skupin**, ve kterých se provádí hromadná správa jejich přístupu do zón. Uživatel se na zařízení autentizuje a zařízení následně vyhodnotí, má-li uživatel na zařízení platný přístup. Platnost přístupu se řídí podle **Přístupových práv**. Vybraní uživatelé mohou mít také oprávnění ke správě **Access Commanderu** nebo jeho částí.

Časové profily nastavují časy, ve kterých zařízení povoluje přístup nebo ve kterých je možné uživatelům volat.

Modul docházka umožňuje sledování docházky uživatelů.

Modul přítomnost umožňuje sledovat, v jakých zónách se uživatelé aktuálně nacházejí.

Návštěvy jsou lidé, jejichž přístupová práva jsou platná pouze omezenou dobu.

Uživatelská oprávnění

Správu v **Access Commanderu** může provádět více uživatelů v závislosti na jim přiřazených oprávněních.

Účty s rozšířeným oprávněním se nastavují prostřednictvím role v nastavení uživatele. Jednomu uživateli je možné přiřadit více rolí.

POZNÁMKA
Uživatelská oprávnění se vztahují na správu v rámci společnosti daného uživatele. Administrátor má přístup ke kompletní správě napříč společnostmi.

Administrátor

- Nastavení systému a jednotlivých modulů dle platné licence.
- Změna licence.
- Veškerá oprávnění ostatních rolí vztahující se na všechny společnosti.

Správce přístupu

- Vytváření a správa skupin.
- Přidávání uživatelů do skupin.
- Vytváření a správa časových profilů.
- Nastavení přístupových pravidel.

Správce uživatelů

- Vytváření a správa uživatelů.
- Vytváření a správa návštěv.
- Správa jejich členství ve skupinách.
- Nahlížení do přístupového a systémového logu.

Správce návštěv

- Vytváření a správa návštěv.
- Správa jejich členství ve skupinách (nedostupné ve zjednodušeném rozhraní).
- Nahlížení do přístupového logu návštěv (nedostupné ve zjednodušeném rozhraní).

Správce dveří

- Sledování kamerového přenosu z přidělených zařízení.
- Vzdálené otevírání přidělených zařízení.
- Nouzové uzamknutí přidělených zařízení.
- Nahlížení do přístupového logu přidělených zařízení.
- Sledování stavů a bezpečnostních událostí v systémovém logu.

Správce docházky

- Sledování a správa docházky přidělených skupin.
- Nahlížení do přístupového logu uživatelů přidělených skupin.

Podporovaná zařízení a aplikace

Tato kapitola obsahuje seznamy podporovaných zařízení, podporovaných webových prohlížečů a kompatibilních virtualizačních platforem, prostřednictvím kterých je možné **Access Commander** instalovat.

Podporovaná zařízení

Níže je uveden přehled zařízení podporovaných přístupovým systémem **Access Commander**. Tato zařízení lze v systému spravovat.

POZNÁMKA
Podporované verze firmwaru těchto zařízení jsou uvedeny v kapitole Firmware (str. 40).

Interkomy 2N

- 2N IP Style – podporuje čtení QR kódů
- 2N IP Verso 2.0 – podporuje čtení QR kódů
- 2N IP Verso
- 2N LTE Verso
- 2N IP Force
- 2N IP Safety

- 2N IP Vario
- 2N IP Base
- 2N IP Solo
- 2N IP Uni
- 2N IP Video Kit
- 2N IP Audio Kit
- 2N IP Audio Kit Lite

Přístupové jednotky 2N

- Access Unit QR – podporuje čtení QR kódů
- 2N Access Unit 2.0
- 2N Access Unit
- 2N IP Access Unit M

Odpovídací jednotky 2N

- 2N Indoor View
- 2N Indoor Compact
- 2N Indoor Talk
- 2N Indoor Touch 2.0
- 2N Clip

Webové prohlížeče

Konfigurace **Access Commanderu** se provádí prostřednictvím webového rozhraní. Systém byl optimalizován pro prohlížeč Google Chrome (verze 90 a vyšší.)

Další podporované prohlížeče:

- Mozzila Firefox (verze 78 a vyšší)
- Microsoft Edge (verze 91 a vyšší)
- Safari (verze 14 a vyšší)

Ostatní prohlížeče nebyly testovány, nelze tak zaručit jejich plnou funkčnost.

Virtualizační platformy

- Virtual Box
- VMware Player (verze 6.5 a vyšší)
- VMware vSphere (verze 6.5 a vyšší)
- Hyper-V

Použité porty

Tabulka 1. Seznam služeb a potřebných portů

Služba	Port
HTTP/HTTPS[a.]	80/443
SMTP	225
DHCP	68
DNS	53
NTP	123
LDAP[b.]	389
SSH	22

[a.] Používá se jak pro komunikaci s klientem, tak pro komunikaci s vrátníky.

[b.] Uživatel může v nastavení **Access Commanderu** zvolit jiný port pro službu LDAP.

Přehled licencí

Po úvodní instalaci **Access Commanderu** je k dispozici zkušební Trial licence. Trial licence umožňuje zkoušku všech funkcí na správě 1 zařízení a 5 uživatelů. Pro plnohodnotnou správu je potřeba aktivovat jednu ze čtyř licencí: *Basic* (zdarma), *Advanced*, *Pro* nebo *Unlimited*.

Licence:	Trial	Basic	Advanced	Pro	Unlimited
Objednací číslo	n/a	n/a	91379031	91379032	91379033
Maximální počet uživatelů	5	50	300	1000	Neomezeno[a.]
Maximální počet zařízení (aktivovaná i deaktivovaná)	1	5	30	100	Neomezeno
Maximální počet administrátorů/manažerů	5	1	5	1000	Neomezeno
Přístupové a systémové logy	✓	✓	✓	✓	✓
Přístupová pravidla	✓	✓	✓	✓	✓
API správa	✓	✓	✓	✓	✓
Aktivace/deaktivace účtu	✓	✓	✓	✓	✓
Omezení počtu neúspěšných přístupů	✓	✓	✓	✓	✓
Tichý alarm	✓	✓	✓	✓	✓
Zónový kód	✓	✓	✓	✓	✓
Monitorování zařízení	✓	✓	✓	✓	✓
Správa logů	✓	✓	✓	✓	✓
Import uživatelů z CSV nebo ze zařízení	✓	×	✓	✓	✓
Hromadná správa firmwaru	✓	×	✓	✓	✓
Vícenásobná autentizace	✓	×	✓	✓	✓
Oprávnění uživatele	✓	×	✓	✓	✓

Licence:	Trial	Basic	Advanced	Pro	Unlimited
Objednací číslo	n/a	n/a	91379031	91379032	91379033
Notifikace	✓	×	✓	✓	✓
Přítomnost	✓	×	✓	✓	✓
API přístupový klíč	✓	×	✓	✓	✓
CAM Logs	✓	×	✓	✓	✓
Ovládání výtahu	✓	×	✓	✓	✓
Dashboard	✓	×	✓	✓	✓
Nouzové uzamknutí	✓	×	✓	✓	✓
Mobile Credential Support	✓	×	✓	✓	✓
Správa návštěv	✓	×	✓	✓	✓
Správa obsazenosti	✓	×	×	✓	✓
Synchronizace (LDAP & CSV)	✓	×	×	✓	✓
Anti-passback	✓	×	×	✓	✓
Docházka	✓	Volitel-né	Volitelné	Volitelné	Volitelné

[a.] Neomezeno v rámci maximálních možností softwarové platformy, viz Doporučený hardware (str. 15).

Instalace

Access Commander může být distribuován dvěma způsoby:

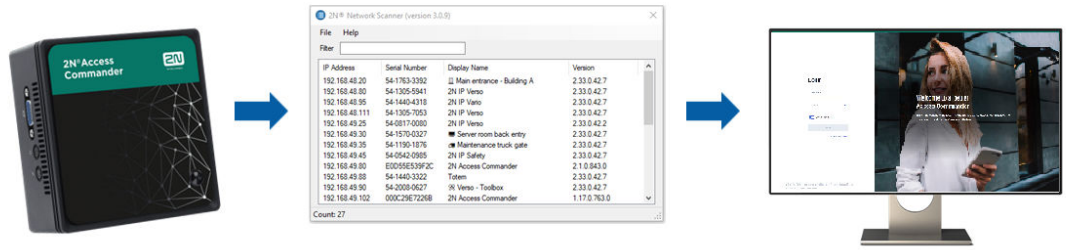
- Malý stolní počítač 2N Access Commander Box (obj. č. 91379030)
- Virtuální počítač

Řešení Access Commander Box je omezené na 2000 připojených zařízení. Ostatní vlastnosti softwaru jsou pro obě řešení totožné.

Distribuce přes Access Commander Box

Access Commander Box (obj. č. 91379030, Axis Part No. 01672-001) je kompaktní stolní minipočítač s předinstalovaným softwarem. Jedná se o „plug and play“ řešení, kdy stačí k tomuto minipočítači připojit zdroj napájení a ethernetový kabel. Pro správnou a plnou funkčnost systému se doporučuje tento minipočítač umístit na bezpečné místo a nechat jej trvale běžet. Access Commander Box slouží jako server pro sběr dat, událostí a logů z celého přístupového systému.

Přihlášení se k Access Commanderu s dynamickou IP adresou



1. Připojte Access Commander Box do sítě pomocí ethernetového kabelu.
2. Pomocí aplikace 2N IP Network Scanner lokalizujte Access Commander Box v síti.
3. Ve webovém prohlížeči přejděte na IP adresu Access Commander Box a přihlaste se do **Access Commanderu**.
   Defaultní heslo uživatele Admin je 2n a po přihlášení musí být změněno.

> **POZNÁMKA**
> V případě distribuce přes Access Commander Box se k webovému rozhraní připojte z jiného počítače v síti. Operační systém Access Commander Box zajišťuje chod **Access Commanderu** a jeho základní linuxové nastavení, neumožňuje spuštění webového prohlížeče.

Nastavení statické adresy Access Commanderu pomocí Access Commander Boxu

1. Připojte Access Commander Box do sítě pomocí ethernetového kabelu.
2. Připojte k Access Commander Box klávesnici a monitor. Zobrazí se černá obrazovka.
3. Přihlaste se do systému jako „root“ s heslem „2n“. Jakmile se zobrazí modrá obrazovka, změňte defaultní heslo.
4. V Advanced Menu zvolte „Networking“ a následně „Static IP“.
5. Nastavte statickou IP adresu, bránu a DNS.

6. Uložte toto nastavení a pomocí logout opusťte konzolové menu.
7. Připojte se k nastavené IP adrese přes webový prohlížeč.

Technické parametry Access Commander Box

- Ultrakompaktní provedení – 0,69 l (56,1 x 107,6 x 114,4 mm)
- Procesor Intel® Celeron® J3160 (2M cache; max. 2.24 GHz)
- 2.5” SSD SATA III hard disk (120 GB)
- DDR3 SODIMM paměť (4 GB) – 1.35 V, 1600 MHz
- Podpora duálního displeje přes VGA a HDMI port
- Gigabitový LAN port pro ethernetové připojení
- Montážní rám VESA (75 x 75 mm + 100 x 100 mm)
- Skladovací teplota: -20 °C až +60 °C
- Provozní teplota okolí: 0 °C až +35 °C

Distribuce přes virtuální stroj

Access Commander může být distribuován jako virtuální stroj. Níže jsou instalační postupy na podporovaných virtualizačních platformách.

Virtual Box

TIP
Povolení VT-X virtualizační technologie v BIOSu je doporučeno.

1. Z https://www.virtualbox.org/wiki/Downloads stáhněte poslední verzi VirtualBoxu.
   Je doporučeno stáhnout verzi včetně VirtualBox Extension Pack.
2. Stáhněte příslušný software ze sekce Software & Firmware na webu 2N.com. Po stažení soubor rozbalte.
3. Otevřete aplikaci VirtualBox a vyberte "Soubor – Importovat applianci...".
4. Upravte název.
5. Zkontrolujte nastavení CPU (minimálně 2), nastavení RAM (nejméně 2048 MB a volbu síťové karty).
6. Potvrďte licenční podmínky.

Po instalaci se otevře konfigurační konzole systému Linux, kde můžete provést základní nastavení systému. Kompletní konfigurace se provádí ve webovém rozhraní.

VMware Player

VÝSTRAHA
Podporovaná verze VMWare je 6.5 a vyšší.

1. Stáhněte příslušný software ze sekce Software & Firmware na webu 2N.com. Po stažení soubor rozbalte.
2. Ve VMware Player "File – Open..." vyberte cestu k OVA souboru.
3. Podle potřeby přejmenujte a klikněte na "Import".
4. Zkontrolujte nastavení CPU (minimálně 2), nastavení RAM (nejméně 2048 MB a volbu síťové karty).

Po instalaci se otevře konfigurační konzole systému Linux, kde můžete provést základní nastavení systému. Kompletní konfigurace se provádí ve webovém rozhraní.

VMware vSphere

VÝSTRAHA
Podporovaná verze VMWare je 6.5 a vyšší.

1. Stáhněte příslušný software ze sekce Software & Firmware na webu 2N.com. Po stažení soubor rozbalte.
2. Ve VMware vSphere vyberte "File – Deploy OVF Template" a pokračujte dle průvodce.
3. Po naimportování zkontrolujte nastavení "Edit Settings..."
   Upravte název (na kartě Options).
   Zkontrolujte nastavení CPU (minimálně 2), nastavení RAM (nejméně 2048 MB a volbu síťové karty).

Po instalaci se otevře konfigurační konzole systému Linux, kde můžete provést základní nastavení systému. Kompletní konfigurace se provádí ve webovém rozhraní.

Hyper-V

1. Stáhněte příslušný software ze sekce Software & Firmware na webu 2N.com. Po stažení soubor rozbalte.
2. Spusťte Hyper-V Manager a vyberte u požadovaného hostitele možnost Import Virtual Machine.
3. V průvodci instalací zkontrolujte zobrazené informace a potvrďte jejich přečtení tlačítkem Next.
4. Vyberte cestu ke složce z kroku 1.
5. Potvrďte výběr virtuálního stroje.
6. Vyberte typ importu.
7. Vyberte virtuální síťovou kartu pro virtuální stroj.
8. Zkontrolujte shrnutí nastavení, které bylo zvoleno v předchozích krocích, a potvrďte tlačítkem Finish.

Po instalaci se otevře konfigurační konzole systému Linux, kde můžete provést základní nastavení systému. Kompletní konfigurace se provádí ve webovém rozhraní.

Doporučený hardware

Počet připojených zařízení ovlivňuje **Access Commander**. Proto nastavte velikost hardwarových prvků podle skutečného stavu. Tabulka níže zobrazuje doporučený minimální počet CPU jader a velikostí RAM pro různý počet zařízení a uživatelů spravovaných **Access Commanderem**.

VÝSTRAHA
Doporučuje se udržovat nepřetržité spojení mezi **Access Commanderem** a zařízeními. Pokud dojde k odpojení, zařízení ukládají záznamy událostí offline, a po následném znovupřipojení dochází k synchronizaci dat z logu s **Access Commanderem**. Během procesu synchronizace aplikace nadále běží, ale u vyššího počtu zařízení může celý proces trvat déle.

Tabulka 2. Hardware pro virtuální stroj

Počet zařízení	Počet uživatelů	Minimální počet CPU jader	Minimální velikost RAM	Minimální alokace na pevném disku
1 000	10 000	2	2 GB	120 GB
2 000	100 000	2	4 GB	120 GB
2 000	200 000	4	8 GB	120 GB
7 000	200 000	4	16 GB	120 GB

Tabulka 3. Access Commander Box

Počet připojených zařízení 2.0	Počet uživatelů 2.0	Počet uživatelů ve skupině
2000	100000	1500

Doporučujeme nepřekračovat počet 1500 uživatelů ve skupině. Pokud jsou pro oblasti nějaká omezení, např. Anti-passback nebo kontrola obsazenosti pro velký počet uživatelů, aplikace se může zpomalit.

Aktivace licence

Pro aktivaci licencí je nutné získat licenční soubor a nahrát jej do **Access Commanderu**. Licenci Basic je možné aktivovat přímo v **Access Commanderu** na stránce Nastavení > karta Licence.

Získání licenčního souboru

K získání licence je potřeba sdělit distributorovi sériové číslo jednoho ze zařízení 2N připojených do **Access Commanderu**. Licenční soubor je vygenerován na základě sériového čísla tohoto licenčního zařízení.

Připojení licenčního zařízení zajišťuje platnost licence. V případě odpojení licenčního zařízení začne běžet ochranná lhůta, po jejímž vypršení dojde k pozastavení licence.

Nahrání licence

VÝSTRAHA

- Po přepnutí z Trial licence už není možné Trial licenci reaktivovat.
- Nastavení pokročilých funkcí, které nová licence nepodporuje, se neukládá.

1. Přejděte do **Nastavení** > **karta Licence**.
2. Klikněte na Nahrát licenci a v otevřeném okně nahrajte z úložiště získaný licenční soubor.

3. Po nahrání souboru klikněte na Aktivovat licenci.
4. Ujistěte se, že je aktivované licenční zařízení, pro které byla licence vygenerována.

