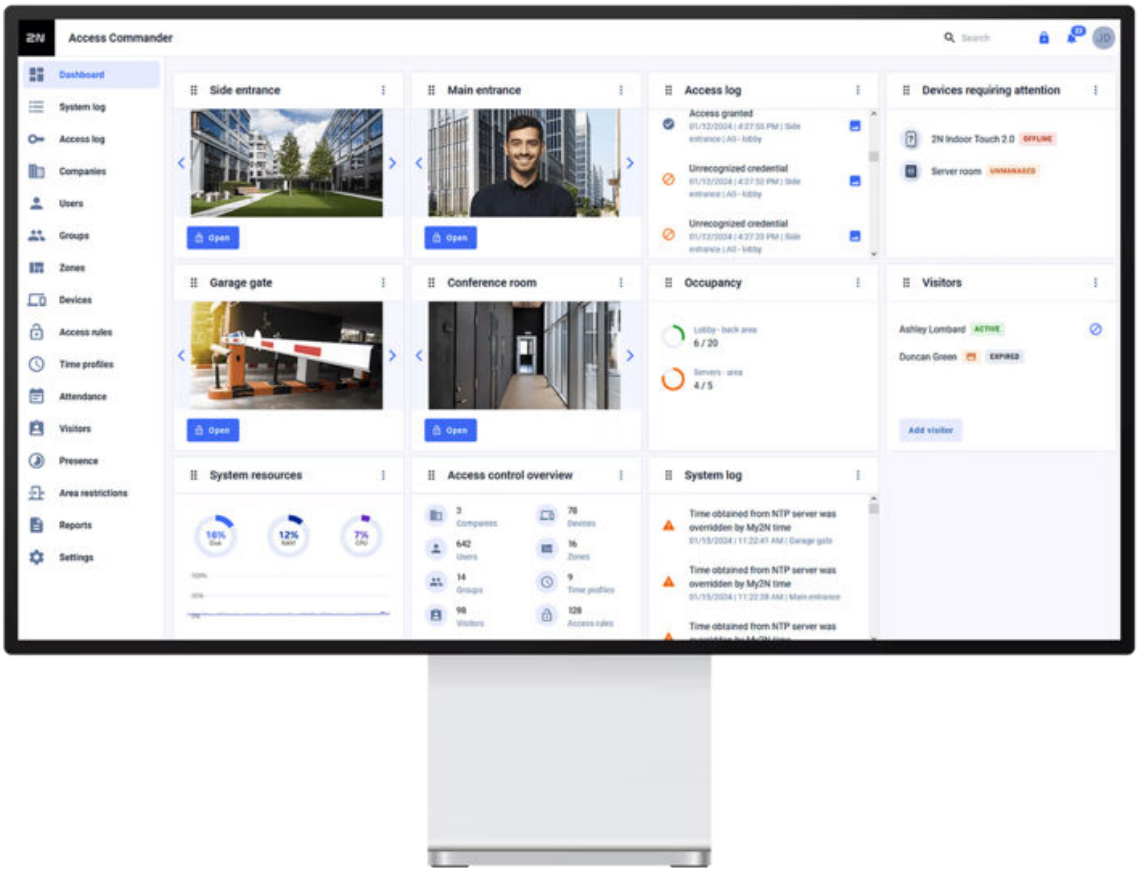
2N Access Commander

Instalační manuál



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

2N.com

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 (interkomy 2N, přístupové jednotky 2N, elektronické zámky 2N) nebo umožňující komunikaci (odpovídací jednotky 2N). 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.
- Správa členství uživatelů ve skupinách.
- Vytváření a správa návštěv.
- Vytváření a správa časových profilů.
- Nastavení přístupových pravidel.

Správce uživatelů

- Vytváření a správa uživatelů.
- Vytváření a správa návštěv.
- Správa členství uživatelů 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.

Administrátor společnosti

- Nastavení výchozího jazyka společnosti.
- Sledování systémového logu (omezeno na události dané společnosti).
- Možnost nastavení widgetu pro systémový log a funkci Nouzové uzamknutí na zařízeních, které společnost používá (včetně společných zařízení s jinými společnostmi).

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. 63).

Interkomy 2N

- 2N IP Style – podporuje čtení QR kódů
- 2N IP Verso 2.0 – podporuje čtení QR kódů
- 2N IP Force 2.0 – podporuje čtení QR kódů
- 2N IP Verso
- 2N LTE Verso
- 2N IP One
- 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 Access Unit M

Elektronické zámky 2N

- 2N Fortis Handle
- 2N Fortis Cylinder

Odpovídací jednotky 2N

- 2N Indoor View (Wi-Fi)
- 2N Indoor Compact
- 2N Indoor Talk
- 2N Indoor Touch 2.0
- 2N Clip
- 2N Clip 2wire-IP

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

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

Licence:	Trial	Basic	Advanced	Pro	Unlimited
Objednací číslo	n/a	n/a	91379031	91379032	91379033
Přístupové a systémové logy	✓	✓	✓	✓	✓
Přístupová pravidla	✓	✓	✓	✓	✓
API správa	✓	✓	✓	✓	✓
Aktivace/deaktivace účtu	✓	✓	✓	✓	✓
Omezení počtu neúspěšných přístupů	✓	✓	✓	✓	✓
Tichý alarm	✓	✓	✓	✓	✓
Zónový kód	✓	✓	✓	✓	✓
Monitorování zařízení	✓	✓	✓	✓	✓
Správa logů	✓	✓	✓	✓	✓
Správa elektronických zámků	✓	✓	✓	✓	✓
Import uživatelů z CSV nebo ze zařízení	✓	×	✓	✓	✓
Hromadná správa firmwaru	✓	×	✓	✓	✓
Vícenásobná autentizace	✓	×	✓	✓	✓
Oprávnění uživatele	✓	×	✓	✓	✓
Notifikace	✓	×	✓	✓	✓
Přítomnost	✓	×	✓	✓	✓

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

[a.] Neomezeno v rámci maximálních možností softwarové platformy, viz Doporučený hardware pro virtuální stroj (str. 19).

Instalace

Access Commander může být distribuován dvěma způsoby:

- Malý stolní počítač 2N Access Commander Box 2.0 (obj. č. 1120120xx)
- Virtuální počítač

Řešení Access Commander Box je omezené na 7000 připojených zařízení. Ostatní vlastnosti softwaru jsou pro obě řešení totožné.

Distribuce přes Access Commander Box

Access Commander Box 2.0 (1120120xx, 03129-00) 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 2.0 slouží jako server pro sběr dat, událostí a logů z celého přístupového systému.

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.

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 a Axis IP Utility 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 na Access Commander Boxu **přímým propojením s počítačem**

1. Propojte Access Commander Box přímo s počítačem pomocí síťového kabelu.
2. Po přibližně **15 sekundách** se automaticky nastaví link-local adresa.
3. Otevřete v prohlížeči adresu **accesscommander.local**.
   Alternativně můžete využít nástroje 2N IP Network Scannder nebo Axis IP Utility a vyhledat zařízení i v případě, že nedostalo IP adresu přes DHCP.
4. Ve webovém rozhraní nastavte statickou adresu podle potřeby.

Nastavení statické adresy Access Commanderu na 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.

TIP
Přímé propojení s počítačem a použití adresy **accesscommander.local** je doporučený a nejjednodušší způsob nastavení statické adresy na Access Commander Boxu.

POZNÁMKA
Sériové číslo zobrazené v aplikacích 2N Network Scanner nebo Axis IP Utility se může lišit od sériového čísla uvedeného na štítku Access Commander Boxu.

Fortis Commander

Fortis Commander je samostatná aplikace, která propojuje elektronické zámky **Fortis** se systémem **Access Commander**. Aplikace nastavuje zámky podle projektového souboru vytvořeného v **Access Commander**u, který obsahuje konfiguraci zámků. Soubor je šifrovaný a lze jej použít pouze na jedné konkrétní instalaci.

Instalace

Aplikace Fortis Commander je určena pro instalaci na počítači s operačním systémem Windows s podporou Bluetooth Low Energy (BLE).

Aplikaci můžete najít na webu 2N Download Centre.

Postup instalace

1. Stáhněte instalační balíček z uvedeného odkazu.
2. Spusťte instalátor a dokončete instalaci podle pokynů na obrazovce.

Projektový soubor

Projektový soubor je vytvořen v **Access Commanderu** a obsahuje kompletní konfiguraci projektu. Soubor je šifrovaný a chráněný heslem.

Nastavení zámků v Access Commanderu

Před nahráním klíčů do jednotlivých zámků je potřeba spárovat **Access Commander** s aplikací **Fortis Commander**.

Vygenerování hlavního šifrovacího klíče (MEK) a příprava projektu

1. Přihlaste se do systému Access Commander.
2. Přejděte na stránku **Nastavení > Elektronické zámky**.
3. V kartě **Počáteční nastavení** klikněte na Vygenerovat klíče.

4. Vytvořte Hlavní šifrovací klíč.

> **VÝSTRAHA**
> Hlavní šifrovací klíč nelze později **zobrazit ani změnit**.

> **POZNÁMKA**
> Podle hlavního šifrovacího klíče (MEK) generuje **2N Access Commander** sadu šifrovacích klíčů. Klíč by tak měl být unikátní a dostatečně bezpečný. Sada klíčů vychází z hlavního šifrovacího klíče, proto projekty se stejným hlavním šifrovacím klíčem generují stejné sady klíčů. Při ztrátě projektu je možné vytvořit nový projekt se stejným hlavním šifrovacím klíčem a pokračovat s šifrováním.

5. Po vygenerování klíčů a nastavení hesla k projektovému souboru je možné stáhnout **projektový soubor**, který představuje obraz konfigurace elektronických zámků v systému **Access Commander**.
6. V kartě **Fortis Commander** klikněte na Stáhnout aplikaci, odkud se začne stahovat **Fortis Commander** (aplikace pro konfiguraci elektronických zámků).

> **VÝSTRAHA**
> Informace o projektu jsou citlivá data. Chraňte je před zneužitím.

Propsání konfigurace elektronického zámku pomocí Fortis Commander

1. Nainstalujte aplikaci **Fortis Commander** a otevřete ji.
2. Klikněte na Open project a otevřete stažený projektový soubor v Průzkumníku souborů.
3. V zobrazeném dialogu zadejte heslo k projektovému souboru.
4. Po otevření projektového souboru zvolte Connect to device a přiložte servisní kartu k zámku.
5. Klikněte na **Assign**, čímž přiřadíte zámek k projektu.
6. Odpojte zařízení a klikněte na **File > Close project**.
7. Po dokončení konfigurace otevřete systém **Access Commander**. Přejděte do karty **Nastavení > Elektronické zámky** a znovu klikněte na tlačítko Fortis Commander. Nahrajte projektový soubor.

> **POZNÁMKA**
> Při přesunu zámku mezi instalacemi nebo při reklamaci je nutné provést **Factory reset**. Tato operace obnoví zámek do továrního nastavení a odstraní veškerou předchozí konfiguraci.

Postup aktualizace konfigurace

1. Proveďte změny v **Access Commanderu**.
2. Stáhněte nový projektový soubor.
3. Nahrajte soubor do **Fortis Commanderu** a proveďte požadované změny na zámcích.
4. Pokud provedete další změny v **Access Commander**u, vždy stáhněte nový projektový soubor.

VÝSTRAHA
Pro každou změnu konfigurace v **Access Commander**u je nutné stáhnout nový projektový soubor – nelze použít starší soubor, který byl již nahrán do **Fortis Commanderu**.

Trvalé zamknutí a odemknutí

Aplikace umožňuje trvalé zamknutí a odemknutí zámku. Funkce slouží pro servisní zásahy nebo nouzové ovládání bez použití karty.

Sběr událostí z elektronických zámků pomocí RFID karet / čipů

Nastavení sběru událostí

1. Otevřete **Nastavení > Elektronické zámky > Události na kartách**.
2. Vyberte typ událostí:
   - **Shromažďovat přístupové a systémové události** – na kartu/čip se zaznamenávají všechny přístupové a systémové události, které se propisují do **Systémového logu** a **Přístupového logu**.
   - **Shromažďovat pouze systémové události** – zaznamenají se pouze systémové události, přístupové události se neukládají na karty.
   - **Neshromažďovat události na kartách** – žádné události se nezapisují na kartu; přístup k nim je možný pouze prostřednictvím **Fortis Commander**u.

TIP
Výběrem vhodné množiny událostí lze snížit zatížení systému a využití úložiště. Podrobné protokolování je však důležité pro diagnostiku a bezpečnostní audity.

Export událostí z karty

Na kartu se ukládá maximálně **16 prvních událostí**. Události lze vyčíst dvěma způsoby:

- V **Access Commanderu** klikněte na ikonu ve vyhledávacím poli v záhlaví a načtěte kartu.
- Pomocí zařízení s **2N OS** se události z karty vyčtou a odešlou do **Access Commander**u.

Nahrání událostí do zámku

1. Otevřete **Nastavení > Elektronické zámky > Fortis Commander** a klikněte na Stažení souboru.
2. Otevřete soubor v aplikaci **Fortis Commander**.
3. V aplikaci **Fortis Commander** se připojte k elektronickému zámku.
4. Nahrajte aktualizovaný soubor zpět do **Access Commanderu**.
5. Po nahrání se události zobrazí v **Přístupové logy** a **Systémové logy**.

Servisní operace

Tyto operace jsou dostupné pro **Fortis Cylinder**:

- **Demontáž** – rozebrání zámků pro servisní účely.
- **Výměna baterie** – výměna baterie v zámku.

VÝSTRAHA
Servisní operace nejsou relevantní pro jiné typy zámků.

POZNÁMKA
Ze servisního módu se zámek vrátí do běžného režimu stisknutím tlačítka Lock pro trvalé zamknutí.

Distribuce přes virtuální počítač

Access Commander může být distribuován jako virtuální počítač. 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 Podpora > Download Center > 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 Podpora > Download Center > 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 Podpora > Download Center > 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).
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.

Hyper-V

1. Stáhněte příslušný software ze sekce Podpora > Download Center > 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 počítače.
6. Vyberte typ importu.
7. Vyberte virtuální síťovou kartu pro virtuální spočítač.
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 pro virtuální stroj

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 znovu-připojení 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.

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

Technické parametry

Možnosti programu na Access Commander Box 2.0

Počet připojených zařízení	Počet uživatelů	Počet uživatelů ve skupině
7 000	200 000	1 500

Technické parametry Access Commander Box

1. generace obj. č. 91379030	2. generace obj. č. 1120120E, 1120120GB, 1120120US
• rozměry: 56,1 x 107,6 x 114,4 mm (2,21" x 4,24" x 4,50") • 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	• rozměry: 127,5 x 132 x 57,6 mm (5,02 " x 5,20" x 2,27") • Intel® Processor N100, 6W TDP • SSD 980 NVMe M.2 – 250 GB • DDR4 SO-DIMM memory – 16 GB, 1,2 V, 3200 MHz • podpora HDMI 2.1, DisplayPort 1.4 a VGA • 2.5G RJ45 LAN port pro ethernetové připojení • Skladovací teplota: −40 °C až +85 °C • Provozní teplota: 0 °C až +50 °C

Doporučený hardware pro virtuální stroj

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 znovu-připojení 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.

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

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. Musí se jednat o sériové číslo hlavní jednotky interkomu, přístupové jednotky nebo odpovídací jednotky (nelze použít 2N Indoor Touch).

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.

Obnovení licence

Pro obnovení pozastavené licence je potřeba připojit a aktivovat licenční zařízení nebo nechat vygenerovat a nahrát nový licenční soubor pro jiné 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.

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.

POZNÁMKA
Vyřazení zařízení ze správy znamená, že nelze provádět změny v jejich konfiguraci prostřednictvím **Access Commanderu**. Změny provedené v **Access Commanderu** se na zařízení nepřenesou. Zařízení ovšem dále fungují na základě dat z poslední přenesené konfigurace z **Acccess Commanderu**. To znamená, že přístupy i ostatní nastavení zůstává na zařízeních stejné, jaké bylo před pozastavením licence.

Změnu konfigurace nespravovaného zařízení je možné provádět pouze ve webovém konfiguračním rozhraní jednotlivého zařízení. Po opětovném připojení zařízení do správy **Access Commanderem** dojde k synchronizaci a změny provedené přímo ve webovém konfiguračním rozhraní zařízení budou přepsány nastavením v **Access Commanderu**.

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

Elektronické zámky

Systém **Access Commander** zajišťuje správu přístupů přes elektronické zámky 2N Fortis, které se odemykají RFID kartou s technologií MIFARE® DESFire®. Při konfiguraci elektronických zámků je každému zámku

přidělen šifrovací klíč. Klíče zámků jsou pak uloženy na RFID kartách oprávněných uživatelů. Při shodě klíčů na kartě a v zámku dojde k odemknutí uzamykacího mechanismu.

Jednu přístupovou RFID kartu je možné používat pro přístup až k 90 dveřím se zámky 2N Fortis, v závislosti na počtu uplatněných časových profilů. Při překročení kapacity paměti karty zápis dat na kartu selže. Událost selhání zápisu se zaznamenává v přístupovém logu systému. Pokud jsou použity Skupiny zámků, může být na jednu kartu zapsáno více dveří než při individuálním přiřazení.

Fortis Commander

Fortis Commander je samostatná aplikace, která propojuje elektronické zámky **Fortis** se systémem **Access Commander**. Aplikace nastavuje zámky podle projektového souboru vytvořeného v **Access Commander**u, který obsahuje konfiguraci zámků. Soubor je šifrovaný a lze jej použít pouze na jedné konkrétní instalaci.

Instalace

Aplikace Fortis Commander je určena pro instalaci na počítači s operačním systémem Windows s podporou Bluetooth Low Energy (BLE).

Aplikaci můžete najít na webu 2N Download Centre.

Postup instalace

1. Stáhněte instalační balíček z uvedeného odkazu.
2. Spusťte instalátor a dokončete instalaci podle pokynů na obrazovce.

Projektový soubor

Projektový soubor je vytvořen v **Access Commanderu** a obsahuje kompletní konfiguraci projektu. Soubor je šifrovaný a chráněný heslem.

Nastavení zámků v Access Commanderu

Před nahráním klíčů do jednotlivých zámků je potřeba spárovat **Access Commander** s aplikací **Fortis Commander**.

Vygenerování hlavního šifrovacího klíče (MEK) a příprava projektu

1. Přihlaste se do systému Access Commander.
2. Přejděte na stránku **Nastavení > Elektronické zámky**.
3. V kartě **Počáteční nastavení** klikněte na Vygenerovat klíče.
4. Vytvořte Hlavní šifrovací klíč.

VÝSTRAHA
Hlavní šifrovací klíč nelze později **zobrazit ani změnit**.

POZNÁMKA
Podle hlavního šifrovacího klíče (MEK) generuje **2N Access Commander** sadu šifrovacích klíčů. Klíč by tak měl být unikátní a dostatečně bezpečný. Sada klíčů vychází z hlavního šifrovacího klíče, proto projekty se stejným hlavním šifrovacím klíčem generují stejné sady klíčů. Při ztrátě projektu je možné vytvořit nový projekt se stejným hlavním šifrovacím klíčem a pokračovat s šifrováním.

