An Axis company

Access Unit

Access Control

Konfigurační manuál

Firmware: 2.29
Verze: 2.29

www.2n.cz

Společnost 2N TELEKOMUNIKACE a.s. je českým výrobcem a dodavatelem telekomunikační techniky.

K produktovým řadám, které společnost vyvíjí, patří GSM brány, pobočkové ústředny, dveřní a výtahové komunikátory. 2N TELEKOMUNIKACE a.s. se již několik let řadí mezi 100 nejlepších firem České republiky a již dvě desítky let symbolizuje stabilitu a prosperitu na trhu telekomunikačních technologií. V dnešní době společnost vyváží do více než 120 zemí světa a má exkluzivní distributory na všech kontinentech.

Pro rychlé nalezení informací a zodpovězení dotazů týkajících se 2N produktů a služeb 2N TELEKOMUNIKACE spravuje databázi FAQ nejčastějších dotazů. Na www.faq.2n.cz naleznete informace týkající se nastavení produktů, návody na optimální použití a postupy „Co dělat, když...".

Společnost 2N TELEKOMUNIKACE a.s. tímto prohlašuje, že zařízení 2N je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES. Plné znění prohlášení o shodě naleznete na CD-ROM (pokud je přiloženo) nebo na www.2n.cz.

Společnost 2N TELEKOMUNIKACE a.s. je vlastníkem certifikátu ISO 9001:2009. Všechny vývojové, výrobní a distribuční procesy společnosti jsou řízeny v souladu s touto normou a zaručují vysokou kvalitu, technickou úroveň a profesionalitu všech našich výrobků.

Obsah:

1. Popis produktu

Dveřní přístupový systém **2N Access Unit** je schopen, spolu s doplňkovým software a případně **2N IP interkomy,** nabídnout ucelené řečení přístupového systému do jakéhokoliv objektu.

Přístupový systém **2N Access Unit** lze dovybavit numerickou klávesnicí, kterou lze použít jako kódový zámek.

Přístupový systém **2N Access Unit** může být vybaven druhou čtečkou RFID karet, která umožňuje nejen zpřístupnit objekt autorizovaným osobám, ale zároveň se stát součástí zabezpečovacího systému objektu nebo docházkového systému ve vaší firmě.

2N Access Unit může být vybavena reléovým spínačem (volitelně dalšími relé a výstupy), kterým lze ovládat elektrický zámek nebo jiné zařízení připojené k tomuto přístupovému systému. Přístupový systém je možné velmi flexibilně nastavit, kdy a jak se mají tyto spínače aktivovat – kódem, automaticky, stiskem tlačítka apod.

V manuálu jsou použity následující symboly a piktogramy:

Nebezpečí úrazu

- **Vždy dodržujte** tyto pokyny, abyste se vyhnuli nebezpečí úrazu.

Varování

- **Vždy dodržujte** tyto pokyny, abyste se vyvarovali poškození zařízení.

Upozornění

- **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.

2. Expresní průvodce základním nastavením

Nastavení připojení k lokální síti

Abyste se mohli přihlásit ke konfiguračnímu rozhraní 2N Access Unit, musíte znát jeho IP adresu. Přístupový systém 2N Access Unit mají z výroby nastaveno automatické získání IP adresy z DHCP serveru. Pokud tedy připojíte tuto jednotku do sítě, ve které se nachází DHCP server nakonfigurovaný tak, aby přiděloval IP adresy všem novým zařízením, získá svou vlastní IP adresu i 2N Access Unit. IP adresu 2N Access Unit můžete zjistit buď přímo ze stavu DHCP serveru (podle MAC adresy uvedené na výrobním štítku), příp. vám ji může sdělit přímo 2N Access Unit pomocí hlasové funkce – viz Instalační manuál (odkaz níže).

Pokud ve vaší síti není DHCP server, musíte nastavit 2N Access Unit na statickou IP adresu pomocí RESET tlačítka, viz Instalační manuál k příslušnému modelu. Váše jednotka poté získá pevnou adresu 192.168.1.100, kterou použijete pouze pro první přihlášení a poté ji můžete změnit.

V případě, že již znáte IP adresu, zadejte ji do vašeho oblíbeného prohlížeče. Doporučujeme použít aktuální verzi prohlížeče Chrome, Firefox nebo Internet Explorer (Edge). 2N Access Unit není plně kompatibilní se staršími verzemi prohlížečů.

Pro první přihlášení do konfiguračního rozhraní použijte jméno "admin" a heslo "2n" (heslo platné po uvedení zařízení do výchozího stavu). Výchozí heslo doporučujeme po prvním přihlášení ihned změnit – viz nastavení v menu Služby / Web Server – parametr Heslo. Heslo si dobře zapamatujte, příp. zapište. V případě, že heslo zapomenete, budete muset uvést přístupový terminál do výchozího stavu (viz instalační manuál k příslušnému modelu), a tím ztratíte zároveň veškeré provedené změny v nastavení.

Tip

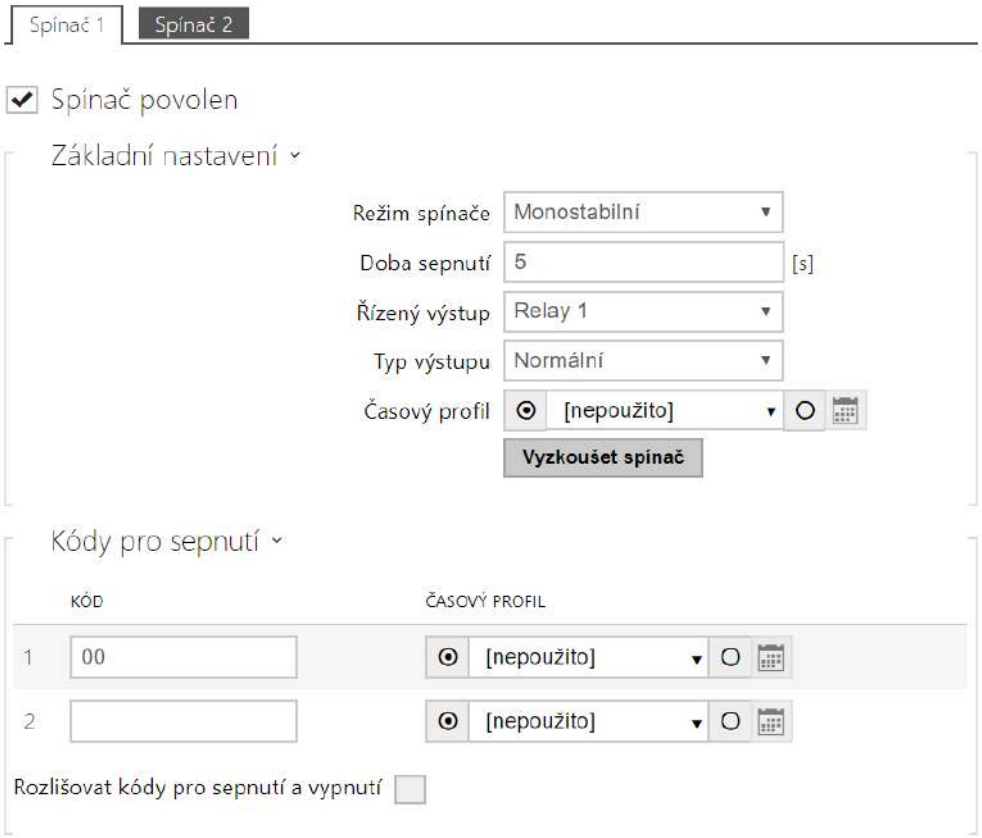
- Instalační manuál: 2.3 Elektrická instalace

Aktualizace firmware

Po prvním přihlášení k **2N Access Unit** doporučujeme zároveň aktualizovat firmware. Nejnovější firmware pro svoji jednotku naleznete na stránkách **www.2n.cz**. K aktualizaci firmware slouží tlačítko **Aktualizovat Firmware** v menu **Systém / Údržba**. Po uploadu firmwaru do zařízení se zařízení jednou restartuje a aktualizace je hotova. Aktualizace trvá přibližně jednu minutu.

Nastavení spínání elektrického zámku

K přístupovému systému **2N Access Unit** lze připojit elektrický dveřní zámek, který lze ovládat pomocí kódu zadaného na numerické klávesnici. Elektrický dveřní zámek připojte podle návodu v Instalačním manuálu k příslušnému modelu.



V záložce **Hardware / Spínače / Spínač 1** povolte spínač pomocí políčka Spínač povolen, nastavte parametr Řízený spínač na výstup interkomu, ke kterému je elektrický dveřní zámek připojen. Poté nastavte jeden nebo více kódů pro sepnutí spínače – elektrického dveřního zámku.

3. Licencované funkce

2N Access Unit podporuje pouze dvě licencované funkce, 2N Access Unit Lift module license a 2N Access Unit – NFC license. NFC licenci lze použít pouze s variantou 2N Access Unit, která obsahuje 13MHz čtečku karet.

Obj. číslo	Název licence
916012	2N Access Unit NFC license
9160401	2N Access Unit Lift module license

Info

- Pomocí webového rozhraní zařízení v sekci Systém / Licence lze aktivovat zkušební verze licencí na omezenou dobu 800 hodin.

Licence	Vlastnosti	2N® IP Verso	2N® LTE Verso	2N® IP Solo	2N® IP Base	2N® IP Force	2N® IP Safety	2N® IP Vario	2N® IP Vario s displejem
Enhanced Audio (součást Gold)	Uživatelské zvuky	★	★	★	★	★	★	★	✓
	Automatický audio test	★	★	★	★	★	★	★	✓
	Detekce hluku	★	★	★	★	★	★	★	✓
Enhanced Video (součást Gold)	Audio/video streaming (RTSP Server)	★	★*	★	★	★	★	★	✓
	Podpora externí IP kamery	★	★*	★	★	★	★	★	✓
	Podpora ONVIF	★	★*	★	★	★	★	★	✓
	Podpora funkce PTZ	★	★	★	★	★	★	★	✓
	Podpora detekce pohybu	★	★	★	★	★	★	★	✓
Enhanced Integration (součást Gold)	Rozšířené možnosti nastavení spínačů	★	★	★	★	★	★	★	✓
	HTTP API	★	★*	★	★	★	★	★	✓
	Funkce pro automatizaci	★	★	★	★	★	★	★	✓
	Odesílání E-mailů (SMTP Client)	★	★	★	★	★	★	★	✓
	Automatický update (TFTP/HTTP klient)	★	★	★	★	★	★	★	✓
	FTP klient	★	★	★	★	★	★	★	✓
	SNMP klient	★	★*	★	★	★	★	★	✓
	TR-069	★	★	★	★	★	★	★	✓
	Synergis	★	★*	★	★	★	★	★	✓
Enhanced Security (součást Gold)	Podpora 802.1x	★	✗	★	★	★	★	★	✓
	Podpora SIPS (TLS)	★	★	★	★	★	★	★	✓
	Blokování spínačů tamperem	★	★	★	★	★	★	★	✓
	Podpora SRTP	★	★	★	★	★	★	★	✓
	Tichý alarm	★	★	★	★	★	★	★	✓
	Omezení neúspěšných pokusů o přístup	★	★	★	★	★	★	★	✓
	Anti-Passback	★	★	✗	★	★	✗	★	✓
	Promíchaná klávesnice	★	★	✗	✗	✗	✗	✗	✗
NFC (součást Gold)	Podpora NFC	★	★	✗	★	★	✗	✗	✗
InformaCast	Podpora InformaCast protokolu	★	★*	★	★	★	★	★	★
Lift Module	Řízení výtahu	★	✗	✗	✗	★	★	★	★

✓

– Obsahuje z výroby

★ – Licencovaná funkce, lze dokoupit

✗ – Nelze použít

*) Dostupnost služby závisí na nastavení sítě mobilního operátora.

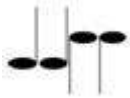
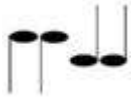
**) Funkce promíchané klávesnice je dostupná pouze na modelech 2N Access Unit 2.0.

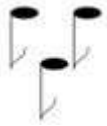
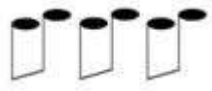
4. Signalizace provozních stavů

2N Access Unit signalizuje pomocí zvukových hlášení změny a přechody mezi různými provozními stavy. Pro každý typ změny stavu existuje jiný typ hlášení. Seznam jednotlivých hlášení je uveden v následující tabulce:

Poznámka

- *Signalizaci některých z výše uvedených stavů je možné upravit, viz kapitola Uživatelské zvuky.*

Tóny	Význam
	Uživatel aktivován Po vložení aktivačního kódu uživatele. Aktivační kód slouží k aktivaci uživatele (pozice v seznamu uživatelů). Nastavení aktivačního kódu je popsáno v kap. Uživatelé.
	Uživatel deaktivován Po vložení deaktivačního kódu uživatele. Deaktivační kód slouží k deaktivaci uživatele (pozice v seznamu uživatelů). Nastavení deaktivačního kódu je popsáno v kap. Uživatelé.
	Profil aktivován Slouží pro aktivování profilu. Může být například využito k zapnutí vyzvánění celé skupiny uživatelů na telefonní čísla přímo v kanceláři. Nastavení aktivačního kódu je popsáno v kap. Profily.
	Profil deaktivován Slouží pro deaktivování profilu. Nastavení deaktivačního kódu je popsáno v kap. Profily.

	**Vnitřní aplikace spuštěna** Po zapnutí napájení nebo po restartu **2N Access Unit** je zahájen start vnitřní aplikace. Úspěšný start vnitřní aplikace je signalizován touto tónovou kombinací.
	**Připojeno do lokální sítě, obdržena IP adresa** Po startu vnitřní aplikace se **2N Access Unit** přihlašuje do lokální sítě. Úspěšné přihlášení do lokální sítě je signalizováno touto tónovou kombinací.
	**Odpojeno od lokální sítě, IP adresa ztracena** V případě, že dojde k odpojení UTP kabelu z **2N Access Unit**, je tento stav signalizován touto tónovou kombinací.
	**Uvedení síťových parametrů do výchozího stavu** Po zapnutí napájení je nastaven časový limit 30 sekund pro zadání kódu uvedení síťových parametrů do výchozího stavu. Uvedení síťových parametrů do výchozího stavu je popsáno v kap. Konfigurace zařízení v Instalačním manuálu **2N Access Unit**.

5. Konfigurace pomocí webového rozhraní

Úvodní přehledová obrazovka

Úvodní stránka se zobrazí po přihlášení do webového rozhraní přístupového terminálu. Kdykoli se k ní můžete vrátit pomocí tlačítka , umístěného v levém horním rohu dalších stránek webového rozhraní.

V záhlaví stránky se zobrazuje jméno přístupového terminálu (viz parametr Zobrazované jméno v nastavení **Služby / Web Server / Základní nastavení**). Lze volit mezi jazyky webového rozhraní pomocí tlačítek **CZ**, **EN**, **DE**, **FR**, **IT**, **ES** a **RU**. Od přístupového terminálu se můžete odhlásit pomocí tlačítka Odhlásit v pravém horním rohu stránky.

Úvodní stránka slouží jako první úroveň menu a rychlá navigace (kliknutím na libovolnou dlaždici) do vybraných částí konfigurace přístupového terminálu. V některých dlaždicích se zároveň zobrazuje stav vybraných služeb.

Konfigurační menu

Konfigurace přístupového terminálu **2N Access Unit** je rozdělena do 5 hlavních nabídek – **Stav**, **Adresář**, **Hardware**, **Služby** a **Systém**; každá z nabídek je rozdělena do dalších částí, viz následující přehled.

Stav

- **Zařízení** – základní informace o přístupovém terminálu
- **Služby** – informace o spuštěných službách a jejich stavu
- **Licence** – aktuální stav licence a dostupných funkcích přístupového terminálu
- **Historie přístupů** – výpis posledních deseti přiložených přístupových karet
- **Události** – výpis proběhlých událostí

Adresář

- **Uživatelé** – nastavení telefonních čísel uživatelů, tlačítek rychlého volání, přístupových karet a uživatelské kódy pro řízení spínačů
- **Časové profily** – nastavení časových profilů
- **Svátky** – nastavení pravidelných a pohyblivých svátků v kalendářním roce

Hardware

- **Spínače** – nastavení spínání elektrického zámku, osvětlení apod.
- **Audio** – hlasitosti audia, signalizačních tónu apod.
- **Klávesnice** – nastavení klávesnice a zadávání kódů
- **Podsvícení** – nastavení intenzity podsvícení
- **Čtečka karet** – nastavení čtečky karet, Wiegand interface
- **Digitální vstupy** – řízení vstupů
- **Rozšiřující moduly** – nastavení rozšiřujících modulů **2N Access Unit**

Služby

- E-Mail – umožňuje nastavit zasílání emailů například v případě neplatného pokusu o přístup
- Mobile Key – nastavení Bluetooth a správa připojených zařízení
- Automatizace – flexibilní nastavení přístupového terminálu dle specifických požadavků uživatele
- HTTP API – aplikační rozhraní pro ovládání vybraných funkcí interkomu
- Web server – nastavení web serveru a přístupového hesla
- SNMP – funkcionalita umožnující vzdálený dohled interkomů v sítí pomocí protokolu SNMP

Systém

- Síť – nastavení připojení k lokální síti, 802.1x, zachytávání paketů
- Datum a čas – nastavení reálného času a časové zóny
- Licence – nastavení licencí, aktivace trial licence
- Certifikáty – nastavení certifikátů a privátních klíčů
- Aktualizace – nastavení automatických aktualizací firmware a konfigurace
- Syslog – nastavení odesílání systémových zpráv syslog serveru
- Údržba – záloha a obnovení konfigurace, aktualizace firmware

- 5.1 Stav
- 5.2 Adresář
- 5.3 Hardware
- 5.4 Služby
- 5.5 Systém

Upozornění

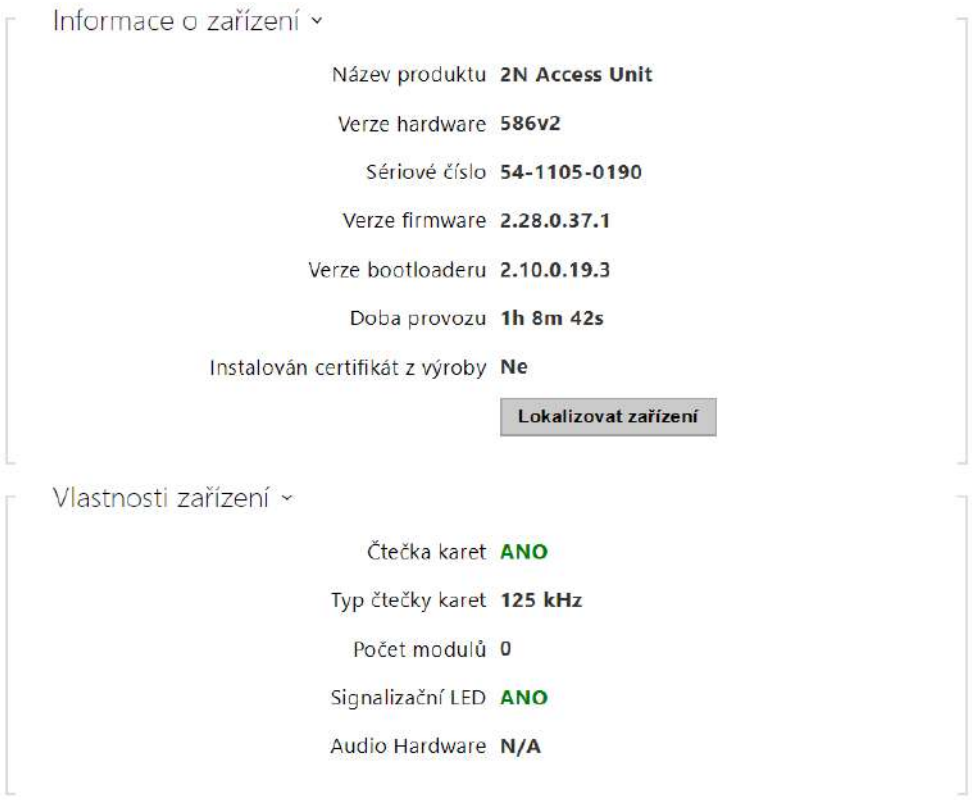
Za účelem dosažení plné funkčnosti a zaručených výkonů důrazně doporučujeme vždy již při instalaci ověřit aktuálnost používané verze produktu či zařízení. Zákazník tímto bere na vědomí, že produkt či zařízení může dosahovat zaručených výkonů a být plně funkční dle propozic výrobce pouze v případě, je-li používána nejnovější verze produktu či zařízení, která byla otestována na plnou interoperabilitu a která nebyla výrobcem označena jako nekompatibilní s určitými verzemi jiných produktů, a to pouze v souladu s pokyny, návodem či doporučením výrobce a pouze ve spojení s vyhovujícími produkty a zařízeními jiných výrobců. Nejnovější verze jsou dostupné na internetových stránkách https://www.2n.cz/cs_CZ/, popř. jednotlivá zařízení podle svých technických možností umožňují aktualizaci v konfiguračním rozhraní. Používá-li zákazník jinou než nejnovější verzi produktu či zařízení, popř. používá-li verzi, kterou výrobce označil za nekompatibilní s určitými verzemi jiných produktů, nebo používá-li zákazník produkt či zařízení v rozporu s pokyny, návodem či doporučením výrobce, nebo ve spojení s nevyhovujícími produkty či zařízeními jiných výrobců, je srozuměn s veškerými případnými omezeními funkčnosti takového produktu či zařízení a s důsledky s tím spojenými. Použitím jiné než nejnovější verze produktu či zařízení, popř. verze, kterou výrobce označil za nekompatibilní s určitými verzemi jiných produktů, nebo použitím produktu či zařízení v rozporu s pokyny, návodem či doporučením výrobce, popř. použitím s nevyhovujícími produkty či zařízeními jiných výrobců, zákazník souhlasí s tím, že společnost 2N TELEKOMUNIKACE a. s. není odpovědná za jakékoli omezení funkčnosti takového produktu ani za újmu související s takovým případným omezením funkčnosti.