Licenční soubor	Soubor s licencí, jehož nahráním se licence aktivuje. Vygenerování licenčního souboru zajišťuje distributor na základě sériové čísla licenčního zařízení.
Licenční zařízení	Vybrané zařízení 2N připojené k **Access Commanderu**, které zajišťuje platnost licence. Licenční zařízení slouží jako hardwarový klíč pro licenci.

Pozastavení licence

K pozastavení licence dojde, pokud je licenční zařízení odpojené od **Access Commanderu** po dobu delší, než je ochranná lhůta licence. Délky ochranné lhůty se odvíjí od toho, jak dlouho bylo licenční zařízení připojené v **Access Commanderu**. Délky ochranných lhůt jsou uvedeny v tabulce níže.

Když je licence pozastavena, všechna připojená zařízení se automaticky vyřadí ze správy a jsou označena jako nespravovaná. Pro jejich opětovnou aktivaci je potřeba připojit a aktivovat licenční zařízení nebo nechat vygenerovat a nahrát nový licenční soubor pro další zařízení.

V případě nahrání nové licence je potřeba nejdříve aktivovat licenční zařízení, pro které je nová licence vygenerována. Po aktivaci licenčního zařízení bude možné aktivovat i všechna ostatní zařízení.

Doba, po kterou bylo licenční zařízení připojeno k Access Commanderu	Ochranná lhůta, po kterou bude Access Commander v provozu bez připojeného licenčního zařízení
méně než 24 hodin	1 den
1 den – 30 dní	10 dní
31 dní – 180 dní	1 měsíc
více než 180 dní	3 měsíce

Základní přístup do rozhraní

*Tato kapitola popisuje zprovoznění a základní používání **Access Commanderu**. Instalace je popsána v kapitole Instalace (str. 13).*

Rozhraní **Access Commanderu** je přístupné prostřednictvím webového prohlížeče. IP adresu webového rozhraní je možné vyhledat pomocí programu 2N Network Scanner.

POZNÁMKA
V případě distribuce přes Access Commander Box se k webovému rozhraní připojte z jiného počítače v síti. Operační systém Access Commander Box zajišťuje chod **Access Commanderu** a jeho základní linuxové nastavení, neumožňuje spuštění webového prohlížeče.

Dashboard

Dashboard je základní zobrazení webového rozhraní **Access Commanderu**. Jedná se o konfigurovatelnou nástěnku zobrazující data v reálném čase. **Access Commander** nabízí několik Widgetů, které se na Dashboard přidávají pomocí tlačítka  . Widgety na Dashboardu je možné různě přesouvat, přejmenovávat, případně provádět jejich základní nastavení. Správa a mazání Widgetů se provádí v rozšířené nabídce  v hlavičce každého Widgetu.

Každý uživatel s účtem na **Access Commanderu** si může nastavit vlastní Dashboard. Dostupnost Widgetů je omezena v závislosti na roli uživatele a na dostupné licenci.

Změna jazyka

Po prvním přihlášení se **Access Commander** zobrazuje v jazyce nastaveném pro společnosti přihlášeného uživatele. Každý uživatel si může jazyk změnit. Po dalším přihlášení se bude rozhraní zobrazovat již v nově nastaveném jazyce.

1. Kliknutím na obrázek uživatele v pravém horním rohu otevřete uživatelské menu.
2. Vyberte Změnit jazyk.
3. Zvolte příslušný jazyk a volbu potvrďte pomocí Změnit jazyk.

Změna hesla účtu

1. Kliknutím na obrázek uživatele v pravém horním rohu otevřete uživatelské menu.
2. Vyberte Zobrazit profil.
3. Klikněte na  u parametru Heslo.
4. Potvrďte dosavadní heslo a zadejte nové.

POZNÁMKA
Pokud je heslo pro účet 'admin' stejné jako heslo root uživatele systému (pro přihlášení do konzole linuxového nastavení), pak se při změně hesla pro účet 'admin' automaticky změní také heslo root účtu.

Změna profilového obrázku

1. Kliknutím na obrázek uživatele v pravém horním rohu otevřete uživatelské menu.
2. Vyberte Zobrazit profil.
3. Klikněte na obrázek v záhlaví detailu uživatele.
4. V otevřeném dialogovém okně nastavte fotografii.
   Rozlišení obrázku bude automaticky upraveno na 432 × 432 px.

Logy

Zde je přehled toho, co v kapitole naleznete:

Systémové logy

POZNÁMKA

- Uživateli se zobrazují logy, které má oprávnění sledovat v závislosti na svých uživatelských oprávněních.
- Data se do logů zapisují v angličtině.

Stránka Systémové logy zobrazuje seznam událostí a notifikací, které vygeneroval.

V seznamu systémových logů se ke každé události a notifikaci uvádí:

- závažnost (info, warning, error);
- čas, kdy k události došlo;
- kategorii, do které akce spadá (Stav zařízení, Import, Synchronizace uživatelů, Systém, Uživatelské akce, Omezení oblastí);
- subjekt, kterého se akce týká (zařízení, uživatel, zóna, návštěva...);
- stručný popis události;
- autor události.

Kliknutím na řádek se rozbalí detailní informace o daném záznamu.

V seznamu je možné filtrovat pomocí nad seznamem. Případně je možné filtry nastavit pro jednotlivé sloupce v rozšířené nabídce, která se otevře kliknutím na v hlavičce každého sloupce. Rozšířená nabídka sloupců dále umožňuje sloupce přesouvat, připínat na první či poslední pozici nebo skrýt.

Sloupce Závažnost a Čas nelze skrýt.

Export logů

Záznamy je možné stáhnout v souboru CSV nebo vytisknout kliknutím na tlačítko Export nad seznamem. V exportovaném CSV souboru je čas uveden v GMT+0.

Životnost logů

Jakmile využití kapacity disku dosáhne 80 %, spustí se automatické mazání logů. Kapacitu disku je možné sledovat na stránce Nastavení. Jako první se mažou logy prvního typu v pořadí, další logy se mažou

postupně, dokud využití diskového prostoru neklesne na 75 % nebo dokud nebudou zůstávat pouze logy s nedovršenou minimální možnou dobou uložení daného typu logu.

Doba uložení daného typu logu se nastavuje na stránce Nastavení > karta Uchovávání záznamů. Uchování záznamů z kamer nemůže být delší než uchování systémových a přístupových logů.

TIP
V případě, že trvale využíváte 70 % kapacity disku, doporučujeme zkrátit maximální dobu uložení logů.

Přístupové logy

POZNÁMKA

- Uživateli se zobrazují logy, které má oprávnění sledovat v závislosti na svých uživatelských oprávněních.
- Data se do logů zapisují v angličtině.

Na stránce Přístupové logy se zobrazují záznamy úspěšných i neúspěšných pokusů o autentizaci a záznamy o nouzových uzamknutí.

V seznamu přístupových logů se uvádí:

- **Kategorie:**
  - Přístup povolen
  - Přístup zamítnut
  - Umožnění veřejného přístupu
  - Uzamknutí zařízení;
- **Čas**, kdy k akci došlo;
- **Uživatel**, který akci provedl;
- **Společnost** daného uživatele;
- **Zóna**, ve které k akci došlo;
- **Zařízení**, na kterém k akci došlo;
- **Autentizace**, která byla pro pokus použita (PIN, QR kód apod.).

Kliknutím na řádek se rozbalí detailní informace o daném záznamu.

V seznamu je možné filtrovat pomocí nad seznamem. Případně je možné filtry nastavit pro jednotlivé sloupce v rozšířené nabídce, která se otevře kliknutím na v hlavičce každého sloupce. Rozšířená nabídka sloupců dále umožňuje sloupce přesouvat, připínat na první či poslední pozici nebo skrýt.

Export logů

Záznamy je možné stáhnout v souboru CSV nebo vytisknout kliknutím na tlačítko Export nad seznamem. V exportovaném CSV souboru je čas uveden v GMT+0.

Životnost logů

Jakmile využití kapacity disku dosáhne 80 %, spustí se automatické mazání logů. Kapacitu disku je možné sledovat na stránce Nastavení. Jako první se mažou logy prvního typu v pořadí, další logy se mažou postupně, dokud využití diskového prostoru neklesne na 75 % nebo dokud nebudou zůstávat pouze logy s nedovršenou minimální možnou dobou uložení daného typu logu.

Doba uložení daného typu logu se nastavuje na stránce Nastavení > karta Uchovávání záznamů. Uchování záznamů z kamer nemůže být delší než uchování systémových a přístupových logů.

TIP
V případě, že trvale využíváte 70 % kapacity disku, doporučujeme zkrátit maximální dobu uložení logů.

Notifikace

Modul Notifikace umožňuje nastavit sledování vybraných událostí a vlastností systému, o kterých má **Access Commander** informovat e-mailem nebo notifikací v horní liště vedle uživatelského menu.

Seznam notifikací se zobrazuje také na stránce Systémové logy > Notifikace.

Záznamy je možné stáhnout v souboru CSV nebo vytisknout kliknutím na tlačítko Export nad seznamem. V exportovaném CSV souboru je čas uveden v GMT+0.

Nastavení nového typu notifikace

1. Přejděte na stránku **Nastavení** > **Notifikace**.
2. Klikněte na tlačítko pro přidání v pravém horním rohu stránky.
3. Zadejte jméno pro typ nové notifikace.

Po vytvoření se zobrazí detail notifikace, ve kterém je možné vybrat zařízení, u kterých se má upozornění sledovat; přidat uživatele, kterým se má upozornění odeslat; vybrat způsob doručení notifikace.

Nastavení notifikace

Typy notifikací se nastavují v detailu daného typu Notifikace. Detail typu notifikace se otevírá kliknutím na vybranou notifikaci v seznamu na stránce Nastavení > Notifikace.

Způsob oznamování

V této kartě se nastavují způsoby oznamování notifikací a seznam příjemců e-mailových notifikací.

Notifikace se v **Access Commanderu** objevují pod ikonou v horní liště, vedle uživatelského menu nebo v Systémový log > Notifikace.

Notifikační e-maily je možné zasílat uživatelům vedeným v **Access Commanderu** i příjemcům mimo systém. Uživatele je možné vybrat ze seznamu. E-mailové adresy ostatních příjemců je potřeba manuálně zadat.

POZNÁMKA
Pro správnou funkci e-mailových notifikací je potřeba mít správně nastavené SMTP, viz Zapnutí a nastavení funkce E-mail (SMTP) (str. 57).

Monitorovaná zařízení

Daný typ notifikace je možné generovat jak pro všechna zařízení, tak jen pro některá zařízení. Pokud je povolené Monitorování všech zařízení, může k události dojít na kterémkoliv zařízení a vygeneruje se notifikace. Pokud je Monitorování všech zařízení zakázáno, vygeneruje se notifikace, pouze pokud k události dojde na vybraném zařízení. Výběr zařízení probíhá v nabídce, která se otevře pomocí  .

Životnost logů

Jakmile využití kapacity disku dosáhne 80 %, spustí se automatické mazání logů. Kapacitu disku je možné sledovat na stránce Nastavení. Jako první se mažou logy prvního typu v pořadí, další logy se mažou postupně, dokud využití diskového prostoru neklesne na 75 % nebo dokud nebudou zůstávat pouze logy s nedovršenou minimální možnou dobou uložení daného typu logu.

Doba uložení daného typu logu se nastavuje na stránce Nastavení > karta Uchovávání záznamů. Uchování záznamů z kamer nemůže být delší než uchování systémových a přístupových logů.

TIP
V případě, že trvale využíváte 70 % kapacity disku, doporučujeme zkrátit maximální dobu uložení logů.

Společnosti

V rámci jedné instalace lze nastavení **Access Commanderu** rozdělit do **Společností**, jejichž správa se provádí odděleně. Tento způsob umožňuje rozdělit správu mezi správce v jednotlivých společnostech. Správce z jedné společnosti tak nemá přístup k informacím o jiné společnosti. Správci z jedné společnosti neuvidí uživatele jiné společnosti.

Zóny nebo zařízení lze sdílet napříč společnostmi, což umožňuje správu přístupu společnosti do společných prostor (vstupy, restaurace, konferenční sály...).

Vytvoření nové společnosti

1. Přejděte na stránku **Společnosti**.
2. Klikněte na tlačítko přidání společnosti v pravém horním rohu.
3. Vyplňte název společnosti.
4. Založení společnosti provedete kliknutím na Vytvořit.

Nově vytvořená společnost se objeví v seznamu. V detailu společnosti je potřeba provést její nastavení. Přidání uživatelů do společnosti se provádí v nastavení jednotlivých uživatelů.

Nastavení společnosti

Informace o společnosti je možné prohlížet a upravovat v detailu společnosti. Detail společnosti se otevírá kliknutím na vybranou společnost v jejich seznamu na stránce Společnosti.

Detail společnosti je rozdělen na karty Přehled, E-maily a Synchronizace uživatelů.

Jazyk společnosti

V kartě Obecné lze vybrat jazyk společnosti, ve kterém se bude rozhraní **Access Commander** zobrazovat uživatelům v dané společnosti. Uživatelé si mohou později jazyk rozhraní změnit. Volba jazyka společnosti má také vliv na šablony e-mailů odesílaných Uživatelům. Znění e-mailů lze změnit v záložce E-maily.

Zóny

Přiřazení zón ke společnosti definuje množinu zařízení, ke kterým budou mít uživatelé společnosti právo přístupu (např. zóna společné prostory a zóna 4. patro, které zahrnují vstupní dveře k recepci a všechny vstupy čtvrtého patra). Zóny mohou být přiřazeny k více společnostem současně a k jedné společnosti může být přiřazeno více zón.

Mobile Key

Ve společnosti je možné nastavit parametry párování s aplikací 2N Mobile Key, která umožňuje autentizaci pomocí Bluetooth. Nastavují se jak zařízení, na kterých budou moct uživatelé provádět párování, tak čas platnosti mobilního klíče potřebného ke spárování. Samotný mobilní klíč se generuje v nastavení uživatele.

Návštěvy

V této kartě je se nastavují skupiny, ke kterým bude moct správce návštěv přiřazovat nové návštěvy. Jednu ze skupin je možné určit jako výchozí. Nová návštěva tak bude automaticky přiřazena k výchozí skupině, nebude-li nastaveno jinak.

VÝSTRAHA
Bez správně nastavené výchozí skupiny není možné ve zjednodušeném rozhraní zajistit návštěvám přístup.

Je možné také vybrat způsoby autentizace, které mohou být návštěvě přiděleny. Způsob autentizace pak přiděluje návštěvě správce návštěv.

Více o zakládání návštěv v Návštěvy (str. 49).

Pracovní fond

Pracovní fond a Svátky slouží k výpočtu měsíčního pracovního fondu uživatelů v modulu docházka. Výběrem dnů je možné určit, které dny v týdnu budou započítávány jako pracovní. Výběr dne se provádí kliknutím. Zelené dny identifikují, které dny jsou brány jako pracovní.

Úprava pracovní doby definuje, kolik času má jedna denní směna.

Svátky

Nastavením svátků se určuje, které dny se nezahrnují do výpočtu měsíčního pracovního fondu. Hodiny odpracované ve svátek jsou počítány stejně jako hodiny odpracované o víkendech – odpracovaný čas je evidován nad rámec běžné pracovní doby.

Rozšířená nabídka ⋮ umožňuje zkopírovat svátky z jiné společnosti. Svátky se zkopírují včetně dat a názvů. Kopírování se může použít opakovaně, ale pokud nově kopírovaný svátek je ve společnosti již nastaven, přepíše se jeho název.

E-maily odesílané členům společnosti

Nastavení e-mailů má vlastní záložku v detailu společnosti. **Access Commander** umožňuje odesílat členům společnosti (včetně návštěv) automatické e-maily s informacemi o přiřazení způsobu autentizace. E-mail se odešle uživateli nebo návštěvě s nastavenou e-mailovou adresou.

Access Commander umožňuje odesílat e-maily s následujícími informacemi:

- PIN kód pro návštěvu
- QR kód pro návštěvu
- PIN kód pro uživatele
- QR kód pro uživatele
- Mobile Key k nastavení Bluetooth autentizace pro uživatele

V detailu společnosti > záložka E-maily > karta Šablony pro e-mail je možné nastavit vzhled těchto e-mailů a upravit jejich znění. Úprava znění e-mailu se provádí v dialogovém okně, které se otevře kliknutím na zvolený typ e-mailu. V dialogovém okně lze upravit:

- subjekt – předmět e-mailu
- hlavičku – zobrazuje se v barevném poli těla e-mailu
- úvod – text uvedený před automaticky vygenerovaným údajem z **Access Commanderu**
- další zprávu – text následující po údaji vygenerovaném z **Access Commanderu**
- signaturu – podpis uvedený na konci e-mailu

Synchronizace společnosti (LDAP)

Synchronizace s LDAP se používá pro stahování uživatelů a jejich změn z externího LDAP systému. Mezi data o uživatelích patří uživatelské jméno, ID, identifikátory karet, PIN/QR kód, obrázek, e-mailová adresa, telefonní číslo, heslo a login, registrační značky vozidel.

POZNÁMKA
Více informací o LDAP naleznete na adrese www.ldap.com.