5. Po vygenerování klíčů a nastavení hesla k projektovému souboru je možné stáhnout **projektový soubor**, který představuje obraz konfigurace elektronických zámků v systému **Access Commander**.
6. V kartě **Fortis Commander** klikněte na Stáhnout aplikaci, odkud se začne stahovat **Fortis Commander** (aplikace pro konfiguraci elektronických zámků).

VÝSTRAHA
Informace o projektu jsou citlivá data. Chraňte je před zneužitím.

Propsání konfigurace elektronického zámku pomocí Fortis Commander

1. Nainstalujte aplikaci **Fortis Commander** a otevřete ji.
2. Klikněte na Open project a otevřete stažený projektový soubor v Průzkumníku souborů.
3. V zobrazeném dialogu zadejte heslo k projektovému souboru.
4. Po otevření projektového souboru zvolte Connect to device a přiložte servisní kartu k zámku.
5. Klikněte na **Assign**, čímž přiřadíte zámek k projektu.
6. Odpojte zařízení a klikněte na **File > Close project**.
7. Po dokončení konfigurace otevřete systém **Access Commander**. Přejděte do karty **Nastavení > Elektronické zámky** a znovu klikněte na tlačítko Fortis Commander. Nahrajte projektový soubor.

POZNÁMKA
Při přesunu zámku mezi instalacemi nebo při reklamaci je nutné provést **Factory reset**. Tato operace obnoví zámek do továrního nastavení a odstraní veškerou předchozí konfiguraci.

Postup aktualizace konfigurace

1. Proveďte změny v **Access Commanderu**.
2. Stáhněte nový projektový soubor.
3. Nahrajte soubor do **Fortis Commanderu** a proveďte požadované změny na zámcích.
4. Pokud provedete další změny v **Access Commander**u, vždy stáhněte nový projektový soubor.

VÝSTRAHA
Pro každou změnu konfigurace v **Access Commander**u je nutné stáhnout nový projektový soubor – nelze použít starší soubor, který byl již nahrán do **Fortis Commanderu**.

Trvalé zamknutí a odemknutí

Aplikace umožňuje trvalé zamknutí a odemknutí zámku. Funkce slouží pro servisní zásahy nebo nouzové ovládání bez použití karty.

Sběr událostí z elektronických zámků pomocí RFID karet / čipů

Nastavení sběru událostí

1. Otevřete **Nastavení > Elektronické zámky > Události na kartách**.

2. Vyberte typ událostí:
   - **Shromažďovat přístupové a systémové události** – na kartu/čip se zaznamenávají všechny přístupové a systémové události, které se propisují do **Systémového logu** a **Přístupového logu**.
   - **Shromažďovat pouze systémové události** – zaznamenají se pouze systémové události, přístupové události se neukládají na karty.
   - **Neshromažďovat události na kartách** – žádné události se nezapisují na kartu; přístup k nim je možný pouze prostřednictvím **Fortis Commander**u.

TIP
Výběrem vhodné množiny událostí lze snížit zatížení systému a využití úložiště. Podrobné protokolování je však důležité pro diagnostiku a bezpečnostní audity.

Export událostí z karty

Na kartu se ukládá maximálně **16 prvních událostí**. Události lze vyčíst dvěma způsoby:

- V **Access Commanderu** klikněte na ikonu ve vyhledávacím poli v záhlaví a načtěte kartu.
- Pomocí zařízení s **2N OS** se události z karty vyčtou a odešlou do **Access Commander**u.

Nahrání událostí do zámku

1. Otevřete **Nastavení > Elektronické zámky > Fortis Commander** a klikněte na Stažení souboru.
2. Otevřete soubor v aplikaci **Fortis Commander**.
3. V aplikaci **Fortis Commander** se připojte k elektronickému zámku.
4. Nahrajte aktualizovaný soubor zpět do **Access Commanderu**.
5. Po nahrání se události zobrazí v **Přístupové logy** a **Systémové logy**.

Servisní operace

Tyto operace jsou dostupné pro **Fortis Cylinder**:

- **Demontáž** – rozebrání zámků pro servisní účely.
- **Výměna baterie** – výměna baterie v zámku.

VÝSTRAHA
Servisní operace nejsou relevantní pro jiné typy zámků.

POZNÁMKA
Ze servisního módu se zámek vrátí do běžného režimu stisknutím tlačítka Lock pro trvalé zamknutí.

Aktualizace karty

Přístupové karty uživatelů je potřeba pravidelně aktualizovat. Aktualizaci karty uživatel provede přiložením karty k IP zařízení 2N, ke kterému má platná přístupová práva. Kartu je nutné u čtečky zařízení přidržet až do sepnutí spínače otevírání dveří. Spínač otevírání dveří se aktivuje až po aktualizaci přístupů k zámkům.

Výchozí desetidenní platnost karet je možné změnit v **Nastavení > Elektronické zámky > karta Parametry karty**.

VÝSTRAHA
Pokud v **Access Commanderu** změníte přístupová práva k zámkům, změny se na přístupové kartě uživatele projeví až po její aktualizaci na čtečce karet zařízení 2N! Z bezpečnostních důvodů doporučujeme nastavit kratší platnost karet pro zajištění jejich pravidelné aktualizace.

Čtečky IP zařízení, které umožňují aktualizaci karty, a jejich nastavení je popsáno v kapitole Nastavení čtečky IP zařízení (str. 28).

Kompatibilní karty

POZNÁMKA
Pro účely této dokumentace označuje pojem **karta** jakýkoli kompatibilní identifikátor využívající technologii MIFARE DESFire.

Pro otevírání elektronických zámků 2N Fortis nelze používat karty s náhodným ID (random ID).

Karty s technologií PICard nelze použít pro otevírání elektronických zámků 2N Fortis.

Časové profily na elektronických zámcích

Elektronické zámky podporují časové profily s následujícími omezeními:

- Svátky se neuplatňují.
- V rámci jednoho dne lze nastavit až 4 různé časové intervaly.
- V rámci jednoho časového profilu lze definovat 4 denní rozvrhy intervalů.

TIP
To znamená, že lze mít například jiná nastavení pro pondělí, úterý, středu a čtvrtek, ale pro pátek, sobotu a neděli už musíte použít jedno z existujících nastavení.

VÝSTRAHA
Pokud časový profil poruší uvedená omezení, bude přístupové pravidlo ignorováno a uživateli nebude udělen přístup.

Fortis Commander

Fortis Commander je samostatná aplikace, která propojuje elektronické zámky **Fortis** se systémem **Access Commander**. Aplikace nastavuje zámky podle projektového souboru vytvořeného v **Access Commander**u, který obsahuje konfiguraci zámků. Soubor je šifrovaný a lze jej použít pouze na jedné konkrétní instalaci.

Instalace

Aplikace Fortis Commander je určena pro instalaci na počítači s operačním systémem Windows s podporou Bluetooth Low Energy (BLE).

Aplikaci můžete najít na webu 2N Download Centre.

Postup instalace

1. Stáhněte instalační balíček z uvedeného odkazu.
2. Spusťte instalátor a dokončete instalaci podle pokynů na obrazovce.

Projektový soubor

Projektový soubor je vytvořen v **Access Commanderu** a obsahuje kompletní konfiguraci projektu. Soubor je šifrovaný a chráněný heslem.

Nastavení zámků v Access Commanderu

Před nahráním klíčů do jednotlivých zámků je potřeba spárovat **Access Commander** s aplikací **Fortis Commander**.

Vygenerování hlavního šifrovacího klíče (MEK) a příprava projektu

1. Přihlaste se do systému Access Commander.
2. Přejděte na stránku **Nastavení > Elektronické zámky**.
3. V kartě **Počáteční nastavení** klikněte na Vygenerovat klíče.
4. Vytvořte Hlavní šifrovací klíč.

VÝSTRAHA
Hlavní šifrovací klíč nelze později **zobrazit ani změnit**.

POZNÁMKA
Podle hlavního šifrovacího klíče (MEK) generuje **2N Access Commander** sadu šifrovacích klíčů. Klíč by tak měl být unikátní a dostatečně bezpečný. Sada klíčů vychází z hlavního šifrovacího klíče, proto projekty se stejným hlavním šifrovacím klíčem generují stejné sady klíčů. Při ztrátě projektu je možné vytvořit nový projekt se stejným hlavním šifrovacím klíčem a pokračovat s šifrováním.

5. Po vygenerování klíčů a nastavení hesla k projektovému souboru je možné stáhnout **projektový soubor**, který představuje obraz konfigurace elektronických zámků v systému **Access Commander**.
6. V kartě **Fortis Commander** klikněte na Stáhnout aplikaci, odkud se začne stahovat **Fortis Commander** (aplikace pro konfiguraci elektronických zámků).

VÝSTRAHA
Informace o projektu jsou citlivá data. Chraňte je před zneužitím.

Propsání konfigurace elektronického zámku pomocí Fortis Commander

1. Nainstalujte aplikaci **Fortis Commander** a otevřete ji.
2. Klikněte na Open project a otevřete stažený projektový soubor v Průzkumníku souborů.
3. V zobrazeném dialogu zadejte heslo k projektovému souboru.
4. Po otevření projektového souboru zvolte Connect to device a přiložte servisní kartu k zámku.
5. Klikněte na **Assign**, čímž přiřadíte zámek k projektu.
6. Odpojte zařízení a klikněte na **File > Close project**.

7. Po dokončení konfigurace otevřete systém **Access Commander**. Přejděte do karty **Nastavení > Elektronické zámky** a znovu klikněte na tlačítko Fortis Commander. Nahrajte projektový soubor.

POZNÁMKA
Při přesunu zámku mezi instalacemi nebo při reklamaci je nutné provést **Factory reset**. Tato operace obnoví zámek do továrního nastavení a odstraní veškerou předchozí konfiguraci.

Postup aktualizace konfigurace

1. Proveďte změny v **Access Commanderu**.
2. Stáhněte nový projektový soubor.
3. Nahrajte soubor do **Fortis Commanderu** a proveďte požadované změny na zámcích.
4. Pokud provedete další změny v **Access Commander**u, vždy stáhněte nový projektový soubor.

VÝSTRAHA
Pro každou změnu konfigurace v **Access Commander**u je nutné stáhnout nový projektový soubor – nelze použít starší soubor, který byl již nahrán do **Fortis Commanderu**.

Trvalé zamknutí a odemknutí

Aplikace umožňuje trvalé zamknutí a odemknutí zámku. Funkce slouží pro servisní zásahy nebo nouzové ovládání bez použití karty.

Sběr událostí z elektronických zámků pomocí RFID karet / čipů

Nastavení sběru událostí

1. Otevřete **Nastavení > Elektronické zámky > Události na kartách**.
2. Vyberte typ událostí:
   - **Shromažďovat přístupové a systémové události** – na kartu/čip se zaznamenávají všechny přístupové a systémové události, které se propisují do **Systémového logu** a **Přístupového logu**.
   - **Shromažďovat pouze systémové události** – zaznamenají se pouze systémové události, přístupové události se neukládají na karty.
   - **Neshromažďovat události na kartách** – žádné události se nezapisují na kartu; přístup k nim je možný pouze prostřednictvím **Fortis Commander**u.

TIP
Výběrem vhodné množiny událostí lze snížit zatížení systému a využití úložiště. Podrobné protokolování je však důležité pro diagnostiku a bezpečnostní audity.

Export událostí z karty

Na kartu se ukládá maximálně **16 prvních událostí**. Události lze vyčíst dvěma způsoby:

- V **Access Commanderu** klikněte na ikonu  ve vyhledávacím poli v záhlaví a načtěte kartu.
- Pomocí zařízení s **2N OS** se události z karty vyčtou a odešlou do **Access Commander**u.

Nahrání událostí do zámku

1. Otevřete **Nastavení > Elektronické zámky > Fortis Commander** a klikněte na Stažení souboru.
2. Otevřete soubor v aplikaci **Fortis Commander**.
3. V aplikaci **Fortis Commander** se připojte k elektronickému zámku.
4. Nahrajte aktualizovaný soubor zpět do **Access Commanderu**.
5. Po nahrání se události zobrazí v **Přístupové logy** a **Systémové logy**.

Servisní operace

Tyto operace jsou dostupné pro **Fortis Cylinder**:

- **Demontáž** – rozebrání zámků pro servisní účely.
- **Výměna baterie** – výměna baterie v zámku.

VÝSTRAHA
Servisní operace nejsou relevantní pro jiné typy zámků.

POZNÁMKA
Ze servisního módu se zámek vrátí do běžného režimu stisknutím tlačítka Lock pro trvalé zamknutí.

Nastavení čtečky IP zařízení

Nastavení ve webovém rozhraní IP zařízení

VÝSTRAHA
Pokud k zařízení 2N nově připojíte rozšiřující modul čtečky RFID karet pomocí VBUS kabelu, je potřeba tento modul se zařízením spárovat. Spárování rozšiřujícího modulu čtečky provedete přes webové rozhraní zařízení v **Přístup > Moduly**.

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 Hardware > Rozšiřující moduly.
3. Na stránce přejděte k nastavení modulu čtečky RFID karet.
4. Klikněte na Spárovat modul.

5. Z nabídky **Povolené typy karet** vyberte možnost „2N elektronické zámky“.

> **VÝSTRAHA**
> Pro optimální funkci mějte povolené pouzy ty typy karet, které skutečně užíváte.

6. Změny uložte.

Kompatibilní moduly

Synchronizaci klíčů k elektronickým zámkům 2N Fortis lze provádět na všech RFID čtečkách 2N uvedených na trh v únoru 2023 nebo později. Většina čteček vyrobených po tomto datu je také kompatibilní, s výjimkou níže uvedených modelů.

Následující modely **nejsou kompatibilní**:

- **2N IP Base**: všechny RFID čtečky
- **2N IP Force**: 9151011, 9151012, 9151016, 9151017, 9151019
- **2N IP Vario**: všechny RFID čtečky
- **2N IP Verso**: 915503x, 915504x, 915508x
- **2N Access Unit M**: 91611x
- **2N Access Unit 1.0**: 916008, 916009, 916010, 916011, 916013, 916016, 916019
- **2N Access Unit 2.0**: 916033x

U následujících modulů je kompatibilita zajištěna pouze u kusů vyrobených na podzim 2023 nebo později:

- **2N IP Force**: 9151031, 9151031S

Nastavení zámků v Access Commanderu

Před nahráním klíčů do jednotlivých zámků je potřeba spárovat **Access Commander** s aplikací **Fortis Commander**.

Vygenerování hlavního šifrovacího klíče (MEK) a příprava projektu

1. Přihlaste se do systému Access Commander.
2. Přejděte na stránku **Nastavení > Elektronické zámky**.
3. V kartě **Počáteční nastavení** klikněte na Vygenerovat klíče.
4. Vytvořte Hlavní šifrovací klíč.

> **VÝSTRAHA**
> Hlavní šifrovací klíč nelze později **zobrazit ani změnit**.

> **POZNÁMKA**
> Podle hlavního šifrovacího klíče (MEK) generuje **2N Access Commander** sadu šifrovacích klíčů. Klíč by tak měl být unikátní a dostatečně bezpečný. Sada klíčů vychází z hlavního šifrovacího klíče, proto projekty se stejným hlavním šifrovacím klíčem generují stejné sady klíčů. Při ztrátě projektu je možné vytvořit nový projekt se stejným hlavním šifrovacím klíčem a pokračovat s šifrováním.

5. Po vygenerování klíčů a nastavení hesla k projektovému souboru je možné stáhnout **projektový soubor**, který představuje obraz konfigurace elektronických zámků v systému **Access Commander**.
6. V kartě **Fortis Commander** klikněte na Stáhnout aplikaci, odkud se začne stahovat **Fortis Commander** (aplikace pro konfiguraci elektronických zámků).

VÝSTRAHA
Informace o projektu jsou citlivá data. Chraňte je před zneužitím.

Propsání konfigurace elektronického zámku pomocí Fortis Commander

1. Nainstalujte aplikaci **Fortis Commander** a otevřete ji.
2. Klikněte na Open project a otevřete stažený projektový soubor v Průzkumníku souborů.
3. V zobrazeném dialogu zadejte heslo k projektovému souboru.
4. Po otevření projektového souboru zvolte Connect to device a přiložte servisní kartu k zámku.
5. Klikněte na **Assign**, čímž přiřadíte zámek k projektu.
6. Odpojte zařízení a klikněte na **File > Close project**.
7. Po dokončení konfigurace otevřete systém **Access Commander**. Přejděte do karty **Nastavení > Elektronické zámky** a znovu klikněte na tlačítko Fortis Commander. Nahrajte projektový soubor.

POZNÁMKA
Při přesunu zámku mezi instalacemi nebo při reklamaci je nutné provést **Factory reset**. Tato operace obnoví zámek do továrního nastavení a odstraní veškerou předchozí konfiguraci.

Postup aktualizace konfigurace

1. Proveďte změny v **Access Commanderu**.
2. Stáhněte nový projektový soubor.
3. Nahrajte soubor do **Fortis Commanderu** a proveďte požadované změny na zámcích.
4. Pokud provedete další změny v **Access Commander**u, vždy stáhněte nový projektový soubor.

VÝSTRAHA
Pro každou změnu konfigurace v **Access Commander**u je nutné stáhnout nový projektový soubor – nelze použít starší soubor, který byl již nahrán do **Fortis Commanderu**.

Trvalé zamknutí a odemknutí

Aplikace umožňuje trvalé zamknutí a odemknutí zámku. Funkce slouží pro servisní zásahy nebo nouzové ovládání bez použití karty.

Karty pro údržbu

Karty pro údržbu zajišťují autorizovaný přístup k zámku. Umožňují uvedení zámku do servisního stavu, výměnu baterie, demontáž zámku.

VÝSTRAHA
Kartu pro údržbu nelze současně použít jako přístupovou kartu uživatele.

Nastavení karty pro údržbu

1. V **Access Commanderu** přejděte na stránku **Nastavení > Elektronické zámky**.
2. V kartě **Karty pro údržbu** klikněte na Vytvořit.
3. V otevřeném dialogovém okně vyberte typ karty, kterou chcete vytvořit.
   - Nastavení nových zámků – aktivuje do servisního módu již dříve konfigurované nové zámky v továrním nastavení.
   - Servis – aktivuje servisní mód u již nastaveného zámku.
   - Demontáž – uvolní již nastavený zámek 2N Fortis Cylinder k demontáži, viz Instalační manuál 2N Fortis.
   - Výměna baterie – uvolní již nastavený zámek 2N Fortis Cylinder k výměně baterie, viz Instalační manuál 2N Fortis.

   TIP
   Na jednu fyzickou kartu je možné nahrát současně **Nastavení nových zámků** a libovolnou druhou servisní kartu. Doporučujeme kombinaci **Nastavení nových zámků** a **Servis**.
4. Klikněte na Pokračovat.
5. Přiložte kartu k připojené USB RFID čtečce. Vyčkejte do načtení dat na kartu.

Platnost dat na kartě pro údržbu je jeden rok. Po uplynutí této doby je nutné data smazat a kartu nastavit znovu.

Podpora DESFire karet třetích stran (Anonymní vytváření aplikací)

Access Commander umožňuje práci s kartami MIFARE DESFire. Podporuje karty, které jsou již používány v jiných přístupových systémech, a umožňuje jejich opětovné využití bez nutnosti znát jejich hlavní klíč (PICC Master Key).