5.1 Stav

V menu **Stav** je přehledně zobrazen aktuální stav a informace o přístupovém terminálu. Menu je rozděleno do následujících záložek.

Záložka Zařízení

Zobrazuje informace o modelu a jeho vlastnostech, verzi firmware a bootloaderu apod.

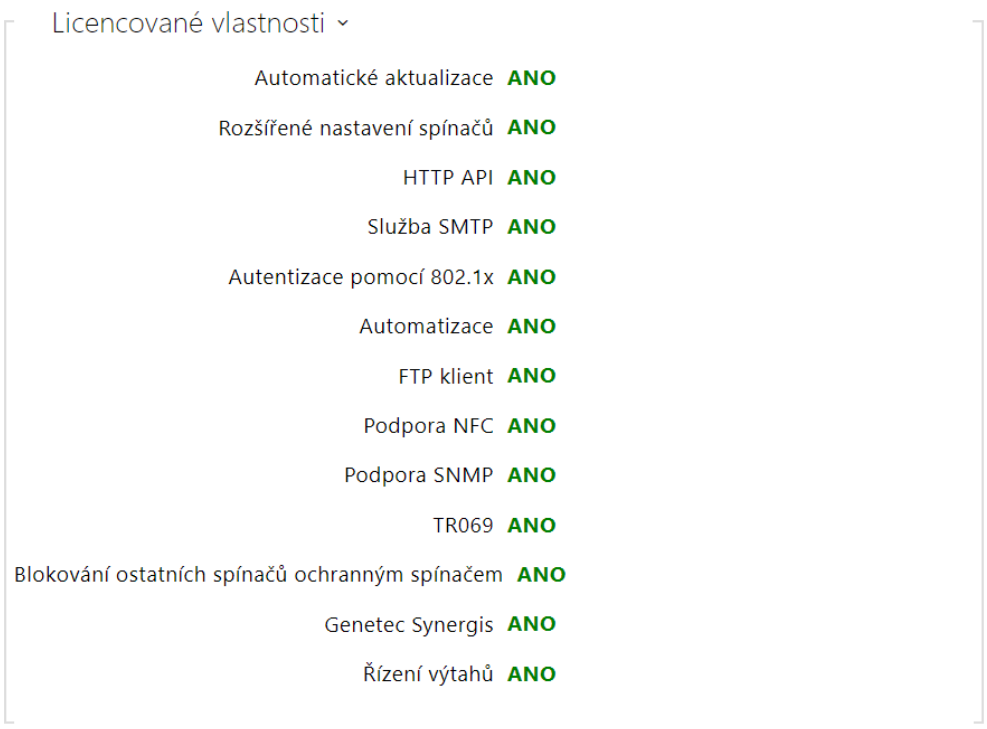


Záložka Služby

Zobrazuje stav síťového rozhraní a vybraných služeb.

Záložka Licence

Zobrazuje seznam licencovaných funkcí přístupového terminálu. U každé funkce se zobrazuje, zda je aktuálně dostupná (na základě platného licenčního klíče zadaného v menu Systém / Licence).



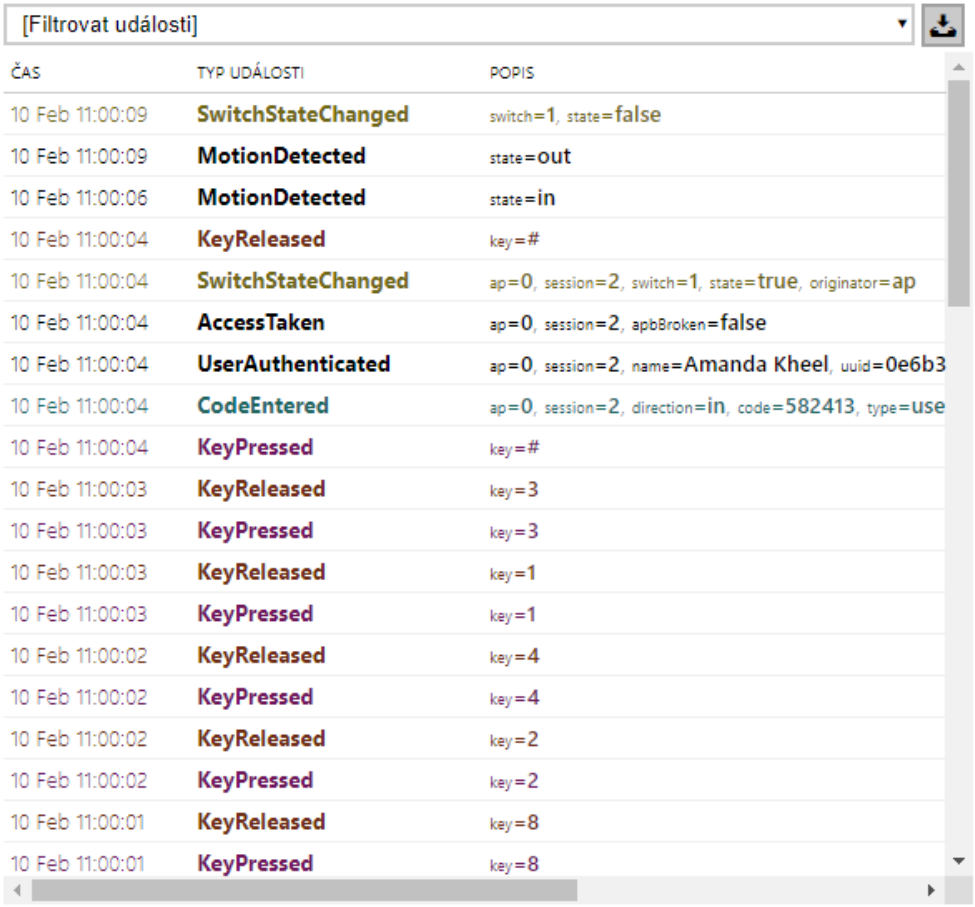
Záložka Historie přístupů

Na záložce **Historie přístupů** se zobrazuje posledních 10 záznamů o přiložených kartách. Každý záznam obsahuje čas přiložení karty, její ID, typ a popis obsahující informaci, zda je karta platná, příp. kterému uživateli byla přiřazena.

	ČAS	ID KARTY	TYP KARTY	POPIS
1	14/12/2015 15:24:55	4BCFDC13	MIFARE Classic 1k	Access denied
2	14/12/2015 15:24:42	04030201	MIFARE Plus S	(user #3)
3	14/12/2015 15:24:36	4BCFDC13	MIFARE Classic 1k	Access denied
4	14/12/2015 15:24:18	1653200A	MIFARE Classic 1k	Access denied
5	14/12/2015 15:24:04	04030201	MIFARE Plus S	(user #3)
6				
7				
8				
9				
10				

Záložka Události

Zobrazuje aktivitu zařízení (spínače, signalizační led, stisknutá tlačítka klávesnice atd.). Umožňuje též filtrovat mezi jednotlivými událostmi pomocí 13 volitelných parametrů.

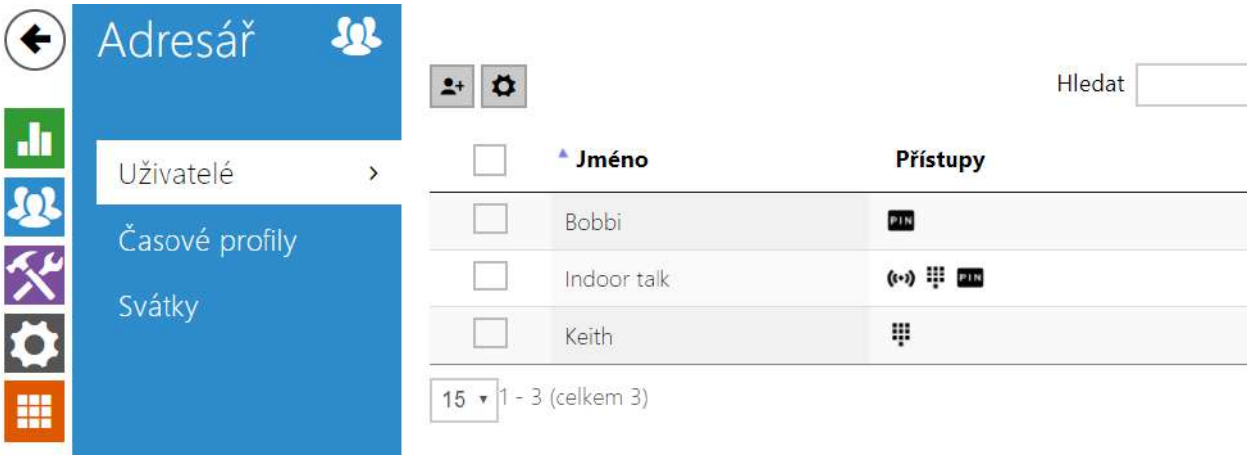


-  – tlačítko slouží k exportu všech zaznamenaných událostí do CSV souboru.

5.2 Adresář

Zde je přehled toho, co v kapitole naleznete:

5.2.1 Uživatelé



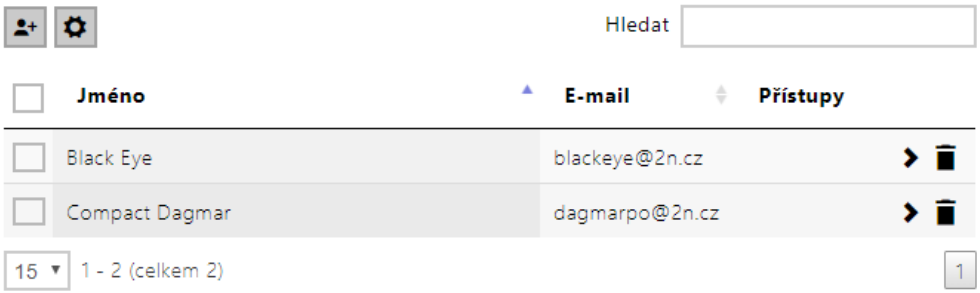
Seznam uživatelů je jednou z nejdůležitějších částí konfigurace interkomu. Seznam uživatelů obsahuje důležité informace o uživatelích, které zpřístupňují funkce interkomu, jako jsou volání pomocí tlačítek rychlé volby, otvírání dveří pomocí RFID karet nebo spínání kódového zámku, informování uživatele o zmeškaných hovorech pomocí e-mailů apod.

Seznam uživatelů je organizovaný jako tabulka obsahující až 10 000 pozic – každému uživateli je přiřazena obvykle právě jedna pozice. Seznam uživatelů obsahuje informace o uživatelích, kteří mají mít přístup do objektu pomocí RFID karty.

Jestliže používáte externí čtečku karet připojenou k interkomu pomocí rozhraní wiegand, dochází při přenosu ID karty pomocí toho rozhraní ke zkrácení ID na 6 nebo 8 znaků (podle nastavení režimu přenosu). Pokud přiložíte stejnou kartu k interní čtečce, obdržíte ID kompletní, které je obvykle delší – 8 znaků a více. Posledních 6 příp. 8 znaků ID je však shodných. Toho se využívá při porovnání ID karet s databází v interkomu – pokud porovnávaná ID mají různou délku, porovnávají se od konce a shoda musí být nalezena nejméně v 6 znacích. Pokud jsou ID stejně dlouhá, porovnávají se všechny znaky. Tímto mechanismem je dosaženo vzájemné kompatibility interní a externí čtečky.

Všechny karty přiložené k interní čtečce nebo přijaté pomocí rozhraní wiegand jsou zaznamenávány a posledních 10 přiložených karet si můžete zobrazit v menu **Stav / Historie přístupů**. V seznamu můžete kromě ID karet nalézt také jejich typ, čas přiložení a příp. další informace. V případě malého systému můžete využít pro zadávání ID karet jednoduchý trik – přiložte kartu ke čtečce interkomu a vyhledejte ji v záložce **Historie přístupů**. ID karty označte pomocí myší, např. dvojklikem na ID karty, a stiskněte klávesy CTRL+C. Nyní máte ID karty ve schránce a pomocí kláves CTRL+V je můžete vložit do libovolného políčka v nastavení interkomu.

Po přiložení karty k RFID čtečce je ID karty porovnáno s databází karet v interkomu. Pokud ID přiložené karty odpovídá jedné z karet v databázi, je provedena příslušná akce – aktivace spínače (odemknutí elektrického zámku dveří apod.). Číslo aktivovaného spínače můžete změnit v nastavení **Hardware / Čtečka karet** pomocí parametru Asociovaný spínač, případně v nastavení **Hardware / Moduly** pomocí parametru **Asociovaný spínač** u modulu čtečky karet.



Funkce Vyhledávání v adresáři funguje jako fulltextové vyhledávání ve jméně, telefonních číslech a emailu. Vyhledává všechny shody v celém seznamu. Ikona

slouží k vytvoření nového uživatele, pro zobrazení detailu nastavení uživatele slouží ikona

. Pro nastavení zobrazení sloupců tabulky slouží ikona

, defaultní nastavení tabulky zobrazuje jméno, e-mail uživatele a jeho nastavené přístupy. Pro odebrání uživatele ze seznamu, kdy se smažou všechny jeho zadané údaje, slouží ikona

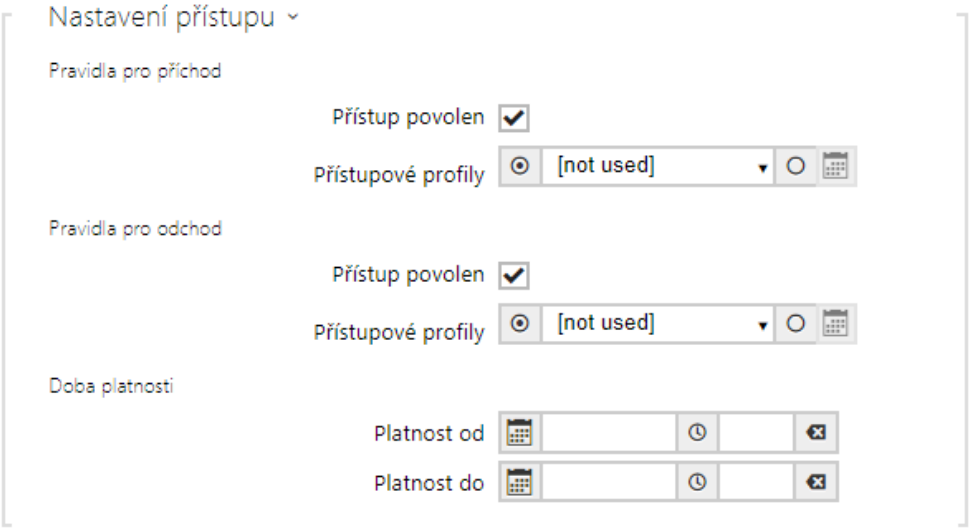
. Ve sloupci pro přístupy se zobrazují ikony

popisující aktivní autentizace uživatele.

Každý záznam v seznamu uživatelů obsahuje následující údaje:

Každý záznam v seznamu uživatelů obsahuje následující údaje:

- **Jméno** – nepovinný údaj sloužící pro lepší orientaci v seznamu, např. při vyhledávání uživatelů.
- **Fotografie** – umožňuje nahrát fotografii uživatele. Po kliknutí na rámeček pro vložení fotografie se zobrazí Editor fotografií, který umožní nahrát vybranou fotografii ze souboru, případně vytvořit fotografii uživatele integrovanou kamerou. Fotografii lze nahrát ve formátu typu .jpg, .png a .bmp. Tato funkce je dostupná pouze pro modely s displejem.
- **E-mail** – adresa uživatele pro odeslání informace o zmeškaném hovoru pomocí e-mailu.



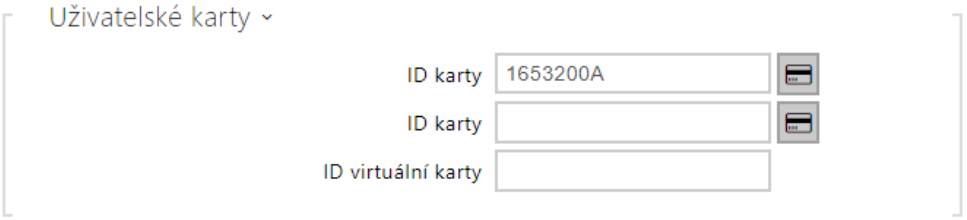
- **Pravidla pro příchod**
  - **Přístup povolen** – povoluje autentizaci na tomto přístupovém bodu.
  - **Přístupové profily** – nabízí výběr z předdefinovaných profilů z Adresář / Časové profily nebo manuální nastavení časového profilu přímo pro tento prvek.
- **Pravidla pro odchod**
  - **Přístup povolen** – povoluje autentizaci na tomto přístupovém bodu.
  - **Přístupové profily** – nabízí výběr z předdefinovaných profilů z Adresář / Časové profily nebo manuální nastavení časového profilu přímo pro tento prvek.
- **Doba platnosti**

- **Platnost od** – umožňuje nastavit začátek platnosti nastaveného přístupu.
- **Platnost do** – umožňuje nastavit konec platnosti nastaveného přístupu.

Každý z uživatelů může mít přiřazen vlastní soukromý kód pro sepnutí spínače. Uživatelské kódy spínačů lze libovolně kombinovat s univerzálními kódy spínačů zadanými v menu **Hardware / Spínače**. Pokud se kódy překrývají s jinými kódy již zadanými v konfiguraci interkomu, pak se u takto kolidujících kódů objeví značka

.

- **PIN kód** – umožňuje nastavit osobní numerický přístupový kód uživatele. Kód musí obsahovat alespoň dva znaky.
- **Spínač 1-2** – umožňuje nastavit soukromý kód uživatele pro sepnutí spínače. Kód může být až 16 znaků dlouhý a může obsahovat pouze číslice 0–9. Kód musí obsahovat alespoň dva znaky pro odemknutí dveří z klávesnice interkomu a minimálně jeden znak pro odemknutí dveří pomocí DTMF z telefonu.



Každý z uživatelů interkomu může mít přiřazené dvě přístupové RFID karty.

- **ID karty** – umožňuje nastavit ID přístupové karty uživatele. Každý uživatel může mít přiřazené max. dvě přístupové karty. ID přístupové karty je sekvence 6–32 znaků z množiny 0–9, A–F. Po přiložení platné karty ke čtečce dojde k sepnutí spínače asociovaného s příslušnou čtečkou karet. V případě, že je navolen režim dvojité autentizace, dojde k sepnutí spínače daného zadaným numerickým kódem po přiložení karty.
- **ID virtuální karty** – umožňuje nastavit ID virtuální přístupové karty uživatele. Každý uživatel může mít přiřazenou 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. Po

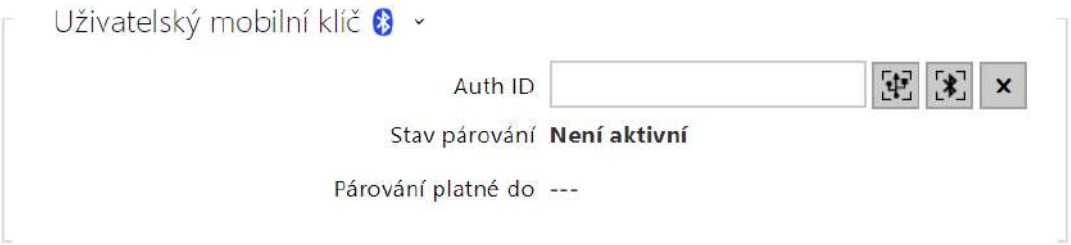
identifikaci uživatele se ID virtuální karty na Bluetooth nebo Biometrické čtečce odesílá na rozhraní Wiegand pokud je v konfiguraci (Dveře / Pravidla pro příchod / Pokročilé nastavení) nastaveno odesílání identifikátorů na Wiegand.

- Patra – výběr pater přístupných pro uživatele.
- Časový profil – nabízí výběr jednoho či více časových profilů zároveň, které se uplatní. Samotné nastavení časových profilů je možné v sekci Adresář / Časové profily.
  - 

    označením se nastavuje výběr z předdefinovaných profilů nebo manuální nastavení časového profilu pro daný prvek.
  - 

    označením se nastavuje časový profil přímo pro daný prvek.



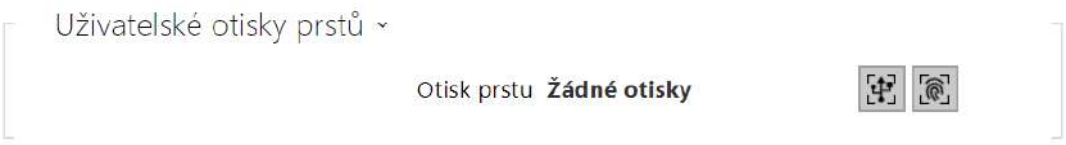
- Auth ID – jednoznačný identifikátor mobilního zařízení (resp. jeho uživatele). Hodnota parametru je automaticky vygenerovaná při párování. Auth ID lze přesunout k jinému uživateli, příp. je možné jej zkopírovat do jiného zařízení v rámci stejné lokace.
- Stav párování – aktuální stav párování (Není aktivní, Čekání na spárování, Platnost PINu vypršela nebo Spárováno).
- Párování platné do – datum a čas konce platnosti vygenerovaného autorizačního PINu.
  -  spárovat přes USB čtečku
  -  spárovat přes toto zařízení

- smazat Auth ID

Párování pomocí Bluetooth modulu v interkomu

Postup pro spárování mobilního telefonu s uživatelem je následující:

1. U vybraného uživatelského účtu zahájíme párování stisknutím tlačítka u položky Auth ID.
2. Objeví se dialogové okno s kódem PIN.
3. V aplikaci 2N® Mobile Key najdeme příslušnou čtečku a stiskneme tlačítko Start pairing.
4. Do pole pro vstup zadáme kód z bodu 2.
5. Párování je dokončeno.