1. Přejděte na Společnosti > detail vybrané společnosti > záložka Synchronizace uživatelů.
2. Pokud není žádné připojení nastaveno, vytvořte jej.
   Vyplňte:

   - **Název serveru** – v případě, že je správně nastavené DNS, stačí zadat jméno serveru („WIN-9ABEB4AUOHD“). Pokud není nastavené DNS, tak se do jména serveru zadá IP adresa serveru, na kterém běží LDAP služba.
   - **Port** – v defaultním nastavení je LDAP port 389 (bez SSL). Pokud chcete ve vaší firmě použít šifrované spojení, zadejte číslo portu 636. Podpora SSL musí být povolena i na straně LDAP serveru. Pokud administrátor nastaví jiné číslo portu, musí to být změněno i v **Access Commanderu**.
   - **Přihlašovací jméno** – přihlašovací jméno uživatele, který má odpovídající práva pro daný root, případně celý strom. Přihlašovací jméno musí být zadáno ve tvaru: „administrator@domain.com“.
   - **Heslo** – heslo daného uživatele na LDAP serveru.
   - **Zabezpečení komunikace (SSL)** – při zakázaném SSL není nutné přepisovat číslo portu. Při povolení SSL je nutné změnit číslo portu na 636.
   - **Base DN** – kořenový bod, ze kterého hledání v adresáři začíná. Může to být přípona nebo kořen adresáře, jako např.: CN=administrator, CN=users, DC=domain, DC=com.

   Otevře se detail nastaveného LDAP spojení. Nastavení spojení lze otestovat. Pomocí tlačítka Synchronizovat nyní spustíte jednorázovou synchronizaci.
3. Automatická synchronizace se nastavuje na kartě **Import**. Při povolení automatické synchronizace vyplňte, v jakých intervalech se má synchronizace provádět. Podle frekvence zvolte, ve které minutě nebo v jakém čase se budou data synchronizovat.
4. Na kartě **Možnosti** můžete přiřazení dat o uživateli k atributům na LDAP serveru.

Nastavené spojení můžete smazat v rozšířené nabídce karty **Import**. Na kartě **Možnosti** se nastavují další parametry synchronizace.

Možnosti synchronizace LDAP

Importované atributy – úpravou schématu se nastavuje přiřazení dat z **Access Commanderu** k atributům na LDAP serveru.

Uživatelé odebraní z LDAP – definuje, co se má v stát s uživateli, kteří byli v LDAP smazáni. Uživatele smazané z LDAP lze v **Access Commanderu** ponechat nebo je také smazat. Pokud mají být uživatelé zakázáni, tak po smazání uživatelů z LDAP zůstanou jejich data v **Access Commanderu**, ale nebudou se synchronizovat se zařízeními.

Uživatelé zakázaní v Active Directory – nastavuje, co se stane s uživateli, kteří byli v Active Directory zakázáni. Zakázání v Active Directory může **Access Commander** ignorovat nebo může uživatele smazat (zakázat). Po opětovné aktivaci v Active Directory se smazaní uživatelé opět nahrají do **Access Commanderu**.

Synchronizace skupin – umožňuje nahrát členství ve skupinách z LDAP do **Access Commanderu**. Pomocí nastavení schématu synchronizace je možné definovat vlastní Base DN a filtr, podle kterého se budou skupiny synchronizovat. Schéma povoluje synchronizaci vnořených skupin.

Synchronizace avatarů – nastavuje stahování fotografií uživatele z LDAP systému.

Sledování odkazů – nastavuje, zda se mají synchronizovat data z odkazů LDAP.

Vnořené vyhledávání – povoluje vyhledávání v celém stromě, v opačném případě se prohledává pouze kořen.

Stránkování povoleno – stránkování používá LDAP rozšíření Simple Paged Results Control. To umožňuje rozdělit výsledky do více stránek, což je nezbytné pro rozsáhlé adresářové služby. Parametr **Velikost stránky** určuje, kolik záznamů bude obsahovat jedna stránka.

Uživatelé

Pomocí **Access Commanderu** lze provádět správu **Uživatelů**, upravovat jejich přístupy, spravovat jejich kontaktní údaje apod.

V seznamu uživatelů se zobrazují veškeří vytvoření uživatelé. Nad seznamem lze uživatele filtrovat nebo lze rovnou vyhledat konkrétního uživatele podle jeho jména, e-mailu nebo telefonního čísla.

Hromadné akce

Označením je možné provést výběr více uživatelů a aplikovat na ně následující hromadné akce:

-  Zapnout sledování docházky u uživatelů.
-  Přidat uživatele do skupiny.
-  Odstranit uživatele.
-  Nastavit časový interval platnosti přístupu.
-  Přiřadit přístupový PIN kód těm uživatelům, kteří ještě nemají přidělený PIN ani QR kód.
-  Přiřadit přístupový QR kód těm uživatelům, kteří ještě nemají přidělený PIN ani QR kód.
-  Přiřadit mobilní klíč těm uživatelům ve výběru, kterým zatím žádný mobilní klíč nebyl přidělen.

POZNÁMKA
Pro přiřazení PIN/QR kódu nebo mobilního klíče uživateli je nutné, aby měl uživatel vyplněnou platnou e-mailovou adresu.

Vytvoření nového uživatele

1. Přejděte na stránku **Uživatelé**.
2. Klikněte na tlačítko pro přidání uživatele v pravém horním rohu.
3. Vyplňte povinné údaje: jméno uživatele a společnost, do které patří.

Nově vytvořený uživatel se objeví v seznamu a otevře se detail uživatele. V detailu se provádí další nastavení uživatele, jako je přiřazení telefonního čísla, nastavení způsobů autentizace, přiřazení do skupin apod.

Nastavení uživatele

Informace o uživateli je možné prohlížet a spravovat v detailu uživatele. Detail uživatele se otevírá kliknutím na vybraného uživatele v seznamu na stránce Uživatelé.

Detail uživatele je rozdělen na záložky Přehled, Docházka a Protokol změn. Záložka docházka se zobrazuje jen u těch uživatelů, u kterých bylo sledování zapnuté, viz Docházka uživatele (str. 31). Modul docházka je dostupný v závislosti na licenci.

Změna jména a fotografie uživatele

Možnosti přejmenování uživatele a nastavení fotografie jsou v rozšířené nabídce  v záhlaví detailu uživatele.

Rozlišení obrázku bude automaticky upraveno na 432 × 432 px.

Autentizace

Tato karta slouží k nastavení způsobů autentizace uživatele na zařízeních. Uživatel se musí na zařízení autentizovat a pokud má platný přístup, bude mu povolen přístup na zařízení.

RFID karta – přidá uživateli existující RFID kartu. Otevře se dialogové okno, do kterého je potřeba zadat identifikátor karty. Načtení identifikátoru lze provést přiložením karty ke čtečce nebo zadáním ID karty pomocí klávesnice. Identifikátor musí být musí být hexadecimální číslo dlouhé alespoň 6 znaků. Jeden uživatel může mít přiřazené až 2 přístupové karty.

Mobile Key – slouží k propojení s aplikací 2N Mobile Key umožňující autentizaci prostřednictvím Bluetooth, viz kapitola Autentizace přes Bluetooth (str. 30).

PIN kód – automaticky vygeneruje 6místný PIN.

Uživateli lze pro přístup přiřadit PIN, nebo QR kód, nelze mít oba zároveň.

QR kód – automaticky vygeneruje QR kód. Zařízení umožňující čtení QR kódů jsou uvedena v Podporovaná zařízení a aplikace (str. 8).

Uživateli lze pro přístup přiřadit PIN, nebo QR kód, nelze mít oba zároveň.

Otisk prstu – otevře dialogové okno pro nahrání otisku prstů, kterými se může uživatel autentizovat na zařízeních, které podporují jejich čtení. Každému uživateli je možné nahrát až 2 otisky prstů. Postup je popsán v kapitole Nahrání otisku prstů (str. 30).

Poznávací značka – nastavuje poznávací značku vozidla uživatele, kterou může zařízení snímat a pomocí ní uživatele autentizovat.

Virtuální karta – umožňuje nastavit ID virtuální přístupové karty uživatele. Každý uživatel může mít přiřazenu právě jednu virtuální kartu. ID virtuální karty je sekvence 6–32 znaků z množiny 0–9, A–F. Číslo virtuální karty se použije pro identifikaci uživatele v zařízeních připojených přes rozhraní Wiegand.

Kód spínače – umožňuje nastavení až 4 kódů pro aktivací spínačů (např. dveřního zámku). Kód spínače slouží k otevření zámku pomocí klávesnice na zařízení i jako DTMF kód.

VÝSTRAHA
Při vícefaktorové autentizaci je nutné dodržovat pořadí způsobů autentizace.

TIP
Při vyplnění e-mailové adresy je možné odeslat vygenerovaný přístupový PIN/QR kód na uvedenou adresu.

Účet

Nastavením přihlašovacího jména a jednorázového hesla je možné udělit uživateli přístup do rozhraní **Access Commanderu**. Po přihlášení může uživatel sledovat svou docházku (je-li dostupná), změnit svůj

e-mail nebo změnit svůj profilový obrázek. Při prvním přihlášení bude uživatel vyzván ke změně hesla. Je-li u uživatele vyžadováno dvoufaktorové ověření, bude uživatel vyzván k propojení s vlastní ověřovací aplikací, viz Dvoufaktorové ověření (str. 63). Na této kartě je možné propojení s ověřovací aplikací také odstranit.

Na kartě Účet je možné uživatelům s přihlašovacími údaji udělovat oprávnění ke správě **Access Commanderu** pomocí uživatelských rolí. Oprávnění jednotlivých rolí jsou popsána v kapitole Uživatelská oprávnění (str. 7).

Zjednodušené rozhraní

Pro správce návštěv jedné společnosti je možné spustit zjednodušené uživatelské rozhraní. Zjednodušené rozhraní umožňuje správci návštěv přidávat, odebírat a spravovat návštěvy. Ve zjednodušeném rozhraní nelze nahlížet logy a přítomnost. Účelem zjednodušeného rozhraní je především usnadnit uživatelům bytu umožnění přístupu svým návštěvám. Všechny návštěvy vytvořené ve zjednodušeném rozhraní jsou vždy přiřazeny k *výchozí skupině pro nové návštěvy*. Správce návštěv nemá možnost tuto skupinu měnit. Výchozí skupinu pro nové návštěvy je potřeba dopředu vybrat v nastavení společnosti a je potřeba nastavit skupině platná přístupová pravidla pro přístup do bytu, včetně cesty k němu. Uživatel bytu pak ve zjednodušeném rozhraní může spravovat způsoby autentizace a délku trvání návštěv.

VÝSTRAHA
Před zapnutím zjednodušeného rozhraní **musí administrátor systému nastavit výchozí skupinu pro nové návštěvy** v Nastavení společnosti (str. 24). Výchozí skupině musí být přiřazena taková přístupová pravidla, aby měla návštěva přístup do navštěvovaných prostor. Bez správně nastavené výchozí skupiny není možné ve zjednodušeném rozhraní zajistit návštěvám přístup.

Osobní údaje

Slouží k přidání základních informací o uživateli. Umožňuje přidání e-mailové adresy uživatele, na kterou budou uživateli zasílány informace související s jeho účtem, a přidání telefonního čísla pro kontaktování uživatele.

Na kartu je možné zapsat:

- **E-mail** – adresa, na kterou budou uživateli zasílány informace související s jeho účtem v **Access Commanderu**;
- **Číslo uživatele** – specifický identifikátor, nutný pro hromadnou synchronizaci s CSV souborem (viz Synchronizace uživatelů s FTP (str. 59));
- **Poznámku**.

Přístupy

Karta přístupy slouží k přiřazení uživatele do skupiny a k nastavení časového intervalu, ve kterém budou přístupové údaje uživatele platné. Časový interval se nastavuje v rozšířené nabídce karty, která se otevře kliknutím na ⋮.

TIP
Časová omezení umožnění přístupu ze strany zařízení se nastavují prostřednictvím časových profilů.

Je-li uživatel členem skupiny, karta tuto skupinu zobrazuje. Pokud uživatel není přiřazen do skupiny, lze jej v kartě přidat. Skupinu lze změnit nebo vymazat v rozšířené nabídce .

Telefonní čísla

Pomocí této karty se nastavuje spojení s uživatelem. Telefonní číslo je volací destinace zařízení náležící tomuto uživateli.

Virtuální telefonní číslo lze použít pro volání na uživatele pomocí numerické klávesnice na zařízení. Virtuální číslo může mít dvě až čtyři číslice. Virtuální čísla nesouvisí s vlastními telefonními čísly uživatele, umožňuje tak skrýt vlastní telefonní čísla uživatelů na zařízení. V kartě je možné také nastavit zástupce, na kterého se hovor přesměruje v případě nedostupnosti tohoto uživatele. Zástupce je možné zvolit z dalších uživatelů ve společnosti.

Přístupový log

Přístupový log zobrazuje historii přístupů.

Protokol změn

V záložce Protokol změn je možné zobrazit všechny změny v nastavení uživatele. Základní řazení je dle času změny. V protokolu je možné zjistit, kdo změnu provedl. Po rozkliknutí řádku je možné zjistit podrobnosti k provedené změně.

Nahrání otisku prstů

Každému uživateli je možné nahrát až 2 otisky prstů. Pro jejich nahrání použijte externí čtečku otisků prstů. Zkontrolujte, zda máte nainstalovaný ovladač 2N USB Driver. Ovladač je ke stažení zde.

Nahraný otisk prstu uživatele lze použít k následujícím akcím:

- Otevřít dveře;
- Spustit tichý alarm – lze nastavit pouze v případě aktivní funkce Otevření dveří;
- Automatizace F1 a F2 – generuje událost FingerEntered v Automation. F1 a F2 slouží k rozlišení přiloženého prstu v Automation.

Nahrání otisku prstů

1. Ujistěte se, že je v **Nastavení** > **Přístupy** povolená USB čtečka pro snímání otisků prstů.
2. V nastavení uživatele v **kartě Autentizace** zvolte autentizaci Otisk prstu.
3. Vyberte prst, pro který chcete otisk nahrát.
   Zobrazí se okno s nadpisem "Nahrání otisku prstu".
4. Přiložte vybraný prst na čtečku. Tento krok opakujte 3×, vždy po vyzvání.
   Po posledním oskenování budete informováni o úspěšném skenování otisku.
5. Stisknutím tlačítka **Vytvořit** je proces dokončen.

Autentizace přes Bluetooth

Autentizace uživatele prostřednictvím Bluetooth se provádí prostřednictvím aplikace Mobile Key, kterou musí mít uživatel staženou ve svém mobilním telefonu.

GET IT ON Google Play

Download on the App Store

Spojení aplikace na telefonu uživatele se zařízeními v **Access Commanderu** se provádí zadáním párovacího kódu v aplikaci Mobile Key.

Párovací kód lze získat dvěma způsoby:

- prostřednictvím USB Bluetooth čtečky připojené k počítači,
- propojením se zařízením.

Vytvoření párovacího kódu prostřednictvím počítače

1. Stáhněte do počítače 2N IP USB Driver a nainstalujte ji.
2. Ujistěte se, že je USB Bluetooth čtečka povolená v **Nastavení** > **Autentizace** > **karta Povolené USB čtečky**.
3. Připojte USB Bluetooth čtečku k počítači.
4. V nastavení uživatele v **kartě Autentizace** zvolte autentizaci Mobile Key.
5. V otevřeném dialogovém okně vyberte Párovat pomocí čtečky.
   V dialogovém okně se objeví párovací kód.
6. Pro párování v aplikaci následujte postup níže.

Vytvoření párovacího kódu na zařízení

1. Ujistěte se, že
   - je nastavené párovací zařízení pro společnost daného uživatele, viz Nastavení společnosti (str. 24);
   - je párovací zařízení umístěno v zóně, do které má uživatel platný přístup, viz Přístupová pravidla (str. 43);
   - je nastaven adekvátní čas pro párování, viz Nastavení společnosti (str. 24).
2. V nastavení uživatele v **kartě Autentizace** zvolte autentizaci Mobile Key.
3. V otevřeném dialogovém okně vyberte Párovat pomocí zařízení.
4. Vygenerovaný párovací kód se zobrazuje na kartě spolu se zbývajícím časem pro párování. Párovací kód předejte uživateli. Pokud má uživatel vyplněnou e-mailovou adresu, můžete mu odeslat mobilní klíč na e-mail kliknutím na .
5. Pro párování v aplikaci následujte postup níže.

Párování v mobilní aplikaci Mobile Key

1. Stáhněte si aplikaci Mobile Key do svého mobilního telefonu. Aplikace je dostupná na App Store a Google Play.
2. Otevřete aplikaci a povolte aplikaci Mobile Key přístup k Bluetooth.
3. Podle typu mobilního klíče se přibližte s mobilním telefonem k USB čtečce nebo k párovacímu zařízení.
4. V aplikaci Mobile Key klikněte na nabízené zařízení pro párování.
5. Aplikace vás vyzve k zadání PIN kódu. Zadejte párovací kód a jeho zadání potvrďte.

Docházka uživatele

Access Commander umožňuje sledování docházky uživatelů. V režimu docházka se zaznamenávají časy vstupů a odchodů jednotlivých uživatelů.

Zaznamenávání docházky uživatele je nutné aktivovat. Aktivace se provádí v rozšířené nabídce v záhlaví detailu uživatele. Aktivace zaznamenávání docházky u více uživatelů současně je možné provést výběrem uživatelů v seznamu na stránce Uživatelé a použitím hromadné akce .