Jedná se o speciální režim, ve kterém karta povolí vytvoření nové nezávislé aplikace bez nutnosti znalosti jejího hlavního klíče (PICC Master Key).

Díky této funkcionalitě mohou administrátoři:

- Opětovně použít stávající fyzické karty.
- Zapsat na ně aplikaci OSO pro **Access Commander**.
- Vyhnout se nutnosti znát nebo spravovat PICC Master Key původních systémů.

Postup vytvoření aplikace OSO na kartě

1. Přiložte stávající DESfire kartu uživatele ke čtečce připojené k **Access Commanderu**.
2. Vytvořte přístupové údaje pro uživatele.
3. Access Commander automaticky detekuje, zda karta podporuje anonymní vytváření aplikací.
4. Je-li režim podporován, **Access Commander** na kartu zapíše novou anonymní aplikaci, aniž by ovlivnil stávající data nebo aplikace třetích stran.

   VÝSTRAHA
   Pokud je režim podporován, Access Commander zapíše novou anonymní aplikaci bez možnosti pozdějšího formátování karty pomocí funkce v sekci Nastavení. Lze odstranit pouze obsah aplikace, nikoliv uvolnit dříve zabrané místo na kartě.

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 nebo Axis IP Utility. K webovému rozhraní lze také přistoupit přímo na adrese **accesscommander.local**. Tato funkcionalita je ve výchozím stavu zapnuta.

POZNÁMKA

- Pokud je v síti spuštěno více instancí Access Commanderu, systém automaticky přiděluje jedinečné názvy: **accesscommander.local**, **accesscommander-2.local**, **accesscommander-3.local** a další instance podle počtu serverů v síti.
- 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.

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.

Výchozí přihlašovací údaje jsou:

Uživatelské jméno: **Admin**

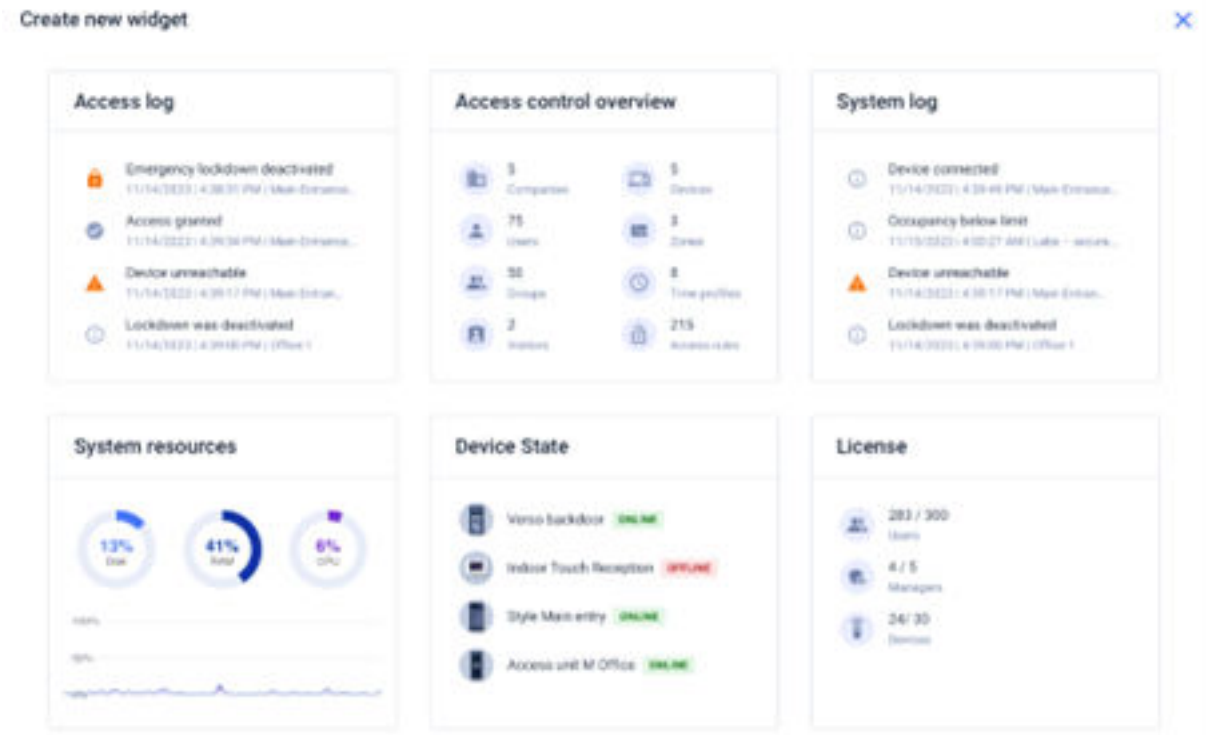
Heslo: **2n**

Po prvním přihlášení je třeba neprodleně změnit heslo.

POZNÁMKA
Zaškrtněte volbu **Neodhlašovat**, pokud se chcete při příštím přihlášení vyhnout opětovnému zadávání přihlašovacích údajů. Přihlášení je platné maximálně 7 dní, poté je nutné se znovu přihlásit.

Pro přihlášení může být vyžadováno Dvoufaktorové ověření (str. 97).

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 vygenerovala.

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 kliknutím na tlačítko Export nad seznamem. V exportovaném CSV souboru je čas uveden v GMT+0.

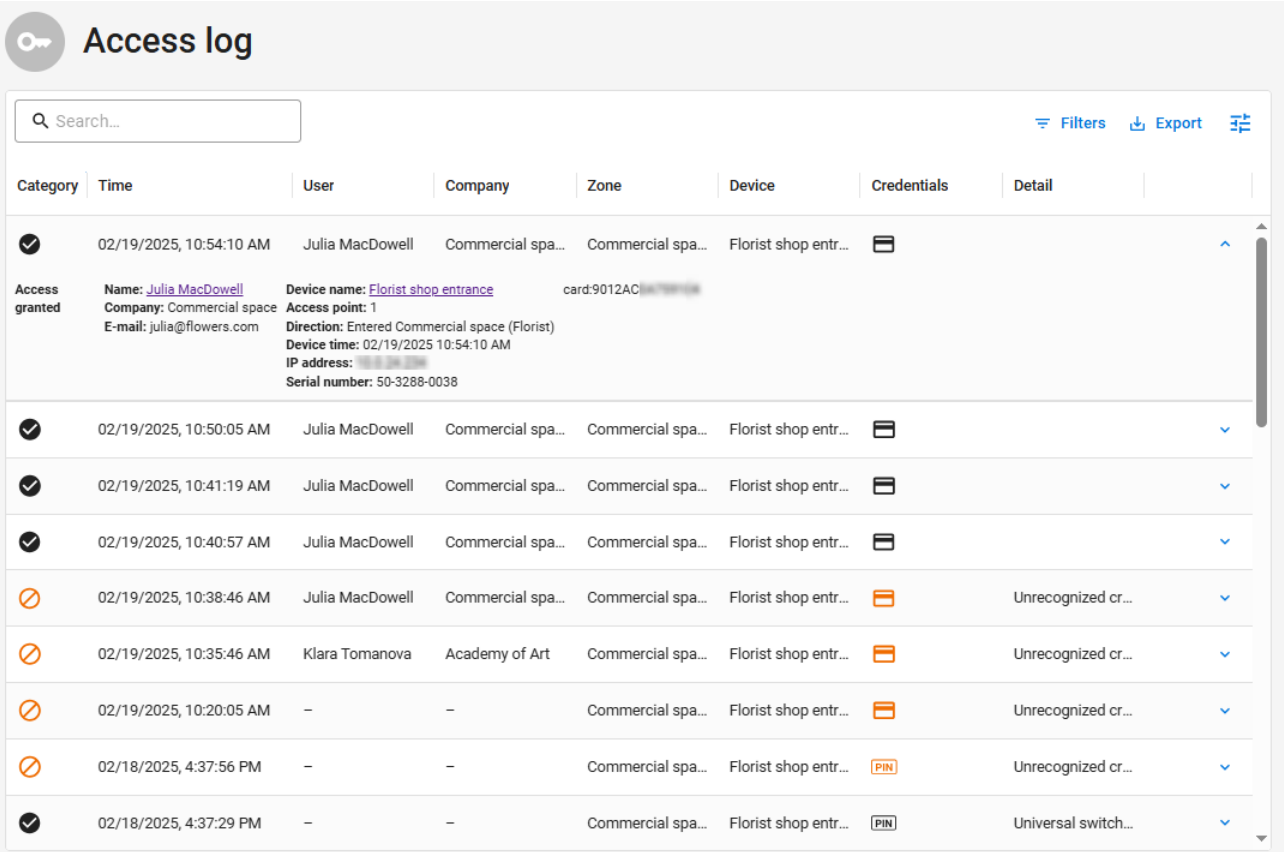
Životnost logů

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**. Uchovávání 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 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**. Uchovávání 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.

Log hovorů

Stránka Log hovorů zaznamenává veškerou aktivitu volání z připojených interkomů a dalších SIP zařízení (např. odpovídacích jednotek nebo výtahových komunikátorů).

POZNÁMKA
Log hovorů je dostupný pouze pro uživatelské oprávnění Administrátor.

V seznamu log hovorů se ke každé události uvádí:

- typ hovoru
- čas, kdy k hovoru došlo
- zda jsou dveře odemčené
- typ zařízení
- protistrana
- délka hovoru
- důvod ukončení hovoru

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 kliknutím na tlačítko Export nad seznamem. V exportovaném CSV souboru je čas uveden v GMT+0.

Životnost logů

Doba uložení daného typu logu se nastavuje na stránce *Nastavení* > *karta Uchovávání záznamů*.

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

VÝSTRAHA
Pro správné fungování všech funkcionalit Logu hovorů je doporučeno používat nejnovější verzi firmwaru na zařízeních. Některé informace a sloupce nemusí být dostupné nebo se nemusí zobrazovat správně na zařízeních se staršími verzemi firmwaru.

- **Délka hovoru:** Sloupec Délka hovoru není podporován na starších verzích firmwaru. Tato informace je dostupná od verze firmwaru 2.49 a vyšší.
- **Identifikace protistrany:** Pro správnou identifikaci Protistrany z adresáře zařízení je vyžadována verze firmwaru 2.50 a vyšší. Na starších verzích se nemusí vyhledávání v adresáři zařízení chovat správně.

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 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. 97).

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**. Uchovávání 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.

V záhlaví detailu společnosti se nachází tlačítko Uzamknout, které aktivuje Nouzové uzamknutí (str. 60) všech zařízení v zónách této 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.

My2N aplikace

Ve společnosti je možné nastavit parametry párování s My2N aplikace, která umožňuje autentizaci pomocí Bluetooth. Nastavují se jak zařízení, na kterých budou moct uživatelé provádět párování, tak čas platnosti mobilního přístupu potřebného ke spárování. Samotný mobilní přístup 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. 76).

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
- My2N aplikace 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.

   Povolením TLS aktivujete Transport Layer Security (TLS) pro vaše FTP spojení. TLS bude šifrovat data přenášená mezi **Access Commanderem** a serverem.
   Povolením Ověřování TLS certifikátů aktivujete ověřování TLS certifikátů poskytnutých serverem. Když je tato možnost povolena, **Access Commander** bude ověřovat, že komunikuje s důvěryhodným serverem, což zvyšuje bezpečnost spojení.
3. Otevře se detail nastaveného LDAP spojení. Nastavení spojení lze otestovat. Pomocí tlačítka Synchronizovat nyní spustíte jednorázovou synchronizaci.
4. Na kartě **Možnosti** můžete spravovat, jak se mají data synchronizovat.

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

TIP
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.

Nastavení synchronizace dat z LDAP

Importované atributy – úpravou schématu se nastavuje přiřazení atributů z LDAP serveru k parametrům **Access Commanderu**.

POZNÁMKA
Atributy telefonních čísel se rozšiřují o filtr, který čísla převede do požadovaného formátu kompatibilního se seznamem uživatelů ve společnosti v **Access Commanderu**. K dispozici jsou dva filtry:

- `toPhoneNumber` – odstraní nepotřebné znaky (mezery, spojovníky atd.) z telefonních čísel.
- `skipExtension` – odstraní linku (extension) z telefonních čísel.

Příklad použití: Pokud zapíšete atribut `{telephoneNumber|toPhoneNumber|skipExtension}`, původní hodnota telefonního čísla v Active Directory „+420 123 456 789 x2222“ se převede na „+420123456789“.

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 deaktivování, tak po smazání uživatelů z LDAP zůstanou jejich data v **Access Commanderu**, ale nebudou se synchronizovat se zařízeními. Deaktivovaní uživatelé nemají přístupová práva, nelze se jim dovolat apod.

Uživatelé zakázaní v Active Directory – nastavuje, co se stane s uživateli, kteří byli v Active Directory zakázáni. Tuto změnu v Active Directory může **Access Commander** ignorovat nebo může uživatele deaktivovat. Deaktivovaní uživatelé nemají přístupová práva, nelze se jim dovolat apod. Po opětovné aktivaci v Active Directory se zakázaní uživatelé opět aktivují i **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. V nastavení schématu je možné povolit synchronizaci uživatelů z 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 synchronizování uživatelů z celého stromu. Při zakázání se prohledávají a synchronizují data pouze z kořenu.

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.

Import uživatelů do společnosti

Rozšířená nabídka ⋮ v záhlaví detailu společnosti umožňuje do společnosti jednorázově importovat nové uživatele, a to buď ze souboru CSV, nebo z jiného zařízení 2N.

Import uživatelů z CSV souboru

TIP
Vzorový CSV soubor pro import uživatelů můžete stáhnout pomocí tohoto odkazu.

Access Commander umožňuje hromadné nahrání uživatelů do společnosti. Základní informace o uživatelích je tedy možné si předpřipravit v externím souboru a poté uživatele jednoduše importovat. Uživatele v jednom souboru je možné nahrát vždy jen do jedné konkrétní společnosti.

Tato funkce neumožňuje uživatele mazat.

POZNÁMKA
Uživatelé s rolí Administrátor mohou provádět komplexní, opakovatelnou synchronizaci seznamu uživatelů napříč společnostmi, viz Synchronizace uživatelů s FTP (str. 88).

Import ze zařízení 2N

Do **Access Commanderu** je možné převést seznam uživatelů ze zařízení 2N. Import lze provést pouze ze zařízení, které doposud nebylo přidané do **Access Commanderu**. Zařízení nemůže obsahovat uživatele, kteří již jsou v **Access Commanderu** (tzn. mají stejné UUID). Všechny uživatele je možné hromadně importovat pouze do jedné konkrétní společnosti.

1. Před importem je vhodné provést zálohu konfigurace. Systém **Access Commanderu** se zálohuje v **Nastavení > karta Záloha systému**. Záloha konfigurace zařízení se provádí v jeho webovém konfiguračním rozhraní, v sekci **Systém > Údržba**.
2. Zařízení, ze kterého chcete importovat seznam uživatelů, přidejte mezi zařízení **Access Commanderu**.

   VÝSTRAHA
   Zařízení zatím nepřidávejte do zón! Zařízení by přejalo přístupové pravidla a seznam uživatelů by se v zařízení přepsal.

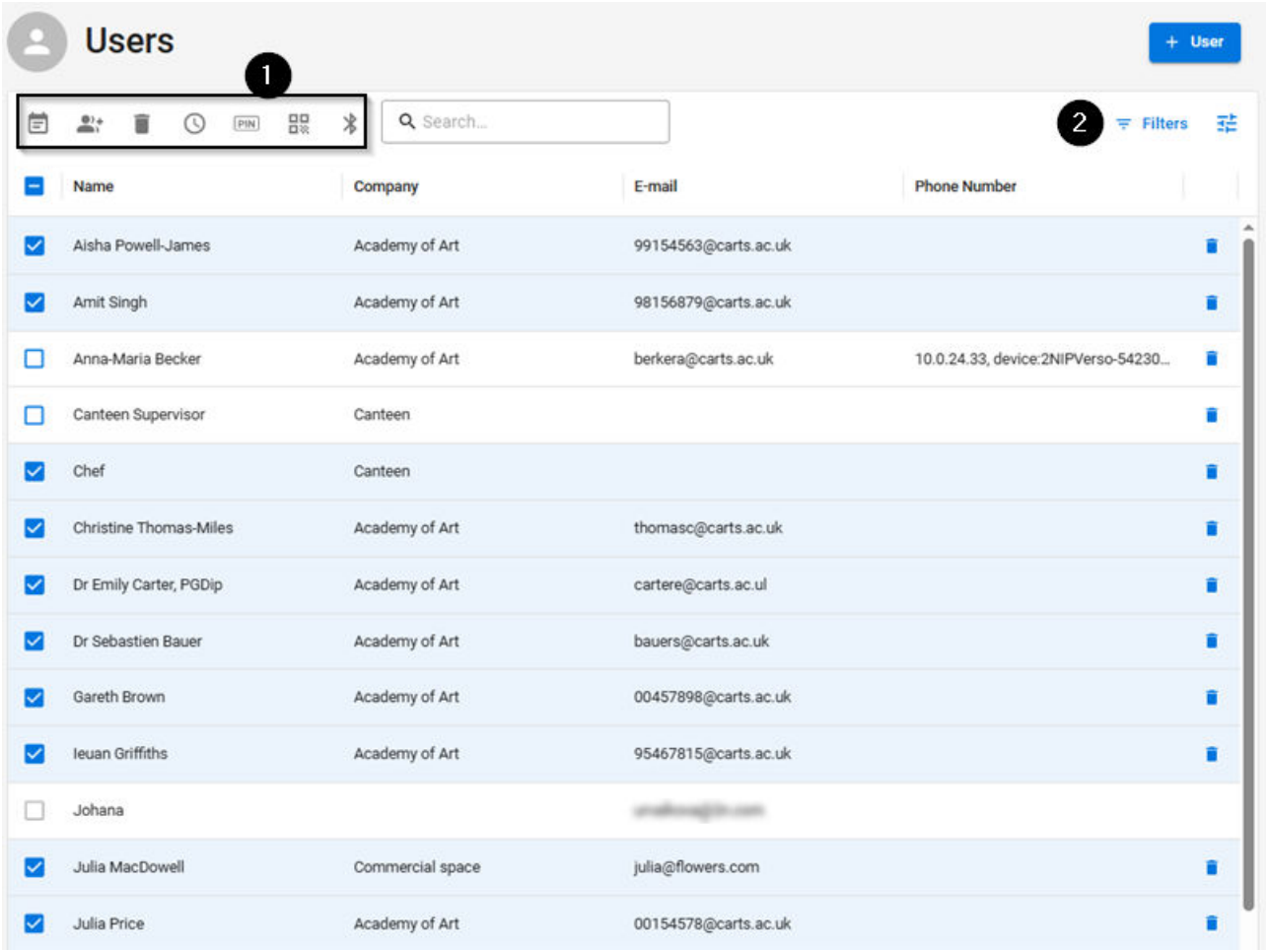
3. Přejděte na detail společnosti, do které chcete uživatele importovat. V rozšířené nabídce ⋮ zvolte Import ze zařízení.
4. Otevře se dialogové okno. Z rozevíracího seznamu dostupných zařízení zvolte zařízení, ze kterého zařízení chcete importovat seznam uživatelů.
5. Kliknutím na Importovat se spustí import na pozadí. Ukončení procesu se zapíše do Systémového logu.
6. Po úspěšném importu je možné zařízení přidat do zón a zahrnout jej do přístupových pravidel.