- Otisky prstu – zobrazuje počet nastavených otisků prstů, nastavit lze až 2 různé otisky prstů. Tato sekce se zobrazuje pouze při přítomnosti modulu Biometrické čtečky.
  - načtení prstu přes USB čtečku
  - načíst přes modul čtečky otisků prstů

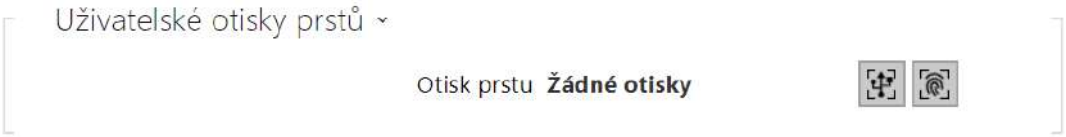
Upozornění

- Kapacita nahraných uživatelských otisků prstů je limitována na max. 2000 pro jedno zařízení.

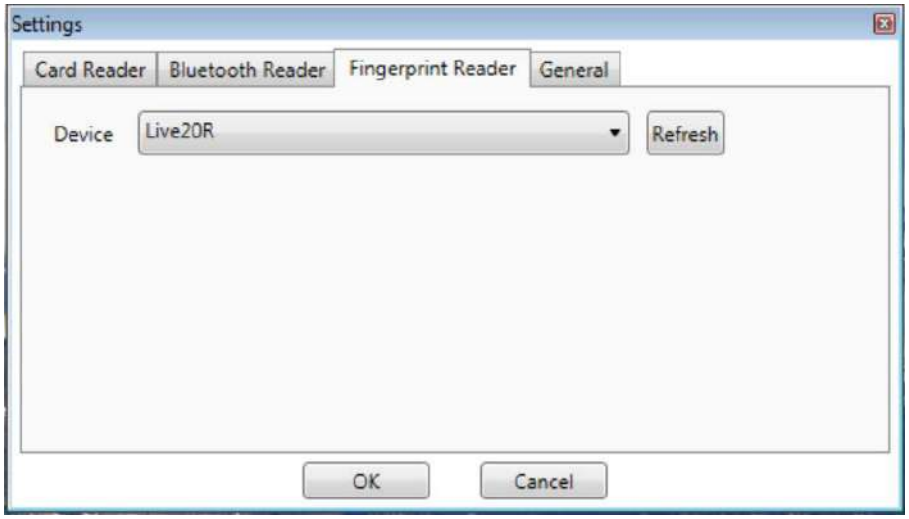
Pokyny pro nastavení uživatelských otisků prstů

Načítat otisky prstů je možné přes 2N® Access Unit Biometrickou čtečku otisku prstů (obj.č. 916019) nebo externí USB čtečku otisků prstů (obj. č. 9137423E). Postup je následující:

1a) Načtení přes modul **2N® Access Unit Biometrická čtečka otisku prstů** lze provést přes webové rozhraní zařízení u konkrétního uživatele v sekci Adresář / Uživatelé / Uživatelské otisky prstů zvolením Načíst přes modul čtečky otisků prstů  .



1b) Načtení přes externí USB čtečku otisků prstů lze provést pomocí **2N® IP USB Driveru**, v jeho nastavení vyberte Fingerprint Reader (čtečka otisků prstů) a potvrďte tlačítkem OK. Na webovém rozhraní zařízení u konkrétního uživatele v sekci Adresář / Uživatelé / Uživatelské otisky prstů zvolte Načíst přes modul čtečky otisků prstů  .

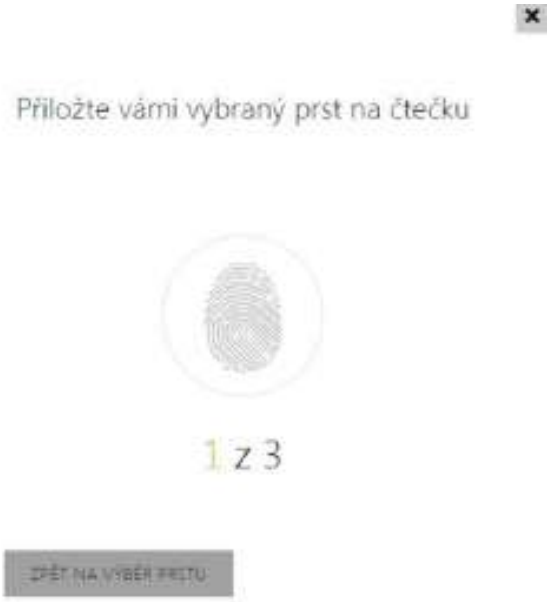


2) Kliknutím vyberte prst k nahrání otisku.

Pro jednoho uživatele lze nastavit až dva otisky prstů.

3) Pro nahrání otisku prstu klikněte na tlačítko SKENOVAT PRST.

4) Přiložte vámi vybraný prst na externí USB čtečku. Pro vyšší přesnost se tento proces opakuje, celkem třikrát.



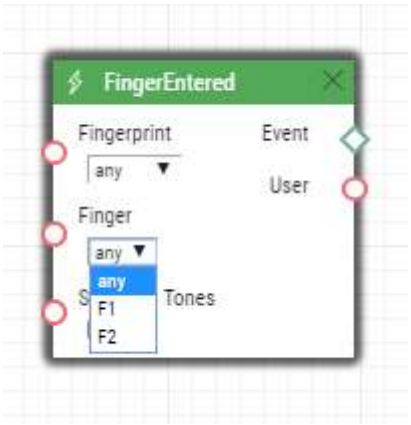
V případě neshody načtení otisků prstů proces opakujte.

5) Pokud skenování prstů proběhlo v pořádku, nastavení potvrďte kliknutím na tlačítko HOTOVO.

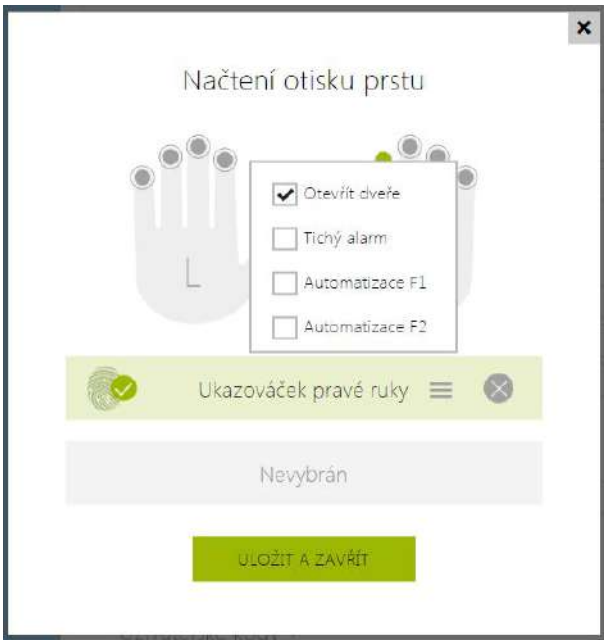
Pro nastavení funkce prstu klikněte na ikonu menu

, zobrazí se nabídka dostupných funkcí:

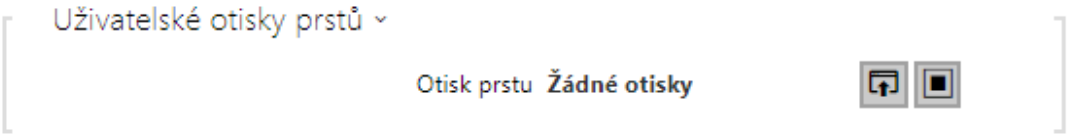
- Otevřít dveře
- Tichý alarm. Lze nastavit pouze v případě aktivní funkce Otevření dveří.
- Automatizace F1 – generuje událost FingerEntered v Automation. F1 slouží k rozlišení přiloženého prstu v Automation.
- Automatizace F2 – generuje událost FingerEntered v Automation. F2 slouží k rozlišení přiloženého prstu v Automation.



Po nastavení otisků prstů a jejich funkcí proces potvrďte kliknutím na ULOŽIT A ZAVŘÍT.



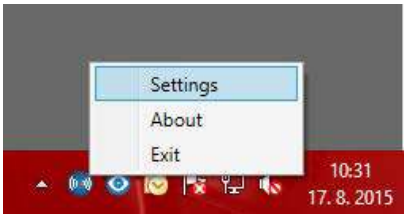
6) V záložce Uživatelé je možné zkontrolovat aktuální nastavení.



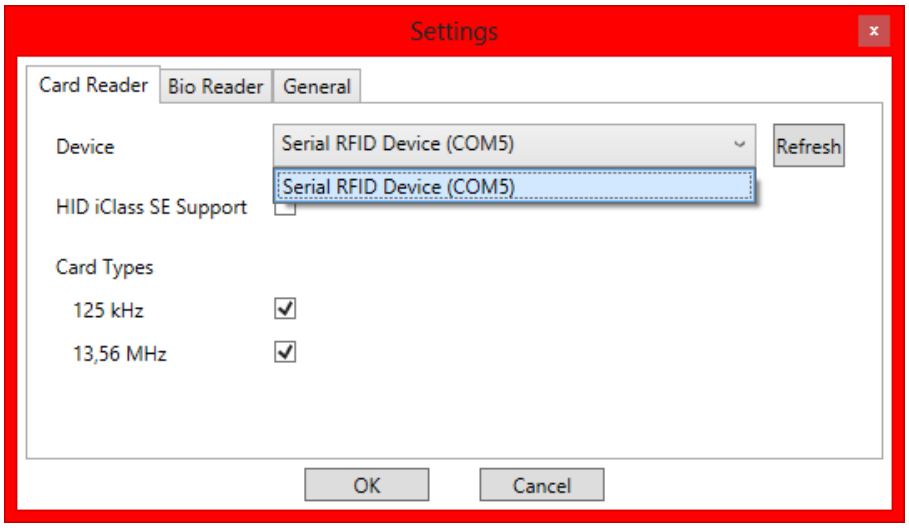
USB RFID čtečka karet

Načítat ID karet je možné přes USB RFID čtečku. Postup je následující:

1. Jděte do nastavení **2N® IP USB Driver**

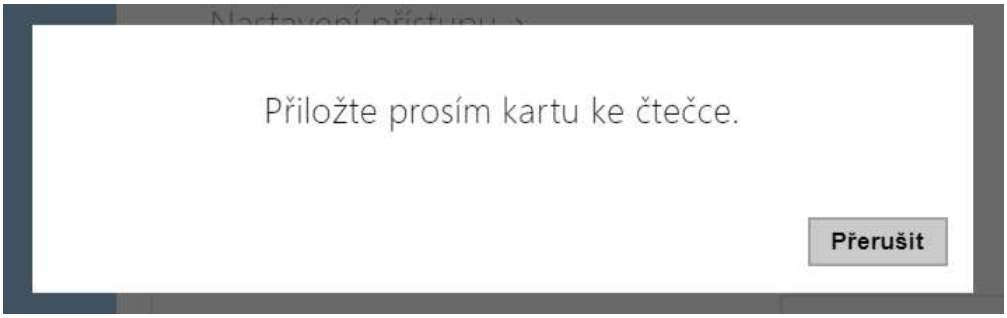


2. Nastavte COM port připojené čtečky



3. Na webu **2N Acess Unit** u uživatele zmáčkněte tlačítko načtení karty

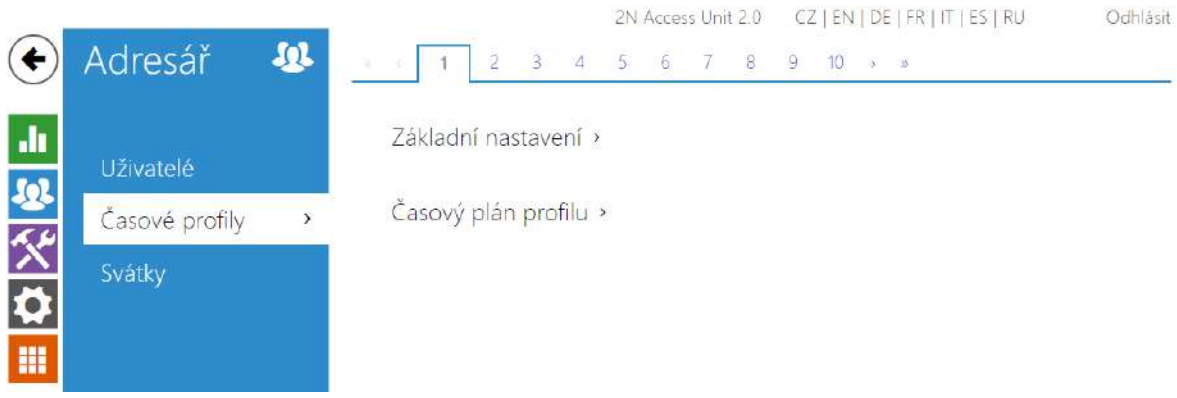
Přiložte kartu na čtečku



4. Karta je načtená

Nezapomeňte konfiguraci uložit.

5.2.2 Časové profily



Vybrané funkce přístupového terminálu, jako je např. přístup pomocí RFID karty nebo numerického kódu, lze časově omezit. Uvedeným funkcím lze přiřadit tzv. **časový profil**, který určuje, kdy je daná funkce dostupná a kdy ne. Časovými profily lze řešit následující požadavky:

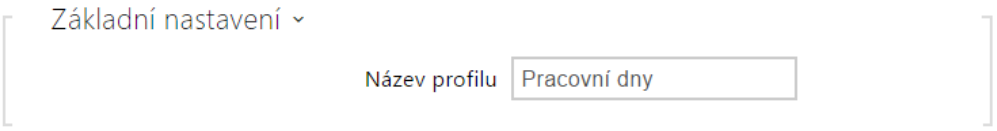
- zcela blokovat volání na vybraného uživatele mimo vyhrazený čas
- blokovat volání na vybraná telefonní čísla uživatele mimo vyhrazený čas
- blokovat přístup pomocí RFID karty uživatele mimo vyhrazený čas
- blokovat přístup pomocí vybraného numerického kódu mimo vyhrazený čas
- blokovat sepnutí spínače 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. **2N Access Unit** umožňuje vytvořit až 20 různých časových profilů. Dané funkci můžete přiřadit libovolný vytvořený časový profil, viz nastavení Uživatelé, Přístupové karty, Spínače.

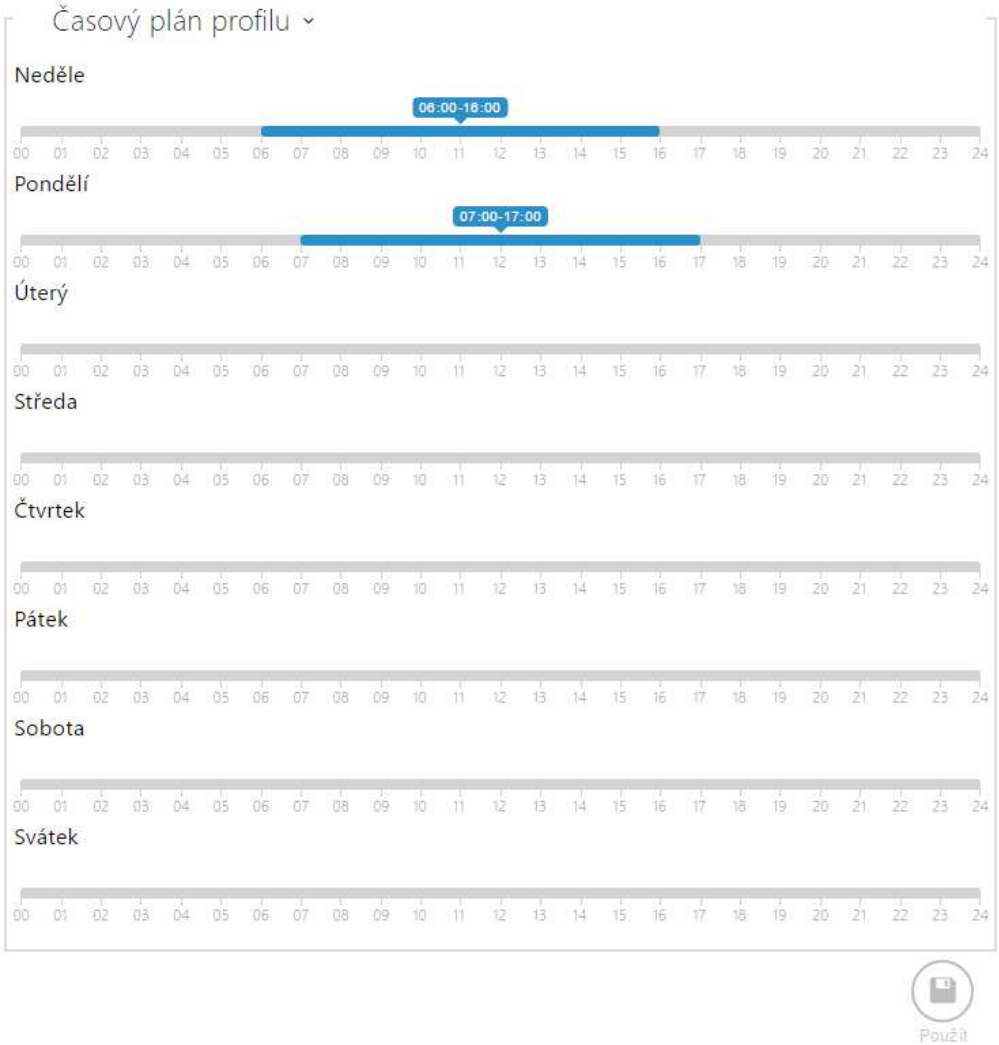
Platnost časového profilu můžete řídit nejen nastavením týdenního kalendáře, ale i pomocí speciálních aktivačních a deaktivačních kódů přiřazených danému profilu. Aktivační a deaktivační kódy lze kdykoli zadat pomocí numerické klávesnice interkomu. Tímto způsobem lze manuálně aktivovat příp. deaktivovat některé z funkcí např. při příchodu nebo odchodu z objektu.

Nastavení časových profilů se nachází v menu **Adresář / Časové profily**.

Seznam parametrů



- **Název profilu** – vámi zvolený název profilu. Tento parametr je nepovinný a slouží pouze pro jednodušší orientaci v seznamu profilů a pro snadnější výběr profilu v nastavení spínačů, karet a telefonních čísel.



Slouží k nastavení času aktivního profilu v rámci týdenní periody. Profil je aktivní, pokud aktuální čas spadá do nastavených intervalů.

V případě, že daný den je označen jako svátek (viz nastavení **Adresář / Svátky**), pak se bez ohledu na to, jaký je den v týdnu, uplatní poslední řádek tabulky označený jako Svátek.

Pro správné použití této funkce je nezbytné, aby zařízení mělo správně nastavený aktuální čas (viz kapitola Datum a čas).

Poznámka

- *V rámci jednoho dne lze nastavit libovolný počet intervalů např. 8:00–12:00, 13:00–17:00, 18:00–20:00.*
- *Pokud chcete, aby profil byl aktivní celý den, vložte jeden interval pokrývající celý den, tj. 00:00–24:00*

5.2.3 Svátky

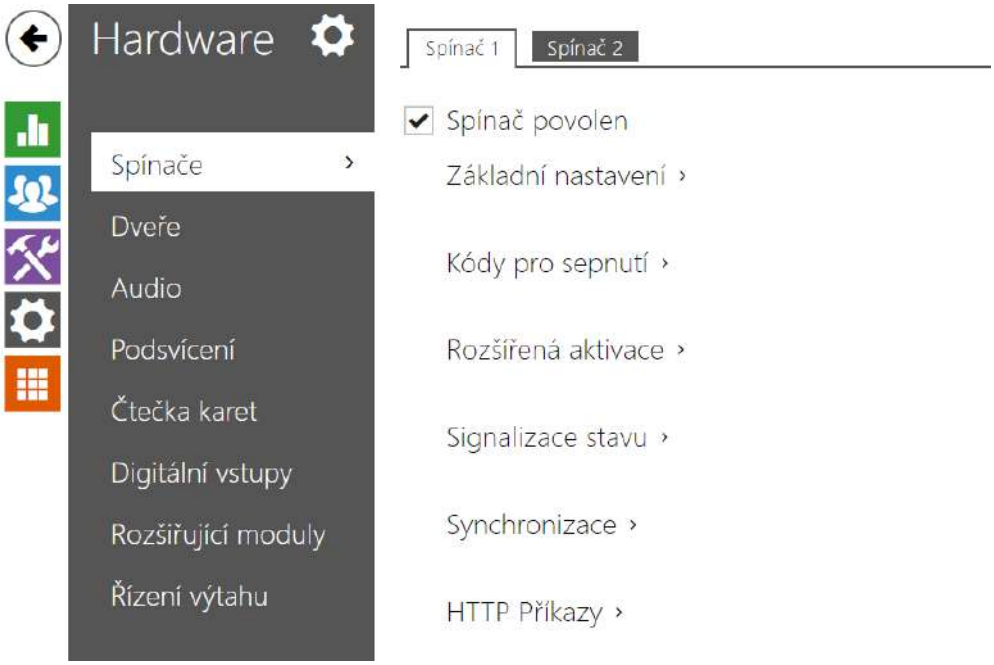
Na této stránce se nastavují dny, na které připadá svátek (příp. den pracovního klidu). Pro dny, na které připadá svátek, lze v časovém profilu nastavit odlišné časové intervaly než pro ostatní dny.