Správce docházky může data o docházce uživatelů upravovat. Úprava se provádí kliknutím na časový interval, který má být změněn. Po otevření lze upravit hraniční časy a přidat k intervalu poznámku.

VÝSTRAHA
Pro správnou funkci docházky je potřeba mít v **Access Commanderu** dostupnou aktivní licenci pro sledování docházky uživatelů. Sledování docházky je nutné aktivovat v nastavení jednotlivých uživatelů.

Sledování a úprava docházky jsou popsány v kapitole Docházka (str. 46).

Skupiny

Skupina slouží pro sdružování uživatelů a pro jednodušší nastavení práv jejích členů pro přístup do zóny. Práva se nemusí nastavovat na úrovni jednotlivých uživatelů a návštěv, ale skupina se spojí se zónou.

V seznamu je možné filtrovat pomocí nad seznamem. Případně je možné filtry nastavit pro jednotlivé sloupce v rozšířené nabídce, která se otevře kliknutím na v hlavičce každého sloupce. Rozšířená nabídka sloupců dále umožňuje sloupce přesouvat, připínat na první či poslední pozici nebo skrýt.

Vytvoření nové skupiny

1. Přejděte na stránku **Skupiny**.
2. Klikněte na tlačítko pro přidání skupiny v pravém horním rohu.
3. V otevřeném dialogovém okně je nutné zadat jméno skupiny a vybrat, do které společnosti patří.

> **VÝSTRAHA**
> Po vytvoření skupiny nejde změnit nadřazená společnost.

Nově vytvořená skupina se objeví v seznamu a otevře se její detail. V detailu skupiny je potřeba přidat členy a nastavit jejich přístupová pravidla.

Nastavení skupiny

Informace o skupině je možné prohlížet a upravovat v detailu skupiny. Detail skupiny se otevírá kliknutím na vybranou skupinu v seznamu skupin. V detailu se nachází přehled členů skupiny a přehled jejich přístupových pravidel.

Členové

Karta zobrazuje všechny uživatele, kteří do skupiny patří. Do skupiny lze přidat pouze uživatele nebo návštěvnické karty, které spadají pod stejnou společnost jako skupina.

Přístupová pravidla

Zobrazuje přehled všech již vytvořených přístupových pravidel a nabízí jejich úpravu nebo vytvoření. Vytvořením přístupového pravidla se umožňuje přístup konkrétní skupině do zóny. Při vytvoření pravidla je potřeba zadat skupinu a časový profil, ve kterém má mít skupina do zóny přístup.

Zóny

Zóny slouží k jednodušší správě přístupů na jednotlivá zařízení. Zóny slučují zařízení do logických celků. Na stránce je zobrazen seznam všech zón.

V seznamu je možné filtrovat pomocí nad seznamem. Případně je možné filtry nastavit pro jednotlivé sloupce v rozšířené nabídce, která se otevře kliknutím na v hlavičce každého sloupce. Rozšířená nabídka sloupců dále umožňuje sloupce přesouvat, připínat na první či poslední pozici nebo skrýt.

Povolení přístupových bodů

Pomocí se otevře dialogové okno, ve kterém se spouští podpora přístupových bodů, více v Nastavení přístupových bodů zařízení (str. 47).

Vytvoření nové zóny

1. Přejděte na stránku **Zóny**.
2. Klikněte na tlačítko pro přidání zóny v pravém horním rohu.
3. V otevřeném dialogovém okně je nutné zadat jméno zóny a vybrat, do kterých společností patří.

Nově vytvořená zóna se objeví v seznamu. Zařízení do zóny lze přidat v detailu zóny nebo v detailu zařízení. V detailu zóny je možné provádět další nastavení.

Nastavení zóny

Informace o zóně je možné prohlížet a upravovat v detailu zóny. Detail zóny se otevírá kliknutím na vybranou zónu v seznamu.

Vícefaktorová autentizace

Pro všechna zařízení v zóně je možné nastavit nutnost autentizace více způsoby. Je možné vybrat jen některé způsoby autentizace, ale při použití musí být striktně dodrženo následující pořadí:

1. Mobile Key
2. RFID karta
3. Otisk prstu
4. PIN kód

VÝSTRAHA
Při vícefaktorové autentizaci je nutné dodržovat pořadí způsobů autentizace.

Nutnost vícefaktorové autentizace je možné omezit časovým profilem. Při zapnuté vícefaktorové autentizaci se zobrazí možnost **Použít vícefaktorovou autentizaci**, ve které lze pomocí vybrat časový profil. Při volbě režimu Anytime bude vícefaktorová autentizace vyžadována pořád.

Vícefaktorovou autentizaci je možné vyžadovat pouze pro vstup do zóny. Toto nastavení je platné pouze při používání přístupových bodů.

Nastavení přístupů

V kartě je možné nastavit hromadný **PIN kód pro přístup do zóny** nebo jej zobrazit, je-li už PIN kód vytvořen.

Dále je možné v nastavení přístupu povolovat a zakazovat následující funkce:

Tichý alarm – při použití speciálního kódu se aktivuje spuštění tiché akce, která odešle hlášení o poplachu; zařízení při tichém alarmu nevydává poplašné zvuky. Nastavení speciálního kódu pro tichý alarm a jeho přesnou funkci se provádí v konfiguraci zařízení.

Blokování přístupu – po pěti neúspěšných pokusech bude další pokus o přístup povolen až po uplynutí 30 sekund.

Ověřování registračních značek – vozidla budou mít přístup do zóny na základě ověření SPZ u všech zařízení, která tuto funkci podporují.

Zařízení

Karta zobrazuje přehled zařízení přidaných do dané zóny. V této kartě je možné přidat další zařízení.

Pokud jsou používány přístupové body, přidávají se do zóny jednotlivé přístupové body. Typ přístupového bodu daného zařízení je popsán jako Vstup do zóny.

U každého zařízení / přístupového bodu se zobrazují dostupné způsoby autentizace.

Společnosti

V této kartě se spravuje seznam společností, které mohou mít do zóny přístup. Do jedné zóny může mít přístup více spoleřností.

Přístupová pravidla

Zobrazuje přehled všech již vytvořených přístupových pravidel a nabízí jejich úpravu nebo vytvoření. Vytvořením přístupového pravidla se umožňuje přístup konkrétní skupině do zóny. Při vytvoření pravidla je potřeba zadat skupinu a časový profil, ve kterém má mít skupina do zóny přístup.

Úpravu přístupového pravidla je možné provést kliknutím na dané pravidlo.

Zařízení

Stránka Zařízení zobrazuje veškerá zařízení přidaná v daném **Access Commanderu**.

V seznamu je možné filtrovat pomocí nad seznamem. Případně je možné filtry nastavit pro jednotlivé sloupce v rozšířené nabídce, která se otevře kliknutím na v hlavičce každého sloupce. Rozšířená nabídka sloupců dále umožňuje sloupce přesouvat, připínat na první či poslední pozici nebo skrýt.

Záznamy je možné stáhnout v souboru CSV nebo vytisknout kliknutím na tlačítko Export nad seznamem. V exportovaném CSV souboru je čas uveden v GMT+0.

Označením je možné provést výběr více zařízení a aplikovat na ně následující hromadné akce:

- Spravovat vybraná zařízení
- Vyjmout vybraná zařízení ze správy
- Zálohovat vybraná zařízení

Ikona na řádku zařízení přesměrovává do webového konfigurační rozhraní daného zařízení.

Stavy zařízení

- Online
- Nespravováno
- Nekompatibilní
- Offline
  - Přihlášení selhalo – v **Access Commanderu** jsou zadány špatné přihlašovací údaje do webové konfigurace zařízení.
  - Nepřístupný – **Access Commander** nemůže se zařízením navázat spojení.
  - Neplatný certifikát – je vyžadované ověřování certifikátů SSL a zařízení nemá platný SSL certifikát.

Přidání nového zařízení

1. Přejděte na stránku **Zařízení**.
2. Klikněte na tlačítko pro přidání zařízení v pravém horním rohu.
3. V otevřeném dialogovém okně vyhledejte zařízení v lokální síti nebo napište jeho IP adresu a příslušný port ve formátu: „IPadresa:port“.
   Po zadání IP adresy zařízení je možné stisknout na klávesnici ENTER a tak zadat další zařízení.
4. Po zadání všech zařízení, které chcete přidat, vyplňte heslo přístupu do webové konfigurace těchto zařízení. Je možné současně přidat jen ta zařízení, ke kterým se přihlašujete stejným heslem.
5. Před vytvořením zařízení pojmenujte.

Nově přidaná zařízení se objeví v seznamu. Další nastavení zařízení proveďte v detailu zařízení.

Nouzové uzamknutí

Nouzové uzamknutí slouží k plnému uzamčení dveří ovládaných daným zařízením. Během nouzového uzamknutí není možné otevřít dveře pomocí nastavených uživatelských přístupů, a to ani v případě, že uživatel nebo návštěva použije platný přístup s platným časovým profilem.

Nouzové uzamknutí lze aktivovat/deaktivovat:

- v detailu zařízení – uzamkne dané zařízení;
- v detailu zóny – uzamkne všechna zařízení v zóně;
- v detailu společnosti – uzamkne všechna zařízení ve společnosti;
- pomocí globální akce v horní liště stiskem tlačítka  – uzamkne všechna zařízení v **Access Commanderu**;
- ve widgetu na dashboardu.

Ve widgetu Nouzové uzamknutí je možné předdefinovat konkrétní skupinu zařízení, kterou bude možné nouzově uzamykat.

VÝSTRAHA
Off-line zařízení, neaktivní zařízení, zařízení s nekompatibilním firmwarem a zařízení s firmwarem starším než 2.32 nebudou po požadavku na nouzové uzamknutí uzamčena. Offline zařízení se uzamkne, jakmile bude opět dostupné.

Nastavení zařízení

Informace o zařízení je možné prohlížet a spravovat v detailu zařízení. Detail zařízení se otevírá kliknutím na vybranou položku zařízení v jejich seznamu. Podle typu zařízení může být detail rozdělen do záložek Přehled, Volání a Výtah.

Z detailu zařízení lze přejít do webové konfigurace zařízení pomocí tlačítka **Konfigurace hardwaru** v pravé horní části detailu zařízení. Konfigurace jednotlivých zařízení je popsaná v příslušném konfiguračním manuálu. Z webového rozhraní konfigurace je možné se vrátit zavřením konfigurace křížkem v modré horní liště.

Přehled

Stav

Na této kartě se zobrazuje stav navázání spojení se zařízeními. Online zařízení jsou taková, se kterými má **Access Commander** navázané spojení a na kterých je nahrán akceptovaný firmware. Díky navázanému spojení se zařízením může probíhat synchronizace dat. Nekompatibilní firmware je možné povolit na stránce **Zařízení** > **Firmware**.

Automatická synchronizace se spouští po každé změně, která se má promítnout do konfigurace koncových zařízení. Synchronizace probíhá pouze nad zařízeními, kterých se týká. Do fronty pro synchronizaci se řadí pouze požadavky vyvolané změnami, které mohou ovlivnit koncová zařízení. Takovými změnami bývají změny přístupových práv, telefonních čísel, použitých časových profilů apod. Například změna jména uživatele, který není přiřazen do žádné skupiny, automatickou synchronizaci nespustí. Délka samotné synchronizace (promítnutí všech změn do koncových zařízení) je závislá na množství zařízení, která je potřeba synchronizovat, i na množství dat, která se do zařízení nahrávají.

Řízení přístupu

Nastavuje zónu, do které zařízení patří.

Pokud má zařízení nastavené 2 přístupové body a pokud je detekce přístupových bodů povolena (viz Nastavení přístupových bodů zařízení (str. 47)), zobrazuje se možnost přiřazení 2 zón. Jeden přístupový bod zařízení může být pouze v jedné zóně.

Konfigurace

Karta zobrazuje aktuální verzi firmwaru, MAC adresu a IP adresu a umožňuje změnu hesla pro přístup do jeho webové konfigurace.

Ovládání dveří

Tato karta zobrazuje záběry z kamer zařízení a umožňuje vzdálené otevření dveřního spínače ovládaného tímto zařízením. Otevření dveří na určitou dobu je možné nastavit v rozšířené nabídce, která se otevře kliknutím na .

Aktuální stav dveřního spínače se zobrazuje vedle tlačítka Otevřít.

K uzamknutí dveří i pro skupiny s platným přístupem slouží Nouzové uzamknutí (str. 36).

Zálohování

Umožňuje zálohu konfigurace interkomu v souboru xml. Záloha se spouští pomocí Spustit zálohu. Poslední záloha se zobrazuje na kartě, odkud je možné stáhnout soubor se zálohou. Zařízení je možné automaticky synchronizovat s poslední zálohou pomocí nabídky v Restore. V této nabídce je možné zařízení synchronizovat podle zálohy uložené na jiném nařízení.

POZNÁMKA
Zálohovat lze všechna dostupná zařízení (online zařízení a připojená zařízení s nekompatibilním firmwarem).

Volání

Tato záložka se zobrazuje v detailu zařízení, ze kterého je možné provádět hovory.

Telefonní seznam displeje

V kartě Kontakty se spravuje zobrazování adresáře na zařízeních s displejem. Na kartě se zobrazuje strom kontaktů tak, jak se zobrazuje v adresáři na zařízení. Kliknutím na Změnit se otevře dialogové okno pro úpravu stromu kontaktů. V levé části otevřeného dialogového okna se zobrazuje řazení složek kontaktů. V pravé části se nastavují kontakty v rámci zvolené složky. Kmenová složka představuje první stránku, která se zobrazí při otevření adresáře na zařízení. Kontakty se budou zobrazovat všechny na jedné stránce adresáře, pokud budou všechny uloženy v této kmenové složce. Kontakty je možné dále seskupovat do složek a ty řadit pod kmenovou složku.

Přidání kontaktů na displej zařízení

1. Přejděte na **Zařízení** > detail zařízení > **záložka Volání** > **karta Kontakty**.
2. Otevřete správu zobrazování kliknutím na Změnit.

3. V pravé části otevřeného dialogového okna vyberte složku, do které chcete kontakty přidat.
   Do složky můžete přidat:

   1. **Uživatele**
      Je možné vybrat více uživatelů současně.
   2. **Skupiny**
      Uživatele je možné do složky přidat hromadně po skupinách. V adresáři se bude zobrazovat každý uživatel ze skupiny pod svým jménem. Je možné vybrat více skupin současně.
   3. **Volací skupiny**
      Volací skupiny jsou skupiny kontaktů, které se budou vytáčet současně. Při zakládání volací skupiny je nutné zadat její název, pod kterým se bude volací skupina zobrazovat v adresáři. Kontakty uživatelů se do volací skupiny přidávají stejně jako kontakty do složek.

      Volací skupinu můžete přejmenovat v rozšířené nabídce u složky, kterou otevřete kliknutím na .

4. Složku můžete přejmenovat v rozšířené nabídce u složky, kterou otevřete kliknutím na . V rozšířené nabídce je možné k dané složce přidat obrázek, který se poté zobrazí na zařízení u této složky.
5. Složky nebo volací skupiny, které chcete zobrazovat na prvních místech, připněte v rozšířené nabídce u dané složky pomocí .

Další virtuální čísla

Na zařízení s numerickou klávesnicí je možné zahájit odchozí hovor zadáním virtuálního čísla. V této kartě je možné přidávat uživatele, kterým bude možné volat na virtuální čísla, i když tito uživatelé přístup na zařízení nemají. Volání na virtuální čísla uživatelů, kteří mají k zařízení přístup, je povolené automaticky.

Při výběru uživatelů se zobrazují pouze ti uživatelé, kteří mají vyplněné virtuální číslo.

Tlačítka

Tato karta se zobrazuje v detailu zařízení, která mají tlačítka, pomocí nichž je možné vytáčet telefonní čísla uživatelů. Na kartě Tlačítka se přiřazují jednotliví uživatelé k jednotlivým tlačítkům na zařízení. Stiskem tlačítka na zařízení se započne odchozí hovor na destinace přiřazeného uživatele. Uživatel se k tlačítku přiřadí kliknutím na a výběrem uživatele.

Výtah

Pomocí připojení reléového modulu AXIS A9188 k 2N IP interkomu (2N IP Verso, 2N IP Force, 2N IP Safety, 2N IP Vario) nebo k Access Unit lze řídit přístup na jednotlivá patra v budově za použití výtahu. K jednomu 2N IP interkomu či Access Unit je možné připojit max. 8 těchto reléových modulů, přičemž každý z modulů může ovládat 8 pater, dohromady tedy max. 64 pater. Pro využití této funkce je nutné mít aktivní licenci pro 2N IP interkomy (obj. č. 9137916) a licenci Access Unit (obj. č. 9160401).