VÝSTRAHA
Postup importu funguje pouze pro specifické uživatele (UUID) v zařízení a importuje všechny uživatele ze zařízení naráz do jedné společnosti.

Uživatelé

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

V seznamu uživatelů se zobrazují všichni vytvoření uživatelé. Nad seznamem lze uživatele filtrovat (číslo 2 na obrázku) nebo lze 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 (číslo 1 na obrázku):

- 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 přístup těm uživatelům ve výběru, kterým zatím žádný mobilní přístup nebyl přidělen.

POZNÁMKA
Pro přiřazení PIN/QR kódu nebo mobilního přístupu 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.

POZNÁMKA
Access Commander umožňuje hromadné nahrání uživatelů do společnosti. Základní informace o uživatelích je tedy možné si předpřipravit v externím souboru a poté uživatele jednoduše importovat. Uživatele v jednom souboru je možné nahrát vždy jen do jedné konkrétní společnosti.

Hromadný import se provádí v detialu společnoti, viz Import uživatelů do společnosti (str. 43).

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. 52). 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 k USB 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.

Jednu přístupovou RFID kartu je možné používat pro přístup až k 90 dveřím se zámky 2N Fortis, v závislosti na počtu uplatněných časových profilů. Při překročení kapacity paměti karty zápis dat na kartu selže. Událost selhání zápisu se zaznamenává v přístupovém logu systému. Pokud jsou použity Skupiny zámků, může být na jednu kartu zapsáno více dveří než při individuálním přiřazení.

TIP
Správce uživatelů a Administrátor si mohou zobrazit identifikátor karty v Přístupovém logu. Novou/nepřiřazenou kartu je tak možné načíst na přístupném zařízení a poté zkopírovat její identifikátor z logu. Po vložení identifikátoru mezi RFID karty, může uživatel začít kartu používat. Zobrazení identifikátorů v Přístupovém logu je potřeba povolit v **Nastavení > Autentizace**.

POZNÁMKA
Pokud **Access Commander** hlásí, že právě přidaná zcela nová karta je již v systému použita, může být důvodem zapnutý režim kompatibility RFID karet. Tento režim aktivuje Administrátor v **Nastavení > Autentizace > karta Nastavení režimu kompatibility**.

My2N aplikace – slouží k propojení s aplikací My2N aplikace umožňující autentizaci prostřednictvím Bluetooth, viz kapitola Autentizace přes Bluetooth (str. 50).

PIN kód – automaticky vygeneruje 5místný 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. 49).

Poznávací značka – nastavuje poznávací značku vozidla, kterou se uživatel autentizuje.

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. 97). 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. 40). 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. 88))
- **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 ⋮. Nastavení začátku doby platnosti se uplatňuje pouze na přístupy k IP zařízením. Přístup k elektronickým zámkům 2N Fortis je v platný od okamžiku přiřazení přístupové karty uživateli.

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 číslo
Virtuální telefonní číslo lze použít pro volání na uživatele pomocí numerické klávesnice na zařízení. Virtuální čísla nesouvisí s vlastními telefonními čísly uživatele, umožňuje tak skrýt vlastní telefonní čísla uživatelů na zařízení. Virtuální čísla lze například nastavit podle čísel bytů. Virtuální čísla tak lze využít v instalacích, kde je počet tlačítek rychlé volby nedostačující.

Virtuální číslo může mít 1 až 7 míst. První a poslední místo může být buď číslice nebo písmeno, zbytek mohou tvořit pouze číslice (např. A123, 456B, C12E).

Zástupce
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 My2N aplikace, kterou musí mít uživatel staženou ve svém mobilním telefonu.

Tento proces je zabezpečen mechanismem **důvěryhodného párování přes Bluetooth**. Proces párování se liší v závislosti na verzi firmwaru připojeného zařízení.

GET IT ON Google Play Download on the App Store

Spojení aplikace na telefonu uživatele se zařízeními 2N se provádí zadáním párovacího kódu v My2N aplikaci.

Párovací kód lze získat dvěma způsoby:

- propojením s **2N OS** zařízením
- prostřednictvím USB Bluetooth čtečky připojené k počítači

VÝSTRAHA
Pro úspěšné důvěryhodné párování musí mít zařízení firmware verze 2.50 (nebo 3.0) a vyšší. Pokud má zařízení starší firmware, párování bude provedeno pomocí staršího mechanismu pomocí **PINu** bez **QR kódu**.

TIP
Pro vyšší úroveň zabezpečení je vhodné preferovat párování pomocí **QR kódu**. Pokud **QR kód** není dostupný nebo jej zařízení nepodporuje, použijte **PIN**.

Vytvoření párovacího kódu prostřednictvím počítače

1. Stáhněte do počítače aplikaci 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 My2N aplikace.
5. V otevřeném dialogovém okně vyberte Párovat pomocí čtečky.
   V dialogovém okně se objeví párovací kód.
6. Pro párování v aplikaci následujte postup níže (Párování v mobilní aplikaci My2N (str. 51)).

Vytvoření párovacího kódu na zařízení

1. Ujistěte se, že
   - je nastavené párovací zařízení pro společnost daného uživatele, viz Nastavení společnosti (str. 40)
   - je párovací zařízení umístěno v zóně, do které má uživatel platný přístup, viz Přístupová pravidla (str. 69)
   - je nastaven adekvátní čas pro párování, viz Nastavení společnosti (str. 40)
2. V nastavení uživatele v **kartě Autentizace** zvolte autentizaci My2N aplikace.
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 My2N (str. 51)).

Párování v mobilní aplikaci My2N

1. Stáhněte si My2N aplikaci do svého mobilního telefonu. Aplikace je dostupná na App Store a Google Play.
2. Otevřete aplikaci My2N a zadejte párovací PIN.

> **POZNÁMKA**
> Pokud aplikace zobrazí **QR kód**, ale zařízení používá firmware starší než 2.50.0, párování bude úspěšné pouze zadáním **PINu**.

3. Povolte všechna důležitá oprávnění, ať aplikace My2N funguje správně.
4. Postupujte podle instrukcí na mobilním telefonu – přibližte se k zařízení v párovacím režimu a klikněte na Začít párovat. Následně bude mobilní telefon vyhledávat zařízení ke spárování.
5. Udělte přístup zvolenému mobilnímu telefonu. Následně můžete otevírat dveře v celé lokaci.

> **VAROVÁNÍ**
> Pro mobilní telefony se staršími operačními systémy (Android 9 / iOS 17 a nižší) bude třeba k párování využít aplikaci Mobile Key.
>
> #### 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.

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.
- Správa členství uživatelů ve skupinách.
- Vytváření a správa návštěv.
- Vytváření a správa časových profilů.
- Nastavení přístupových pravidel.

Správce uživatelů

- Vytváření a správa uživatelů.
- Vytváření a správa návštěv.
- Správa členství uživatelů 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.

Administrátor společnosti

- Nastavení výchozího jazyka společnosti.
- Sledování systémového logu (omezeno na události dané společnosti).
- Možnost nastavení widgetu pro systémový log a funkci Nouzové uzamknutí na zařízeních, které společnost používá (včetně společných zařízení s jinými společnostmi).

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 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. 73).

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. 74).

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. My2N aplikace
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 „Kdykoli“ 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.

Skupiny zámků

Karta zobrazuje přehled skupiny zámků. V této kartě je možné přidat další skupinu.

U každé skupiny zámků lze zobrazit detaily skupin.

Společnosti

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

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 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 konfiguračního rozhraní daného zařízení.

Stavy zařízení

- Online
- Nespravováno – správa zařízení byla vypnuta uživatelem.
- Nekompatibilní – zařízení nemá podporovanou verzi firmwaru.
- Nenakonfigurováno – je potřeba nahrát konfiguraci elektronických zámků z programu třetí strany.
- 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 IP zařízení

POZNÁMKA
Přidání elektronických zámků 2N Fortis je popsáno v Elektronické zámky (str. 21).

1. Přejděte na stránku **Zařízení**.
2. Klikněte na tlačítko pro přidání zařízení v pravém horním rohu.
3. Pro přidání interkomu 2N, přístupové jednotky 2N nebo odpovídací jednotky 2N zvolte možnost „2N IP zařízení“.
4. 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.
5. 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.

6. Aplikování šablony (volitelné): Pokud chcete na právě přidávané zařízení aplikovat šablonu, aktivujte přepínač **Po přidání zařízení použijte konfigurační šablonu**.
   - Princip výběru a aplikace konfigurace ze šablony je stejný jako při ruční aplikaci šablony na existující zařízení, jak je detailně popsáno v kapitole Šablony zařízení (str. 66).
7. Před vytvořením zařízení pojmenujte.
8. Nově přidaná zařízení se objeví v seznamu. Další nastavení zařízení proveďte v detailu zařízení.

Skupiny zámků

Skupiny zámků umožňují seskupovat jednotlivé zámky do logických celků, které lze následně použít při definici přístupových pravidel, monitoringu nebo správě zařízení.

Zobrazení skupin

Otevřete **Zařízení > Skupiny zámků**.

POZNÁMKA
V seznamu se zobrazují všechny vytvořené skupiny zámků. Pomocí vyhledávacího pole lze filtrovat záznamy podle názvu.

Vytvoření nové skupiny zámků

1. Otevřete **Zařízení > Skupiny zámků**.
2. Klikněte na + Skupina zámků.
3. Zadejte název skupiny a zvolte kartu Vytvořit.
4. V modulu **Zámky** klikněte na Přidat zámky. Vyberte zámky, které mají být součástí skupiny.
5. V modulu **Zóny** klikněte na Přidat zóny. Vyberte zóny, které mají být součástí skupiny.
6. Zvolte ⋮ pro možnost přidání, přejmenování nebo odstranění skupiny zámků.

VAROVÁNÍ
Změna přiřazení zámku do jiné skupiny vyžaduje opakovanou konfiguraci. Před exportem konfiguračního souboru se ujistěte, že jsou dokončeny všechny systémové změny.

Nastavení zámků v Access Commanderu

Před nahráním klíčů do jednotlivých zámků je potřeba spárovat **Access Commander** s aplikací **Fortis Commander**.

Vygenerování hlavního šifrovacího klíče (MEK) a příprava projektu

1. Přihlaste se do systému Access Commander.
2. Přejděte na stránku **Nastavení > Elektronické zámky**.
3. V kartě **Počáteční nastavení** klikněte na Vygenerovat klíče.

4. Vytvořte Hlavní šifrovací klíč.

VÝSTRAHA
Hlavní šifrovací klíč nelze později **zobrazit ani změnit**.

POZNÁMKA
Podle hlavního šifrovacího klíče (MEK) generuje **2N Access Commander** sadu šifrovacích klíčů. Klíč by tak měl být unikátní a dostatečně bezpečný. Sada klíčů vychází z hlavního šifrovacího klíče, proto projekty se stejným hlavním šifrovacím klíčem generují stejné sady klíčů. Při ztrátě projektu je možné vytvořit nový projekt se stejným hlavním šifrovacím klíčem a pokračovat s šifrováním.

5. Po vygenerování klíčů a nastavení hesla k projektovému souboru je možné stáhnout **projektový soubor**, který představuje obraz konfigurace elektronických zámků v systému **Access Commander**.
6. V kartě **Fortis Commander** klikněte na Stáhnout aplikaci, odkud se začne stahovat **Fortis Commander** (aplikace pro konfiguraci elektronických zámků).

VÝSTRAHA
Informace o projektu jsou citlivá data. Chraňte je před zneužitím.

Propsání konfigurace elektronického zámku pomocí Fortis Commander

1. Nainstalujte aplikaci **Fortis Commander** a otevřete ji.
2. Klikněte na Open project a otevřete stažený projektový soubor v Průzkumníku souborů.
3. V zobrazeném dialogu zadejte heslo k projektovému souboru.
4. Po otevření projektového souboru zvolte Connect to device a přiložte servisní kartu k zámku.
5. Klikněte na **Assign**, čímž přiřadíte zámek k projektu.
6. Odpojte zařízení a klikněte na **File > Close project**.
7. Po dokončení konfigurace otevřete systém **Access Commander**. Přejděte do karty **Nastavení > Elektronické zámky** a znovu klikněte na tlačítko Fortis Commander. Nahrajte projektový soubor.

POZNÁMKA
Při přesunu zámku mezi instalacemi nebo při reklamaci je nutné provést **Factory reset**. Tato operace obnoví zámek do továrního nastavení a odstraní veškerou předchozí konfiguraci.

Postup aktualizace konfigurace

1. Proveďte změny v **Access Commanderu**.
2. Stáhněte nový projektový soubor.
3. Nahrajte soubor do **Fortis Commanderu** a proveďte požadované změny na zámcích.
4. Pokud provedete další změny v **Access Commander**u, vždy stáhněte nový projektový soubor.

VÝSTRAHA
Pro každou změnu konfigurace v **Access Commander**u je nutné stáhnout nový projektový soubor – nelze použít starší soubor, který byl již nahrán do **Fortis Commanderu**.

Trvalé zamknutí a odemknutí

Aplikace umožňuje trvalé zamknutí a odemknutí zámku. Funkce slouží pro servisní zásahy nebo nouzové ovládání bez použití karty.

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. 74)), 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.

V kartě je možné změnit IP adresu, na které se zařízení nachází, což umožňuje **Access Commander** nasměrovat k zařízení, které bylo odpojeno a znovu připojeno do sítě na jiné IP adrese.

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. 60).

Zálohování

Tato karta umožňuje zálohu konfigurace interkomu v souboru xml. Záloha se spouští pomocí Spustit zálohu. Když se záloha uloží do lokálního úložiště, bude uložena ve vymezené paměti **Access Commanderu**. Při uložení do souboru se otevře dialogové okno, v němž je možné soubor se zálohou zašifrovat pomocí hesla. Soubor obsahuje citlivé informace, proto je doporučeno soubor chránit. Šifrování zálohy je dostupné u zařízení s firmwarem 2.45 a vyšší.

Každá poslední záloha se zobrazí na kartě. Zařízení je možné automaticky synchronizovat s poslední zálohou pomocí nabídky v Obnovit. V rozbalovacím menu u této nabídky je také možné zvolit obnovení ze zálohy jiného připojeného zařízení nebo z externího souboru.

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

Volání

Karta volání se zobrazí, pokud je na zařízení dostupné a povolené telekomunikační spojení. Karta zobrazuje všechny povolené účty zajišťující spojení a zobrazuje jejich stav. Telekomunikační spojení se nastavuje přímo v konfiguračním rozhraní daného zařízení, v sekci Volání. Do konfiguračního rozhraní se vchází pomocí tlačítka Konfigurace hardwaru v záhlaví detailu zařízení.

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 interkomu 2N nebo k přístupové jednotce 2N lze řídit přístup na jednotlivá patra výtahu v budově. K jednomu interkomu 2N či přístupové jednotce 2N 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 IP interkomy (obj. č. 9137916) nebo pro přístupové jednotky (obj. č. 9160401).

Nastavení ovládání výtahu

1. Před prováděním konfigurace v **Access Commanderu** se ujistěte, že je réléový modul AXIS A9188 propojen se zařízením 2N, které bude zajišťovat autorizaci přístupu do pater. Dále se ujistěte, že je na modulu nastavené HTTPS a je změněno root heslo.
2. 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**.
3. V záhlaví detailu zařízení přejděte do konfigurace hardwaru zařízení. Přejděte do **Integrace > Řízení přístupu > záložka Výtah**. Povolte všechny reléové 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.
4. V detailu zařízení přejděte do záložky Výtah.
5. 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 .
6. 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 IP zařízeních (interkomy, přístupové jednotky, odpovídací jednotky). 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.

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

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.

Získání verzí firmwaru z 2N Update Serveru může trvat několik minut.

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

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

- 3.0
- 2.50
- 2.49
- 2.48
- 2.47
- 2.46
- 2.45

Zabezpečení

Způsob zabezpečení komunikace mezi Access Commanderem a zařízeními se nastavuje v **Zařízení > Zabezpečení > karta Ověření certifikátů zařízení**.

Access Commander umožňuje tři úrovně zabezpečení komunikace se zařízeními:

1. **Šifrovaná komunikace bez ověřování certifikátů** – **Access Commander** využívá pro HTTPS komunikaci tzv. self-signed certifikát. Tento certifikát je z hlediska webových prohlížečů považován za nedůvěryhodný.

2. **Ověřování otisků certifikátů** – komunikace je pojištěna kontrolou certifikátu nahraného na zařízení. Při komunikaci je ověřován otisk tohoto certifikátu.
   Když je zapnuté ověřování otisků, správce zařízení musí při přidání nového zařízení potvrdit platnost otisku certifikátu. Správce zařízení bude vyzván k ověření otisku i v případě, že dojde ke změně certifikátu již přidaného zařízení.
3. **Kompletní ověřování certifikátů** – komunikace je zajištěna certifikátem podepsaným tzv. certifikační autoritou. Při komunikaci je ověřováno celé certifikační řetězení dle požadavků PKI.

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

Jak spravovat certifikáty

Způsob zabezpečení komunikace mezi Access Commanderem a zařízeními se nastavuje v **Zařízení > Zabezpečení > karta Ověření certifikátů zařízení**.

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. Zařízení se přepnou do offline stavu.

Certifikát podepisující autority musí být důvěryhodný na serveru, na kterém běží **Access Commander**.

TIP
Proces nahrání certifikátů na server je popsáno v FAQ.

Pro úspěšné ověření musí být certifikáty zařízení podepsány certifikační autoritou a obsahovat IP adresu nebo doménové jméno zařízení.

Nahrání certifikátu zařízení

1. Vstupte do webového konfiguračního rozhraní daného zařízení.
2. Přejděte do **Systém > Certifikáty > záložka Uživatelské Certifikáty**.
3. Nahrajte připravený certifikát.
4. Přejděte do **Systém > Připojení k síti > záložka Web server**.
5. V parametru **Certifikát HTTPS serveru** vyberte vámi nahraný nahraný certifikát.
6. Uložte změny.

Nastavení přístupových bodů zařízení

Každé zařízení můžete logicky rozdělit na dva přístupové body – příchod a odchod. Každý přístupový bod představuje průchod v jednom směru a určuje, zda uživatel zařízení vstupuje do zóny, nebo ji opouští. Jeden přístupový bod může být ovládán jedním nebo více moduly zařízení. Všechny přiřazené moduly pak spravují průchody ve směru konkrétního přístupového bodu. Přístupové body se využívají zejména v situacích, kdy zařízení leží na hranici dvou zón a je potřeba přesně zaznamenat směr pohybu mezi nimi (například pro funkce typu anti-passback).

Přístupové body dále slouží ke sledování uživatelů v modulu Přítomnost (str. 79). Přístupové body se také využívají pro sledování vstupu a výstupu v Omezení oblastí (str. 81).

POZNÁMKA
Ve webovém konfiguračním rozhraní jednotlivých zařízení se přístupové body označují jako **Příchod** a **Odchod**. Jejich nastavení provedete v **Přístupy > Přístupová pravidla > záložky Přístup a Odchod**.

Povolení přístupových bodů v Access Commanderu

1. Přejděte na stránku Zóny v **Access Commanderu**.
2. V pravém horním rohu stiskněte a povolte použití přístupových bodů.