Svátky lze nastavit až na následujících 10 let dopředu (rok lze zvolit kliknutím na číslo roku v horní části stránky). Na stránce je zobrazen kalendář pro celý rok. Kliknutím na kalendářní den se označí nebo zruší svátek. Pravidelné svátky (opakující se každý rok ve stejný kalendářní den) jsou označeny zelenou barvou. Nepravidelné svátky (připadající na konkrétní kalendářní den pouze daném roce) jsou označeny modrou barvu. První kliknutí označí den jako pravidelný svátek, následující kliknutí označí den jako nepravidelný svátek a další kliknutí den ze seznamu svátků vyjme.

5.3 Hardware

Zde je přehled toho, co v kapitole naleznete:

5.3.1 Spínače



Spínače umožňují velmi flexibilní řízení různých periferií připojených k **2N Access Unit** (jako jsou elektrické dveřní zámky, osvětlení, doplňková signalizace zvonění apod.). **Zařízení** umožňuje nakonfigurovat 2 nezávislé spínače, které lze použít k libovolnému účelu.

Spínač může být aktivován:

- zadáním platného kódu na numerické klávesnici přístupového terminálu
- přiložením platné RFID karty ke čtečce
- s definovaným zpožděním od sepnutí jiného spínače
- časovým profilem
- přijetím HTTP příkazu z jiného zařízení v síti 1)
- pomocí automatizace pomocí akce Action.ActivateSwitch

Pokud je potřeba, aktivaci spínače lze blokovat pomocí zvoleného časového profilu.

Pokud je spínač aktivní, lze nastavit:

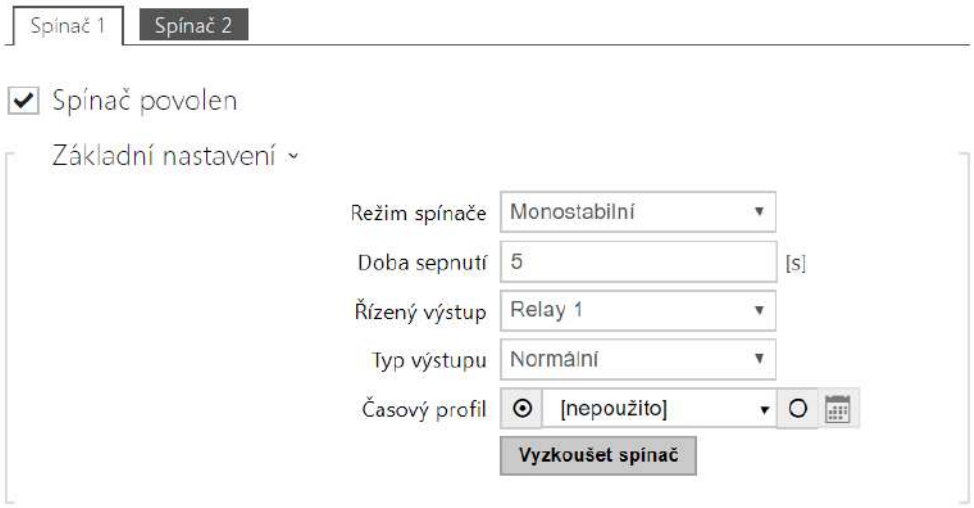
- sepnutí libovolného logického výstupu přístupového terminálu (relé, výkonový výstup)
- sepnutí výstupu, na který je připojen modul **2N® IP Bezpečnostní relé**
- odeslání HTTP příkazu jinému zařízení

Spínač může pracovat v monostabilním anebo bistabilním režimu. V monostabilním režimu je spínač automaticky vypnut po nastavené době. V bistabilním režimu je spínač první aktivací zapnut a další vypnut.

Spínač může signalizovat svůj stav pomocí:

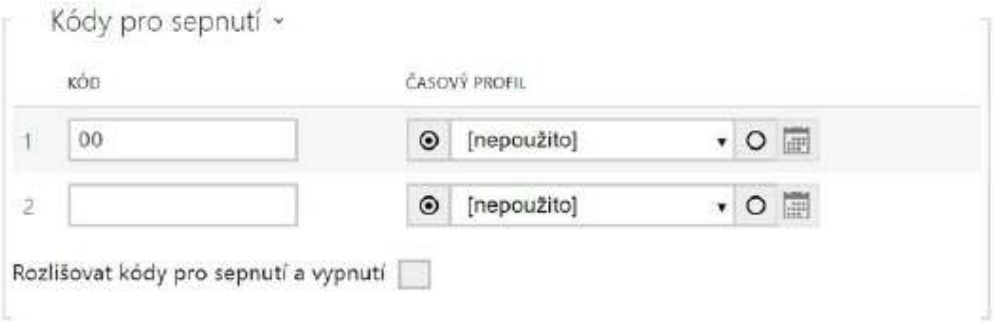
- konfigurovatelného pípnutí
- signalizační LED diodou

Seznam parametrů



- **Spínač povolen** – globálně povoluje nebo zakazuje řízení spínače. Pokud spínač není povolen, nelze jej sepnout žádným ze zadaných kódů (včetně uživatelských kódů spínačů), nelze jej aktivovat tlačítkem rychlé volby.
- **Režim spínače** – nastavuje monostabilní nebo bistabilní režim spínače. V monostabilním režimu je spínač automaticky vypnut po nastavené době sepnutí. V bistabilním režimu se spínač první aktivací zapne a druhou vypne.
- **Doba sepnutí** – nastavuje dobu sepnutí spínače v monostabilním režimu. V bistabilním režimu spínače se nastavená doba sepnutí neuplatní.
- **Řízený výstup** – umožňuje přiřadit spínači elektrický výstup. Lze vybrat mezi všemi dostupnými výstupy příslušného modelu interkomu – relé, výkonové výstupy, výstupy na rozšiřujících modulech apod. Pokud zvolíte volbu **žádný**, spínač nebude ovládat žádný elektrický výstup, můžete jej stále však použít pro řízení externího zařízení pomocí HTTP příkazů.
- **Typ výstupu** – pokud používáte **2N® IP Interkom Bezpečnostní relé**, nastavte typ výstupu na hodnotu **security**. V režimu **security** výstup pracuje v inverzním režimu, tj. je stále sepnutý, a modul **2N® IP Interkom Bezpečnostní relé** ovládá pomocí specifické sekvence pulzů. Pokud používáte reverzní zámek dveří (tj. dveře jsou při přivedení napětí na zámek uzamčeny), nastavte typ výstupu na hodnotu **inverzní.**

- **Časový profil** – umožňuje přiřadit spínači předdefinovaný časový profil nebo manuálně nastavit časový profil, který povoluje sepnutí spínače. Pokud přiřazený časový profil není aktivní, nelze spínač sepnout pomocí kódu, nelze jej aktivovat hovorem ani tlačítkem rychlé volby.
- **Tlačítko „Vyzkoušet spínač“** – umožňuje ručně aktivovat spínač pro ověření jeho funkce, například elektrického zámku nebo jiného připojeného zařízení.

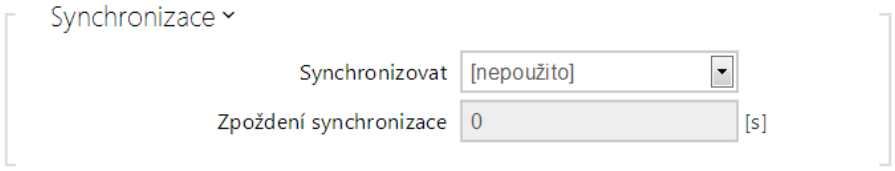


Seznam univerzálních kódů, pomocí kterých lze z klávesnice přístupového terminálu aktivovat spínače. Pro každý spínač lze zadat až 10 univerzálních kódů.

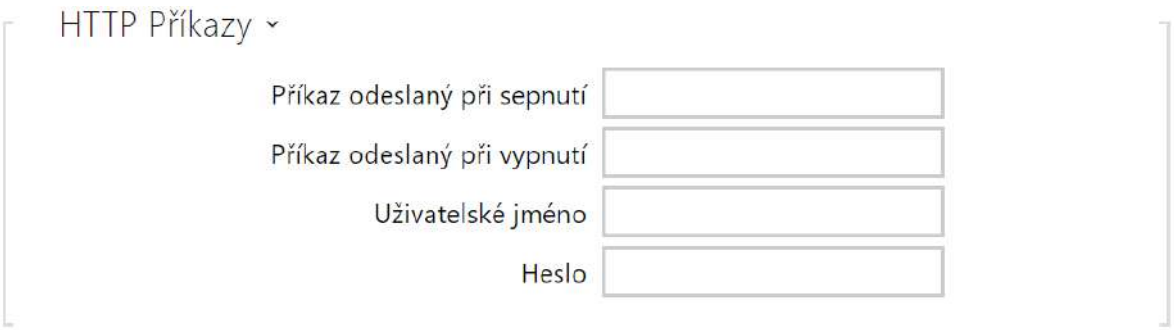
- **Kód** – umožňuje zadat číselný kód spínače. Kód musí obsahovat alespoň dva znaky pro odemknutí dveří z klávesnice interkomu a minimálně jeden znak pro odemknutí dveří pomocí DTMF z telefonu. Doporučujeme použít alespoň čtyři znaky. Kódy 00 a 11 nelze zadávat z numerické klávesnice. Kód se potvrzuje znakem *. Kód může být až 16 znaků dlouhý.
- **Časový profil** – umožňuje přiřadit ke kódu spínače časový profil a tak řídit jeho platnost.
- **Rozlišovat kódy pro sepnutí a vypnutí** – umožňuje nastavit režim kódů spínačů, kdy liché kódy (1., 3., atd.) jsou určeny pro sepnutí a sudé kódy (2., 4., atd) jsou pro vypnutí spínače. Tento režim lze použít pouze, pokud je spínač nastaven do bistabilního režimu.

- **Aktivace časovým profilem** – aktivuje spínač podle časového profilu. Spínač zůstane zapnutým v době platnosti zvoleného časového profilu.

- **Zvuková signalizace** – umožňuje nastavit typ zvukové signalizace při sepnutí spínače. Je možné vybrat mezi Krátkým tónem, Dlouhý tónem (po celou dobu sepnutí) a uživatelským zvukem, viz kapitola Uživatelské zvuky.



- **Synchronizovat** – povoluje funkci synchronizace spínače, která umožňuje automatické sepnutí spínače po nastavené době od okamžiku sepnutí jiného spínače. Délku intervalu mezi sepnutím spínačů určuje parametr **Zpoždění synchronizace**.
- **Zpoždění synchronizace** – nastavuje délku intervalu mezi synchronizovaným sepnutím dvou spínačů. Parametr se neuplatní, pokud není povolena funkce **Synchronizovat**.



- **Příkaz odeslaný při sepnutí** – umožňuje nastavit příkaz odesílaný externímu zařízení (např. WEB relé) při sepnutí spínače. Příkaz se odesílá pomocí protokolu HTTP (GET request). Příkaz musí být ve tvaru **http://ip_adresa/cesta**. Např. **http://192.168.1.50/relay1=on**.
- **Příkaz odeslaný při vypnutí** – umožňuje nastavit příkaz odesílaný externímu zařízení (např. WEB relé) při vypnutí spínače. Příkaz se odesílá pomocí protokolu HTTP (GET request). Příkaz musí být ve tvaru **http://ip_adresa/cesta**. Např. **http://192.168.1.50/relay1=off**
- **Uživatelské jméno** – jméno uživatele pro autentizaci připojení k externímu zařízení (WEB relé atd.). Parametr je povinný pouze tehdy, pokud externí zařízení vyžaduje autentizaci.
- **Heslo** – heslo pro autentizaci připojení k externímu zařízení (WEB relé atd.). Parametr je povinný pouze tehdy, pokud externí zařízení vyžaduje autentizaci.

Tip

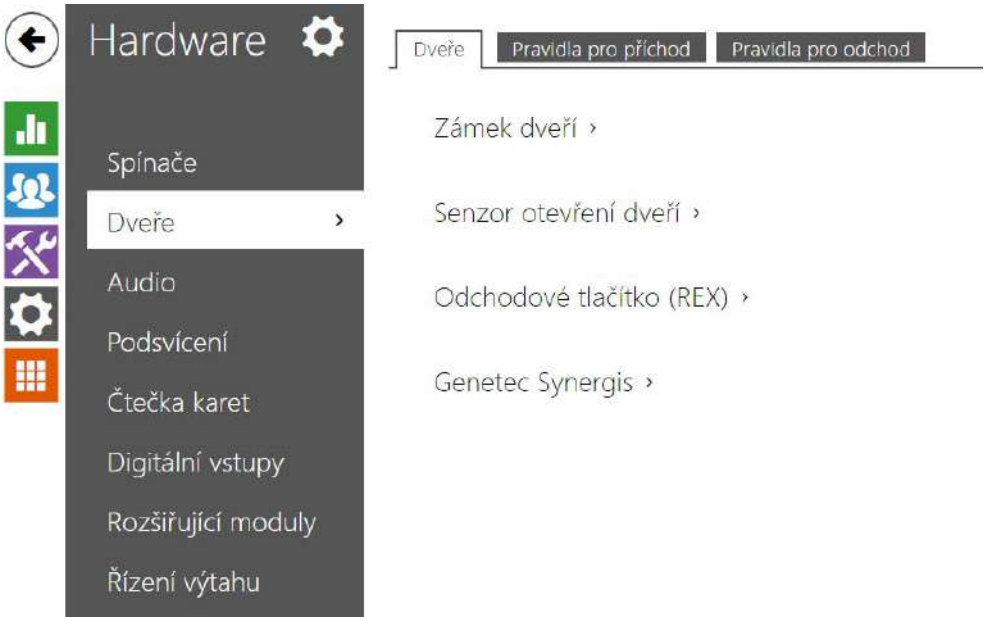
V případě použití externího relé **obj.č.: 9137410E** jsou použity následující HTTP příkazy:

- Pro trvalé sepnutí – http://ip_adresa/state.xml?relayState=1 (např.: http://192.168.1.10/state.xml?relayState=1)
- Pro sepnutí na předdefinovaný čas (defaultně 1,5 s) – http://ip_adresa/state.xml?relayState=2 (např.: http://192.168.1.10/state.xml?relayState=2)
- Pro vypnutí – http://ip_adresa/state.xml?relayState=0 (např.: http://192.168.1.10/state.xml?relayState=0)

V případě použití externího relé **obj.č.: 9137411E** jsou použity následující HTTP příkazy (znak X v příkazech je třeba nahradit číslem relé):

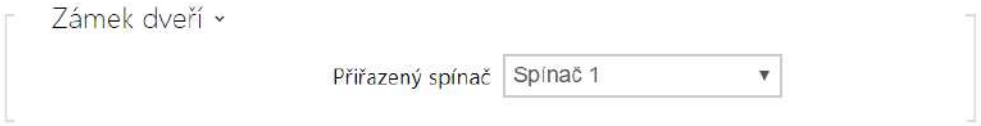
- Pro trvalé sepnutí – http://ip_adresa/state.xml?relayXState=1 (např.: http://192.168.1.10/state.xml?relay1State=1)
- Pro sepnutí na předdefinovaný čas (defaultně 1,5 s) – http://ip_adresa/state.xml?relayXState=2 (např.: http://192.168.1.10/state.xml?relay1State=2)
- Pro vypnutí – http://ip_adresa/state.xml?relayXState=0 (např.: http://192.168.1.10/state.xml?relay1State=0)

5.3.2 Dveře

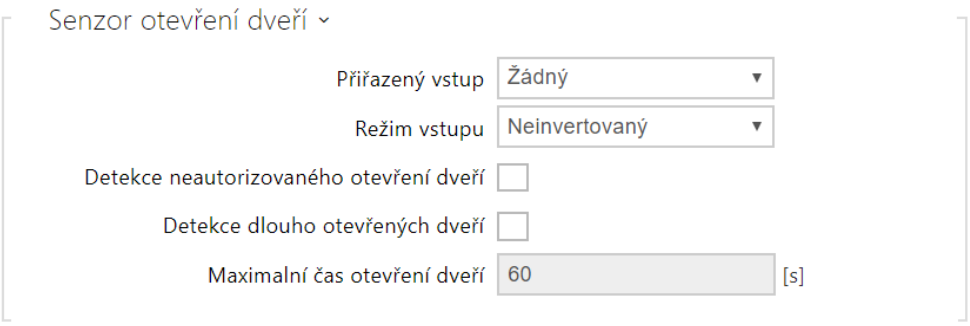


Seznam parametrů

Záložka Dveře



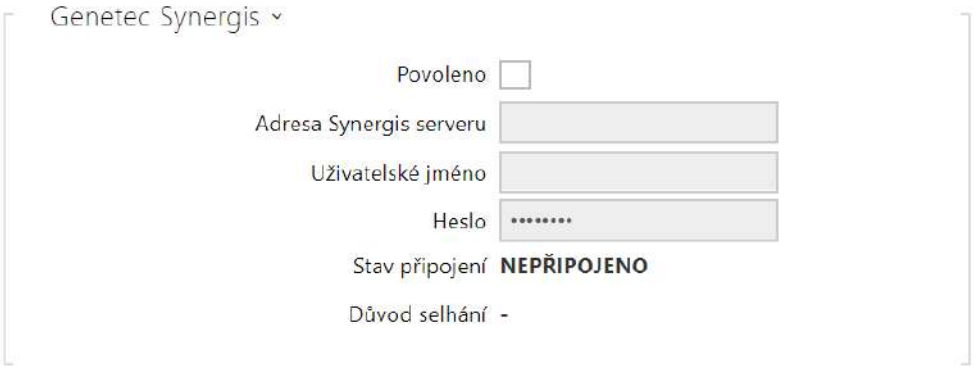
- **Přiřazený spínač** – Umožňuje vybrat spínač určený pro ovládání elektromagnetického zámku dveří. Podle stavu tohoto spínače se řídí signalizace odemknutí dveří (zelený symbol dveří, zelená LED).



- **Přiřazený vstup** – Umožňuje určit jeden z logických vstupů (příp. žádný vstup) pro detekci otevřených dveří.

- **Režim vstupu** – Umožňuje nastavit aktivní úroveň (polaritu) vstupu. Neinvertovaný / Invertovaný.
- **Detekce neautorizovaného otevření dveří** – Umožňuje detekovat otevření dveří při zamčeném zámku.
- **Detekce dlouho otevřených dveří** – Umožňuje detekovat dlouho otevřené dveře.
- **Maximální čas otevření dveří** – Maximální povolená doba otevřených dveří v sekundách.

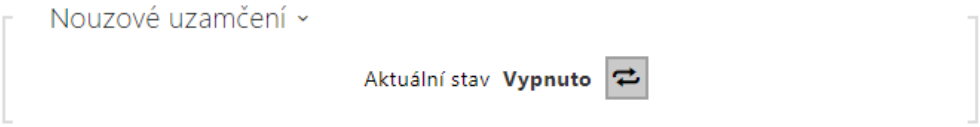
- **Přiřazený vstup** – Umožňuje určit jeden z logických vstupů (příp. žádný vstup) pro funkci odchodového tlačítka. Aktivací vstupu odchodového tlačítka dojde k sepnutí zvoleného spínače. Doba a způsob sepnutí jsou dány aktuálním nastavením zvoleného spínače.
- **Režim vstupu** – Umožňuje nastavit aktivní úroveň (polaritu) vstupu. Neinvertovaný / Invertovaný.



- **Povoleno** – Povoluje spojení s externím bezpečnostním systémem Genetec Synergis.
- **Adresa Synergis serveru** – IP adresa nebo doménové jméno Synergis Serveru.
- **Uživatelské jméno** – Uživatelské jméno používané při autenzizaci.
- **Heslo** – Heslo používané při autentizaci.
- **Stav připojení** – Zobrazuje aktuální stav připojení k Synergis serveru, příp. popis chybového stavu.
- **Důvod selhání** – Zobrazuje důvod selhání posledního pokusu o připojení k Synergis serveru – zobrazuje poslední chybovou odpověď, např. Připojení k serveru selhalo.

Záložka Pravidla pro příchod

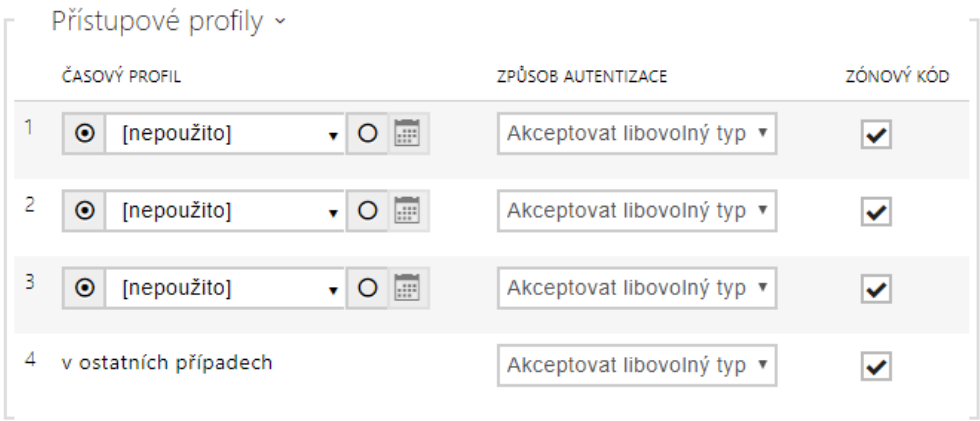
- **Přístup povolen** – Povoluje jakýkoliv přístup z konkrétní strany dveří (příchod, odchod). Pokud není přístup povolen, není možno dveře z této strany otevřít.