Nastavení ovládání výtahu

1. Přejděte do detailu zařízení, které má řídit přístup do jednotlivých pater. V rozšířené nabídce v záhlaví aktivujte ovládání výtahu. V detailu zařízení se zobrazí záložka **Výtah**.
2. V záhlaví detailu zařízení přejděte do konfigurace hardwaru zařízení. V sekci Hardware > Řízení výtahu zapněte moduly, které mají ovládat přístupy z výtahu. Pokud moduly vyžadují autentizaci, zadejte uživatelské jméno a heslo. Nastavení uložte. Opusťte konfiguraci hardwaru pomocí křížku v horní modré liště.
3. V detailu zařízení přejděte do záložky Výtah.
4. V kartě Výtahová podlaží vyberte reléový výstup pro podlaží, do kterého chcete nastavit přístup. Označení výstupů je ve formátu: *io_modul_reléový výstup*. Klikněte na .

5. V otevřeném dialogovém okně pojmenujte podlaží a vyberte zónu, do které se v daném podlaží vstupuje. Do tohoto podlaží budou smět vstupovat pouze uživatelé oprávnění vstupovat do dané zóny dle definovaných přístupových pravidel. Pokud se nemá vstup do podlaží řídit dle pravidel zóny, zaškrtněte **veřejný přístup povolen**. Výběrem časového profilu omezíte veřejný přístup pouze na dobu definovanou vybraným časovým profilem. Mimo tento časový profil bude vstup opět umožněn pouze uživatelům s platným přístupem na základě přístupových pravidel.

VÝSTRAHA
Pokud je nastaven přístup dle přístupových pravidel zóny, výtahové zařízení nepřebírá žádné další nastavení této zóny (PIN kód, vícenásobnou autentizaci, tichý alarm, …).

Výtahová podlaží
Po povolení se v této kartě zobrazuje seznam všech konfigurovatelných pater. Každé patro má své označení v pořadí modulu a reléového výstupu. Každému patru je pak možné přiřadit vlastní jméno.

Moduly pro ovládání výtahu
V této kartě se zobrazují všechny připojené moduly AXIS A9188 a jejich aktuální stavy. Jednotlivé moduly se zapínají v konfiguraci zařízení, v sekci Hardware > Řízení výtahu.

Monitoring
Stránka slouží ke zjištění informací o připojených zařízeních. Tabulku si může každý správce nastavit podle vlastních potřeb pomocí . Nastavení je unikátní pro každý účet. Nastavení se provádí výběrem zobrazovaných sloupců.

Kliknutím na řádek se přejde na detail daného zařízení.

Firmware
Stránka Firmware zajišťuje hromadný upgrade firmwaru jednotlivých typů připojených zařízení a pomáhá je tak udržovat v optimální kondici. Hromadnou správu zařízení je možné pozastavit. Volitelně je možno některá zařízení z hromadné správy firmwaru vyloučit.

Aktuální verze firmwaru je k dispozici online prostřednictvím 2N Update Serveru, volitelně je také možno nahrát soubor pro upgrade manuálně. Nasazení nové verze vždy podléhá schválení administrátorem, který tak má proces upgradu plně pod kontrolou.

Verze v hromadné správě zobrazuje seznam připojených typů 2N IP interkomů, 2N odpovídacích jednotek a 2N přístupových jednotek.

TIP
Novou verzi firmwaru je nejprve možno nasadit na jedno nebo více vybraných zařízení v testovacím režimu a až poté povolit upgrade ostatních zařízení.

Vyloučení zařízení
Zařízení je možno vyloučit z hromadné správy firmwaru přidáním na seznam v Zařízení > Firmware > karta Vyloučená zařízení.

Nekompatibilní verze firmwaru
Po přidání nebo upgradu zařízení, které nemá kompatibilní firmware, přejde toto zařízení do nekompatibilního stavu. Nekompatibilní stav znamená, že se na zařízení neukládají noví uživatelé. Ze zařízení se dále

stahují události a je možné použít konfiguraci nebo zálohu zařízení. V tabulce se vytvoří nový záznam a administrátor má možnost používání nekompatibilního firmwaru povolit.

Access Commander automaticky vyřadí zařízení s firmwarem, který není jeho aktuální verzí podporován. Karta zobrazuje tyto nepodporované verze firmwaru na připojených zařízeních. Seznam podporovaných verzí firmwaru je uveden níže.

Access Commander může ovládat všechna zařízení používající nepodporovanou verzi firmwaru, pokud bude tato verze schválena. Schválení se provádí v Zařízení > Firmware > karta Nekompatibilní verze firmwaru pomocí ikony .

VÝSTRAHA
Schválení nepodporované verze může vést k problémům jako je ztráta dat nebo může jinak bránit správnému fungování.

Podporované verze firmwaru

- 2.43
- 2.42
- 2.41
- 2.40
- 2.39
- 2.38

Zabezpečení

Po zapnutí ověřování certifikátů SSL bude probíhat synchronizace pouze na zařízeních, která mají SSL certifikát s podepsanou důvěryhodnou autoritou. Synchronizace zařízení bez takových SSL certifikátů bude vypnuta.

Pro úspěšné ověření musí být certifikáty zařízení podepsány certifikační autoritou a obsahovat IP adresu nebo doménové jméno zařízení. Certifikát podepisující autority musí být důvěryhodný na serveru, na kterém běží **Access Commander**. Certifikáty zařízení musí být nahrány přes webové rozhraní zařízení (Systém > Certifikáty > Osobní Certifikáty) a nastaveny jako Certifikát HTTPS serveru v Služby > Web Server > Pokročilá nastavení.

VÝSTRAHA
Na zařízení 2N Indoor Touch nelze nahrávat vlastní SSL certifikáty, po zapnutí ověřování certifikátů bude spojení s nimi ztraceno.

Nastavení přístupových bodů zařízení

Zařízení (2N interkom nebo 2N Access Unit) mohou mít až dva přístupové body. Každý přístupový bod umožňuje průchod v jednom směru. Přístupové body rozlišují směr průchodu přes zařízení. Každý přístupový bod může mít přidělenu jednu nebo více čteček, které jsou připojeny k zařízení a fungují ve směru bodu. Přístupové body jsou použity pro zaznamenání vstupu do zóny nebo jejího opuštění. Jejich použití je nutné v případě, že se zařízení nachází na rozhraní mezi dvěma zónami.

Přístupové body dále slouží ke sledování uživatelů v modulu Přítomnost (str. 51). Přístupové body se také využívají pro sledování vstupu a výstupu v Omezení oblastí (str. 53).

POZNÁMKA
Nastavení jednotlivých přístupových bodů v **Access Commanderu** se do webového rozhraní zařízení propisuje do sekce Služby > Řízení přístupu:

- Přístupový bod 1 = Pravidla pro příchod
- Přístupový bod 2 = Pravidla pro odchod

Nastavení přístupových bodů

1. Vstupte do webového konfiguračního rozhraní daného zařízení.

   TIP

   Do webového konfiguračního rozhraní je možné přejít kliknutím na v seznamu na stránce Zařízení.

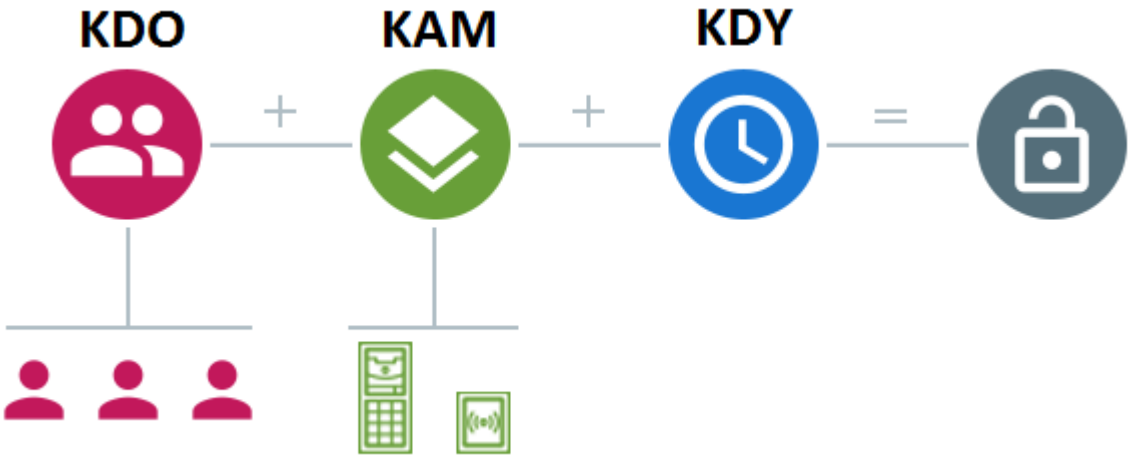
2. Přejděte do sekce Hardware > menu Rozšiřující moduly.
3. Najděte modul umožňující přístup, který má být používán jako přístupový bod 1 (Příchod) nebo přístupový bod 2 (odchod).
4. V parametru Dveře nastavte požadovaný směr a nastavení uložte.
5. Přejděte na stránku Zóny v **Access Commanderu**.
6. V pravém horním rohu stiskněte a povolte použití přístupových bodů.

Přístupová pravidla

Přístupová pravidla jsou nástroj pro přehledné řízení přístupů skupin uživatelů do zón. Přístupy je možné udělit na základě časových profilů.

Přístupová pravidla určují KDO, KAM a KDY má přístup.

- **KDO** je určeno skupinou a uživateli, kteří jsou do ní přiřazeni (uživatel může být současně ve více skupinách v rámci jedné společnosti).
- **KAM** je určeno zónou nebo zařízeními (jedno zařízení může být vždy jen v jedné zóně).
- **KDY** je určeno přiřazeným časovým profilem. Tato položka není povinná. Nevyplněný časový profil znamená neomezený přístup (24/7).



POZNÁMKA
Jedna skupina může mít přístup do více zón, stejně tak do jedné zóny může mít přístup více skupin.

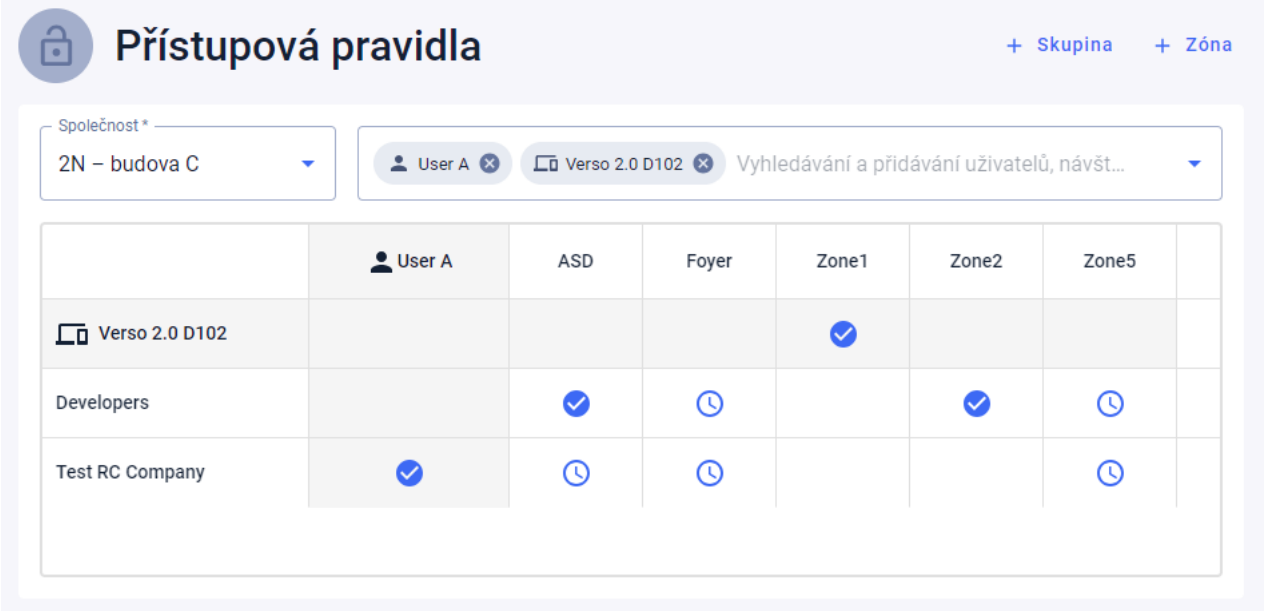
Maticové zobrazení

Maticové zobrazení pravidel na stránce přístupová pravidla zobrazuje přehled přístupů a umožňují jejich nastavení. Matice je dostupná pro každou existující společnost a zobrazuje všechny jí přiřazené skupiny a zóny. Administrátor může přepnout společnost v nabídce nad maticí.

Kliknutím na buňku odpovídající vybrané zóně a skupině se nastavuje přístup skupiny do zóny. Zobrazí se nabídka, ve které se volí buď neomezený přístup nebo přístup omezený časovým profilem. Časové profily musí být přednastaveny na stránce Časové profily (str. 45). V případě potřeby lze přidat do matice společnosti novou skupinu či zónu.

Ve vyhledávacím poli nad maticí je možné do matice přidat uživatele nebo zařízení. Průnikem uživatele a skupiny je možné uživatele přidávat do skupiny. Průnikem zařízení a zóny se zařízení přidávají do zóny.

Příklad maticového zobrazení



Obrázek uvádí přehled matice pro společnost 2N Telekomunikace. Z přehledu je zřejmé, že:

- Vyfiltrované zařízení Verso 2.0 D102 je součástí zóny Zone1.
- Vyfiltrovaný uživatel User A je součástí skupiny Test RC Company.
- Uživatelé ze skupiny Developers mají neomezený přístup do zón ASD a Zone2, omezený přístup do zón Foyer a Zone5 (dle nastaveného časového profilu) a nemají přístup do zóny Zone1.
- Uživatelé ze skupiny Test RC Company mají omezený přístup do zón ASD, Foyer a Zone5 (dle nastaveného časového profilu) a nemají přístup do zón Zone1 a Zone2.

Seznam pravidel

Stránka Seznam pravidel zobrazuje seznam všech aktuálně platných přístupových pravidel. Kliknutím na pravidlo je možné jej upravit. Nové přístupové pravidlo je možné přidat kliknutím na tlačítko pro přidání v pravém horním rohu. Před vytvořením je potřeba nastavit parametry pravidla.

Seznam pravidel i matice zobrazují stejná přístupová pravidla. Změna v jednom zobrazení se automaticky propíše do druhého zobrazení. Přístupová pravidla se upravují i v nastavení zón a v nastavení skupin.

Časové profily

Vybrané funkce interkomu lze časově omezit. Uvedeným funkcím lze přiřadit tzv. časový profil, který určuje, kdy je daná funkce dostupná.

Časovými profily lze řešit následující požadavky:

- zcela blokovat volání na vybraného uživatele mimo vyhrazený čas,
- blokovat volání na vybraná telefonní čísla uživatele mimo vyhrazený čas,
- blokovat přístup uživatele mimo vyhrazený čas.

Každý časový profil definuje dostupnost funkce, se kterou je spojen pomocí týdenního kalendáře. Jednoduše lze nastavit čas od–do a příp. dny v týdnu, kdy má být funkce dostupná. Určování přístupu pomocí časového profilu se nastavuje přístupovými pravidly. Omezení dostupnosti uživatele mimo časový profil se nastavuje spolu s telefonním číslem uživatele.

Volitelně lze vytvořit až 20 obecných časových profilů, které je kromě řízení přístupů možno použít i pro speciální případy lokální konfigurace. Tyto časové profily jsou nahrány do všech synchronizovaných zařízení.

Vytvoření časového profilu

1. Přejděte na stránku **Časové profily**.
2. Klikněte na tlačítko pro přidání časového profilu v pravém horním rohu.
3. V otevřeném dialogovém okně nastavte jméno časového profilu.
4. Pro volbu časového omezení vyberte možnost Přidat časové úseky. Zelené dny identifikují dny spadající do časového profilu. Výběr dne se provádí kliknutím. V rámci dnů je možné nastavit časový interval určující platnost časového profilu.
   Rozdílné doby pro každý den je možné nastavit, až když je časový profil vytvořen.

Nově vytvořený časový profil se přidá do seznamu a otevře se jeho detail, ve kterém je možné provádět další nastavení. V detailu časového profilu je možné nastavit pozici profilu na zařízeních.

Nastavení časového profilu

V detailu časového profilu se zobrazuje rozpis dnů a časů. Modré intervaly zobrazují, kdy je daný profil aktivní. V rámci jednoho dne lze nastavit libovolný počet intervalů.

Interval se přidává kliknutím na hodinový slot a nastavením přesného času, kdy má být profil aktivní. Čas jednotlivého intervalu lze změnit po kliknutí na interval. Pokud má být profil aktivní celý den, musí se vytvořit jeden interval pokrývající celý den, tj. 00:00–23:59.

V rozšířené nabídce, která se otevře kliknutím na ⋮, lze nastavit pozici na zařízení. Pozice na zařízení definuje pozici v seznamu časových profilů, který se nahrává na všechna zařízení, ke kterým je časový profil přiřazen.

Omezení dostupnosti uživatele mimo časový profil se nastavuje spolu s telefonním číslem v nastavení uživatele.

Docházka

Access Commander umožňuje sledování docházky uživatelů. V režimu docházka se zaznamenávají časy vstupů a odchodů jednotlivých uživatelů.

Nastavení docházky a jejich režimů se provádí v **Nastavení** > **Konfigurace** > **karta Docházka**, viz Nastavení docházky (str. 46).

VÝSTRAHA
Pro správnou funkci docházky je potřeba mít v **Access Commanderu** dostupnou aktivní licenci pro sledování docházky uživatelů. Sledování docházky je nutné aktivovat v nastavení jednotlivých uživatelů.