Rozřazení modulů pro příchod nebo odchod

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 **Přístup > Přístupová pravidla**.
3. Na záložce **Příchod** nebo **Odchod** v kartě **Moduly** klikněte na tlačítko Správa.
4. Otevře se dialogové okno s přehledem dostupných modulů spravujících přístup.
5. Přetáhněte dané moduly do skupin podle směru, který mají zajišťovat.

TIP
Kliknutím na můžete konkrétní modul lokalizovat. Modul spustí vizuální nebo akustickou signalizaci v závislosti na svých možnostech.

Šablony zařízení

Funkce Šablony zařízení umožňuje konfiguraci více zařízení. Šablony zjednodušují počáteční instalaci systému a sjednocují nastavení napříč projekty.

Šablony fungují na principu vzoru. Šablony umožňují uložit celou konfiguraci jakéhokoliv zařízení s **2N OS** nebo jen vybrané části konfigurace a následně ji aplikovat na další zařízení. Konfigurace může vycházet z již nakonfigurovaného zařízení, ze zálohy zařízení nebo z dříve exportované šablony.

Při vytváření šablony lze zvolit, které části konfigurace budou zahrnuty. Jednotlivé části se liší podle typu zařízení (např. nastavení relé, audio výstupy, automatizace). Tento výběr je součástí procesu vytváření šablony a po jejím uložení už jej nelze změnit.

POZNÁMKA
Použitím šablon lze výrazně zkrátit dobu potřebnou pro prvotní zprovoznění zařízení.

Vytvoření a správa šablon

Pro přístup k funkci šablon přejděte do sekce Zařízení > Šablony.

1. Klikněte na + Vytvořit šablonu ze zařízení.
2. Otevře se dialog **Vytvořit šablonu**.
3. V rozbalovacím menu **Zařízení*** vyberte existující zařízení, které bude sloužit jako základní zařízení pro vaši šablonu. Zobrazena budou pouze zařízení kompatibilní s šablonami.
4. Klikněte na Další a pokračujte v konfiguraci šablony.

VÝSTRAHA
U některých konfigurací se mohou zobrazit upozornění. Ty informují o tom, že vybrané konfigurace mohou mít omezení nebo potenciální rizika. Výběr je i přesto umožněn, ale doporučuje se upozornění zkontrolovat.

Import šablony nebo zálohy ze souboru

Máte-li již vytvořenou šablonu nebo zálohu zařízení uloženou v souboru, můžete ji snadno importovat:

1. Přejděte do sekce Zařízení > Šablony.
2. Klikněte na Import ze souboru vpravo nahoře.
3. Vyberte soubor se šablonou nebo zálohou z vašeho počítače a klikněte na Importovat.

POZNÁMKA
Při importu se některé sekce mohou zobrazit jako deaktivované. Jedná se o části konfigurace, které by mohly způsobit nechtěné změny nebo narušit funkci zařízení. Tyto sekce se při importu automaticky odstraňují a uživatel je může krátce vidět při načítání.

Úprava šablony

Šablona může být po vytvoření dále upravena. V rozhraní se zobrazují pouze ty části konfigurace, které byly zahrnuty při vytváření šablony.

1. Přejděte do Zařízení > Šablony.
2. Vyberte šablonu v seznamu.
3. Klikněte na tlačítko Úprava šablony.

Zobrazí se dialog s jednotlivými sekcemi konfigurace.

Úprava hodnot

- Hodnota se upravuje dvojklikem.
- Upravená položka je ihned označená jako změněná.
- Varovná ikona označuje hodnoty, které nemusí projít plnou validací na zařízení.

VÝSTRAHA
Validace prováděná při úpravě šablony je pouze orientační, a provádí se **na úrovni jednotlivých položek**. Kontrola nezachycuje všechny konflikty napříč zařízeními a verzemi firmwaru a neodpovídá plné validaci, která probíhá na **2N OS**.

Položka označená varováním může být na zařízení přesto použitelná a naopak položka bez varování může být při aplikaci odmítnuta. Skutečné vyhodnocení probíhá až na zařízení.

Aplikování šablony na zařízení

Šablonu lze aplikovat na jedno nebo více zařízení. Lze ji také aplikovat pomocí hromadných akcí v seznamu zařízení nebo přímo z detailu zařízení.

1. Přejděte do sekce Zařízení > Šablony.
2. Vyberte šablonu, kterou chcete na zařízení aplikovat.
3. Klikněte na Použít na zařízení.
4. Vyberte zařízení a potvrďte.
5. Zobrazí se přehled konfigurace. Tyto části odpovídají výběru provedenému při vytváření šablony, ale lze je upravit.
6. Klikněte na Použít.

VÝSTRAHA

Pokud se při aplikaci šablony zjistí nesoulad mezi verzí firmwaru nebo typem zařízení, pro které byla šablona vytvořena, a verzí či typem cílového zařízení, zobrazí se upozornění. Nesoulad je nutné před pokračováním potvrdit.

POZNÁMKA

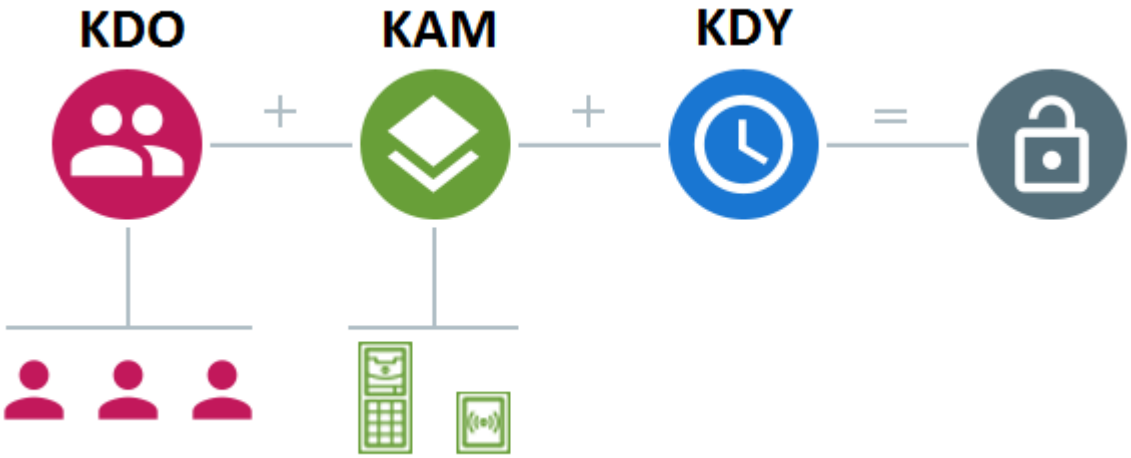
- Stav potvrzuje pouze úspěšné zahájení procesu. Neinformuje o skutečném průběhu nebo dokončení aplikace.
- Návod na použití šablony při přidání zařízení naleznete zde Přidání nového zařízení (str. 57).

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.

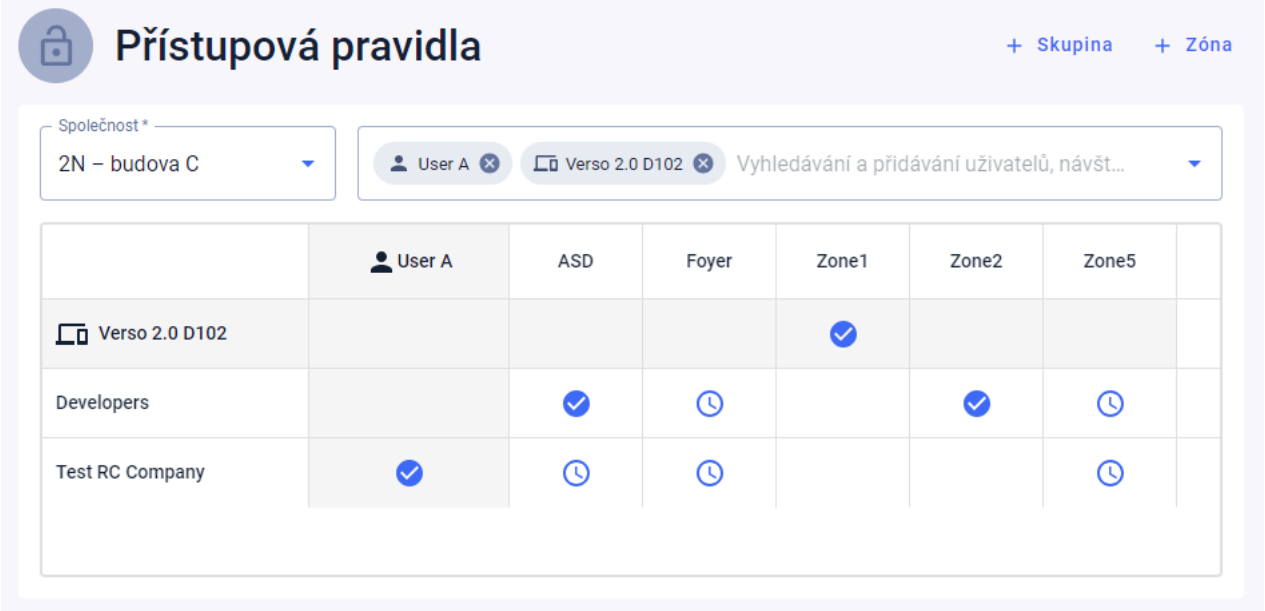
Maticové zobrazení

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. 71). 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.

Časové profily na elektronických zámcích

Elektronické zámky podporují časové profily s následujícími omezeními:

- Svátky se neuplatňují.
- V rámci jednoho dne lze nastavit až 4 různé časové intervaly.
- V rámci jednoho časového profilu lze definovat 4 denní rozvrhy intervalů.

TIP
To znamená, že lze mít například jiná nastavení pro pondělí, úterý, středu a čtvrtek, ale pro pátek, sobotu a neděli už musíte použít jedno z existujících nastavení.

VÝSTRAHA
Pokud časový profil poruší uvedená omezení, bude přístupové pravidlo ignorováno a uživateli nebude udělen přístup.

Vytvoření časového profilu

1. Přejděte na **Časové profily**.
2. Klikněte na tlačítko + Časový profil v pravém horním rohu.
3. V otevřeném dialogovém okně nastavte jméno časového profilu.

4. Pro volbu časového omezení vyberte možnost Přidat časové úseky. Modře zvýrazněné dny identifikují dny spadající do časového profilu. Výběr dne se provádí kliknutím. V rámci dnů je možné nastavit časový interval určující platnost časového profilu.

> **POZNÁMKA**
> V rámci dní je možné nastavit časový interval určující platnost časového profilu.

> **VÝSTRAHA**
> Rozdílné doby pro každý den je možné nastavit, až když je časový profil vytvořen.

5. 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.

> **POZNÁMKA**
> Globální profily mohou ovlivnit přístup napříč všemi společnostmi. Může je upravovat pouze administrátor.
>
> Správce přístupu může opravovat pouze časové profily své společnosti.

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. 73).

VÝSTRAHA
Pro 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. 45).

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

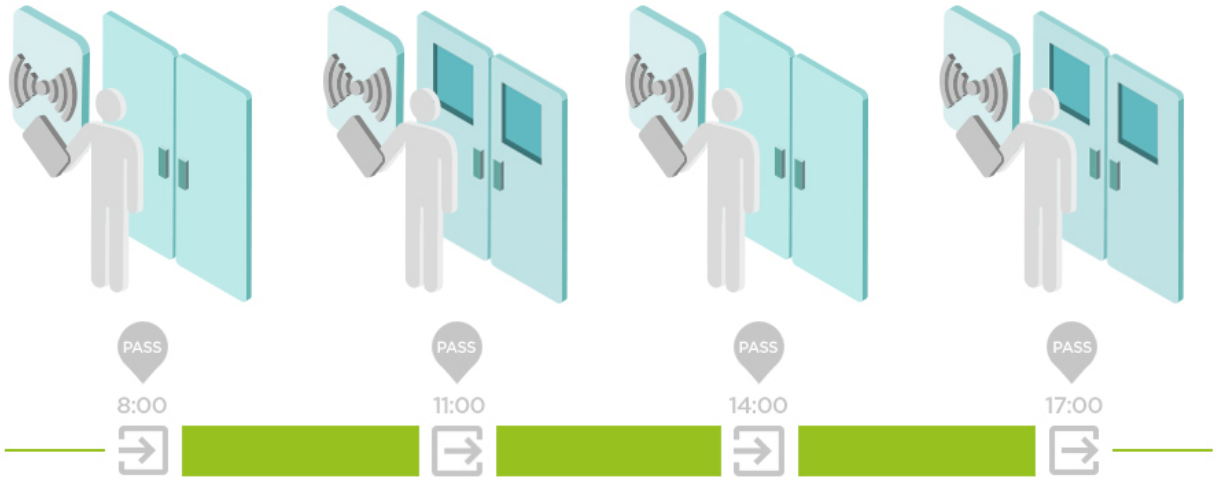
Správce docházky může data o docházce uživatelů upravovat. Úprava se provádí kliknutím na časový interval, který má být změněn. Po otevření lze upravit hraniční časy a přidat k intervalu poznámku.

Nastavení docházky

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

Režimy docházky

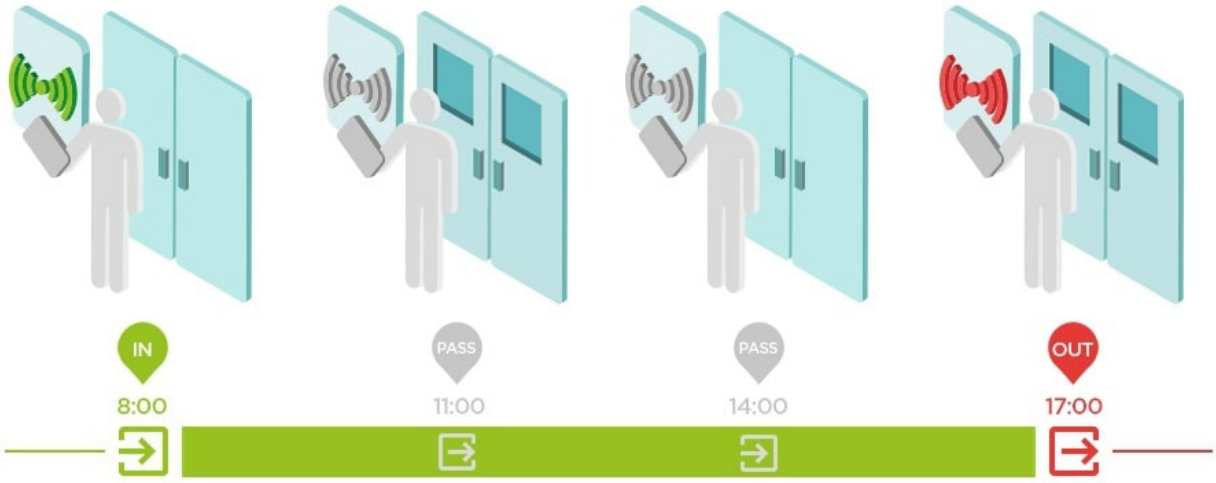
- **FREE**



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 zařízení pro vstup a výstup z oblasti.



- **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

Každé zařízení můžete logicky rozdělit na dva přístupové body – příchod a odchod. Každý přístupový bod představuje průchod v jednom směru a určuje, zda uživatel zařízení vstupuje do zóny, nebo ji opouští. Jeden přístupový bod může být ovládán jedním nebo více moduly zařízení. Všechny přiřazené moduly pak spravují průchody ve směru konkrétního přístupového bodu. Přístupové body se využívají zejména v situacích, kdy zařízení leží na hranici dvou zón a je potřeba přesně zaznamenat směr pohybu mezi nimi (například pro funkce typu anti-passback).

Přístupové body dále slouží ke sledování uživatelů v modulu Přítomnost (str. 79). Přístupové body se také využívají pro sledování vstupu a výstupu v Omezení oblastí (str. 81).

POZNÁMKA
Ve webovém konfiguračním rozhraní jednotlivých zařízení se přístupové body označují jako **Příchod** a **Odchod**. Jejich nastavení provedete v **Přístupy > Přístupová pravidla > záložky Přístup a Odchod**.

Povolení přístupových bodů v Access Commanderu

1. Přejděte na stránku Zóny v **Access Commanderu**.
2. V pravém horním rohu stiskněte a povolte použití přístupových bodů.

Rozřazení modulů pro příchod nebo odchod

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 **Přístup > Přístupová pravidla**.
3. Na záložce **Příchod** nebo **Odchod** v kartě **Moduly** klikněte na tlačítko Správa.
4. Otevře se dialogové okno s přehledem dostupných modulů spravujících přístup.
5. Přetáhněte dané moduly do skupin podle směru, který mají zajišťovat.

TIP
Kliknutím na můžete konkrétní modul lokalizovat. Modul spustí vizuální nebo akustickou signalizaci v závislosti na svých možnostech.

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 90 dní.

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. 76).

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. 77).

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 návštěvy. 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.

POZNÁMKA
Pokud **Access Commander** hlásí, že právě přidaná zcela nová karta je již v systému použita, může být důvodem zapnutý režim kompatibility RFID karet. Tento režim aktivuje Administrátor v **Nastavení > Autentizace > karta Nastavení režimu kompatibility**.

Správa zabezpečené karty pomocí USB čtečky

Pomocí USB čtečky lze provádět diagnostiku a správu zabezpečené karty ve vyhledávacím poli v záhlaví.

TIP
Před použitím USB čtečky je nutné ji povolit v systému **Access Commander**. Více informací najdete v kapitole Povolené USB čtečky (str. 103).

1. Připojte USB čtečku k počítači.
2. Klikněte na ikonu ve vyhledávacím poli v záhlaví.
3. Přiložte ke čtečce.

Dostupné operace

- Načtení dat z karty
- Vyhledávání uživatele podle karty
- Zobrazení událostí uložených na kartě
- Aktualizace přístupových údajů
- Smazání nebo formátování aplikace
- Prodloužení platnosti servisní karty

Přítomnost

Modul **Přítomnost** umožňuje sledovat aktivitu uživatelů v reálném čase. Funguje nezávisle na modulu **Docházka**, který je samostatně licencován. Přítomnost lze monitorovat i bez aktivní licence Docházky.

Obě funkce jsou zobrazeny společně na kartě **Docházka a přítomnost** v rozhraní Access Commander, ale každá z nich má vlastní účel a funguje samostatně.

Pro funkci modulu je potřeba nastavit režim docházky IN-OUT v **Nastavení > Konfigurace > karta Docházka**, viz Nastavení docházky (str. 73).

- 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 uživatele 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.

- **My2N aplikace** – Paired and unpaired users with pairing time remaining
  V reportu jsou vypsána data o stavu párování uživatelů přes aplikaci My2N aplikace, 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. 88).

  VÝSTRAHA
  Soubor obsahuje citlivá data!

Omezení oblastí

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

POZNÁMKA
Modul Omezení oblastí a modul Přítomnost (včetně Docházky) jsou na sobě nezávislé. Pro moduly Docházka a Přítomnost nelze použít funkce obsazenost a anti-passback. Obsazenost a anti-passback fungují pouze v modelu Omezení oblastí.

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. 74). Vlastnosti přístupového bodu se rozbalí kliknutím na šipku.

Obsazenost

Pro správnou funkci je nutné nastavit zařízení pro vstup a výstup z oblasti.