- **Zamykání dveří** – Zobrazuje aktuální nastavení zamykání dveří. Odemknuto /Uzamknuto.

Upozornění

- Nouzové uzamčení je nadřazené všem časovým a přístupovým profilům.

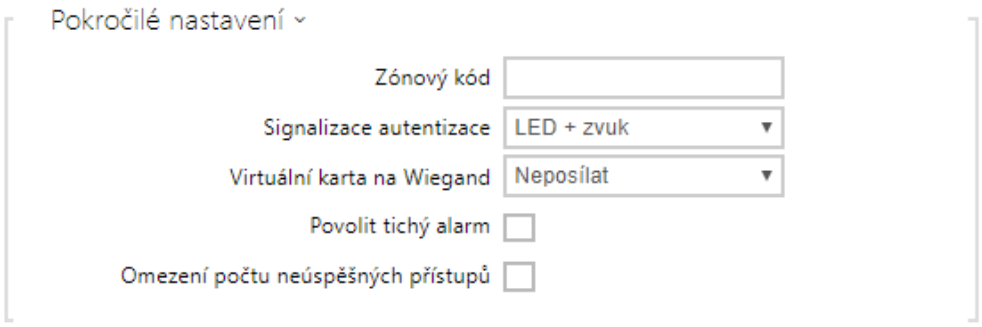


- **Časový profil** – Nabízí výběr jednoho či více časových profilů zároveň, které se uplatní. Samotné nastavení časových profilů je možné v sekci Adresář / Časové profily.
  - označením se nastavuje výběr z předdefinovaných profilů nebo manuální nastavení časového profilu pro daný prvek.

- Způsob autentizace – Nastavuje způsob autentizace (Bluetooth, otisk prstu, přístupová karta, numerický kód) v době platnosti časového profilu v tomto řádku včetně možnosti vícenásobné autentizace pro zvýšenou bezpečnost. Možností ´Přístup odepřen´ lze přístup zcela zakázat.
- Zónový kód – Povoluje zónový kód pro kombinaci časového profilu a způsobu autentizace v tomto řádku. Zónový kód je pak možno použít místo PIN kódu uživatele.

Upozornění

- Pokud není časový profil nastaven, způsob autentizace je na daném řádku ignorován.

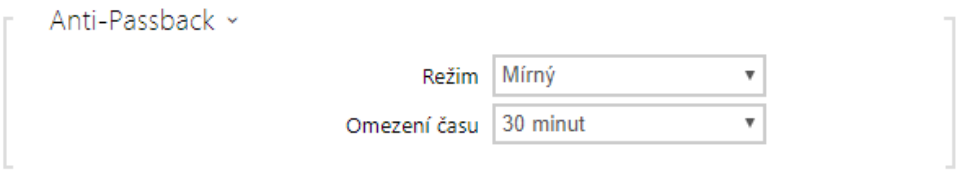


- **Zónový kód** – Umožňuje zadat numerický kód spínače. Kód musí obsahovat alespoň dva znaky, ale doporučujeme použít nejméně čtyři znaky.
- **Signalizace autentizace** – Volí signalizaci přečtené karty nebo jiného identifikátoru. Volby jsou Pouze LED (světelná signalizace), nebo LED + zvuk (světelná a zvuková signalizace), vždy po přečtení karty, bez rozlišení platné a neplatné karty.
- **Virtuální karty na wiegand** – Umožňuje zvolit Wiegand výstup, na který bude odesláno číslo virtuální karty uživatele po jeho úspěšné autentizaci. Lze použít s libovolným způsobem autentizace včetně kódů, otisků prstu apod.
- **Povolit tichý alarm** – Každému přístupovému kódu je přidělen jeden virtuální kód, který je o jedničku vyšší než přístupový a je určený pro aktivaci tichého alarmu. Například, máme-li přístupový kód 0000 pak kód pro aktivaci tichého alarmu je 0001. Délka kódu musí být zachována, znamená to tedy, že například pro přístupový kód 9999 je tichý alarm 0000 a podobně. Provedenou akci pro tichý alarm je možné nastavit v sekci pro automatizaci.
- **Omezení počtu neúspěšných přístupů** – Povoluje omezení počtu neúspěšných pokusů o autentizaci. Po pěti neúspěšných pokusech o přístup (nesprávný numerický kód, neplatná karta atd.) bude přístupový modul zablokován po dobu třiceti sekund i v případě, že autentizace by byla platná.

Servisní karty jsou dvě běžné karty, pouze vámi vyhrazené pro tento speciální účel. Jejich ID musíte uvést v položkách ID přidávací karty a ID odebírací karty v této sekci. Počet znaků ID přístupové karty je dán typem karty a může se lišit. Platí však, že karty stejného typu mají ID vždy stejně dlouhé.

Pro správu karet uživatelů slouží tzv. přidávací a odebírací karty. Přiložením přidávací karty ke čtečce je poté každá následující přiložená karta přidána jako nový uživatel s přiřazenou přístupovou kartou do seznamu v Adresáři. V zařízení je automaticky vytvořen uživatel !Visitor #ID_karty. Přiložením odebírací karty ke čtečce je poté každá následující přiložená karta a její uživatel smazán ze seznamu Adresáře. Záznam o přiložené kartě bude zrušen a přístup pomocí této karty bude blokován.

- **ID přidávací karty** – ID servisní karty určené pro přidávání do seznamu instalovaných karet. ID karty je sekvence 6–32 znaků z množiny 0–9, A–F.
- **ID odebírací karty** – ID servisní karty určené pro odebírání ze seznamu instalovaných karet. ID karty je sekvence 6–32 znaků z množiny 0–9, A–F.

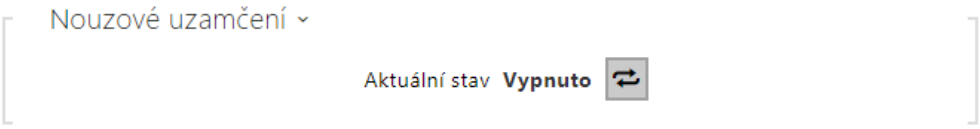


Anti-Passback je zabezpečovací funkce zabraňující použití přístupové karty nebo jiné autentizace ke vstupu do oblasti podruhé, aniž by ji předtím uživatel opustil (takže karta nemůže být předána zpět druhé osobě, která chce vstoupit).

- **Režim** – volí režim funkce Anti-Passback:
  - **Vypnuto** – funkce je defaultně vypnuta, uživatel smí použít přístupovou kartu nebo jinou autentizaci pro přístup ke vstupu do oblasti podruhé, aniž by ji předtím opustil.
  - **Mírný** – uživatel smí použít přístupovou kartu nebo jinou autentizaci pro přístup ke vstupu do oblasti podruhé, aniž by ji předtím opustil. V sekci Stav / Události bude vytvořen nový záznam typu **AccessTaken**.
  - **Přísný** – uživateli není povoleno použití přístupové karty nebo jiné autentizace pro přístup ke vstupu do oblasti podruhé, aniž by ji předtím opustil. V sekci Stav / Události bude vytvořen nový záznam typu **UserRejected**.
- **Omezení času** – volí čas omezení přístupu pro funkci Anti-Passback. Po zvolenou dobu od posledního přístupu s danou autentizací (kartou, kódem atd.) ji není možno znovu použít ve stejném směru.

Záložka Pravidla pro odchod

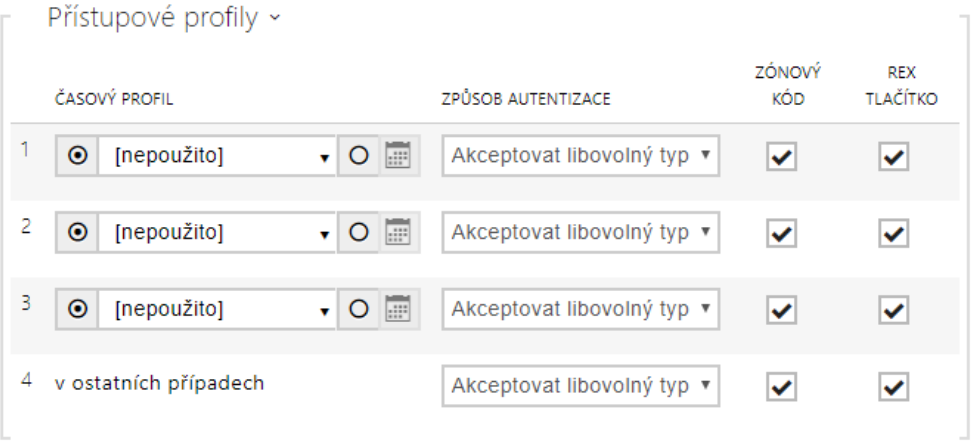
- **Přístup povolen** – Povoluje jakýkoliv přístup z konkrétní strany dveří (příchod, odchod). Pokud není přístup povolen, není možno dveře z této strany otevřít.



- **Zamykání dveří** – Zobrazuje aktuální nastavení zamykání dveří. Odemknuto /Uzamknuto.

Upozornění

- Nouzové uzamčení je nadřazené všem časovým a přístupovým profilům.

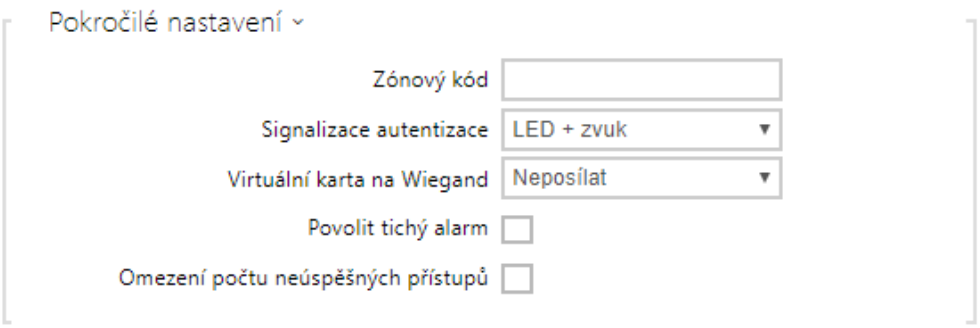


- **Časový profil** – Nabízí výběr jednoho či více časových profilů zároveň, které se uplatní. Samotné nastavení časových profilů je možné v sekci Adresář / Časové profily.
  - označením se nastavuje výběr z předdefinovaných profilů nebo manuální nastavení časového profilu pro daný prvek.

- **Způsob autentizace** – Nastavuje způsob autentizace (Bluetooth, otisk prstu, přístupová karta, numerický kód) v době platnosti časového profilu v tomto řádku včetně možnosti vícenásobné autentizace pro zvýšenou bezpečnost. Možností ´Přístup odepřen´ lze přístup zcela zakázat.
- **Zónový kód** – Povoluje zónový kód pro kombinaci časového profilu a způsobu autentizace v tomto řádku. Zónový kód je pak možno použít místo PIN kódu uživatele.
- **REX tlačítko** – Povoluje funkci odchodového tlačítka pro daný časový profil. Vstup přiřazený odchodovému tlačítku se nastavuje v sekci Hardware / Dveře, záložka Dveře.

Upozornění

- Pokud není časový profil nastaven, způsob autentizace je na daném řádku ignorován.

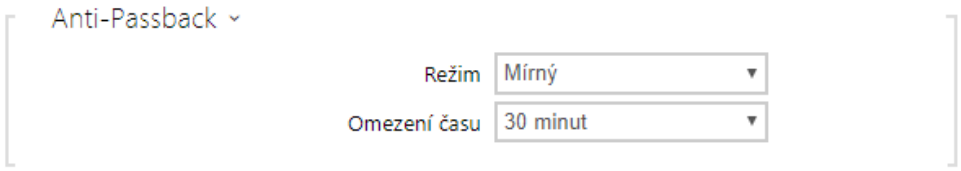


- **Zónový kód** – Umožňuje zadat numerický kód spínače. Kód musí obsahovat alespoň dva znaky, ale doporučujeme použít nejméně čtyři znaky.
- **Signalizace autentizace** – Volí signalizaci přečtené karty nebo jiného identifikátoru. Volby jsou Pouze LED (světelná signalizace), nebo LED + zvuk (světelná a zvuková signalizace, vždy po přečtení karty, bez rozlišení platné a neplatné karty).
- **Virtuální karty na wiegand** – Umožňuje zvolit Wieagnd výstup, na který bude odesláno číslo virtuální karty uživatele po jeho úspěšné autentizaci. Lze použít s libovolným způsobem autentizace včetně kódů, otisků prstu apod.
- **Povolit tichý alarm** – Každému přístupovému kódu je přidělen jeden virtuální kód, který je o jedničku vyšší než přístupový a je určený pro aktivaci tichého alarmu. Například, máme-li přístupový kód 0000 pak kód pro aktivaci tichého alarmu je 0001. Délka kódu musí být zachována, znamená to tedy, že například pro přístupový kód 9999 je tichý alarm 0000 a podobně. Provedenou akci pro tichý alarm je možné nastavit v sekci pro automatizaci.
- **Omezení počtu neúspěšných přístupů** – Povoluje omezení počtu neúspěšných pokusů o autentizaci. Po pěti neúspěšných pokusech o přístup (nesprávný numerický kód, neplatná karta atd.) bude přístupový modul zablokován po dobu třiceti sekund i v případě, že autentizace by byla platná.

Servisní karty jsou dvě běžné karty, pouze vámi vyhrazené pro tento speciální účel. Jejich ID musíte uvést v položkách ID přidávací karty a ID odebírací karty v této sekci. Počet znaků ID přístupové karty je dán typem karty a může se lišit. Platí však, že karty stejného typu mají ID vždy stejně dlouhé.

Pro správu karet uživatelů slouží tzv. přidávací a odebírací karty. Přiložením přidávací karty ke čtečce je poté každá následující přiložená karta přidána jako nový uživatel s přiřazenou přístupovou kartou do seznamu v Adresáři. V zařízení je automaticky vytvořen uživatel !Visitor #ID_karty. Přiložením odebírací karty ke čtečce je poté každá následující přiložená karta a její uživatel smazán ze seznamu Adresáře. Záznam o přiložené kartě bude zrušen a přístup pomocí této karty bude blokován.

- **ID přidávací karty** – ID servisní karty určené pro přidávání do seznamu instalovaných karet. ID karty je sekvence 6–32 znaků z množiny 0–9, A–F.
- **ID odebírací karty** – ID servisní karty určené pro odebírání ze seznamu instalovaných karet. ID karty je sekvence 6–32 znaků z množiny 0–9, A–F.

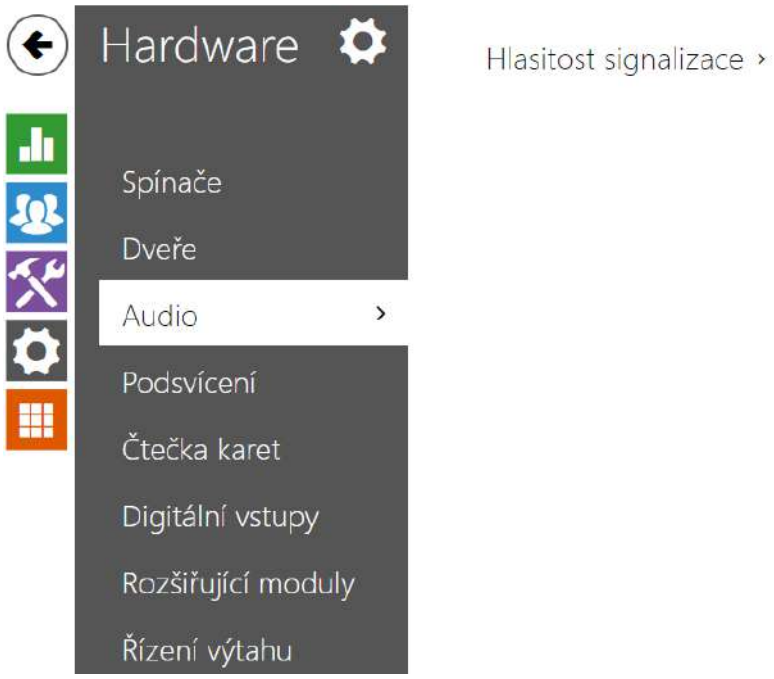


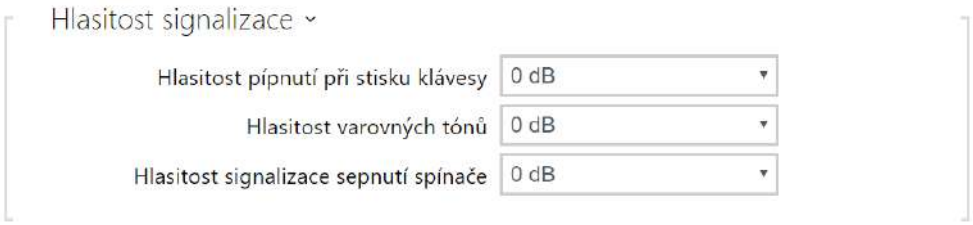
Anti-Passback je zabezpečovací funkce zabraňující použití přístupové karty nebo jiné autentizace ke vstupu do oblasti podruhé, aniž by ji předtím uživatel opustil (takže karta nemůže být předána zpět druhé osobě, která chce vstoupit).

- **Režim** – volí režim funkce Anti-Passback:
  - **Vypnuto** – funkce je defaultně vypnuta, uživatel smí použít přístupovou kartu nebo jinou autentizaci pro přístup ke vstupu do oblasti podruhé, aniž by ji předtím opustil.
  - **Mírný** – uživatel smí použít přístupovou kartu nebo jinou autentizaci pro přístup ke vstupu do oblasti podruhé, aniž by ji předtím opustil. V sekci Stav / Události bude vytvořen nový záznam typu **AccessTaken**.
  - **Přísný** – uživateli není povoleno použití přístupové karty nebo jiné autentizace pro přístup ke vstupu do oblasti podruhé, aniž by ji předtím opustil. V sekci Stav / Události bude vytvořen nový záznam typu **UserRejected**.

- Omezení času – volí čas omezení přístupu pro funkci Anti-Passback. Po zvolenou dobu od posledního přístupu s danou autentizací (kartou, kódem atd.) ji není možno znovu použít ve stejném směru.

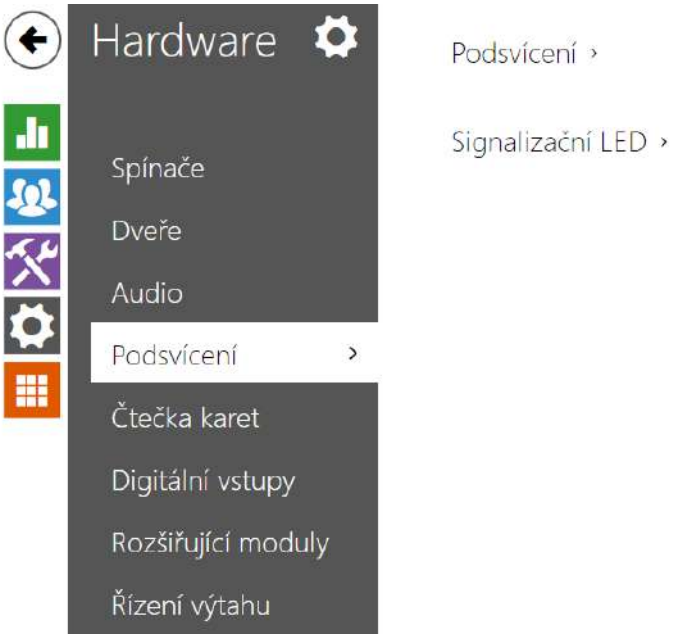
5.3.3 Audio





- **Hlasitost pípnutí při stisku klávesy** – nastavuje hlasitost pípnutí generovaného při stisku klávesy. Nastavená hlasitost je relativní vůči nastavené celkové hlasitosti.
- **Hlasitost varovných tónů** – nastavuje hlasitost varovných a signalizačních tónů popsaných v kapitole Signalizace provozních stavů. Nastavená hlasitost je relativní vůči nastavené celkové hlasitosti.
- **Hlasitost signalizace sepnutí spínače** – nastavuje hlasitost tónu generovaného při aktivaci spínače. Nastavená hlasitost je relativní vůči nastavené celkové hlasitosti.

5.3.4 Podsvícení



Na této záložce lze nastavit nezávisle úroveň podsvícení modulů a úroveň svitu signalizačních LED.

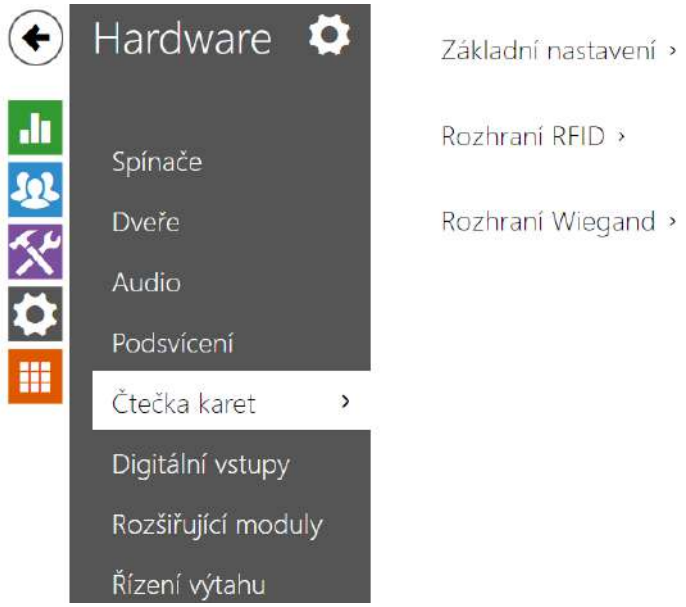
- **Podsvícení** – nastavuje hodnotu jasu podsvícení ve dne. Hodnota se udává v procentech z maximálního možného jasu LED.