Stránka docházka nabízí seznam uživatelů se sledovanou docházkou. V pravém horním rohu se nachází ikona , pomocí které je možné stáhnout soubor CSV se souhrnnými daty o docházce všech uživatelů. Při stahování dat je potřeba zadat časový úsek, pro který se má docházka vygenerovat.

Docházka konkrétního uživatele

Ze seznamu uživatelů na stránce Docházka lze vybrat konkrétního uživatele a zobrazit detailnější informace pouze o jeho docházce. V seznamu se zobrazují pouze ti uživatelé, u kterých je sledování docházky povoleno, viz Uživatelé (str. 27).

V horní části výpisu lze vybrat měsíc, pro který chcete docházku zobrazit. Vedle výběru měsíce se zobrazuje nastavený pracovní fond pro daný měsíc, saldo a odpracované hodiny.

Vedle jména uživatele se nachází rozšiřující nabídka umožňující stažení dat o docházce zobrazeného uživatele a to v souboru CSV nebo PDF. Oba soubory obsahují záznamy jednotlivých dnů.

TIP
Docházku uživatele je možné prohlížet také v detailu uživatele, do kterého se přechází výběrem v seznamu uživatelů na stránce **Uživatelé**.

Změna docházky uživatele

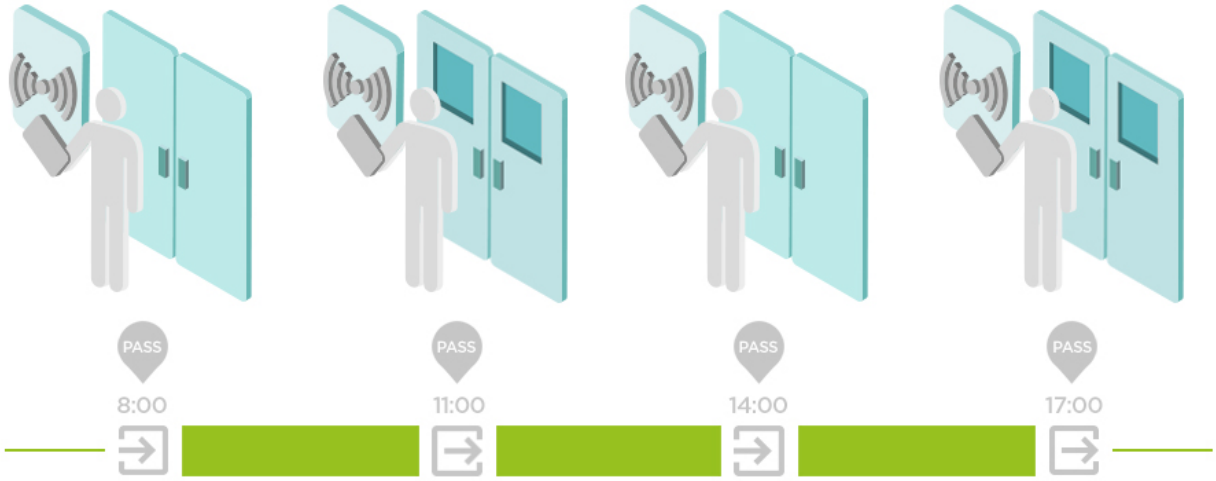
Správce docházky může data o docházce uživatelů upravovat. Úprava se provádí kliknutím na časový interval, který má být změněn. Po otevření lze upravit hraniční časy a přidat k intervalu poznámku.

Nastavení docházky

Access Commander umožňuje sledování docházky uživatelů. V režimu docházka se zaznamenávají časy vstupů a odchodů jednotlivých uživatelů.

Režimy docházky

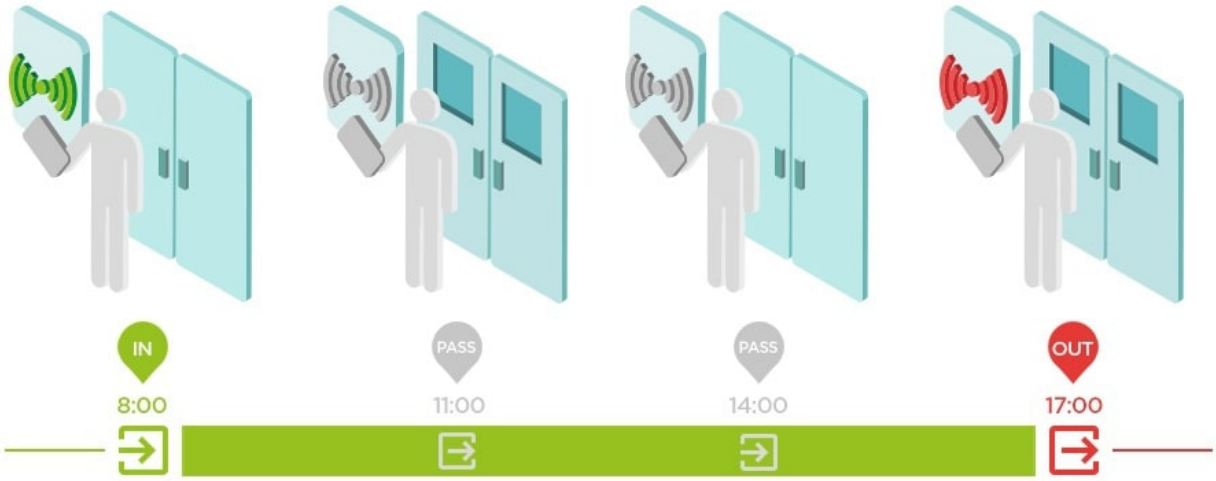
- **FREE**



Příchody a odchody jsou počítány z první a poslední autentizace uživatele na libovolném zařízení v jednom dni. V tomto režimu nefunguje modul přítomnost.

- **IN-OUT**

Pro správnou funkci je nutné nastavit příchodová a odchodová zařízení.



- **IN-OUT pro všechna zařízení**
  Tento režim umožňuje sledování přítomnosti. Příchody jsou zaznamenávány na příchodových zařízeních, odchody jsou zaznamenány na odchodovém zařízení. Pohyb mezi zónami se jako příchod/odchod neregistruje.
- **IN-OUT pro vybraná zařízení**
  Tento režim umožňuje sledování přítomnosti. Příchody a odchody jsou zaznamenávány na vybraných zařízeních, které jsou nastavené jako příchodové nebo odchodové. Eviduje se příchod a odchod pouze na těchto vybraných zařízeních. Zaznamenávání příchodu/odchodu je tak možné nastavit například pouze na hlavním vstupu do budovy.

Nastavení přístupových bodů zařízení

Zařízení (2N interkom nebo 2N Access Unit) mohou mít až dva přístupové body. Každý přístupový bod umožňuje průchod v jednom směru. Přístupové body rozlišují směr průchodu přes zařízení. Každý přístupový bod může mít přidělenu jednu nebo více čteček, které jsou připojeny k zařízení a fungují ve směru bodu. Přístupové body jsou použity pro zaznamenání vstupu do zóny nebo jejího opuštění. Jejich použití je nutné v případě, že se zařízení nachází na rozhraní mezi dvěma zónami.

Přístupové body dále slouží ke sledování uživatelů v modulu Přítomnost (str. 51). Přístupové body se také využívají pro sledování vstupu a výstupu v Omezení oblastí (str. 53).

POZNÁMKA
Nastavení jednotlivých přístupových bodů v **Access Commanderu** se do webového rozhraní zařízení propisuje do sekce Služby > Řízení přístupu:

- Přístupový bod 1 = Pravidla pro příchod
- Přístupový bod 2 = Pravidla pro odchod

Nastavení přístupových bodů

1. Vstupte do webového konfiguračního rozhraní daného zařízení.

   TIP

   Do webového konfiguračního rozhraní je možné přejít kliknutím na v seznamu na stránce Zařízení.

2. Přejděte do sekce Hardware > menu Rozšiřující moduly.
3. Najděte modul umožňující přístup, který má být používán jako přístupový bod 1 (Příchod) nebo přístupový bod 2 (odchod).
4. V parametru Dveře nastavte požadovaný směr a nastavení uložte.
5. Přejděte na stránku Zóny v **Access Commanderu**.
6. V pravém horním rohu stiskněte a povolte použití přístupových bodů.

Návštěvy

Ve **Access Commanderu** je možné vytvářet profily návštěv, které mají oprávnění vstupu na omezenou dobu. Návštěvě je možné přidat přístupovou kartu, přístupový kód a vyplnit registrační značku vozidla. Návštěvě nebude počítána docházka. Počet návštěv není limitován žádnou licencí.

Nastavení uchování návštěvnických dat

Administrátor může nastavit dobu uchovávání návštěvnických dat. Lhůta pro uchování návštěvnických dat se nastavuje ve dnech kliknutím na ikonu  vedle tlačítka pro vytvoření nové návštěvy.

Po vypršení časového intervalu návštěvy a uplynutí nastavené lhůty pro uchování dat jsou návštěvy automaticky mazány každou půlnoc. Návštěvy, kterým jsou stále přiřazeny návštěvnické karty, nebudou smazány.

POZNÁMKA
Nastavení může být použito pro splnění lokálních nařízení pro ochranu dat. Jméno návštěvy a poznámka budou zachovány v přístupovém logu podle nastavení životnosti ve správě logů.

Vytvoření nové návštěvy

1. Přejděte na stránku **Návštěvy**.
2. Klikněte na tlačítko pro přidání návštěvy v pravém horním rohu.
3. V otevřeném dialogovém okně je nutné vyplnit jméno návštěvy, vybrat navštěvovanou skupinu a nastavit začátek a konec návštěvy. Pokud nenastavíte začátek a konec návštěvy, začne časový interval pro přístup návštěvy okamžitě a skončí na konci dne.

   VÝSTRAHA
   Časový interval pro přístup návštěvy nesmí být delší než jeden měsíc.
4. Před vytvořením návštěvy můžete nastavit způsoby autentizace, které bude návštěva používat pro přístupy.

Nově vytvořená návštěva se objeví v seznamu. V detailu návštěvy je možné přidat návštěvě způsoby autentizace a spravovat její přístupy.

Ukončení návštěvy

Po uplynutí časového intervalu vyprší návštěvě platnost přístupu.

Pokud administrátor nebo správce ukončí návštěvu pomocí tlačítka Ukončit na kartě Přístupy v nastavení návštěvy, dojde k okamžitému zablokování přístupu této návštěvy. Pro návštěvníka, u kterého došlo k automatickému ukončení návštěvy, je dostupné tlačítko Ukončit z toho důvodu, že na zařízeních může být odlišná časová zóna. Může se totiž stát, že zatímco na jednom zařízení nemá návštěva platný přístup, tak na jiném stále ano. Děje se tak v případě, pokud jsou pro zařízení nastavené různé časové zóny.

Byla-li návštěvě přiřazena návštěvnická karta, karta se odváže a je možné ji použít pro jinou návštěvu.

Nastavení návštěvy

Informace o návštěvě je možné prohlížet a upravovat v detailu návštěvy. Detail návštěvy se otevírá kliknutím na vybranou návštěvu v seznamu.

Přístupy

Karta přístupy zobrazuje přístupovou skupinu a časový interval, během kterého má návštěva platný přístup. Časový interval pro přístup návštěvy je možné znovu nastavit volbou Obnovit návštěvu v rozšířené nabídce  .

V této kartě je možné návštěvu ukončit, viz Ukončení návštěvy (str. 49).

Návštěva

V kartě se zobrazuje navštěvovaná osoba a navštěvovaná společnost. Navštívenou osobu je možné změnit.

V této kartě je možné připsat k návštěvě poznámku.

Osobní údaje

Karta zobrazuje kontaktní údaje návštěvy a umožňuje jejich změnu. Nastavený e-mail umožňuje zaslání kódů pro Autentizaci.

Autentizace

Návštěvě je možné přidat přístupovou kartu, přístupový PIN nebo QR kód a vyplnit poznávací značku vozidla. Pro návštěvu je možné vyplnit pouze jednu poznávací značku. Návštěvě je možné přiřadit návštěvnickou přístupovou kartu, viz Karty (str. 50).

Při vyplnění e-mailové adresy je možné odeslat vygenerovaný přístupový PIN/QR kód na uvedenou adresu.

Přidělenou návštěvnickou kartu je zde možné vrátit.

Přístupový log

Přístupový log zobrazuje historii přístupů.

Karty

Podstránka Karty slouží ke správě návštěvnických přístupových karet, které jsou k dispozici pro přidání návštěvě. Nová karta se přidává pomocí tlačítka pro přidání v pravém horním rohu.

Karty je vždy potřeba přiřadit ke společnosti. Kartu je možné používat pouze pro návštěvy, které budou navštěvovat tuto společnost.

Existující kartu je možné přepsat nebo smazat výběrem v rozšířené nabídce .

VÝSTRAHA
Kartu přiřazenou aktivní návštěvě nelze smazat.

Přítomnost

Modul přítomnost je rozšířením modulu docházka a slouží k zobrazení seznamu uživatelů, kteří se aktuálně nachází v budově. Pro funkci modulu je potřeba nastavit režim docházky IN-OUT v **Nastavení** > **Konfigurace** > **karta Docházka**, viz Nastavení docházky (str. 46).

- Pokud je poslední událostí uživatele v daném dnu příchod (**IN** událost), je brán jako přítomný.
- Pokud uživatel projde přes čtečku, která má nastavený nespecifikovaný směr, tak se u daného uživatele změní zóna, ve které se nachází. Totéž se stane, pokud projde přes čtečku v režimu **IN**.
- Pokud je poslední Událostí v daném dnu odchod (**OUT** událost), je brán jako nepřítomný.

VÝSTRAHA
Modul přítomnost nefunguje, pokud je v rámci systému pro sledování docházky použit režim FREE. Sledování přítomnosti je možné pouze v režimu IN-OUT.

Vypršení přítomnosti uživatele

Kliknutím na ikonu vpravo nahoře se nastavuje Vypršení přítomnosti uživatele. Vypršením přítomnosti uživatele se nastavuje automatické mazání záznamu o přítomnosti uživatele, pokud uživatel zapomene označit svůj odchod. Tento časový limit je vyjádřen v hodinách a určuje, za jak dlouho od posledního průchodu přítomného uživatele bude jeho záznam přítomnosti automaticky smazán. Nastavení tohoto časového limitu umožňuje definovat, jak dlouho může záznam o přítomnosti zůstat v systému, pokud uživatel není označen jako nepřítomný. To zajišťuje, že seznam přítomných uživatelů zůstane aktuální a neobsahuje záznamy o uživatelích, kteří již opustili budovu a zapomněli se odhlásit.

Reporty

Ze stránky Reporty je možné stahovat souhrnná data o přidaných uživatelích. Stažené soubory jsou ve formátu CSV (Comma-Separated Values). Název souboru vždy uvádí datum a čas vygenerování daného reportu.

POZNÁMKA
Některé tabulkové programy používají jiné oddělovače a po otevření v nich se CSV soubor nemusí zobrazovat správně. V takových případech je doporučeno data z CSV souboru importovat do otevřeného sešitu.

- **Mobile Key** – Paired and unpaired users with pairing time remaining
  V reportu jsou vypsána data o stavu párování uživatelů přes aplikaci Mobile Key, případně údaje o čase platnosti aktivního párovacího kódu.
- **Users** – Access rules with groups, zones, devices and time profiles
  V reportu jsou vypsána data o přiřazení uživatelů do skupin, o jejich přístupu k zónám a k zařízením v zónách a o časových profilech, v kterých je uživatelům přístup umožněn. Každá jedna kombinace je vypsána právě na jednom řádku tabulky.
- **Users** – Detailed export
  V reportu jsou vypsány veškeré informace o uživatelích, které jsou vyplněné v jejich profilech, včetně jejich osobních a přístupových údajů.

  VÝSTRAHA
  Soubor obsahuje citlivá data!
- **Users** – Global synchronisation export
  V reportu jsou vypsána data o přiřazení uživatelů do skupin, o jejich přístupu k zónám a k zařízením v zónách a o časových profilech, v kterých je uživatelům přístup umožněn. Každá jedna kombinace je vypsána právě na jednom řádku tabulky.
  Tento report může sloužit jako CSV soubor pro synchronizaci uživatelů, viz Synchronizace uživatelů s FTP (str. 59).

  VÝSTRAHA
  Soubor obsahuje citlivá data!

Omezení oblastí

Omezení oblastí slouží k definování oblastí, ve kterých je možné použít funkci Anti-passback a Obsazenost.

Tato opatření zlepšují úroveň ochrany a zamezují potenciálním bezpečnostním hrozbám. Konkrétněji pomáhají zabránit neoprávněnému vstupu do vybraných míst, umožňují sledování pohybu osob v rámci daného prostoru a zaznamenávají vstupy a výstupy, což může být užitečné pro monitorování a analýzu bezpečnostních událostí.

Seznam zobrazuje vytvořené oblasti v systému. Na této záložce lze oblasti vytvářet, mazat a přecházet na jejich detaily. Zároveň umožňuje oblast deaktivovat a zobrazit její stav.