Karta obsazenosti poskytuje přehled o počtu osob v dané oblasti a umožňuje nastavit limity obsazenosti. Pokud je limit obsazenosti dosažen, je možné buď odepřít další vstupy nebo tyto vstupy pouze zaznamenat do systémového logu. Funkce obsazenost nesleduje, jaké osoby jsou v oblasti. Pro sledování přítomnosti jednotlivých osob je určen samostatný modul Přítomnost.

VÝSTRAHA
Při opakované autorizaci jednoho uživatele se každá autorizace počítá jako jeden vstup. To znamená, že pokud se jeden uživatel zaznamená na příchodovém zařízení třikrát za sebou, bude to vyhodnoceno jako tři osoby v oblasti. Pokud tedy fyzická instalace zařízení umožňuje opakované načtení karty jednoho uživatele, je vhodné funkci obsazenost kombinovat s funkcí anti-passback.

Anti-passback

Pro správnou funkci je nutné nastavit zařízení pro vstup a výstup z oblasti.

Na oblasti je možné aktivovat funkci anti-passback, která zajišťuje rozšíření kontroly přístupů o monitoring a zamezení neužití 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, které má připojené aktivní tlačítko REX umožňující 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.

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.

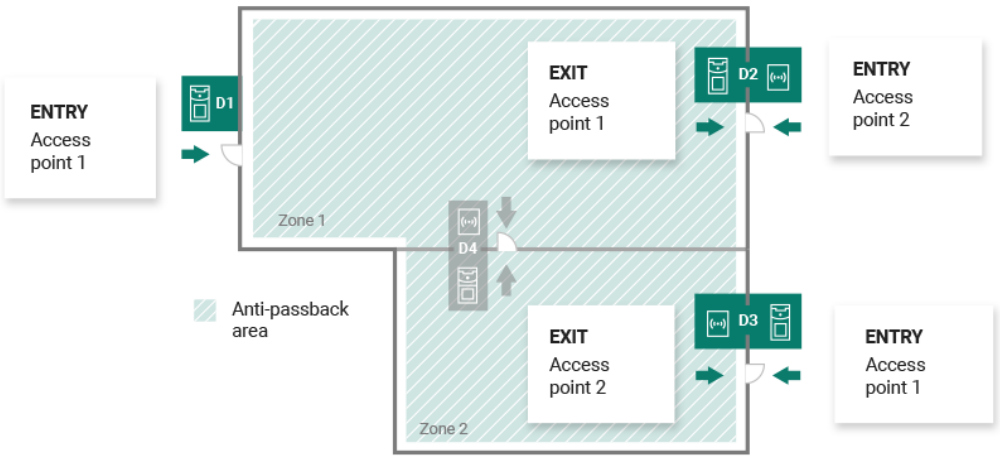
Nejčastější chyby nastavení

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.

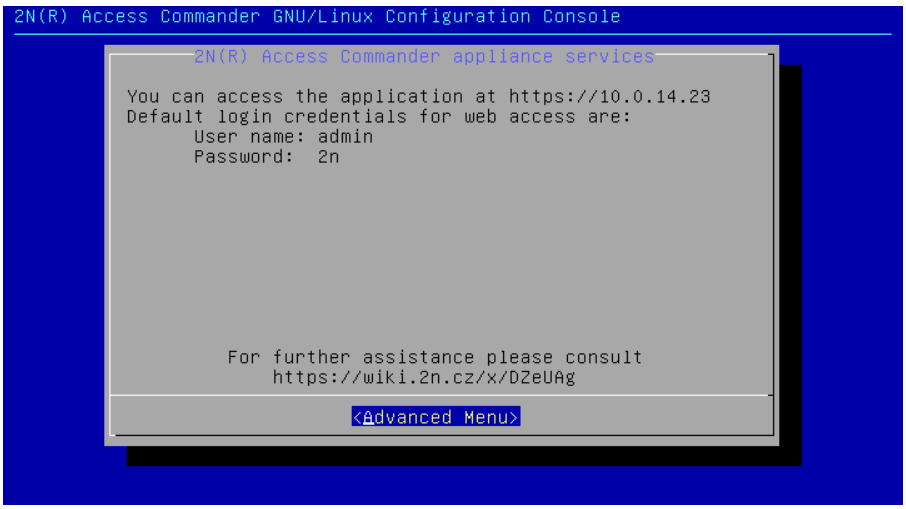
Nastavení systému

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.

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. 87). 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.

Požadované domény pro aktualizaci systému

VÝSTRAHA
Připojení 2N Access Commanderu k níže uvedeným serverům je zásadní pro úspěšnou aktualizaci systému. Bez povoleného přístupu k těmto doménám proces aktualizace selže a systém se nepodaří aktualizovat.

Tento přístup je kriticky důležitý pro stahování nejnovějších verzí aplikace, systémových balíčků, bezpečnostních záplat a dalších komponent, které udržují systém v optimálním a zabezpečeném stavu.

- .2n.cz
- .2n.com
- .deb.nodesource.com
- .packages.microsoft.com
- .security.debian.org
- .apt.postgresql.org
- .httpredir.debian.org

Downgrade

Návrat k předchozí verzi firmwaru není možný.

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.
5. 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.
5. 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 (v rozšířené nabídce).

TIP
Seznam s aktuálními uživateli, který odpovídá struktuře vzorového CSV souboru, je možné stáhnout na stránce Reporty (str. 80).

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. Přejděte do **Nastavení > karta Synchronizace uživatelů**.
2. Klikněte na v parametru Úložiště.
3. V otevřeném dialogovém okně nastavte adresu FTP serveru, na kterém je CSV soubor uložen.
4. Povolením TLS aktivujete Transport Layer Security (TLS) pro vaše FTP spojení. TLS bude šifrovat data přenášená mezi **Access Commanderem** a serverem.
   Povolením Ověřování TLS certifikátů aktivujete ověřování TLS certifikátů poskytnutých serverem. Když je tato možnost povolena, **Access Commander** bude ověřovat, že komunikuje s důvěryhodným serverem, což zvyšuje bezpečnost spojení.

   VÝSTRAHA
   Proxy pro FTP s TLS ověřením není podporováno.
5. Zadejte přihlašovací údaje pro přístup k FTP serveru.

CSV soubor

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.

Datum a čas

Změna způsobu získávání času se provádí v **Nastavení > Konfigurace > karta Datum a Čas**.

Datum a čas v **Access Commanderu** lze synchronizovat s internetem nebo je nastavit manuálně. 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**.

  TIP
  Čas z NTP serveru zajišťuje nejlepší přesnost času na zařízení.

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

Automatizace

Funkce Automatizace je v programu **2N Access Commander** dostupná od verze firmwaru 3.2 a je podmíněna licencemi Advanced, Pro nebo Unlimited. Funkce je postavena na platformě Node-RED a nabízí rozsáhlé možnosti programování na základě sestavování toků v programu **Access Commander**. Funkce umožňuje

uživatelům propojit **Access Commander** se systémy třetích stran a automatizovat vlastní pracovní postupy na základě událostí v rámci platformy.

VÝSTRAHA
Pro plné využití tohoto všestranného automatizačního nástroje je nutné zohlednit následující:

- **Odpovědnost zákazníka za bezpečnost**: Uživatelé jsou odpovědní za to, že jejich konfigurace a pracovní postupy automatizace jsou bezpečné a že jsou v souladu s osvědčenými postupy kybernetické bezpečnosti. Rozsah odpovědnosti zahrnuje zabezpečení prostředí Node-RED, vhodnou správu oprávnění a ochranu citlivých dat, se kterými automatizace pracují.
- **Použití uzlu REST API**: Při nesprávném použití uzlu REST API hrozí ztráta dat nebo jejich nežádaná změna. Uživatel je odpovědný za správnou konfiguraci a implementaci tohoto uzlu. Je třeba postupovat opatrně a pečlivě zkontrolovat nastavení, aby se předešlo rizikům spojeným s daty.
- **Uzly a doplňky třetích stran**: 2N Telekomunikace a.s. neodpovídá za použití a integraci uzlů nebo doplňků třetích stran nebo za vlastní úpravy systému Node-RED v rámci funkce Automatizace. Zákazníci by měli pečlivě vyhodnotit a zajistit bezpečnost a stabilitu všech dalších komponent, které se rozhodnou nainstalovat. Jakékoli problémy vyplývající z rozšíření třetích stran bude muset řešit zákazník nebo příslušný poskytovatel třetích stran.
- **Limity technické podpory**: Tým technické podpory pomůže s problémy souvisejícími se základními funkcemi Automatizace v programu 2N Access Commander a funkcí uzlů Access Commanderu, ale není schopen poskytnout pomoc s návrhem, vývojem nebo laděním vlastních toků v Node-RED. Uživatelé, kteří chtějí vytvářet složité automatizace, jsou odkázáni na podporu u kvalifikovaných odborníků na Node-RED nebo mohou využít veřejně dostupné zdroje.

Před začátkem práce s Node-RED je doporučeno seznámit se s dostupnými online zdroji, jako jsou podrobné příručky Node-RED a četné výukové programy na YouTube. Tyto materiály poskytují návod na vytváření, správu toků apod.

Následující manuál se zaměřuje na základní principy tvoření automatizovaných úloh, na popis uzlů vytvořených speciálně pro **Access Commander** a na popis příkladů použí automatizací s **Access Commanderem**.

Funkce Automatizace rozšiřuje možnosti programu **Access Commander**. Při prozkoumávání jejích možností je ovšem třeba dbát na bezpečnost nastavení s ní spojených.

Vytváření automatizací

Automatizované úlohy se vytváří v externím editoru. Do editoru se vstupuje z karty na stránce **Nastavení > Konfigurace > karta Automatizace**. Změny provedené v editoru se projeví až po jejich nasazení na server, které se provede tlačítkem Deploy v pravém horním rohu editoru.

Vytváření automatizovaných úloh je založeno na sestavování toků (flows). Toky se sesavují z jednotlivých, na sebe navázaných uzlů (nodes). Nabídka uzlů se zobrazuje v levém panelu. V levém panelu je možné uzly vyhledávat podle jejich názvu. Nový uzel je možné také přidat po vytvoření nového spoje z již existujícího uzlu.

Data, které se mezi uzly předávají, se označují jako messages (zprávy). Jejich popis a práce s nimi jsou podrobně rozepsány zde. Na této stánce jsou popsány i základní uzly (nodes), které zpracovávájí formát jednotlivých messages nebo jejich sekvencí jako jsou uzly Change, Split, Join,... Automatizace mohou pracovat nejen s daty získanými v tomto unikátním úkolu (msg.), ale mohou pracovat také s dynamickými hodnotami v kontextu celé historie toku (flow.) nebo dokonce všech toků v instalaci (global.).

VÝSTRAHA
Tlačítko Deploy odešle nastavené toky na server. Teprve odesláním na server se spustí účinnost nových toků!

Bezpečný režim (safe mode)

Bezpečnostní režim (Safe Mode) je klíčovým nástrojem pro řešení problémů automatizací. Spuštění editoru v bezpečném režimu umožňuje provádět změny na tocích, aniž by tyto toky běžely na pozadí. To znamená, že můžete přejít do editoru, upravit co je třeba a poté změny opět nasadit pomocí tlačítka Deploy. Tento režim je obzvláště užitečný, pokud některý z toků způsobuje, že Node-RED nefunguje správně nebo selhává, například kvůli chybě v toku nebo v uzlu třetí strany, nebo je nutné tok okamžitě zastavit.

Uzly (nodes) Access Commander

REST API

Uzel REST API odesílá definovaný HTTP API požadavek. Vstupní data obsažená ve vlastnosti **body** jsou použita jako request body tohoto použadavku. Výstupem z uzlu jsou data z odpovědi na požadavek. Výběr a řazení výstupních dat je možné upřesnit v parametru **Query**.

Parametry uzlu

- **Method** – nabízí výběr z metod API požadavků
- **Endpoint** – slouží k zadání celé endpointu, na který bude požadavek směřován. Cesta endpointu může být dokončena parametrem body.
  Práce s HTTP požadavky je popsána v HTTP API (str. 112).
- **Query** – slouží k upřesnění, které parametry dat mají být v endpointu adresovány a jak mají být vráceny ve výstupu. Tento parametr může být zadán vstupní hodnotou, vlastností **query**. Popis sestavování **query** je popsán v dokumentu Data Query Customization (pouze v angličtině).
- **Only send non-2xx responses to Catch node** – tato možnost ovlivňuje, jaký druh HTTP odpovědí bude zachytáván v Catch uzlu.
- **Name** – umožňuje přejmenovat uzel pro lepší orientaci při práci s tokem.

Access log

Uzel načítá záznamy v Přístupovém logu a umožňuje tyto záznamy dále zpracovávat.

Administrátor může nastavit automatizované úlohy, které se spustí, jakmile **Access Commader** zaznamená definovaný záznam v logu. Definování akce se provádi v nastavení uzlu. Výstupem jsou konkrétní data o zaznamenané události. Na pozadí této funkce běží funkce založená na SignalR.

Parametry uzlu

- **Filter** – slouží k upřesnění, které záznamy má uzel zpracovávat. Záznamy neodpovídající tomuto filtru budou tokem ignorovány. Formát filtru je JSON object. Tento parametr může být přepsán vstupní hodnotou.
- **Name** – umožňuje přejmenovat uzel pro lepší orientaci při práci s tokem.

System Log

Uzel načítá záznamy v Systémovém logu a umožňuje tyto záznamy dále zpracovávat.

Administrátor může nastavit automatizované úlohy, které se spustí, jakmile **Access Commader** zaznamená definovaný záznam v logu. Definování akce se provádi v nastavení uzlu. Výstupem jsou konkrétní data o zaznamenané události. Na pozadí této funkce běží funkce založená na SignalR.

Parametry uzlu

- **Filter** – slouží k upřesnění, které záznamy má uzel zpracovávat. Záznamy neodpovídající tomuto filtru budou tokem ignorovány. Formát filtru je JSON object. Tento parametr může být přepsán vstupní hodnotou.
- **Name** – umožňuje přejmenovat uzel pro lepší orientaci při práci s tokem.

SignalR

Uzel SignalR čte data v odebíraném topicu. Uzel získává data v reálném čase, proto je vhodný pro scénáře, kdy má automatizovaný úkol získávat informace z Access Commanderu bez nutnosti neustálého dotazování.

Parametry uzlu

- **Topic** – nabízí dostupné topicy k odběru.
- **Filter** – slouží k upřesnění, které záznamy má uzel zpracovávat. Záznamy neodpovídající tomuto filtru budou tokem ignorovány. Formát filtru je JSON object. Tento parametr může být přepsán vstupní hodnotou.
- **Name** – umožňuje přejmenovat uzel pro lepší orientaci při práci s tokem.

Další informace o funkcionalitě SignalR jsou uvedené v kapitole SignalR (str. 112).

Dynamic SignalR

Uzel Dynamic SignalR proti uzlu SignalR umožňuje dynamické změny v odběru dat. To může zahrnovat změnu topicu nebo způsobu odběru na základně vstupních hodnot. Výstupní hodnoty uzlu jsou jednak získávaná data z topiců (Data), jednak informace o úspěšném nebo neúspěšném provedení akce tohoto uzlu.

Parametry uzlu

- **Topic** – definuje topic, u kterého má proběhnout změna získávání dat.
- **Filter** – slouží k upřesnění, které záznamy má uzel zpracovávat. Záznamy neodpovídající tomuto filtru budou tokem ignorovány. Formát filtru je JSON object. Tento parametr může být přepsán vstupní hodnotou.
- **Records** – definuje počet záznamů, které se načtou při použití typu čtení fetch.
- **Fetch When Ready** – nastavuje, zda se mají hodnoty načíst zpětně, když je aktivován příkaz fetch.
- **Name** – umožňuje přejmenovat uzel pro lepší orientaci při práci s tokem.

Platné vstupní hodnoty

Uzel akceptuje jako vstupní hodnoty následující vlastnosti. Platné vstupní hodnoty dočasně přepíší parametry nastavené v konfiguraci uzlu.

- **topic** – řetězec určující odebíraný topic.
- **filter** – řetězen ve formátu JSON, který upřesňuje získávané záznamy.
- **fetchWhenReady** – bootlean určující parametr uzlu Fetch When Ready.
- **action** – řetězec určující akce, která se má provést. Může to být přihlášení k subscribe, unsubscribe....
- **update** – může obsahovat timestamp (řetězec) a timeWindow (object) označující, kdy proběhlo ke změně akce, která se má provádět.

Další informace o funkcionalitě SignalR jsou uvedené v kapitole SignalR (str. 112).

Write system log

Uzel Write system log vytváří záznam v systémovém logu Access Commanderu. Záznam protokolu obsahuje zadanou závažnost, popis události a další podrobnosti. Pokud během procesu dojde k chybě, je zaznamenána a stav uzlu je odpovídajícím způsobem aktualizován. Uzel nemá výstupní hodnoty.

Parametry uzlu

- **Severity** – určuje závažnost záznamu. Tento parametr může být zadán vstupní hodnotou query.
- **Filter** – slouží k upřesnění, které záznamy má uzel zpracovávat. Záznamy neodpovídající tomuto filtru budou tokem ignorovány. Formát filtru je JSON object. Tento parametr může být přepsán vstupní hodnotou.

- **Detail** – slouží k podrobnějšímu popisu záznamu, který se zobrazí v systémovém logu. Tento parametr může být přepsán vstupní hodnotou.
- **Name** – umožňuje přejmenovat uzel pro lepší orientaci při práci s tokem.

Platné vstupní hodnoty

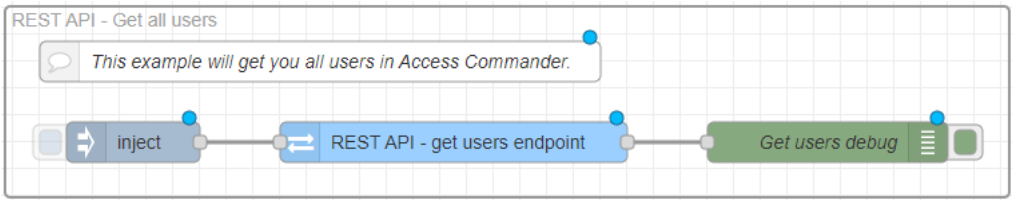
Uzel akceptuje jako vstupní hodnoty následující vlastnosti. Platné vstupní hodnoty dočasně přepíší parametry nastavené v konfiguraci uzlu.

- **severity** – řetězec určující závažnost záznamu.
- **event** – řetězec stručně popisující zaznamenanou akci.
- **detail** – řetezec, který vyplňuje podrobný popisu záznamu, který se zobrazí v systémovém logu.

Příklady toků (flows)

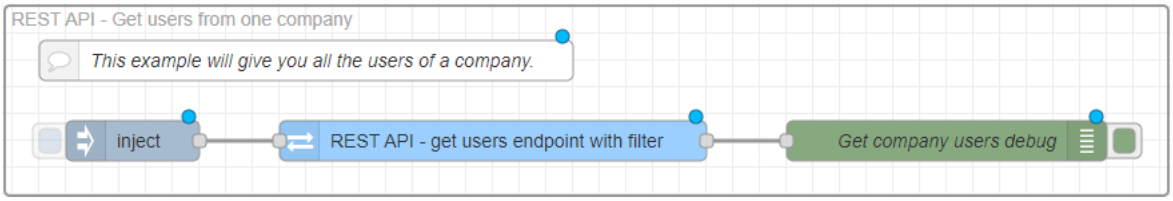
Access Commander nabízí několik základních automatizovaných úloh představujících možnosti použití automatizací. Toky (flows) těchto úloh mohou být nainstalovány při prvním spuštění funkce Automatizace v **Access Commanderu**, ale je možné je importovat i později, viz Export/Import toků (str. 96). Tyto předpřipravené toky lze jednoduše upravit pro vlastní účely.