- **Signalizační LED** – nastavuje hodnotu jasu signalizačních LED ve dne. Hodnota se udává v procentech z maximálního možného jasu LED.

Poznámka

- Nastavení úrovně intenzity jasu ovlivňuje funkčnost, spotřebu a celkový vzhled zařízení. Vysoký jas podsvícení jmenovek a tlačítek může při nízké úrovni okolního světla způsobit oslnění osoby stojící před interkomem, zároveň obecně zvyšuje spotřebu zařízení. Nízký jas signalizační led vede při použití interkomu přímém slunci snížení kontrastu mezi zhasnutou a rozsvícenou LED a obtížné rozpoznání stavu LED.

5.3.5 Čtečka karet

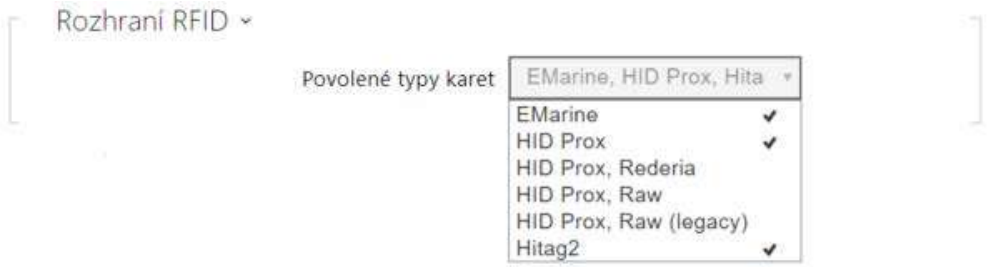


Čtečka karet umožňuje efektivní řízení přístupu do budovy pomocí bezkontaktních RFID karet. Typ podporovaných karet závisí na konkrétním modelu použité čtečky.

Seznam parametrů

- **Dveře** – umožňuje nastavit směr pro zaznamenání do systému: **Příchod/Odchod.** Parametr dveře je využíván docházkovým systémem.
- **Asociovaný spínač** – umožňuje vybrat spínač aktivovaný po přiložení platné karty. Nastavená hodnota se neuplatní v případě přiložení platné karty uživatele při zároveň nastavené funkci dvojité autentizace tohoto uživatele. V takovém případě se po přiložení platné karty očekává zadání numerického kódu pro sepnutí spínače a tento numerický kód identifikuje následně sepnutý spínač.

- Rozhraní RFID – umožňuje vybrat povolené typy karet (označením/odznačením).



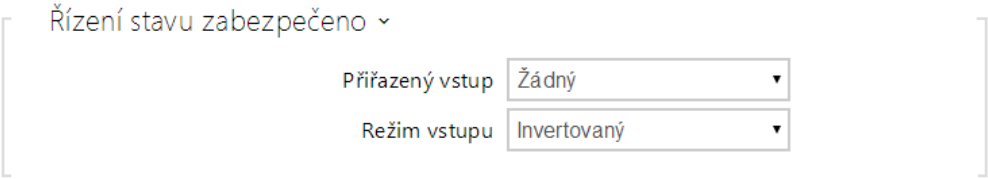
Upozornění

- Pro 2N Access Unit 2.0 platí, že čtečky karet se nezobrazují samostatně jako u starších verzí Access Unit, ale jejich nastavení je umístěno v sekci Hardware / Rozšiřující moduly.

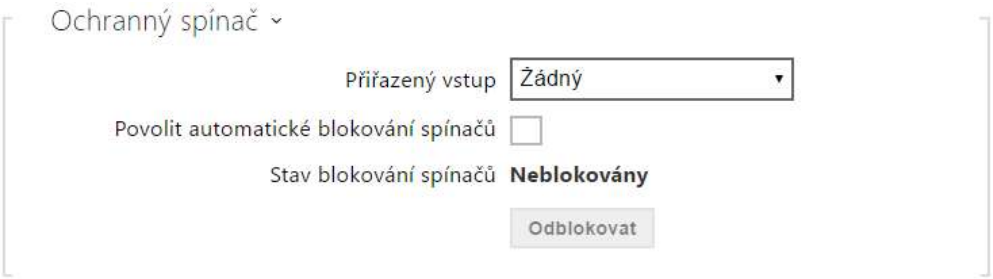
5.3.6 Digitální vstupy

V této části konfigurace interkomu můžete nastavit parametry související s digitálními vstupy a jejich propojení s dalšími funkcemi.

Seznam parametrů



- **Přiřazený vstup** – umožňuje určit jeden z logických vstupů (příp. žádný vstup) pro signalizaci stavu "Zabezpečeno". Stav "Zabezpečeno" je poté signalizován červenou LED na přístupovém terminálu.
- **Režim vstupu** – umožňuje nastavit aktivní úroveň (polaritu) vstupu.



Modely vybavené ochranným spínačem umožňují detekovat otevření krytu zařízení a signalizovat tuto situaci jako událost TamperSwitchActivated. Události jsou zapisovány do logu, který lze vyčítat pomocí HTTP API (viz manuál 2N HTTP API).

Pokud je funkce povolena, po aktivaci ochranného spínače dojde k zablokování všech ostatních spínačů po dobu 30 minut. Blokování bude aktivní i po restartu zařízení. Jednotlivé porty je možné dále ovládat pomocí Automation. Odblokování spínačů lze provést tlačítkem Odblokovat, zakázáním této funkce nebo obnovením konfigurace do továrního nastavení.

- Přiřazený vstup – umožňuje vybrat logický vstup, ke kterému je připojen ochranný spínač. Při aktivaci ochranného spínače je signalizována událost TamperSwitchActivated.
- Povolit automatické blokování spínačů – zablokuje ostatní spínače aktivací ochranného spínače na dobu 30 minut.
- Stav blokování spínačů – zobrazuje a umožňuje nastavení blokování spínačů.

Poznámka

- Od PCB verze 599v2 jsou všechny modely vybavené optickým ochranným spínačem.
- Od PCB verze 599v2 přiřazený vstup je nově signalizován podsvícením piktogramu na modulu. U nižších verzí PCB je signalizován rozsvícením LED diody na pravé straně modulu.

Poznámka

Menu Digitální vstupy jsou dostupné pro modely:

- 2N® IP Verso
- 2N® IP Vario a 2N® IP Force pokud je přítomna interní čtečka karet
- 2N Access Unit se čtečkou karet

5.3.7 Rozšiřující moduly

2N Access Unit lze rozšiřovat pomocí tzv. rozšiřujících modulů připojených k základní jednotce. K dispozici jsou níže uvedené moduly:

- modul klávesnice
- modul infopanelu
- modul čtečky karet
- modul bluetooth čtečky
- modul vstupů a výstupů I/O
- modul rozhraní Wiegand
- modul indukční smyčky
- modul displeje
- modul čtečky otisků prstů
- modul dotykové klávesnice
- modul dotyková klávesnice & RFID čtečka 125kHz, 13.56MHz, NFC
- modul Bluetooth & RFID čtečka 125kHz, 13.56MHz, NFC

Moduly jsou navzájem propojeny a tvoří řetěz. Každý z modulů má své číslo dané pořadím v řetězu (první modul má číslo 0).

Každý z připojených modulů je možné samostatně konfigurovat. Parametry jsou specifické pro daný typ modulu.

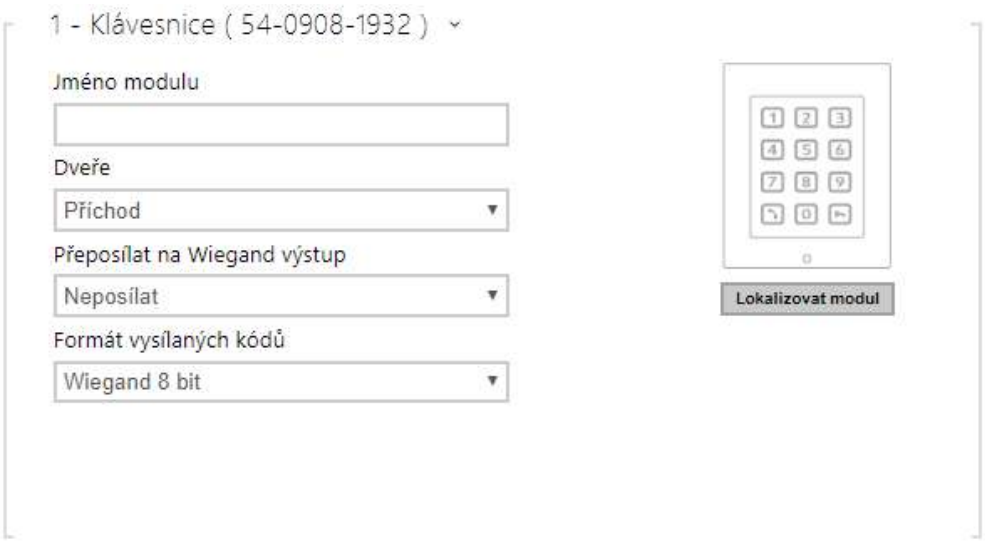
Poznámka

- *Moduly lze konfigurovat pomocí textové řádky obsahující seznam parametrů (název_parametru=hodnota_parametru) oddělený středníky. V současné době jsou zveřejněny pouze některé z parametrů. Ostatní parametry mají spíše experimentální charakter, mohou být v budoucnu změněny, a proto nejsou zveřejněny.*

Upozornění

- Jméno modulu musí být unikátní.
- Moduly, které nemají možnost konfigurace jména, je možné adresovat pomocí ext <pozice_modulu>.

Konfigurace modulu klávesnice

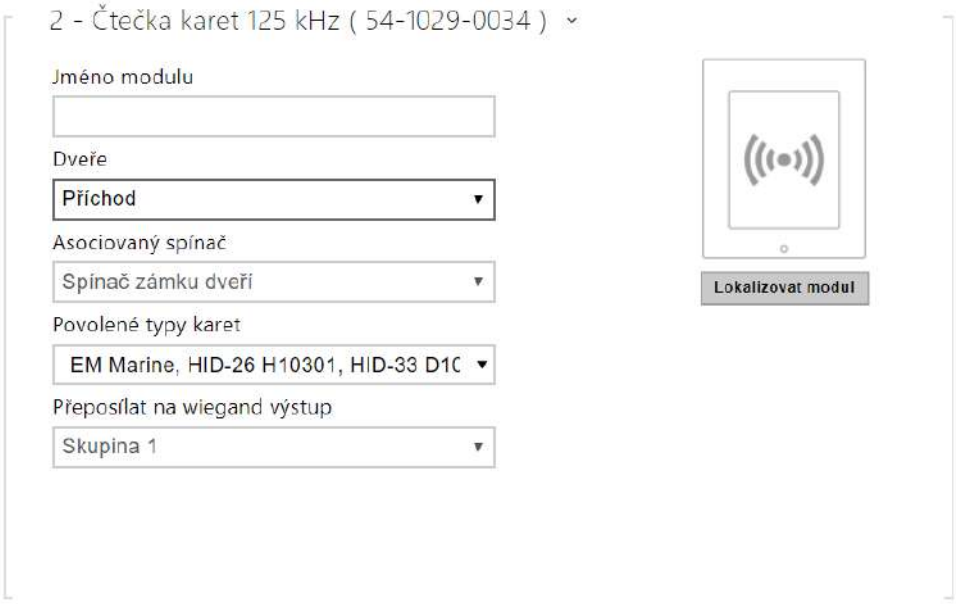


- Jméno modulu – nastavuje název modulu. Název modulu se používá při logování událostí z klávesnice.
- Dveře – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směru je využíván docházkovým systémem.
- Přeposílat na Wiegand výstup – nastavuje skupinu wiegand výstupů, na kterou budou přeposílány všechny stisknuté klávesy.
- Formát vysílaných kódů – výběr ze 4bit a 8bit (vyšší spolehlivost) formátu vysílaných kódů.

Konfigurace modulu infopanelu

- Žádné parametry tohoto modulu nejsou v současné době zveřejněny.

Konfigurace modulu čtečky karet 125 kHz



- Jméno modulu – nastavuje název modulu. Název modulu se používá při logování událostí čtečky karet.
- Dveře – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směr je využíván docházkovým systémem.
- Asociovaný spínač – nastavuje číslo spínače aktivovaného po autentizaci uživatele pomocí tohoto modulu. V případě nastavení volby Spínač zámku dveří se použijí pravidla pro autentizaci v menu Hardware / Dveře.
- Povolené typy karet – umožňuje nastavit typ karty, který bude čtečkou akceptován. Čtečka podporuje v jednom okamžiku pouze jeden typ karty.

- **Přeposílat na wiegand výstup** – nastavuje skupinu wiegand výstupů, na kterou budou přeposílány všechny přijaté ID RFID karet.

Tip

- Pro rychlejší čtení přístupových karet doporučujeme vybrat v nastavení daného modulu pouze typy karet, které jsou používány uživatelem.

Konfigurace modulu čtečky karet 13,56 MHz

- **Jméno modulu** – nastavuje název modulu. Název modulu se používá při logování událostí čtečky karet.
- **Dveře** – nastavuje směr průchodu při použití čtečky (Nespecifikováno, Příchod, Odchod). Parametr směr je využíván docházkovým systémem.
- **Asociovaný spínač** – nastavuje číslo spínače aktivovaného po autentizaci uživatele pomocí tohoto modulu. V případě nastavení volby Spínač zámku dveří se použijí pravidla pro autentizaci v menu Hardware / Dveře.
- **Povolené typy karet** – umožňuje vybrat jeden nebo více typů akceptovaných karet. Pokud není vybrán žádný typ, pak jsou akceptovány všechny typy podporovaných karet.
- **NFC kompatibilita s telefony Samsung** – povoluje NFC kompatibilitu s telefony Samsung.
- **Přeposílat na wiegand výstup** – nastavuje skupinu wiegand výstupů, na kterou budou přeposílány všechny přijaté ID RFID karet.

Tip

- Pro rychlejší čtení přístupových karet doporučujeme vybrat v nastavení daného modulu pouze typy karet, které jsou používány uživatelem.

Konfigurace modulu bluetooth čtečky

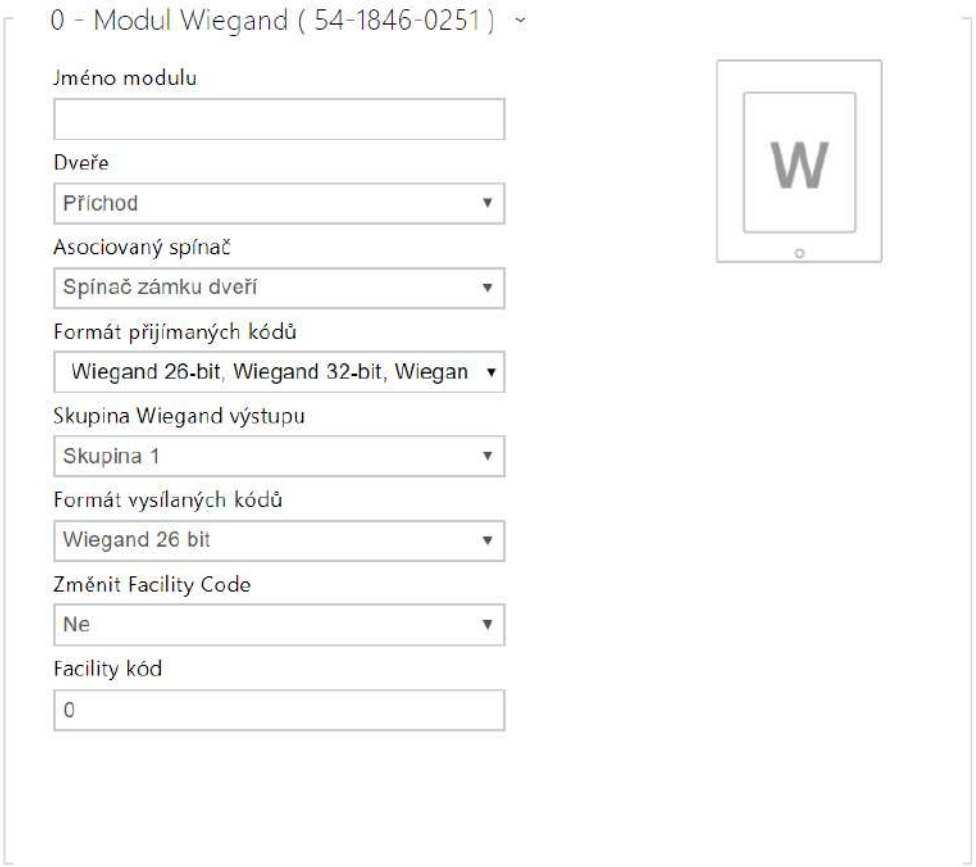
- Jméno modulu – nastavuje název modulu. Název modulu se používá při logování událostí z bluetooth modulu.
- Dveře – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směr je využíván docházkovým systémem.
- Asociovaný spínač – nastavuje číslo spínače aktivovaného po autentizaci uživatele pomocí tohoto modulu. V případě nastavení volby Spínač zámku dveří se použijí pravidla pro autentizaci v menu Hardware / Dveře.
- Dosah signálu – nastavuje maximální dosah signálu, tj. vzdálenost, na kterou ještě bude bluetooth modul komunikovat s mobilním telefonem:
  - Malý – dosah je na většině telefonů menší než 50 cm.
  - Střední – dosah je na většině telefonů menší než 2 m.
  - Velký – dosah je maximální možný
- Operační režim – nastavuje způsob autentizace pomocí mobilního telefonu:
  - Odemčení v aplikaci – autentizaci je nutné potvrdit, klepnutím na ikonu ve spuštěné aplikaci na mobilním telefonu
  - Dotykový mód – autentizaci je nutné potvrdit dotykem na čtečce za přítomnosti telefonu se spárovanou 2N® Mobile Key aplikací.

Konfigurace modulu vstupů a výstupů I/O

- Jméno modulu – nastavuje název modulu. Název modulu se používá při specifikaci vstupu nebo výstupu v objektech SetOutput, GetInput a InputChanged v nastavení Automation.

Konfigurace modulu Wiegand

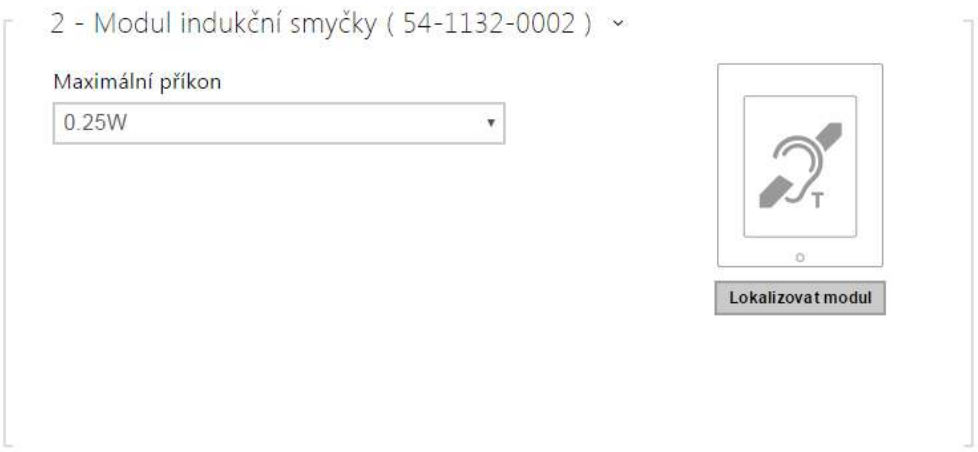
Modul Wiegand je vybaven vstupním a výstupním wiegand rozhraním, které jsou na sobě nezávislé, mají nezávislé nastavení a mohou přijímat a vysílat kódy současně. Vstupní wiegand rozhraní lze použít pro připojení externích zařízení, jako jsou čtečky RFID karet, biometrické čtečky apod. Pomocí výstupního wiegand rozhraní lze interkom připojit např. k zabezpečovacímu systému v budově (lze odesílat ID RFID karet přiložených k připojené RFID čtečce příp. kódy přijaté na libovolném vstupním wiegand rozhraní). Modul Wiegand je dále vybaven jedním logickým vstupem a jedním logickým výstupem, které lze ovládat pomocí Automation.



- Jméno modulu – nastavuje název modulu. Název modulu se používá při specifikaci vstupu nebo výstupu v objektech SetOutput, GetInput a InputChanged v nastavení Automation.
- Dveře – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směr je využíván docházkovým systémem.
- Asociovaný spínač – nastavuje číslo spínače aktivovaného po autentizaci uživatele pomocí tohoto modulu. V případě nastavení volby Spínač zámku dveří se použijí pravidla pro autentizaci v menu Hardware / Dveře.
- Formát přijímaných kódů – nastavuje formát přijímaných kódů (Wiegand 26, 32, 37 a RAW).

- Skupina Wiegand výstupu – přiřazuje wiegand výstupu do skupiny, na kterou mohou být přeposílány kódy z připojených čteček karet, příp. wiegand vstupů.
- Formát vysílaných kódů – nastavuje formát vysílaných kódů (26 bit, 32 bit, 37 bit, RAW formát, 35 bit, Corp. 1000, 48 bit, Corp. 1000 a Auto).
- Změnit Facility Code – umožňuje nastavit první část kódu přes rozhraní Wiegand. Týká se výstupního režimu rozhraní pro formát vysílaného kódu 26 bit. Ověřte u dodavatele vašeho zabezpečovacího systému, zda je Facility Code vyžadován.
- Facility Code – určuje lokaci 2N IP zařízení v zabezpečovacím systému. Zadejte dekadickou hodnotu lokace (0–255).