Vytvoření oblasti pro omezení

1. Přejděte na stránku **Omezení oblastí**.
2. Klikněte na tlačítko pro přidání oblasti v pravém horním rohu.
3. V otevřeném dialogovém okně oblast pojmenujte.
4. V otevřeném detailu oblasti přidejte do oblasti zařízení. Zařízení se přidávají pomocí tlačítka v záhlaví detailu oblasti.
   Nově vytvořená oblast se objeví v seznamu. V jejím detailu je možné nastavovat vstupní a výstupní zařízení, nastavovat povolenou obsazenost, zapínat funkci anti-passback a blokovat přístup vybraným uživatelům do oblasti.

Nastavení omezení oblasti

Nové zařízení se do oblasti přidává pomocí tlačítka v záhlaví detailu oblasti.

Vstup a Výstup

Tyto karty uvádí, která zařízení jsou v dané oblasti vedena jako vstupní nebo výstupní. Pomocí rozšířené nabídky pod lze zařízení mezi kartami přesouvat nebo je z oblasti odstraňovat.

Autentizací uživatele na vstupním zařízení se zaznamenává vstup do oblasti. Autentizací uživatele na výstupním zařízení se zaznamenává odchod uživatele z oblasti. Pomocí toho je možné sledovat, zda se uživatel stále nachází v oblasti a zda do jí chce opětovně vstoupit.

Pokud má přidané zařízení nastavené dva přístupové body, je možné každý bod použít pro jiný směr (Vstup/Výstup). Nastavení přístupových bodů je popsáno v kapitole Nastavení přístupových bodů zařízení (str. 47). Vlastnosti přístupového bodu se rozbalí kliknutím na šipku.

Obsazenost

Pro správnou funkci je nutné nastavit příchodová a odchodová zařízení.

Karta obsazenosti umožňuje sledovat a kontrolovat počet osob v oblasti. Omezení obsazenosti pomáhá řídit počet osob v oblasti. Pokud je limit obsazenosti dosažen, je možné odepřít další přístupy nebo překročení limitu pouze zaznamenat. Pro tuto funkci je požadováno vstupní a výstupní zařízení.

Anti-passback

Na oblasti je možné aktivovat funkci Anti-passback, která zajišťuje rozšíření kontroly přístupů o monitoring a zneužití práv pro opětovný vstup do vyhrazených prostor. Monitorované oblasti jsou definovány hraničními zařízeními, která do prostor vedou či je umožňují opustit. Na těchto zařízeních probíhá při průchodu osob kontrola oprávnění dle pravidel definovaných pro danou oblast. Po opuštění oblasti skrze hraniční zařízení se může uživatel do oblasti vrátit až po uplynutí timeoutu, je-li timeout nastaven. Pokud se uživatel pokusí o dřívější návrat do oblasti, systém mu přístup odepře nebo tuto událost pouze zaznamená do logu.

VAROVÁNÍ
Anti-passback oblast pozbývá smyslu a může být potencionálně nebezpečná, pokud se v oblasti vyskytuje zařízení a má připojené aktivní tlačítko REX, které umožňuje neautorizovaný přístup.

Nastavení výjimky

Někdy může být žádoucí, aby se podmínky anti-passbacku nevztahovaly na vybrané uživatele. Typicky se jedná o uživatele jako je správce budovy, CEO, VIP uživatelé apod. Uživatele či celé skupiny, na které se nemají vztahovat podmínky anti-passbacku, se nastavují v Nastavení > Anti-passback > Výjimky.

POZNÁMKA
Sekce Nastavení je dostupná pouze uživateli s rolí administrátora.

Seznam blokovaných uživatelů

Blokovaní uživatelé jsou ti uživatelé, kteří se pokusili o přístup do Anti-passback oblasti před skončením timeoutu. Pomocí ✕ lze uživatele ze seznamu vyloučit, čímž je jim přístup do oblasti opět umožněn.

TIP
Když je uživateli odmítnut přístup důvodu aktivního anti-passbacku, může být uživateli odeslán automatický informační e-mail. Odesílání e-mailu povolíte v Nastavení > Anti-passback > karta Upozornění blokovaného uživatele e-mailem.

Resetování omezení

V Nastavení > Anti-passback > karta Resetování omezení oblastí se nastavují dny a časy, kdy dojde k vymazání záznamu oblastí, tzn. všichni uživatelé budou moct opět projít bez ohledu na předchozí porušení pravidel.

Nejčastější chyby nastavení

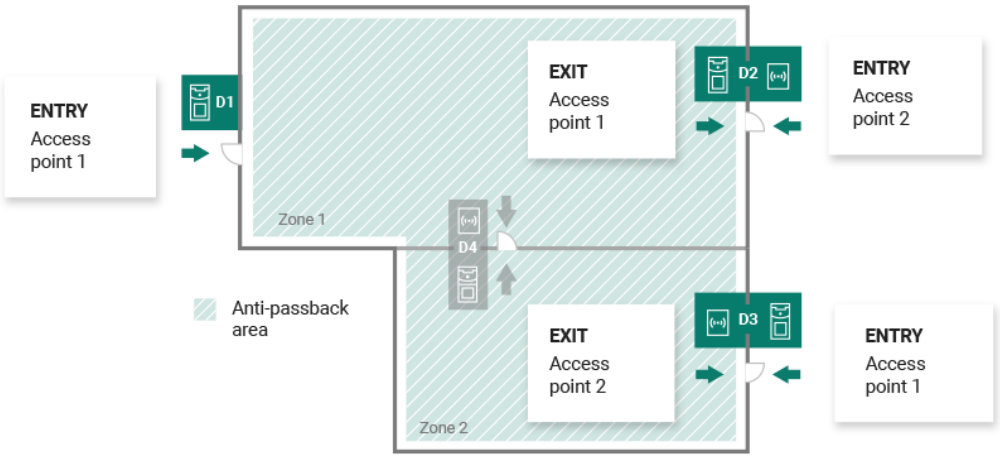
VÝSTRAHA
V případě výskytu chyby v oblasti bude celá oblast deaktivována. Po odstranění chyb bude opět aktivována.

Správné činnosti omezení oblastí můžou bránit následující případy

- Do oblasti není přidáno žádné zařízení. Je třeba přiřadit alespoň jedno zařízení.
- Některé vstupní/výstupní zařízení není nakonfigurováno správně nebo neobsahuje čtečku.

- Některé vstupní zařízení do této oblasti je již použito jako vstup do jiné oblasti.Pro korektní funkci je třeba upravit přiřazení.
- Některé zařízení není vybaveno potřebnou licencí.
- Některé zařízení bylo deaktivováno.
- Některé zařízení bylo odpojeno.
- Některé zařízení nemá kompatibilní verzi firmwaru.
  Některé zařízení je vybaveno tlačítkem REX, které umožňuje opuštění APB oblasti bez autorizace uživatele. Pro korektní funkci je třeba tlačítko REX deaktivovat.

Příklad nastavení omezení



Obrázek zobrazuje jednu Anti-passback oblast se třemi hraničními zařízeními D1, D2 a D3. Pro nastavení funkce Anti-passback slouží pouze hraniční zařízení. Zařízení D4 uvnitř Anti-passback oblasti neslouží ke kontrole vstupu/výstupu z oblasti. Zařízení D2 a D3 mají nastavené vstupní i výstupní směry.

Zařízení D1 slouží pouze pro vstup do Anti-passback oblasti. Zařízení je nastavené jako vstupní.

Zařízení D2 slouží pro vstup i výstup. Zařízení má pro vstup do oblasti nastaven rozšiřující modul a pro výstup má nastavenou hlavní jednotku.

Zařízení D3 slouží pro vstup i výstup. Zařízení má pro vstup do oblasti nastavenou hlavní jednotku a pro výstup má nastavený rozšiřující modul.

Nastavení systému

Datum a čas

Datum a čas v **Access Commanderu** lze synchronizovat s internetem nebo je nastavit manuálně. Změna způsobu získávání času se provádí v Nastavení > Konfigurace > karta Datum a Čas. V případě, že není **Access Commander** připojen k internetu, je třeba nastavit datum, čas a časové pásmo manuálně. V opačném případě je možné přepnout na NTP a získávat čas z NTP serveru. V takovém případě stačí nastavit pouze časové pásmo. NTP server aktualizuje datum a čas automaticky.

VÝSTRAHA
Po uložení změny času se **Access Commander** automaticky restartuje.

Synchronizace času se zařízeními

Čas na připojených zařízeních je možné sjednotit s časem **Access Commanderu**. Sdílení času se zařízeními se aktivuje přepnutím parametru Synchronizace se zařízením v Nastavení > Konfigurace > karta Datum a čas.

Pokud je synchronizace času se zařízením zapnuta, je možné volit z následujících způsobů synchronizace:

- **Zařízení používají stejný server NTP** – čas na zařízeních se řídí podle NTP serveru nastaveného v **Access Commanderu**.
- **Zařízení používají Access Commander jako server NTP** – čas na zařízeních řídí podle času nastaveného v **Access Commanderu**.

Nastavení sítě

Nastavení připojení k síti se provádí v Nastavení > Konfigurace > karta Síť. Karta zobrazuje aktuální síťové parametry **Access Commanderu** a umožňuje jejich nastavení. Nastavení jednotlivých parametrů je možné provést po povolení manuálního způsobu konfigurace.

Způsob konfigurace umožňuje nastavit parametry síťového nastavení automaticky z DHCP serveru nebo ručně. Při změně automaticky nastavené IP adresy z DHCP serveru na ručně zadanou adresu dojde ve webovém prohlížeči k přesměrování na vyplněnou IP adresu. Po přesměrování dojde k restartu **Access Commanderu** a je vyžadováno se do systému opět přihlásit.

VÝSTRAHA

- Pokud změníte způsob konfigurace na DHCP, změníte IP adresu serveru a můžete tím způsobit přerušení spojení.
- Pokud změníte HTTP proxy server, **Access Commander** se automaticky restartuje.

Zapnutí a nastavení funkce E-mail (SMTP)

Funkce E-mail zajišťuje odesílání notifikací nebo zasílání přihlašovacích hesel uživatelům. Odesílání e-mailů probíhá přes protokol SMTP.

Nastavení se provádí v Nastavení > Konfigurace > E-mail.

1. Po zapnutí funkce E-mail se otevře dialogové okno, ve kterém nastavte následující parametry:
   - **Adresu SMTP serveru**, na který budou odesílány e-maily.
   - **Port serveru**, přednastaven na hodnotu 25.
   - **Uživatelské jméno** a **heslo** k účtu na SMTP serveru v případě, že SMTP server vyžaduje autorizaci.
   - **Výchozí adresu odesílatele**, ze které budou e-maily odesílány.
2. Podle potřeby zapněte:
   - **SSL** pro šifrování e-mailů,
   - **Ověřování SSL serverového certifikátu**,
   - **Režim kompatibility** v případě připojení ke starším SMTP serverům, které nepodporují nové funkce (GSSAPI).
3. Po uložení můžete v kartě E-mail nastavit **Základní adresu pro e-mailové odkazy**, která bude součástí odeslaných e-mailových zpráv a může adresáty e-mailu odkazovat na zvolenou část rozhraní **Access Commanderu**.
4. Provedené nastavení můžete zkontrolovat odesláním testovacího e-mailu.

Aktualizace systému

Systém **Access Commander** pravidelně kontroluje aktualizační server a informuje o dostupných aktualizacích a o dostupných nových verzí firmwaru připojených zařízení. V Nastavení > karta Aktualizace systému lze automatickou kontrolu aktualizací vypnout.

Instalace aktualizace Access Commanderu

VAROVÁNÍ
Před instalací aktualizace je doporučeno provést zálohu systému (str. 58). Zálohu proveďte mimo pracovní dobu, aby nedošlo k dočasné nedostupnosti systému pro uživatele.

1. Přejděte do **Nastavení** > **karta Aktualizace systému**.
2. Pokud je automatická kontrola aktualizací vypnutá, klikněte na Zkontrolovat aktualizace.
3. Klikněte na Stáhnout v informační zprávě o dostupné aktualizaci a potvrďte její stažení.
   Karta informuje, že je aktualizace připravena k instalaci.
4. Klikněte na Instalovat v informační zprávě a v otevřeném dialogovém okně instalaci potvrďte.
   Po spuštění instalace dojde k přesměrování na stránku údržby. Stránka údržby informuje administrátora, který instalaci spustil, o průběžných stavech instalace. Ostatním uživatelům zobrazuje informaci, že probíhá aktualizace. Po dobu instalace není možné se do **Access Commanderu** přihlásit.
5. Po dokončení instalace klikněte na Go to login, které vás přesměruje na přihlašovací stránku.

Beta testování

Uživatelé si mohou vybrat, zda se chtějí zapojit do beta testování aktualizací softwaru **Access Commanderu** před oficiálním vydáním aktualizací. Povolení se provádí v Nastavení > karta Aktualizace systému > parametr Aktualizační server.

VAROVÁNÍ
Na testovací verze není poskytnuta záruka a společnost 2N TELEKOMUNIKACE a.s. nenese odpovědnost za funkční omezení a případné škody vzniklé v důsledku funkčních omezení beta verze. Beta verze jsou poskytovány výhradně za účelem testování. Beta verze není určena pro práci s důležitými daty.

Po povolení se budou beta verze zobrazovat v dostupných aktualizacích na kartě Aktualizace systému.

VAROVÁNÍ
Po aktualizaci **Access Commanderu** na nejnovější beta verzi nelze provést downgrade na verzi předchozí.

Záloha systému

Na stránce Nastavení > karta Záloha systému je možné provádět, nastavovat a kontrolovat zálohování a obnovu dat **Access Commanderu**. Data je možné ukládat na lokální úložiště nebo na Server Message Block (SMB). SMB je vhodný pro dlouhodobé uchovávání záloh.

Zálohu dat je možné provádět jednorázově nebo automaticky v pravidelných, předem nastavených intervalech.

Každou zálohu je možné obnovit, stáhnout nebo odstranit v nabídce, která se rozbalí po kliknutí na u položky v seznamu záloh.

Jednorázová záloha dat

1. Přejděte do **Nastavení** > **karta Záloha systému**.
2. Ve spodní části karty klikněte na Zálohovat ihned.
3. Vyberte, zda chcete data souboru zašifrovat. Pokud ano, vyplňte heslo, které bude nutné zadat při při obnově zálohy.

Nastavení automatického zálohování dat

1. Přejděte do **Nastavení** > **karta Záloha systému**.
2. Klikněte na u parametru Pravidelná záloha.
3. Nastavte požadované parametry zálohování:
   - frekvence – interval určující, jak často se bude záloha provádět,
   - čas – záloha se bude provádět příslušný den v tuto dobu,
   - den – den v týdnu nebo v měsíci, ve kterém se bude záloha provádět.
4. Vyberte, zda chcete data souboru zašifrovat. Pokud ano, vyplňte heslo, které bude nutné zadat při při obnově zálohy.

Uložením se budou zálohy provádět automaticky podle zvoleného nastavení.

Nastavení zálohování dat na SMB

1. Přejděte do **Nastavení** > **karta Záloha systému**.
2. Klikněte na u parametru Úložiště.
3. Zvolte typ úložiště: SMB.
4. Vyplňte adresu serveru, přihlašovací údaje a verzi protokolu.

Uložením se budou všechny zálohy odesílat na nastavený Server Message Block.

Obnova ze zálohovaných dat

1. Přejděte do **Nastavení** > **karta Záloha systému**.
2. Otevřete rozšířenou nabídku u vybrané zálohy a zvolte Obnovit.

Obnova ze souboru se zálohou

1. Přejděte do **Nastavení** > **karta Záloha systému**.
2. Ve spodní části karty klikněte na Obnovit ze souboru.
3. Vyberte soubor se zálohou z vašeho úložiště a klikněte na Obnovit.

Přenos dat z jiného Access Commanderu

1. Přejděte do **Nastavení** > **karta Záloha systému**.
2. Ve spodní části karty klikněte na Migrovat.
3. Zadejte IP adresu Access Commanderu, odkud chcete data přenést.
4. Vyplňte přihlašovací údaje administrátorského účtu Access Commanderu, odkud chcete data přenést.

VÝSTRAHA
Pro import dat z jiného Access Commanderu musí být na serveru, ze kterého se budou data stahovat, zapnutá služba SSH.

Synchronizace uživatelů s FTP

Seznam uživatelů a jejich základní nastavení včetně přiřazení do společností a skupin je možné synchronizovat pomocí CSV souboru vedeného externě.

Synchronizace se provádí v **Nastavení** > **karta Synchronizace uživatelů**. Z karty je možné si stáhnout vzorový CSV soubor.

TIP
Seznam s aktuálními uživateli, který odpovídá struktuře vzorového CSV souboru, je možné stáhnout na stránce Reporty (str. 52).

Připravený CSV soubor je možné na kartě přímo naimportovat. Data ze souboru se s **Access Commanderem** začnou synchronizovat automaticky.

Detailní informace o výsledku každé synchronizace jsou uloženy v systémovém logu. Samotný log obsahuje základní informaci o úspěchu nebo neúspěchu synchronizace. Detailní informace jsou uloženy v souboru, který se může stáhnout pomocí ikony na konci řádku.

Automatická synchronizace uživatelů s FTP

Karta Synchronizace uživatelů v Nastavení umožňuje propojit **Access Commander** s FTP úložištěm, na kterém je umístěn CSV soubor se seznamem uživatelů. Karta poté zobrazuje údaje o tomto FTP úložišti.