Get all users



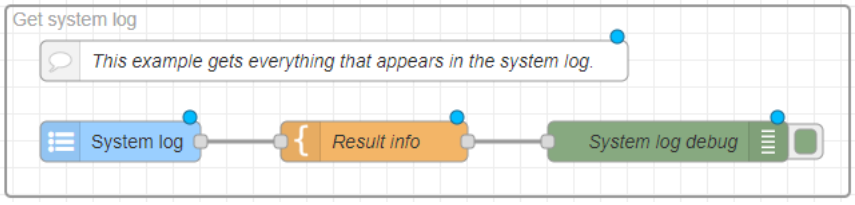
Tento tok generuje seznam všech uživatelů, včetně informací o nich. Úloha je iniciována aktivací uzlu Inject. V uzlu **REST API – get users endpoint** lze aplikovat filtr k upřesnění, jaké uživatele má proces vracet. Tímto způsobem lze přízpůsobit výstup procesu podle potřeb administrátora.

Get users from one company



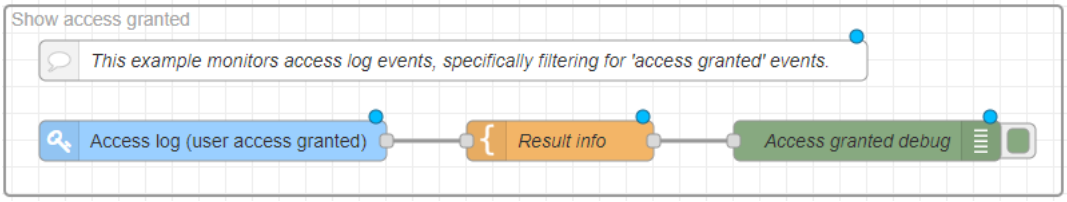
Tento tok generuje seznam všech uživatelů v rámci jedné společnosti, včetně informací o nich. Úloha je iniciována aktivací uzlu Inject. Výber společnosti se nastavuje v uzlu **REST API – get users endpoint with fillter** zadáním jejího id.

Get system log



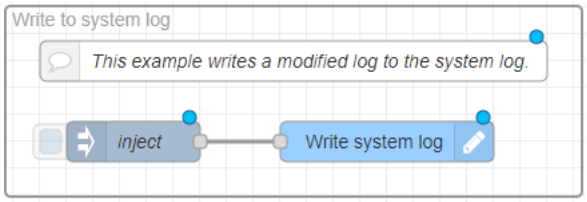
Tento tok načítá všechny nové záznamy v systémovém logu. Výběr událostí lze upřesnit zadáním filtru v uzlu **System log**.

Show access granted



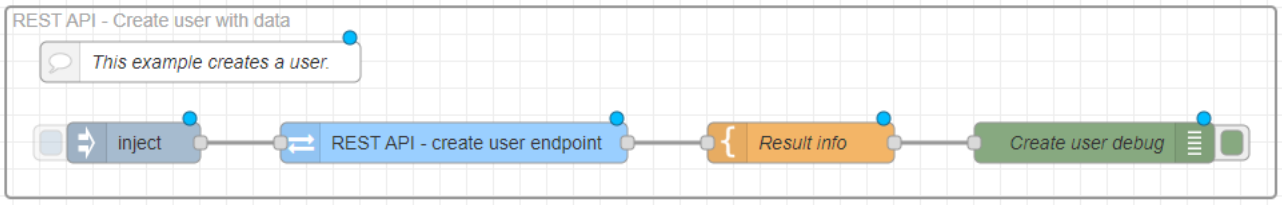
Tento tok načítá všechny nové záznamy v přístupovém logu. Tok je nastaven na načítání pouze povolených přístupů (granted access). V uzlu **Access log** je možné toto omezení změnit.

Write to system log



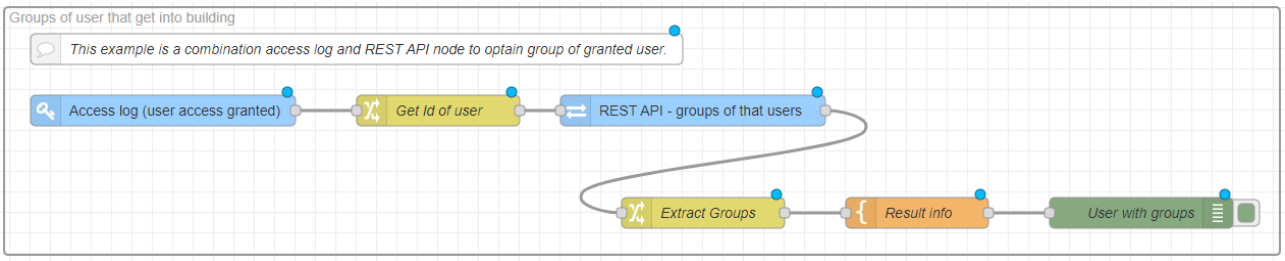
Tento tok vytvoří záznam v systémovém logu. v uzlu **Write system log** lze nastavit Závažnost, název a detailní popis záznamu.

Create user with data



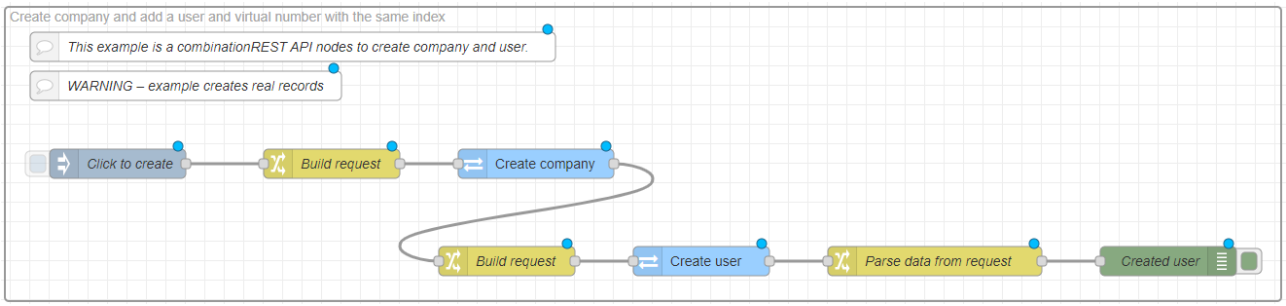
Tento tok slouží k vytvoření nového uživatele. Úloha je iniciována aktivací uzlu **Inject**. Uzel **Inject** obsahuje message body, který určuje jméno uživatele Joe Doe a jeho zařazení do společnosti s ID 1. Toto body se aplikuje v uzlu **Rest API - create user endpoint** a na základě něj je vytvořenuživatele vytvoří. Uzel **Result info** nastavuje znění zprávy, které se bude objevovat v Debug zprávách.

Groups of users that get into building



Tento tok načítá skupiny uživatelů, kterým byl povolen přístup. Povolené přístupy se načítají z přístupového logu. Následně tok získá ID uživatele, jemuž byl přístup povolen, a pomocí uzlu **REST API - groups of that users** načte údaje o tomto uživateli. Uzel **Extrack Groups** získá názvy skupin tohoto uživatele a uzel **Result info** sestaví znění finální zprávy.

Create company and add a user and virtual number with the same index



Tento tok vytvoří novou společnost, prvního uživatele v této společnosti a jeho virtuální číslo. Úloha je iniciována aktivací uzlu **Inject**. Při iniciaci se vygeneruje náhodné celé číslo, které bude použito v názvu společnosti, ve jméně uživatele a bude sloužit jako jeho virtuální číslo. Uzel **Create company** vytvoří společnost s definovaným názvem. Z odpovědi tohoto uzlu se získá ID společnosti, na jehož základě následující uzel **Create user** vytvoří v této společnosti nového uživatele a současně mu přiřadí virtuální číslo. Uzel **Parse data from request** pak načítá název společnosti, jméno uživatele a jeho virtuální číslo.

Export/Import toků

Toky je možné exportovat do .json souborů a později je do rozhraní Automatizace znovu importovat. Export i import se provádí v rozšířené nabídce v pravém horním rohu. Toky přesunuté z jedné instalace **Access Commanderu** do jiné mohou vyžadovat úpravy.

V možnostech importu jsou přednahrané příkladové toky pro **Access Commanderu**. Nachází se v záložce Examples, ve složce Access-Commander-nodes.

VÝSTRAHA
Nastavení pokročilých funkcí, které nová licence nepodporuje, se neukládá.

Proto při ukončení Trial licence nezapomeňte své nastavené toky exportovat.

Chybové stavy

Při práci s automatizacemi se mohou občas vyskytnout chyby, které mají vliv na jejich stabilitu a funkčnost. Pokud k nějakému chybovému stavu dojde, karta Automatizace v **Access Commanderu** na tento stav upozorní a nabídne restartování platformy Node-RED v bezpečnostním režimu. Bezpečnostní režim dočasně zastaví chod toků a umožní bezpečnou opravu toků, které navozují chybový stav. Opětovné spuštění toků se aktivuje tlačítkem Deploy.

Existují dva základní chybové stavy:

- **Node-RED neodpovídá**
  K tomuto stavu dojde, když Node-RED přestane reagovat. Neprobíhají žádné nastavené automatizace. Tento problém může být způsoben různými faktory, jako je přetížení systému, chyby v nastavení toků nebo konflikty mezi importovanými moduly třetích stran.
- **Node-RED je nestabilní**
  Nestabilita Node-RED se projevuje opakovaným restartováním platformy, což může narušit běh automatizací a způsobit ztrátu dat. K opakovanému restartu zpravidla dochází, pokud je některý z toků špatně nastaven a vyvolává restart. Po dobu restartu je pozastaven chod všech toků.

Jméno instalace

V záhlaví webového rozhraní se zobrazuje název konkrétní instalace **Access Commanderu**, název se zobrazuje všem přihlášeným uživatelům. Výchozí název **Access Commander** je možné změnit, např. na adresu budovy, kterou konkrétní instalace spravuje.

Změna názvu se provádí na stránce **Nastavení > Konfigurace > karta Jméno instalace**. Změnou názvu lze odlišit jednotlivé instalace, pokud jich jedna osoba spravuje více. Název instalace se propisuje také do e-mailů odesílaných společnostem.

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.

1. Nastavení se provádí v **Nastavení > Konfigurace > E-mail**.
2. 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.
3. 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).
4. 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**.
5. Provedené nastavení můžete zkontrolovat odesláním testovacího e-mailu.

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.

Access Commander nevyžaduje, abyste při každém přihlášení nebo provádění chráněných akcí znovu ověřovali svou identitu. Jakmile ověření jednou dokončíte, systém si vás po omezenou dobu pamatuje:

- 7 dní pro běžná přihlášení
- 5 minut pro akce považované za bezpečnostně kritické, jako je změna API klíčů, aktualizace vlastního hesla nebo úprava hesla uživatele root.

Systém si dokáže zapamatovat až dvě ověřená zařízení. Pokud provedete ověření z nového zařízení, nejstarší zapamatované zařízení se odebere. Pokusíte-li se provést bezpečnostně kritickou akci mimo povolené časové okno, systém vás jednoduše znovu požádá o ověření, než budete moci pokračovat.

1. Dvoufaktorového ověření nastavuje administrátor na stránce **Nastavení > Konfigurace > karta Dvoufaktorové ověření**.

2. 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.
   - **Povinné pro uživatele s rolí**
     Každý uživatel, kterému byla přiřazena role, musí své přihlášení potvrdit pomocí ověřovací aplikace.
   - **Povinné**
     Všichni uživatelé musí své přihlášení potvrdit pomocí ověřovací aplikace.

Zapnutí dvoufázového ověření

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

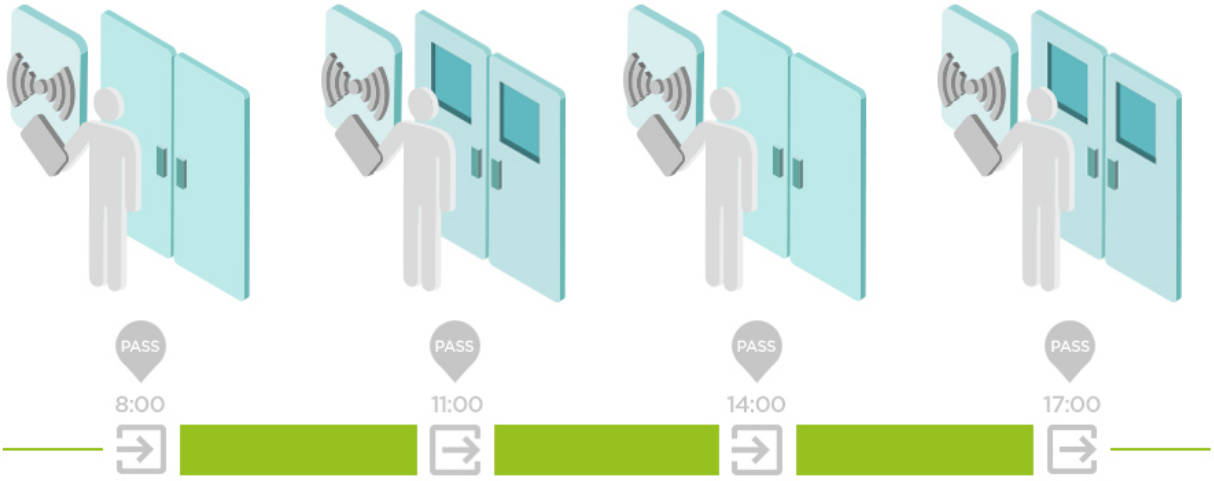
1. Kliknutím na obrázek uživatele v pravém horním rohu otevřete uživatelské menu.
2. Na kartě Ověřovací aplikace propojíte účet s vybranou ověřovací aplikací. Postupujte podle pokynů v **Access Commanderu**.
3. Vyberte Zobrazit profil.

Nastavení docházky

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

Režimy docházky

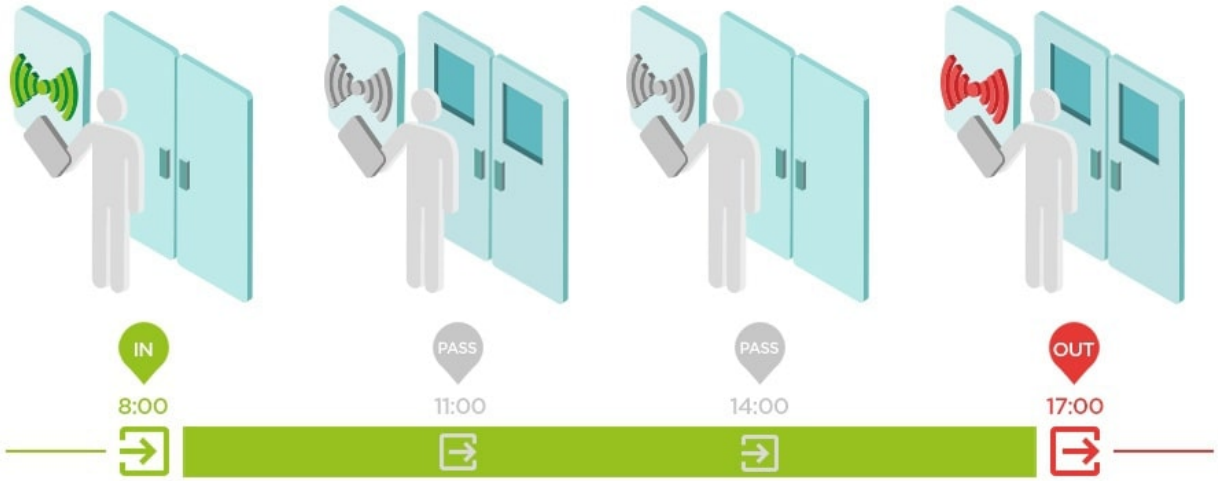
- **FREE**



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 zařízení pro vstup a výstup z oblasti.



- **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

Každé zařízení můžete logicky rozdělit na dva přístupové body – příchod a odchod. Každý přístupový bod představuje průchod v jednom směru a určuje, zda uživatel zařízení vstupuje do zóny, nebo ji opouští. Jeden přístupový bod může být ovládán jedním nebo více moduly zařízení. Všechny přiřazené moduly pak spravují průchody ve směru konkrétního přístupového bodu. Přístupové body se využívají zejména v situacích, kdy zařízení leží na hranici dvou zón a je potřeba přesně zaznamenat směr pohybu mezi nimi (například pro funkce typu anti-passback).

Přístupové body dále slouží ke sledování uživatelů v modulu Přítomnost (str. 79). Přístupové body se také využívají pro sledování vstupu a výstupu v Omezení oblastí (str. 81).

POZNÁMKA
Ve webovém konfiguračním rozhraní jednotlivých zařízení se přístupové body označují jako **Příchod** a **Odchod**. Jejich nastavení provedete v **Přístupy > Přístupová pravidla > záložky Přístup a Odchod**.

Povolení přístupových bodů v Access Commanderu

1. Přejděte na stránku Zóny v **Access Commanderu**.
2. V pravém horním rohu stiskněte ⚙ a povolte použití přístupových bodů.

Rozřazení modulů pro příchod nebo odchod

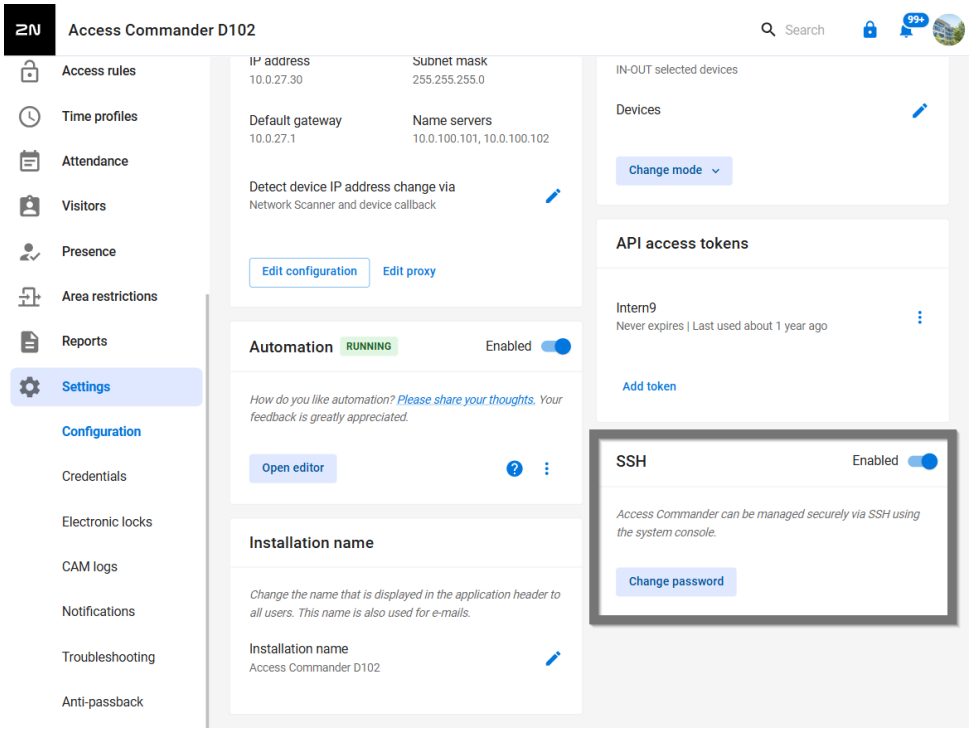
1. Vstupte do webového konfiguračního rozhraní daného zařízení.