Konfigurace modulu indukční smyčky



- Maximální příkon – nastavuje maximální vysílací výkon antény indukční smyčky. Vyšší vysílací výkon znamená vyšší dosah, avšak méně výkonu pro ostatní funkce interkomu. Za běžných okolností by měla být vyhovující výchozí hodnota 0,25 W.

Konfigurace modulu displeje

- Jméno modulu – nastavuje název modulu. Název modulu se používá při logování událostí displeje.
- Dveře – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směr je využíván docházkovým systémem.

Upozornění

- Od FW verze 2.27 není displej podporován na Access Unit 1.0.

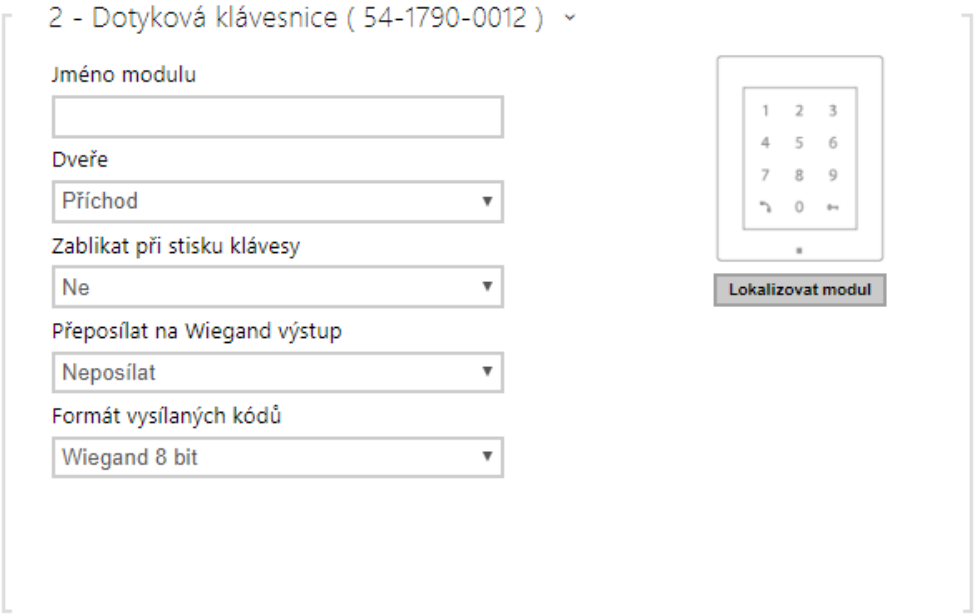
Konfigurace modulu čtečky otisků prstů

- Jméno modulu – nastavuje název modulu. Název modulu se používá při logování událostí čtečky otisků prstů.
- Dveře – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směr je využíván docházkovým systémem.
- Asociovaný spínač – nastavuje číslo spínače aktivovaného po autentizaci uživatele pomocí tohoto modulu. V případě nastavení volby Spínač zámku dveří se použijí pravidla pro autentizaci v menu Hardware / Dveře.

Poznámka

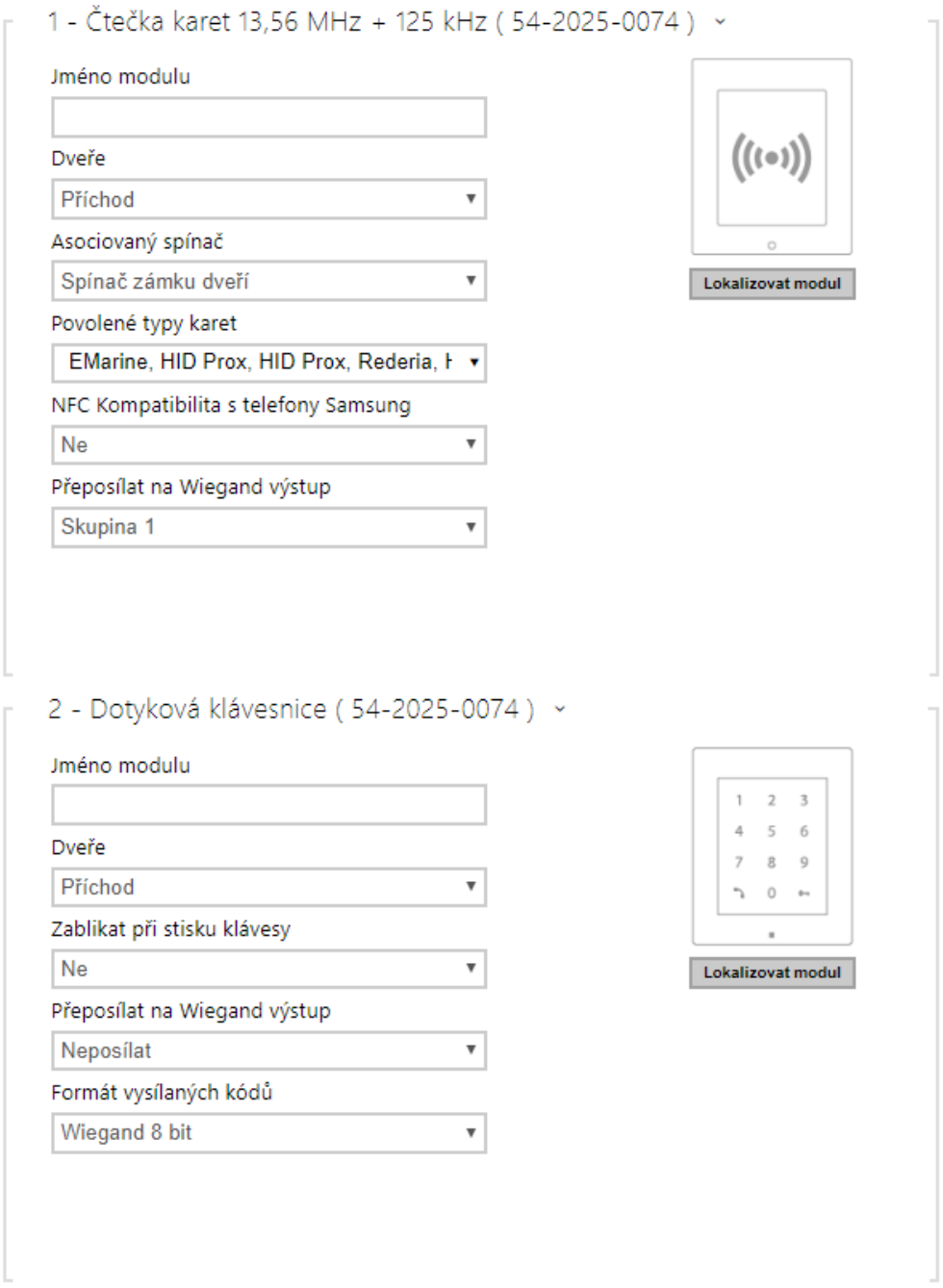
- Při odpojení modulu čtečky otisků prstů bude po restartu zařízení v profilu uživatele v Adresáři skryta část Uživatelské otisky prstů, která zobrazuje, kolik otisků má uživatel nahraných v paměti interkomu. Po opětovném připojení jakéhokoliv modulu čtečky otisků prstů se část konfigurace uživatele opět zobrazí.

Konfigurace modulu dotykové klávesnice



- Jméno modulu – nastavuje název modulu. Název modulu se používá při logování událostí z dotykové klávesnice.
- Dveře – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směru je využíván docházkovým systémem.
- Zablikat při stisku klávesy – nastavuje světelnou signalizaci zablikáním potvrzující stisk klávesy. Užívá se v hlučném prostředí, kdy není zvuková signalizace jasně zřetelná.
- Přeposílat na Wiegand výstup – nastavuje skupinu wiegand výstupů, na kterou budou přeposílány všechny přijaté přístupové kódy uživatelů.
- Formát vysílaných kódů – výběr ze 4bit a 8bit (vyšší spolehlivost) formátu vysílaných kódů.

Konfigurace modulu dotykové klávesnice & RFID čtečky 125 kHz, 13.56MHz, NFC



Čtečka karet 13,56 MHz (125 kHz) (sériové číslo modulu)

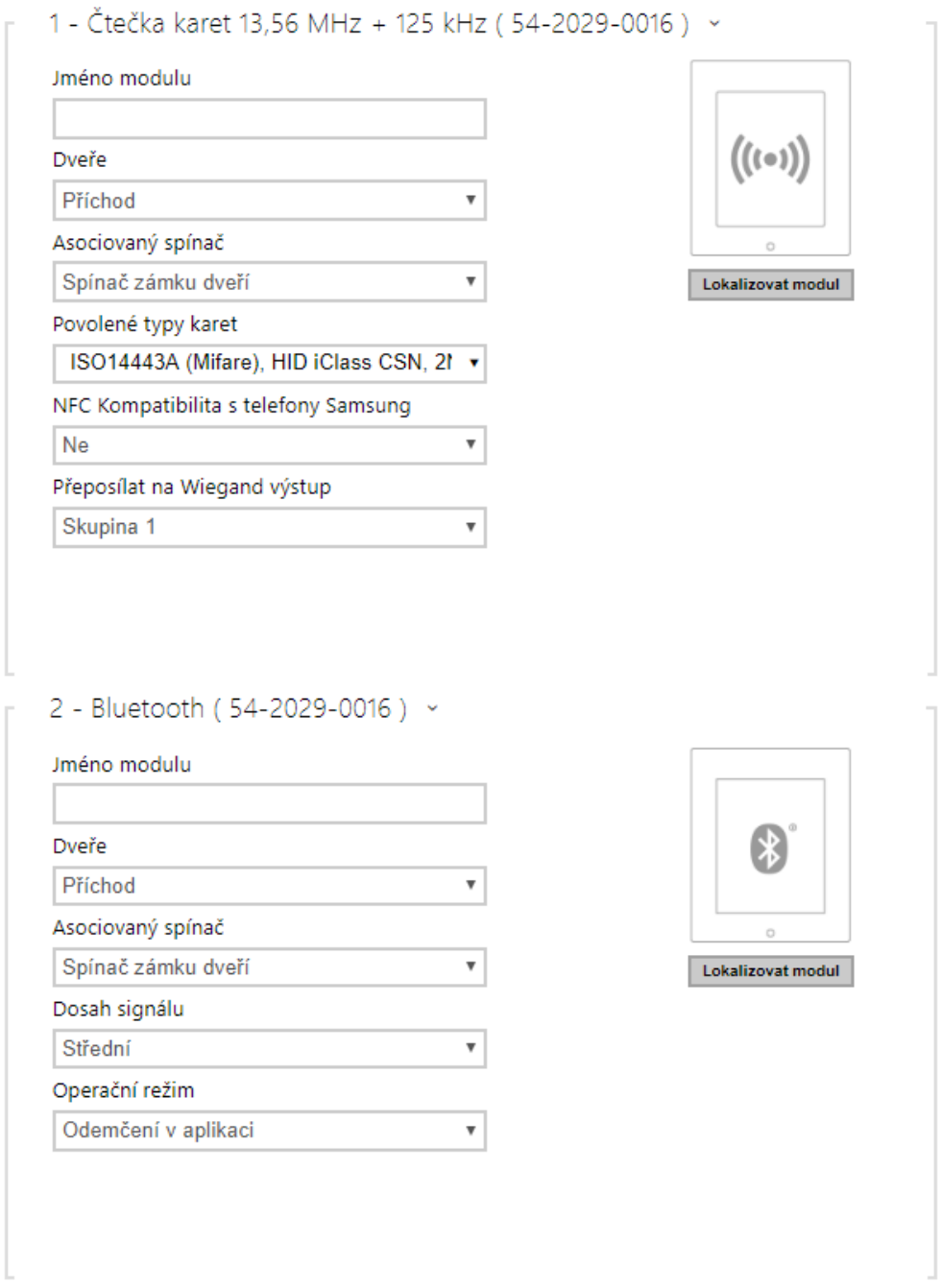
- Jméno modulu – nastavuje název modulu. Název modulu se používá při logování událostí z modulu čtečky karet.
- Dveře – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směr je využíván docházkovým systémem.

- Asociovaný spínač – nastavuje číslo spínače aktivovaného po autentizaci uživatele pomocí tohoto modulu. V případě nastavení volby Spínač zámku dveří se použijí pravidla pro autentizaci v menu Hardware / Dveře.
- Povolené typy karet – umožňuje nastavit typ a karty, který bude čtečkou akceptován. Čtečka podporuje v jednom okamžiku pouze jeden typ karty.
- NFC kompatibilita s telefony Samsung – povoluje NFC kompatibilitu s telefony Samsung.
- Přeposílat na wiegand výstup – nastavuje skupinu wiegand výstupů, na kterou budou přeposílána všechna přijatá ID RFID karet.

Dotyková klávesnice (sériové číslo)

- Jméno modulu – nastavuje název modulu. Název modulu se používá při logování událostí z modulu dotykové klávesnice.
- Dveře – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směru je využíván docházkovým systémem.
- Zablikat při stisku klávesy – nastavuje světelnou signalizaci zablikáním potvrzující stisk klávesy. Užívá se v hlučném prostředí, kdy není zvuková signalizace jasně zřetelná.
- Přeposílat na Wiegand rozhraní – nastavuje skupinu wiegand výstupů, na kterou budou přeposílány všechny přijaté přístupové kódy uživatelů.
- Formát vysílaných kódů – výběr ze 4bit a 8bit (vyšší spolehlivost) formátu vysílaných kódů .

Konfigurace modulu Bluetooth & RFID čtečky 125kHz, 13.56 MHz, NFC



Čtečka karet 13,56 MHz (125 kHz)

- **Jméno modulu** – nastavuje název modulu. Název modulu se používá při logování událostí z modulu čtečky karet.
- **Dveře** – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směr je využíván docházkovým systémem.
- **Asociovaný spínač** – nastavuje číslo spínače aktivovaného po autentizaci uživatele pomocí tohoto modulu. V případě nastavení volby Spínač zámku dveří se použijí pravidla pro autentizaci v menu Hardware / Dveře.
- **Povolené typy karet** – umožňuje nastavit typ, který bude čtečkou akceptován. Čtečka podporuje v jednom okamžiku pouze jeden typ karty.
- **NFC kompatibilita s telefony Samsung** – povoluje NFC kompatibilitu s telefony Samsung.
- **Přeposílat na wiegand výstup** – nastavuje skupinu wiegand výstupů, na kterou budou přeposílány všechny přijaté ID RFID karet.

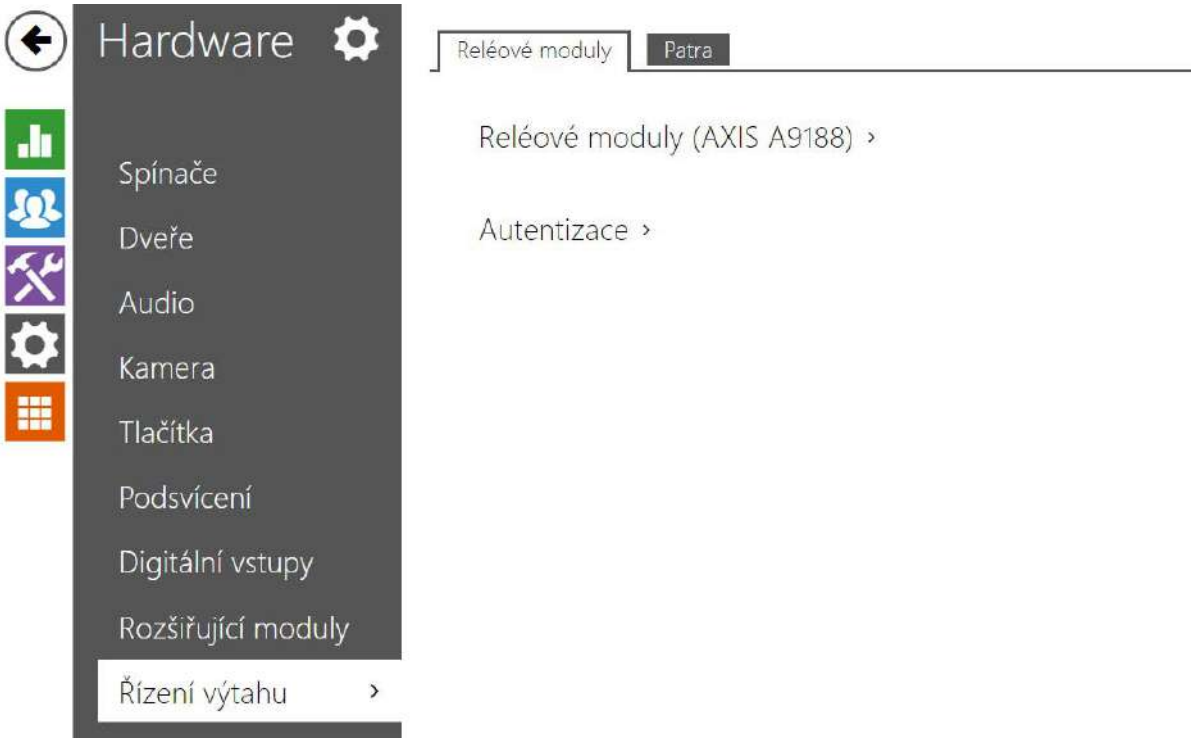
Bluetooth

- **Jméno modulu** – nastavuje název modulu. Název modulu se používá při logování událostí z bluetooth modulu.
- **Dveře** – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směru je využíván docházkovým systémem.
- **Asociovaný spínač** – nastavuje číslo spínače aktivovaného po autentizaci uživatele pomocí tohoto modulu. V případě nastavení volby Spínač zámku dveří se použijí pravidla pro autentizaci v menu Hardware / Dveře.
- **Dosah signálu** – nastavuje maximální dosah signálu, tj. vzdálenost, na kterou ještě bude bluetooth modul komunikovat s mobilním telefonem:
  - **Malý** – dosah je na většině telefonů menší než 50 cm.
  - **Střední** – dosah je na většině telefonů menší než 2 m.
  - **Velký** – dosah je maximální možný
- **Operační režim** – nastavuje způsob autentizace pomocí mobilního telefonu:
  - **Odemčení v aplikaci** – autentizaci je nutné potvrdit, klepnutím na ikonu ve spuštěné aplikaci na mobilním telefonu.
  - **Dotykový mód** – autentizaci je nutné potvrdit dotykem na čtečce za přítomnosti telefonu se spárovanou **2N® Mobile Key** aplikací.

Upozornění

- Po výměně modulů je nutné nové moduly opět nakonfigurovat. Konfigurace je vázaná na sériové číslo modulu.

5.3.8 Řízení výtahů



Pomocí připojení reléového modulu AXIS A9188 k **2N Access Unit** lze řídit přístup na jednotlivá patra v budově za použití výtahu. K jedné **2N Access Unit** je možné připojit max. těchto 5 reléových modulů, přičemž každý z modulů může ovládat 8 pater, dohromady tedy max. 40 pater. Pro využití této funkce je nutné mít aktivní 2N Access Unit Lift module licennci (obj. č. 9160401).

Záložka Reléové moduly

- **Doba sepnutí** – nastavuje dobu sepnutí reléového modulu (rozsah 1–600 s).

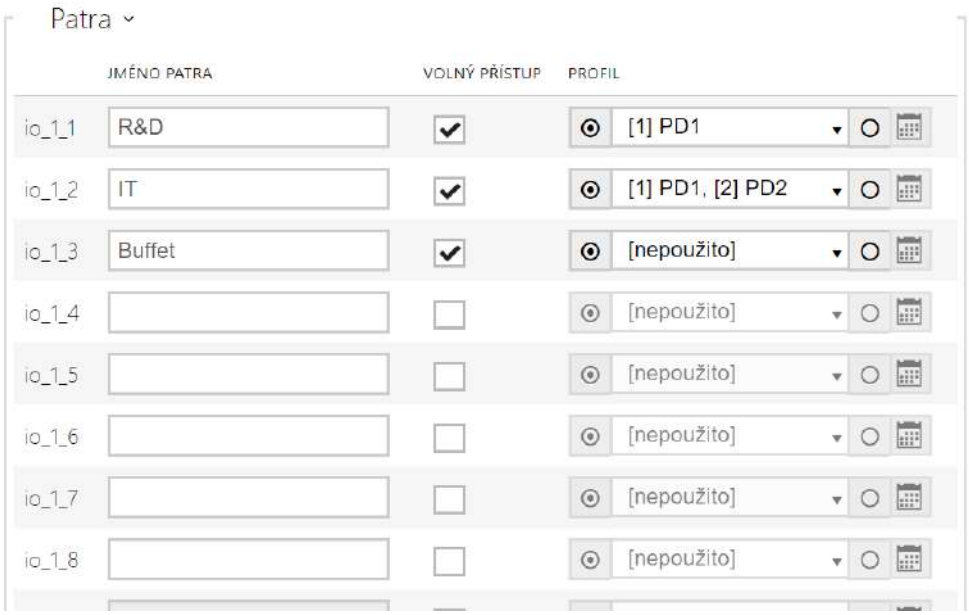
- **Zapnuto** – slouží k aktivaci a deaktivaci modulu AXIS A9188, který slouží ke kontrole řízení výtahu až na 8 patrech.
- **IP Adresa** – IP adresa AXIS A9188.
- **Stav** – zobrazuje stav připojeného modulu AXIS A9188 (Chyba/Přístup odepřen /Připraveno/Zastaveno).
- **Sériové číslo** – sériové číslo modulu AXIS A9188.

- **Uživatelské jméno** – jméno uživatele pro autentizaci připojení k externímu zařízení. Parametr je povinný pouze tehdy, pokud externí zařízení vyžaduje autentizaci.
- **Heslo** – heslo pro autentizaci připojení k externímu zařízení (WEB relé atd.). Parametr je povinný pouze tehdy, pokud externí zařízení vyžaduje autentizaci.

Upozornění

- Autentizace se provádí pro všechny moduly jedním uživatelským jménem a heslem.