1. Klikněte na v parametru Úložiště.
2. V otevřeném dialogovém okně nastavte adresu FTP serveru, na kterém je CSV soubor uložen.
3. Zadejte přihlašovací údaje pro přístup k FTP serveru.

CSV soubor

KE STAŽENÍ
Vzorový CSV soubor pro synchronizaci uživatelů můžete stáhnout pomocí tohoto odkazu.

POZNÁMKA
Některé tabulkové programy používají jiné oddělovače a po otevření v nich se CSV soubor nemusí zobrazovat správně. V takových případech je doporučeno data z CSV souboru importovat do otevřeného sešitu.

CSV soubor má danou strukturu, která se musí dodržet. Všechny hodnoty jsou oddělené čárkou, pouze seznam skupin je oddělený středníkem. CSV soubor má následující strukturu:

- EmployeeID – primární klíč, který musí být vyplněn. Jedná se o jedinečný identifikátor uživatele.
- User Name – jméno uživatele založeného v Access Commanderu.
- Company – jméno společnosti, pod kterou bude uživatel založen. Společnost musí být založena v Access Commanderu. Malá a velká písmena použitá v názvech společností nebo skupin nejsou záměnná.
- User Mail – e-mailová adresa uživatele.
- Card Numbers – číslo karty uživatele. Lze nastavit až dvě karty pro jednoho uživatele. Čísla jednotlivých karet musí být oddělena středníkem (;).
- Switch Code – kód spínače, vždy se vytváří kód pod první spínač.
- Phone Number 1 – telefonní číslo na první pozici.
- Group Call – skupinové volání na výše nastavené telefonní číslo. Nabývá hodnot True/False. Při nastavení na True se aktivuje skupinové volání. Při nastavení na False je skupinové volání vypnuto.
- Phone Number 2 – telefonní číslo na druhé pozici.
- Group Call – skupinové volání na výše nastavené telefonní číslo. Nabývá hodnot True/False. Při nastavení na True se aktivuje skupinové volání. Při nastavení na False je skupinové volání vypnuto.
- Phone Number 3 – telefonní číslo na třetí pozici.
- Virtual Number – virtuální číslo uživatele.
- Groups – seznam skupin, do kterých má být uživatel přidán. Všechny skupiny musí být založeny v **Access Commanderu**. Seznam skupin je oddělen středníkem. Malá a velká písmena použitá v názvech společností nebo skupin nejsou záměnná.
- Is Deleted – příznak, zda má být uživatel smazán. Při nastavení na FALSE je uživatel vytvořen a při další synchronizaci se pouze aktualizují jeho údaje. Při nastavení na TRUE je uživatel při další synchronizaci smazán. Po nastavení na FALSE bude uživatel opět vytvořen.

- License Plates – registrační značky. Je možné nastavit více registračních značek, které je nutné oddělit středníkem.

Povolené USB čtečky

Pro usnadnění nahrávání některých způsobů autentizace uživatelů je možné používat USB čtečky připojené k počítači, na kterém se přistupuje do **Access Commanderu**. Čtečky je nutné v **Access Commanderu** povolit v Nastavení > Přístupy > karta Povolené USB čtečky.

Povolení/zakázání použití externího USB zařízení se provádí v dialogovém okně, které se otevře kliknutím na Povolit čtečky. Následně se jejich povolování upravuje kliknutím na Změnit.

Access Commander umožňuje využití následujících USB zařízení:

- 125 kHz RFID čtečka karet – obj. č. 9137420E
- 13.56 MHz a 125 kHz RFID čtečka karet – obj. č. 9137421E
- Čtečka otisků prstů – obj. č. 9137423E
- Externí USB Bluetooth čtečka (dongle) – obj. č. 9137422E

PICard klíče

V Nastavení > Přístupy > karta PICard klíče jsou uloženy šifrovací klíče aplikace 2N PICard Commander. Pokud jsou šifrovací klíče v **Access Commanderu** nahrané, zobrazuje se na kartě název projektu PICard Commanderu a číselný identifikátor exportu klíčů. Karta umožňuje nahrané klíče z **Access Commanderu** smazat.

VÝSTRAHA
Pokud PICard klíče odstraníte, přestanou fungovat všechny karty, které byly zašifrovány pomocí těchto klíčů.

Import šifrovacích klíčů PICard

1. Po kliknutí na Import nahrajte soubor s šifrovacími klíči z vašeho úložiště.
2. Zadejte heslo pro ochranu souboru, pokud jste jej nastavili při exportu z aplikace PICard Commander.

PICard Commander je softwarová aplikace pro šifrování přihlašovacích údajů na přístupových kartách. Aplikace vytváří projekty, které vygenerují sadu šifrovacích a čtecích klíčů. Čtecí klíče projektu lze importovat do zařízení 2N nebo do **Access Commanderu**, který následně zajišťuje distribuci čtecích klíčů do připojených zařízení 2N.

Šifrovací klíče pro Mobile key

Uživatelé mohou ke spojení se zařízeními 2N používat aplikaci Mobile Key. Komunikace mezi aplikací Mobile Key a zařízením je vždy šifrovaná. Bez znalosti šifrovacího klíče nemůže aplikace Mobile Key uživatele autentizovat. Primární šifrovací klíč je automaticky vygenerován při prvním spuštění interkomu a později jej lze kdykoli ručně přegenerovat. Primární šifrovací klíč je společně s Auth ID přenesen do mobilního zařízení při párování.

Komunikace mezi aplikací Mobile Key a zařízením je vždy šifrovaná. Bez znalosti šifrovacího klíče nemůže aplikace Mobile Key uživatele autentizovat. Primární šifrovací klíč je automaticky vygenerován při prvním spuštění interkomu a později jej lze kdykoli ručně přegenerovat. Primární šifrovací klíč je společně s Auth ID přenesen do mobilního zařízení při párování.

V **Nastavení > Přístupy > karta Šifrovací klíče pro Mobile key** je možné vygenerovat až 4 šifrovací klíče. Nově vygenerovaný klíč se automaticky nahraje do aplikace Mobile Key při prvním použití mobilního telefonu

s již dříve spárovaným zařízením. Při pokusu o vygenerování pátého klíče **Access Commander** upozorní, že jeho vygenerováním dojde k odstranění nejstaršího klíče. V kartě jsou uvedeny časy vygenerování jednotlivých klíčů.

Pokud nebude mít aplikace Mobile Key přístup k žádnému z platných šifrovacích klíčů, nebude možné ji používat pro autentizaci uživatele. Pro obnovení funkce aplikace je nutné provést opětovné spárování aplikace se zařízením připojeným k **Access Commanderu**, čímž dojde k nahrání platných šifrovacích klíčů do aplikace Mobile Key.

POZNÁMKA
Umožnění přístupu na zařízení závisí na nastavených přístupových právech daného uživatele.

CAM logs

CAM logy slouží k automatickému zaznamenání několika snímků předcházejících a následujících vybranou událost. V Nastavení > CAM logs lze spravovat různé typy událostí, pro které se mají CAM logy generovat.

CAM logy se mohou například vygenerovat s každým přiložením karty. Pokud někdo přiloží kartu, bude v přístupových lozích zaznamenáno 5 snímků před přiložením karty a 3 snímky po přiložení karty. Snímky jsou zaznamenávány po 1 sekundě. Na snímky je vytvořeno úložiště o velikosti 1, 3 nebo 5 GB. V případě naplnění úložiště dojde k odmazání nejstarších snímků. Samotné přístupové logy smazány nejsou.

Vytvoření CAM log typu

1. Přejděte na stránku **Nastavení** > **CAM logs**.
2. Klikněte na tlačítko pro přidání v pravém horním rohu stránky.
3. Zadejte jméno pro typ události CAM logu.

Nově vytvořený typ události CAM logu se zobrazí v seznamu a otevře se detail v CAM logu. V detailu CAM logu potřeba nastavit pro jaké události a na kterých zařízeních se budou snímky z kamer generovat.

Nastavení CAM logů

Informace o typu CAM logu je možné spravovat v detailu CAM logu. Detail CAM logu se otevírá kliknutím na vybraný CAM log v seznamu nebo po vytvoření nového CAM logu.

Sledované události

Karta umožňuje vybrat seznam událostí, při kterých se budou zachytávat snímky z kamer.

Sledované události mohou být následující:

- **Přístupy**
  - Uživatel akceptován
  - Poznávací značka auta rozpoznána
  - Uživatel odmítnut
  - Stisk tlačítka REX
- **Bezpečnost**
  - Aktivován ochranný spínač
  - Neautorizované otevření dveří
  - Vzdálené otevření dveří
  - Přístup odmítnut – opakované chybné zadání
  - Tichý alarm aktivován

Monitorovaná zařízení

Je doporučeno nastavit zaznamenávání CAM logů jen ze zařízení vybavených kamerou. Výběr zařízení se provádí v dialogovém okně, které se otevírá pomocí . Současně karta umožňuje zapnutí zaznamenávání CAM logů ze všech zařízení.

Dvoufaktorové ověření

Dvoufaktorové ověření poskytuje vyšší úroveň zabezpečení uživatelského účtu v **Access Commanderu**. Pro přihlášení uživatel zadá přihlašovací údaje a následně musí své přihlášení potvrdit pomocí ověřovací aplikace. Jakmile administrátor zapne nutnost dvoufaktorového ověření, bude uživatel při následujícím přihlášení vyzván k propojení svého účtu s vlastní ověřovací aplikací.

Dvoufaktorového ověření nastavuje administrátor na stránce Nastavení > Konfigurace > karta Dvoufaktorové ověření. Administrátor může vybrat, u kterých uživatelů bude dvoufaktorové ověření vyžadováno.

Možnosti vyžadování dvoufázového ověření

- **Volitelné**
  Dvoufaktorové ověření je dobrovolné. Uživatelé si jej mohou sami zapnout na svém profilu, viz Zapnutí dvoufázového ověření (str. 63).
- **Povinné pro uživatele s rolí**
  Každý uživatel, kterému byla přiřazena role, musí své přihlášení potvrdit pomocí ověřovací aplikací.
- **Povinné**
  Všichni uživatelé musí své přihlášení potvrdit pomocí ověřovací aplikaci.

Zapnutí dvoufázového ověření

Pokud administrátor nastaví volitelné dvoufázové ověření, zapíná si dvoufázové ověření sám uživatel následujícím způsobem:

1. Kliknutím na obrázek uživatele v pravém horním rohu otevřete uživatelské menu.
2. Vyberte Zobrazit profil.
3. Na kartě Dvoufázové ověřování propojíte účet s ověřovací aplikací. Postupujte podle pokynů.

Povolení přístupu SSH

VAROVÁNÍ
Povolení přístupu SSH je doporučeno pouze zkušeným uživatelům. Nesprávné použití představuje bezpečnostní riziko.

Nastavení > Konfigurace > karta SSH slouží k povolení Secure Shell, které poskytuje zabezpečenou vzdálenou komunikaci se systémovou konzolí. Zapnutá služba SSH umožňuje zálohování a obnovu systému nebo úplný restart **Access Commanderu**.

K připojení Access Commander boxu nebo virtuálního stroje potřebuje SSH klient znát IP adresu **Access Commanderu** a heslo root uživatele systému. Heslo root uživatele systému lze nastavit v Nastavení > Konfigurace > karta SSH.

POZNÁMKA
Ke změně hesla root uživatele dojde v konfigurační konzoli, ne v Access Commanderu.

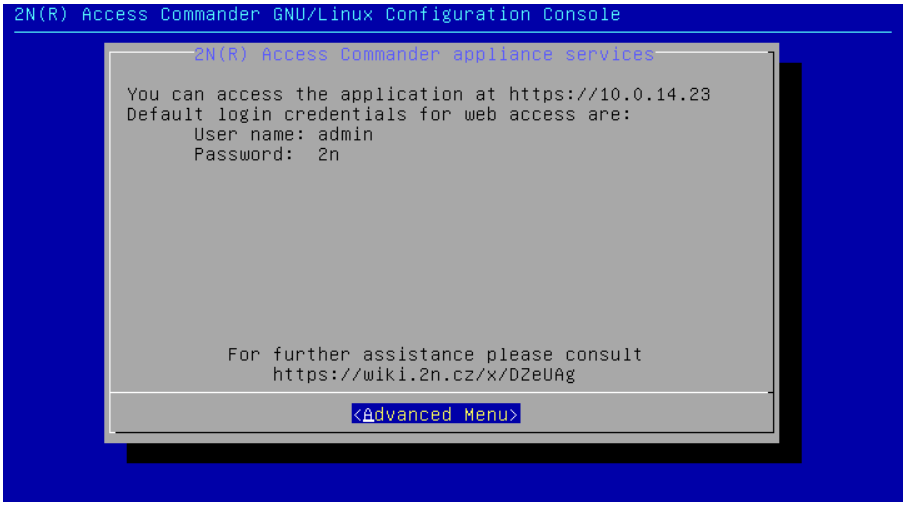
Přístup SSH je možné také povolit a spravovat přímo v konfigurační konzoli Linux, viz Linuxové nastavení (str. 64).

Linuxové nastavení

Základní nastavení systému je možné provádět v konfigurační konzoli systému Linux.

POZNÁMKA
Pokud je **Access Commander** distribuován prostřednictvím virtuálního stroje, je možné se do linuxové verze připojit vzdáleně prostřednictvím SSH připojení.

Konfigurační konzole se otevře přihlášením k **Access Commanderu** pomocí root účtu. Úvodní stránka zobrazuje základní informace o administrátorském přístupu na webové rozhraní a přesměrovává na Advanced Menu.



V Advanced Menu je možné nastavovat:

- **Networking**
  Nastavení proxy serveru, síťových vlastností, možností synchronizace se DHCP serverem.
- **Time**
  Manuální nastavení času, nastavení NTP serveru a časové zóny.
- **SSH**
  Nastavuje vzdálené připojení k **Access Commanderu** přes SSH. Pro povolení SSH musí být nastavené jiné než defaultní heslo, které splňuje nároky na jeho obtížnost.
- **SMB**
  Spouští průvodce pro nastavení připojení ke sdíleným složkám. Nastavuje IP adresu nebo doménové jméno a cestu ke složce. Např. „192.168.1.1/share“. Pro nastavení je potřeba uvést uživatelské jméno uživatele, který získá přístup do dané složky a právo zapisovat. Je potřeba vyplnit heslo uživatele a zvolit verzi Samba protokolu. Po splnění všech povinných kroků se ověří spojení se serverem a zobrazí se informace, zda bylo nastavení úspěšné, nebo chybné.
- **Password**
  Umožňuje změnu hesla root uživatele systému pro přihlášení do konzole nebo pro přístup přes SSH.

POZNÁMKA
Ke změně hesla root uživatele dojde v konfigurační konzoli, ne v Access Commanderu.

- **Backup and restore**
  Slouží k importu dat a konfigurace, nastavení opakované zálohy, obnovení z dřívější zálohy.

Řešení potíží

Diagnostické logy

Diagnostické logy slouží Technické podpoře k identifikaci a řešení hlášených problémů. Logy obsahují informace o prováděných akcích, chybách, změnách stavu a dalších relevantních událostech.

Stažení diagnostických logů

1. Přejděte do **Nastavení** > **Řešení potíží** > **karta Diagnostické logy**.
2. Klikněte na Vygenerovat logy.
   Generování balíčku s logy trvá několik minut.
3. Jakmile je balíček připraven, zobrazí se na kartě a je možné jej Stáhnout.

Statistika využití

Je-li funkce zapnutá, odesílá **Access Commander** jednou denně anonymní data o používaných funkcích na zabezpečený 2N server. Každé odeslání je prováděno pod unikátním identifikátorem, který se s každým novým odesláním automaticky generuje znovu. Straně 2N je tak zamezeno identifikovat danou instalaci **Access Commanderu**. Získané informace slouží ke zlepšení vývoje produktů, rozvoji funkcí a ke zlepšení uživatelské zkušenosti.

Doplňkové informace

HTTP API

Adresa URL pro API **Access Commanderu** je: https://acom_ip_address/api/v3/.

Seznam API endpointů je zveřejňován na na http(s)://acom_ip_address/support/api. Mimo rozhraní **Access Commanderu** je k nahlédnutí seznam endpointů vydaný s verzí firmwaru 2.7.

Autentizace

HTTP API příkazy se odesílají pod přihlašovacími údaji uživatele nebo pomocí tokenové autentizace. Autentizační token vytváří administrátor v Nastavení > Konfigurace > karta API přístupový klíč. API přístupový klíč má funkci Bearer Tokenu. Při vytváření nového API přístupového klíče může administrátor omezit platnost klíče pouze pro čtení, klíč tak bude autentizovat pouze GET příkazy. Klíči je možné omezit platnost na: 1 měsíc, 6 měsíců, 1 rok.

VÝSTRAHA
Po vytvoření přístupového klíče si klíč zkopírujte do schránky a použijte. Později již nebude možné klíč zobrazit.

Licence třetích stran

Kompletní seznam použitých licencí knihoven třetích stran je uveden v uživatelském menu umístěném vpravo na horní liště, v sekci O aplikaci.

wiki.2n.com

2N Access Commander – Uživatelský manuál

2N.com