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

2. Přejděte do **Přístup > Přístupová pravidla**.
3. Na záložce **Příchod** nebo **Odchod** v kartě **Moduly** klikněte na tlačítko Správa.
4. Otevře se dialogové okno s přehledem dostupných modulů spravujících přístup.
5. Přetáhněte dané moduly do skupin podle směru, který mají zajišťovat.

> **TIP**
>
> Kliknutím na můžete konkrétní modul lokalizovat. Modul spustí vizuální nebo akustickou signalizaci v závislosti na svých možnostech.

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. 85).

Šifrovací klíče pro My2N aplikaci

Uživatelé mohou ke spojení se zařízeními 2N používat My2N aplikaci. Komunikace mezi My2N aplikací a zařízením je vždy šifrovaná. **Access Commander** automaticky spravuje systémové párovací klíče, které jsou distribuovány na zařízení s podporou WaveKey a zajišťují tak bezpečné důvěryhodné párování. Bez znalosti šifrovacího klíče nemůže My2N aplikace uživatele autentizovat. Primární šifrovací klíč je automaticky vygenerován buď při prvním spuštění interkomu nebo v případě správy přes **Access Commander** v rámci jeho konfigurace. Klíč lze kdykoli ručně přegenerovat. Primární šifrovací klíč je společně s Auth ID přenesen do mobilního zařízení při párování.

POZNÁMKA
V systému se používají dva typy klíčů: **párovací klíče** a **přístupové klíče**. Párovací klíče slouží k autentizaci mobilní aplikace My2N aplikace se zařízením. Přístupové klíče určují oprávnění k funkcím v rámci mobilní aplikace.

Vytvoření nových klíčů

1. Přejděte do **Nastavení > Autentizace > karta Šifrovací klíče pro My2N aplikaci**.
   Je možné vygenerovat až 4 přístupové klíče. 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.
2. Klikněte na Vygenerovat nový klíč.

   TIP
   Z bezpečnostních důvodů se doporučuje přegenerovat párovací klíče jednou za delší časové období (například jednou ročně).
3. Nově vygenerovaný klíč se automaticky nahraje do My2N aplikace při prvním použití mobilního telefonu s již dříve spárovaným zařízením.

Vygenerovaný klíč lze smazat kliknutím na .

TIP
Pro vyšší úroveň zabezpečení je vhodné preferovat párování pomocí **QR kódu**, který obsahuje veřejný klíč. Pokud QR kód není dostupný, lze použít párování pomocí **PINu**.

VÝSTRAHA
Párování pomocí QR kódu je podporováno pouze u zařízení s firmwarem HIP 2.50.0 a novějším (včetně řady 3.0). V prostředí s Access Commanderem může být **QR kód** zobrazen, ale párování na starších verzích HIP bude úspěšné pouze pomocí **PINu**.

POZNÁMKA

- Pokud nebude mít My2N aplikace 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 My2N aplikace.
- Umožnění přístupu na zařízení závisí na nastavených přístupových právech daného uživatele.

Režim kompatibility RFID karet

Pokud **Access Commander** hlásí, že právě přidaná zcela nová karta je již v systému použita, může být důvodem zapnutý režim kompatibility RFID karet. Tento režim aktivuje Administrátor v **Nastavení > Autentizace > karta Nastavení režimu kompatibility**.

VÝSTRAHA

- Režim kompatibility by měl být aktivován pouze při problémech s načítáním dříve registrovaných karet. Použití režimu kompatibility může ovlivňovat autentizační mechanismy.
- Režim kompatibility není vhodné kombinovat s používáním karet zabezpečených technologií PICard.

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. Přejděte do **Nastavení > Přístupy > karta PICard klíče**.
2. Po kliknutí na Import nahrajte soubor s šifrovacími klíči z vašeho úložiště.

3. 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.

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**.

1. Přejděte do **Nastavení > Přístupy > karta Povolené USB čtečky.**
2. Kliknutím na Povolit čtečky se otevře dialogové okno.
3. Povolení/zakázání použití externího USB zařízení se provádí v dialogovém okně.
4. Následně se jejich povolování čteček 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

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
- **Volání**
  - Hovor zahájen

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.

Elektronické zámky

Systém **Access Commander** zajišťuje správu přístupů přes elektronické zámky 2N Fortis, které se odemykají RFID kartou s technologií MIFARE® DESFire®. Při konfiguraci elektronických zámků je každému zámku přidělen šifrovací klíč. Klíče zámků jsou pak uloženy na RFID kartách oprávněných uživatelů. Při shodě klíčů na kartě a v zámku dojde k odemknutí uzamykacího mechanismu.

Jednu přístupovou RFID kartu je možné používat pro přístup až k 90 dveřím se zámky 2N Fortis, v závislosti na počtu uplatněných časových profilů. Při překročení kapacity paměti karty zápis dat na kartu selže. Událost selhání zápisu se zaznamenává v přístupovém logu systému. Pokud jsou použity Skupiny zámků, může být na jednu kartu zapsáno více dveří než při individuálním přiřazení.

Fortis Commander

Fortis Commander je samostatná aplikace, která propojuje elektronické zámky **Fortis** se systémem **Access Commander**. Aplikace nastavuje zámky podle projektového souboru vytvořeného v **Access Commander**u, který obsahuje konfiguraci zámků. Soubor je šifrovaný a lze jej použít pouze na jedné konkrétní instalaci.

Instalace

Aplikace Fortis Commander je určena pro instalaci na počítači s operačním systémem Windows s podporou Bluetooth Low Energy (BLE).

Aplikaci můžete najít na webu 2N Download Centre.

Postup instalace

1. Stáhněte instalační balíček z uvedeného odkazu.
2. Spusťte instalátor a dokončete instalaci podle pokynů na obrazovce.

Projektový soubor

Projektový soubor je vytvořen v **Access Commanderu** a obsahuje kompletní konfiguraci projektu. Soubor je šifrovaný a chráněný heslem.

Nastavení zámků v Access Commanderu

Před nahráním klíčů do jednotlivých zámků je potřeba spárovat **Access Commander** s aplikací **Fortis Commander**.

Vygenerování hlavního šifrovacího klíče (MEK) a příprava projektu

1. Přihlaste se do systému Access Commander.
2. Přejděte na stránku **Nastavení > Elektronické zámky**.

3. V kartě **Počáteční nastavení** klikněte na Vygenerovat klíče.
4. Vytvořte Hlavní šifrovací klíč.

VÝSTRAHA
Hlavní šifrovací klíč nelze později **zobrazit ani změnit**.

POZNÁMKA
Podle hlavního šifrovacího klíče (MEK) generuje **2N Access Commander** sadu šifrovacích klíčů. Klíč by tak měl být unikátní a dostatečně bezpečný. Sada klíčů vychází z hlavního šifrovacího klíče, proto projekty se stejným hlavním šifrovacím klíčem generují stejné sady klíčů. Při ztrátě projektu je možné vytvořit nový projekt se stejným hlavním šifrovacím klíčem a pokračovat s šifrováním.

5. Po vygenerování klíčů a nastavení hesla k projektovému souboru je možné stáhnout **projektový soubor**, který představuje obraz konfigurace elektronických zámků v systému **Access Commander**.
6. V kartě **Fortis Commander** klikněte na Stáhnout aplikaci, odkud se začne stahovat **Fortis Commander** (aplikace pro konfiguraci elektronických zámků).

VÝSTRAHA
Informace o projektu jsou citlivá data. Chraňte je před zneužitím.

Propsání konfigurace elektronického zámku pomocí Fortis Commander

1. Nainstalujte aplikaci **Fortis Commander** a otevřete ji.
2. Klikněte na Open project a otevřete stažený projektový soubor v Průzkumníku souborů.
3. V zobrazeném dialogu zadejte heslo k projektovému souboru.
4. Po otevření projektového souboru zvolte Connect to device a přiložte servisní kartu k zámku.
5. Klikněte na **Assign**, čímž přiřadíte zámek k projektu.
6. Odpojte zařízení a klikněte na **File > Close project**.
7. Po dokončení konfigurace otevřete systém **Access Commander**. Přejděte do karty **Nastavení > Elektronické zámky** a znovu klikněte na tlačítko Fortis Commander. Nahrajte projektový soubor.

POZNÁMKA
Při přesunu zámku mezi instalacemi nebo při reklamaci je nutné provést **Factory reset**. Tato operace obnoví zámek do továrního nastavení a odstraní veškerou předchozí konfiguraci.

Postup aktualizace konfigurace

1. Proveďte změny v **Access Commanderu**.
2. Stáhněte nový projektový soubor.
3. Nahrajte soubor do **Fortis Commanderu** a proveďte požadované změny na zámcích.
4. Pokud provedete další změny v **Access Commander**u, vždy stáhněte nový projektový soubor.

VÝSTRAHA
Pro každou změnu konfigurace v **Access Commander**u je nutné stáhnout nový projektový soubor – nelze použít starší soubor, který byl již nahrán do **Fortis Commanderu**.

Trvalé zamknutí a odemknutí

Aplikace umožňuje trvalé zamknutí a odemknutí zámku. Funkce slouží pro servisní zásahy nebo nouzové ovládání bez použití karty.

Sběr událostí z elektronických zámků pomocí RFID karet / čipů

Nastavení sběru událostí

1. Otevřete **Nastavení > Elektronické zámky > Události na kartách**.
2. Vyberte typ událostí:
   - **Shromažďovat přístupové a systémové události** – na kartu/čip se zaznamenávají všechny přístupové a systémové události, které se propisují do **Systémového logu** a **Přístupového logu**.
   - **Shromažďovat pouze systémové události** – zaznamenají se pouze systémové události, přístupové události se neukládají na karty.
   - **Neshromažďovat události na kartách** – žádné události se nezapisují na kartu; přístup k nim je možný pouze prostřednictvím **Fortis Commander**u.

TIP
Výběrem vhodné množiny událostí lze snížit zatížení systému a využití úložiště. Podrobné protokolování je však důležité pro diagnostiku a bezpečnostní audity.

Export událostí z karty

Na kartu se ukládá maximálně **16 prvních událostí**. Události lze vyčíst dvěma způsoby:

- V **Access Commanderu** klikněte na ikonu ve vyhledávacím poli v záhlaví a načtěte kartu.
- Pomocí zařízení s **2N OS** se události z karty vyčtou a odešlou do **Access Commander**u.

Nahrání událostí do zámku

1. Otevřete **Nastavení > Elektronické zámky > Fortis Commander** a klikněte na Stažení souboru.
2. Otevřete soubor v aplikaci **Fortis Commander**.
3. V aplikaci **Fortis Commander** se připojte k elektronickému zámku.
4. Nahrajte aktualizovaný soubor zpět do **Access Commanderu**.
5. Po nahrání se události zobrazí v **Přístupové logy** a **Systémové logy**.

Servisní operace

Tyto operace jsou dostupné pro **Fortis Cylinder**:

- **Demontáž** – rozebrání zámků pro servisní účely.
- **Výměna baterie** – výměna baterie v zámku.

VÝSTRAHA
Servisní operace nejsou relevantní pro jiné typy zámků.

POZNÁMKA
Ze servisního módu se zámek vrátí do běžného režimu stisknutím tlačítka Lock pro trvalé zamknutí.

Aktualizace karty

Přístupové karty uživatelů je potřeba pravidelně aktualizovat. Aktualizaci karty uživatel provede přiložením karty k IP zařízení 2N, ke kterému má platná přístupová práva. Kartu je nutné u čtečky zařízení přidržet až do sepnutí spínače otevírání dveří. Spínač otevírání dveří se aktivuje až po aktualizaci přístupů k zámkům.

Výchozí desetidenní platnost karet je možné změnit v **Nastavení > Elektronické zámky > karta Parametry karty**.

VÝSTRAHA
Pokud v **Access Commanderu** změníte přístupová práva k zámkům, změny se na přístupové kartě uživatele projeví až po její aktualizaci na čtečce karet zařízení 2N! Z bezpečnostních důvodů doporučujeme nastavit kratší platnost karet pro zajištění jejich pravidelné aktualizace.

Čtečky IP zařízení, které umožňují aktualizaci karty, a jejich nastavení je popsáno v kapitole Nastavení čtečky IP zařízení (str. 28).

Kompatibilní karty

POZNÁMKA
Pro účely této dokumentace označuje pojem **karta** jakýkoli kompatibilní identifikátor využívající technologii MIFARE DESFire.

Pro otevírání elektronických zámků 2N Fortis nelze používat karty s náhodným ID (random ID).

Karty s technologií PICard nelze použít pro otevírání elektronických zámků 2N Fortis.

Časové profily na elektronických zámcích

Elektronické zámky podporují časové profily s následujícími omezeními:

- Svátky se neuplatňují.
- V rámci jednoho dne lze nastavit až 4 různé časové intervaly.
- V rámci jednoho časového profilu lze definovat 4 denní rozvrhy intervalů.

TIP
To znamená, že lze mít například jiná nastavení pro pondělí, úterý, středu a čtvrtek, ale pro pátek, sobotu a neděli už musíte použít jedno z existujících nastavení.

VÝSTRAHA
Pokud časový profil poruší uvedená omezení, bude přístupové pravidlo ignorováno a uživateli nebude udělen přístup.

Karty pro údržbu

Karty pro údržbu zajišťují autorizovaný přístup k zámku. Umožňují uvedení zámku do servisního stavu, výměnu baterie, demontáž zámku.

VÝSTRAHA
Kartu pro údržbu nelze současně použít jako přístupovou kartu uživatele.

Nastavení karty pro údržbu

1. V **Access Commanderu** přejděte na stránku **Nastavení > Elektronické zámky**.
2. V kartě **Karty pro údržbu** klikněte na Vytvořit.
3. V otevřeném dialogovém okně vyberte typ karty, kterou chcete vytvořit.
   - Nastavení nových zámků – aktivuje do servisního módu již dříve konfigurované nové zámky v továrním nastavení.
   - Servis – aktivuje servisní mód u již nastaveného zámku.
   - Demontáž – uvolní již nastavený zámek 2N Fortis Cylinder k demontáži, viz Instalační manuál 2N Fortis.
   - Výměna baterie – uvolní již nastavený zámek 2N Fortis Cylinder k výměně baterie, viz Instalační manuál 2N Fortis.

   TIP
   Na jednu fyzickou kartu je možné nahrát současně **Nastavení nových zámků** a libovolnou druhou servisní kartu. Doporučujeme kombinaci **Nastavení nových zámků** a **Servis**.
4. Klikněte na Pokračovat.
5. Přiložte kartu k připojené USB RFID čtečce. Vyčkejte do načtení dat na kartu.

Platnost dat na kartě pro údržbu je jeden rok. Po uplynutí této doby je nutné data smazat a kartu nastavit znovu.

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.

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 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. 97).

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 .

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.

Detekce změny IP adresy zařízení

Access Commander navazuje spojení se zařízeními prostřednictvím jejich IP adres. Aby se předešlo ztrátě spojení se zařízením s dynamickou IP adresou, jsou dostupné dvě metody detekce IP adres zařízení.

- **Network Scanner**
  Access Commander pravidelně skenuje lokální síťový segment pomocí integrovaného 2N Network Scanneru, aby identifikoval připojená zařízení a jejich aktuální IP adresy.
- **Device callback**
  Tato metoda detekuje IP adresy zařízení mimo lokální segment sítě. Zařízení se budou hlásit při spuštění, při změně IP adresy a v pravidelných intervalech (jednou za hodinu). Pro správnou funkci je nutné zadat cílovou destinaci, na kterou se budou zařízení hlásit (obvykle IP adresu **Access Commanderu**).

Network Discovery

Zjišťování sítě umožňuje ostatním službám, jako jsou **2N IP Utility** nebo **2N Network Scanner**, najít instalaci **Access Commanderu** v místní síti.

Lze požívat **Network Scanner** a **Axis Utility** zároveň. Z bezpečnostních důvodů je však možné obě detekce **Access Commanderu** zcela vypnout v nastavení systému.

TIP
Access Commander lze v aplikacích **2N Network Scanner** a **2N Axis Utility** zobrazit nebo skrýt. To stejné platí pro přístup do webového rozhraní pomocí **accesscommander.local**. Pokud je v síti spuštěno více instancí Access Commanderu, systém automaticky přiděluje jedinečné názvy: **accesscommander.local**, **accesscommander-2.local**, **accesscommander-3.local** a další instance podle počtu serverů v síti.

Nastavení proxy

Proxy se používá pro služby jako jsou: HTTP požadavky, FTP synchronizaci, upgrade apod.

POZNÁMKA
Proxy pro FTP s TLS ověřením není podporováno.

1. Přejděte do **Nastavení > Konfigurace > karta Síť**.
2. Zvolte Upravit proxy.
3. V otevřeném dialogovém okně zadejte adresy proxy serverů pro požadované protokoly.
4. V posledním poli můžete vyplnit adresy, pro které se proxy server uplatňovat nemá.
   Připojení k localhost a k IP adresy z rozsahu127.0.0.1/8 nebudou nikdy směrována přes proxy server.
5. Po změně nastavení se **2N Access Commander** automaticky restartuje.

Použití NodeRED

Aplikace NodeRED ignoruje systémová nastavení proxy serveru. Pro správnou funkčnost je nutné proxy server explicitně nakonfigurovat v každém uzlu aplikace NodeRED, který vyžaduje jeho použití.

Doplňkové informace

MIFARE and DESFire are registered trademarks of NXP B.V.

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.

Odpovědi na požadavky je možné filtrovat pomocí Query. Sestavování **query** popisuje dokument Data Query Customization (pouze v angličtině).

Autentizace

HTTP API příkazy se odesílají pod přihlašovacími údaji uživatele nebo pomocí tokenové autentizace. Autentizační token vytváří administrátor v **Nastavení > Konfigurace > karta API přístupové tokeny**. Jedná se o Bearer Token. Při vytváření nového API přístupového tokenu může administrátor omezit jeho platnost pouze pro čtení, token tak bude autentizovat pouze GET příkazy. Tokenu je možné omezit platnost na: 1 měsíc, 6 měsíců, 1 rok.

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

SignalR

SignalR je protokol, který umožňuje real-time komunikaci serveru s klientem. To znamená, že server může posílat připojeným klientům zprávy, ihned jakmile se stanou dostupnými, a nemusí čekat na požadavek ze strany klienta. Základní principy SignalR jsou popsány v dokumentu SignalR integration manual (pouze v angličtině). Seznam dostupných topiců SignalR pro použití s **Access Commanderem** jsou popsány v dokumentu SignalR topics reference manual (pouze v angličtině).

Licence třetích stran

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

2N Access Commander – Instalační manuál

2N.com