Záložka Patra



- Jméno patra – nastavuje jméno patra.
- Volný přístup – aktivuje trvalý přístup na patro bez potřeby jakékoliv autentizace.
- Profil – nabízí výběr jednoho či více časových profilů zároveň, které se uplatní. Samotné nastavení časových profilů je možné v sekci Adresář / Časové profily.
  - 

    označením se nastavuje výběr z předdefinovaných profilů nebo manuální nastavení časového profilu pro daný prvek.
  -  označením se nastavuje časový profil přímo pro daný prvek.

Tip

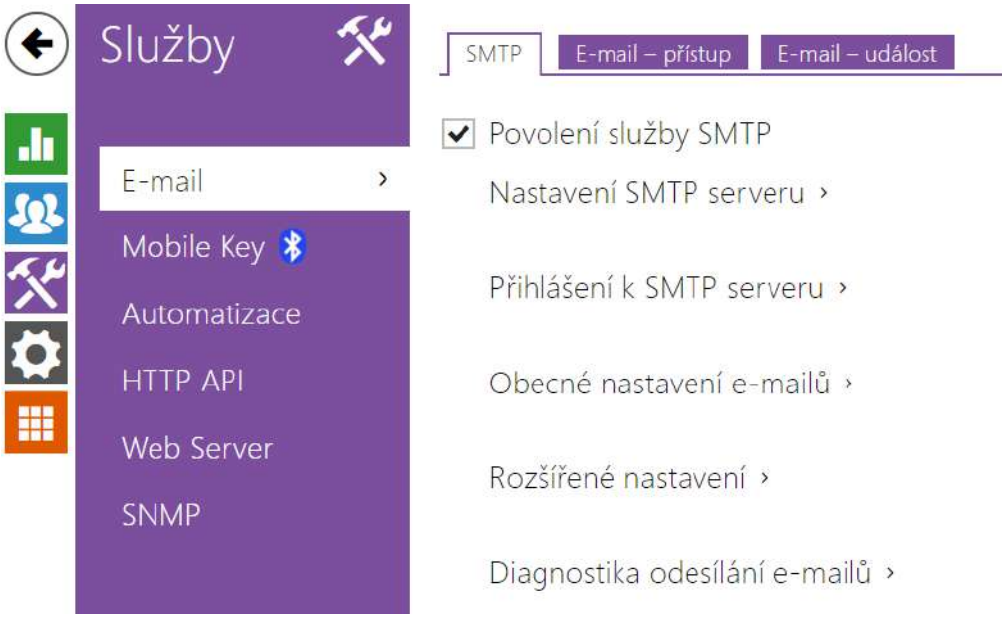
Generování certifikátu pro reléový modul AXIS A9188

1. Vyhledejte reléový modul AXIS A9188 v lokální síti pomocí AXIS IP Utility .
2. Zadejte přihlašovací údaje root/root.
3. V menu vyberte Preferences / Additional device configuration.
4. Zobrazí se nové okno s konfigurací zařízení.
5. V menu vyberte System Options / Security / Certificates.
6. Vytvořte certifikát kliknutím na Create self-signed certificate.
7. Vyplňte všechna požadovaná pole a potvrďte tlačítkem OK.
8. Přejděte do menu System Options / Security / HTTPS.
9. Vyberte certifikát v rozbalovacím menu a uložte stiskem tlačítka Save.
10. Přejděte do webového rozhraní 2N Access Unit, konfigurace Hardware / Řízení výtahu. Zadejte přihlašovací údaje a vyplňte IP adresu reléového modulu.
11. Při úspěšném spojení se u reléového modulu zobrazí READY.

5.4 Služby

Zde je přehled toho, co v kapitole naleznete:

5.4.1 E-mail



Pokud chcete informovat uživatele o zmeškaných, příp. všech realizovaných hovorech z interkomu, můžete nakonfigurovat **2N IP interkom** tak, aby volanému uživateli odeslal po každém takovém hovoru e-mail. Můžete nastavit vlastní předmět a text zprávy e-mailu. Pokud je váš interkom vybaven kamerou, může k e-mailu automaticky přiložit jeden nebo více snímků z kamery sejmutých v průběhu hovoru nebo vyzvánění.

Interkom odesílá e-maily všem uživatelům, kteří mají v seznamu uživatelů nastavenou platnou e-mailovou adresu. V případě, že parametr **E-mail** v seznamu uživatelů ponecháte nevyplněný, e-maily jsou odesílány na nastavenou výchozí e-mailovou adresu.

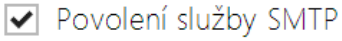
E-maily je možné také odesílat pomocí automatizace pomocí akce **Action.SendEmail**.

Poznámka

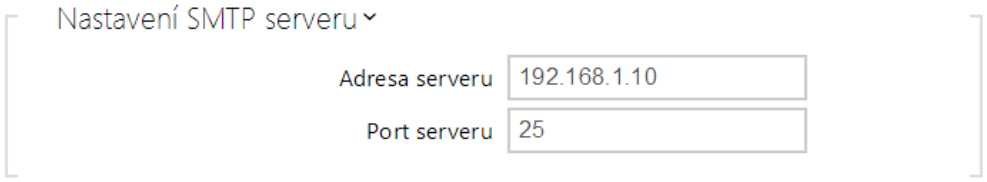
- *Funkce e-mail je dostupná pouze s licencí Gold nebo Enhanced Integration.*

Seznam parametrů

Záložka SMTP

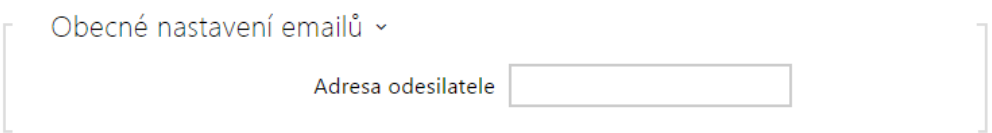


- **Povolení služby SMTP** – umožňuje povolit nebo blokovat službu odesílání e-mailů z interkomu.

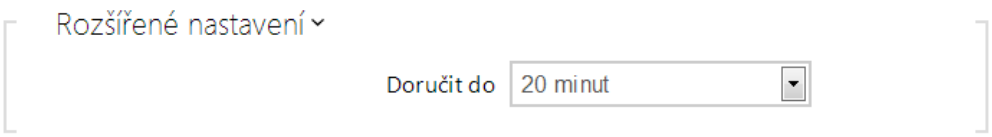


- **Adresa serveru** – adresa SMTP serveru, na který budou odesílány e-maily.
- **Port serveru** – port SMTP serveru. Upravte jen v případě nestandardního nastavení SMTP serveru. SMTP port bývá obvykle nastaven na hodnotu 25.

- **Jméno uživatele** – pokud SMTP server vyžaduje autorizaci, musí být v tomto poli uvedeno platné jméno pro přihlášení k serveru. V opačném případě můžete pole ponechat prázdné.
- **Heslo** – heslo pro přihlášení interkomu k SMTP serveru.
- **Osobní certifikát** – specifikuje uživatelský certifikát a privátní klíč, pomocí kterých se provádí šifrování komunikace mezi interkomem a SMTP serverem. Lze zvolit jednu ze tří sad uživatelských certifikátů a privátních klíčů, viz kapitola Certifikáty, nebo ponechat nastavení **SelfSigned**, kdy se použije automaticky vygenerovaný certifikát vytvořený při prvním spuštění interkomu.



- **Adresa odesilatele** – nastavuje adresu odesilatele pro všechny odchozí e-maily ze zařízení.



- **Doručit do** – nastavuje maximální dobu, po kterou se interkom snaží doručit e-mail na nedostupný SMTP server.

Pomocí tlačítka **Uložit a otestovat** lze odeslat testovací E-mail na zadanou adresu a tak vyzkoušet funkčnost aktuálního nastavení odesílání e-mailů. Do pole Adresa testovacího e-mailu vyplňte cílovou e-mailovou adresu a stiskněte tlačítko. V průběhu odesílání e-mailu se v okně vypisuje aktuální stav odesílání, ze kterého lze detekovat případný problém s nastavením e-mailu na interkomu příp. jiným síťovým prvkem.

Záložka E-mail – přístup

Na této záložce lze nastavit odesílání e-mailů v okamžiku přiložení RFID karty ke čtečce karet, identifikace modulem Bluetooth nebo čtečkou otisků prstů.

Posílat e-mail při – umožňuje nastavit odesílání e-mailu. Lze volit mezi následujícími možnostmi:

- **Neodesílat e-mail** – e-mail nebude odeslán.
- **Všechny přístupy** – e-mail bude odeslán po každém zaznamenaném přístupu.
- **Odmítnuté přístupy** – e-mail bude odeslán pouze při zamítnutém přístupu.

- **Výchozí příjemce** – interkom odesílá zprávy na e-mailovou adresu uvedenou u příslušného uživatele (v případě přiložení platné karty uživatele). V případě neplatné karty, příp. pokud u uživatele není uveden e-mail, zpráva je odeslaná na e-mail uvedený v tomto poli. Pokud příjemce není uveden ani v telefonním seznamu, ani v tomto poli, e-mail nebude odeslán. V případě potřeby lze zadat více e-mailových adres oddělených čárkou.
- **Předmět** – nastavuje předmět odesílané e-mailové zprávy.
- **Obsah zprávy** – umožňuje upravit obsah odesílané zprávy. V textu lze používat formátovací značky jazyka HTML. Do textu lze vkládat speciální zástupné symboly pro jméno uživatele, datum a čas, identifikaci zařízení příp. identifikátor přiložené karty, přečtený identifikátor Bluetooth nebo identifikátor otisku prstu, druh použitého identifikátoru a pro informaci o platnosti identifikátoru. Tyto zástupné symboly budou před odesláním zprávy nahrazeny aktuální hodnotou. Viz následující seznam zástupných symbolů:
  1. $User$ Jméno volaného uživatele
  2. $DateTime$ Aktuální datum a čas
  3. $AuthId$ Identifikátor přiložené karty
  4. $DeviceName$ Identifikace interkomu
  5. $AuthIdType$ Druh autentizace – určuje zařízení, které bylo zdrojem identifikátoru (Card, Bluetooth nebo Fingerprint)
  6. $AuthIdValid$ Platnost použitého identifikátoru; Valid pro platný identifikátor, Invalid pro neplatný

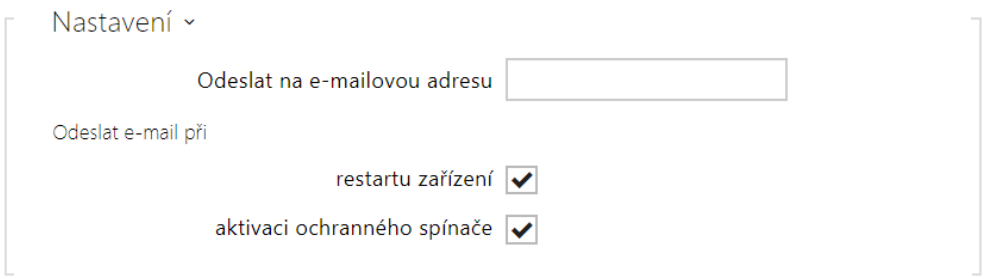
Pro zástupné symboly $AuthIdType$ a $AuthIdValid$ je možno použít rozšířenou syntaxi, která slouží k náhradě vestavěných hodnot, například pro text v češtině:

$AuthIdValid|Valid=platná|Invalid=neplatná$

V případě, že se hodnota zástupného symbolu v řetězci náhrad nenajde, je použita přímo.

Záložka e-mail – událost

Na této záložce lze nastavit odesílání informačních e-mailů v okamžiku, kdy dojde k restartu zařízení nebo aktivaci ochranného spínače na zařízení.



Odeslat na e-mailovou adresu – umožňuje nastavit odesílání e-mailu. Lze volit mezi následujícími možnostmi:

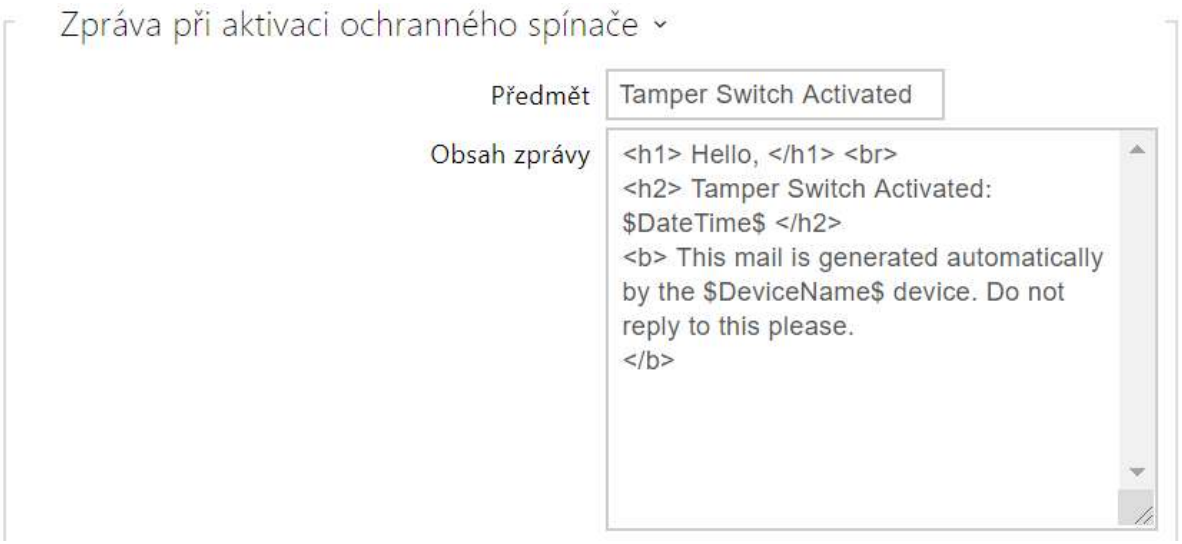
- Restart Zařízení
- Aktivace ochranného spínače

Zpráva při restartu zařízení – nastavení zprávy, která bude zaslána na uvedenou e-mailovou adresu při restartu zařízení.

- **Předmět** – nastavuje předmět odesílané e-mailové zprávy.
- **Obsah zprávy** – umožňuje upravit obsah odesílané zprávy. V textu lze používat formátovací značky jazyka HTML. Do textu lze vkládat speciální zástupné symboly pro jméno uživatele, datum a čas, identifikaci zařízení. Tyto zástupné symboly budou před odesláním zprávy nahrazeny aktuální hodnotou. Viz následující seznam zástupných symbolů:
    - 1. $User$ Jméno volaného uživatele
      2. $DateTime$ Aktuální datum a čas

3. $DeviceName$ Identifikace interkomu

V případě, že se hodnota zástupného symbolu v řetězci náhrad nenajde, je použita přímo.

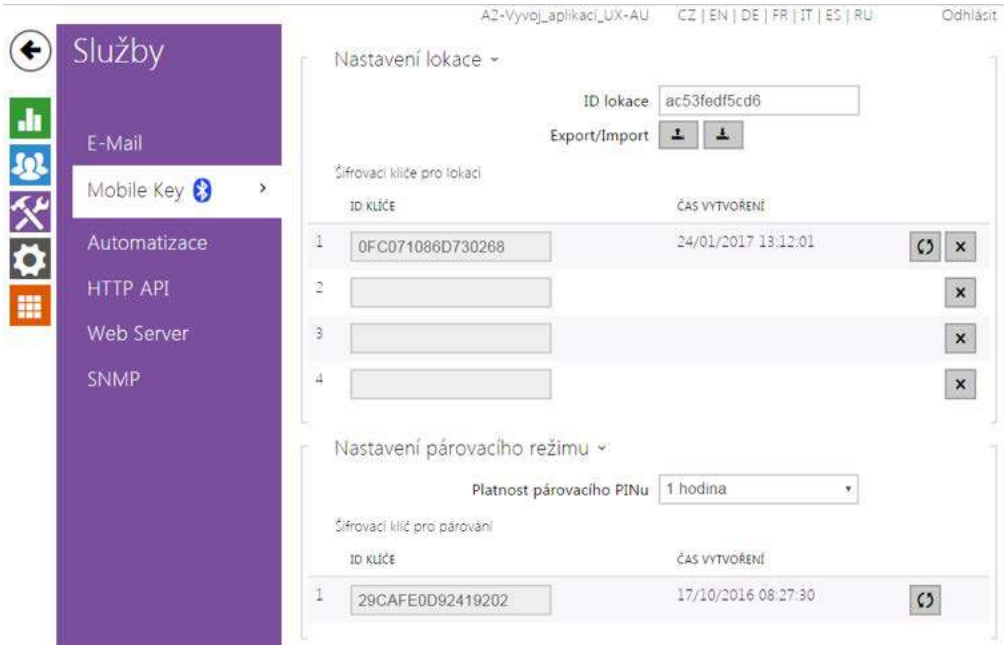


Zpráva při aktivaci ochranného spínače – nastavení zprávy, která bude zaslána na uvedenou e-mailovou adresu při aktivaci ochranného spínače.

- **Předmět** – nastavuje předmět odesílané e-mailové zprávy.
- **Obsah zprávy** – umožňuje upravit obsah odesílané zprávy. V textu lze používat formátovací značky jazyka HTML. Do textu lze vkládat speciální zástupné symboly pro jméno uživatele, datum a čas, identifikaci zařízení. Tyto zástupné symboly budou před odesláním zprávy nahrazeny aktuální hodnotou. Viz následující seznam zástupných symbolů:
    - 1. $User$ Jméno volaného uživatele
      2. $DateTime$ Aktuální datum a čas
      3. $DeviceName$ Identifikace interkomu

V případě, že se hodnota zástupného symbolu v řetězci náhrad nenajde, je použita přímo.

5.4.2 Mobile Key



Přístupové terminály **2N Access Unit** vybavené modulem Bluetooth umožňují autentizovat uživatele pomocí mobilní aplikace **2N® Mobile Key** dostupné pro zařízení s operačními systémy iOS 8.1 a vyšší (telefony iPhone 4S a vyšší) příp. Android 4.4 KitKat a vyšší (telefony s podporou Bluetooth 4.0 Smart).

Identifikace uživatele (Auth ID)

Aplikace **2N® Mobile Key** se na straně přístupového terminálu autentizuje pomocí jednoznačného identifikátoru – tzv. **Auth ID**. Auth ID (128bit číslo) je pro každého uživatele náhodně vygenerováno a procesem tzv. **párování** spojeno s uživatelem zavedeným v přístupovém terminálu a jeho mobilním zařízením.

Poznámka

- Vygenerované Auth ID nemůže být uloženo ve více mobilních zařízeních současně. Tzn. že Auth ID jednoznačně identifikuje konkrétní mobilní zařízení (resp. jeho uživatele).

Hodnotu Auth ID lze u každého uživatele nastavit a upravit v sekci Mobile Key telefonního seznamu přístupového terminálu. Auth ID lze přesunout k jinému uživateli, příp. zkopírovat do jiného přístupového terminálu. Po vymazání hodnoty pole dojde k blokování přístupu uživatele.

Šifrovací klíče a lokace

Komunikace mezi aplikací 2N® Mobile Key a přístupovým terminálem je vždy šifrovaná. Bez znalosti šifrovacího klíče nemůže aplikace 2N® Mobile Key uživatele autentizovat. Primární šifrovací klíč je automaticky vygenerován při prvním spuštění přístupového terminálu a později jej lze kdykoli ručně přegenerovat. Primární šifrovací klíč je společně s Auth ID přenesen do mobilního zařízení při párování.

Šifrovací klíče a identifikátor lokace lze z přístupového terminálu exportovat a následně importovat do dalších přístupových terminálů. Přístupové terminály se stejným názvem lokace a stejnými šifrovacími klíči tvoří tzv. lokace. V rámci jedné lokace se mobilní zařízení páruje pouze jednou a identifikuje se pouze jedním jedinečným Auth ID (tudíž v rámci lokace lze kopírovat Auth ID uživatele z jednoho přístupového terminálu do druhého).

Párování

Procesem tzv. párování se rozumí přenos přístupových údajů uživatele do jeho osobního mobilního zařízení. Přístupové údaje uživatele mohou být uloženy pouze v jednom mobilním zařízení – tj. uživatel nemůže mít např. dvě mobilní zařízení, pomocí kterých se autentizuje. V jednom mobilním zařízení však mohou být současně uloženy přístupové údaje uživatele do více lokací současně (tj. mobilní zařízení slouží jako klíč pro více lokací současně).

Párování uživatele s mobilním zařízením lze vyvolat v telefonním seznamu přístupového terminálu na stránce příslušného uživatele. Párování lze fyzicky provést lokálně pomocí USB bluetooth modulu připojeného k PC, příp. vzdáleně pomocí bluetooth modulu integrovaného v přístupovém terminálu. Oba způsoby párování vedou ke stejnému výsledku.

Při párování se do mobilního zařízení přenášejí následující údaje:

- Identifikátor lokace
- Šifrovací klíč lokace
- Auth ID uživatele

Šifrovací klíč pro párování

V režimu párování se z bezpečnostních důvodů se pro zabezpečení komunikace používá jiný klíč než při komunikaci po spárování. Tento klíč je automaticky vygenerován při prvním spuštění přístupového terminálu a lze jej kdykoli přegenerovat.

Správa šifrovacích klíčů

Přístupový terminál může udržovat v platnosti až 4 šifrovací klíče – tj. 1 primární a až 3 sekundární klíče. Mobilní zařízení může k šifrování komunikace použít libovolný z těchto 4 klíčů. Šifrovací klíče jsou plně pod kontrolou správce systému. Šifrovací klíče je vhodné z bezpečnostních důvodů pravidelně, příp. při ztrátě mobilního zařízení nebo úniku konfigurace přístupového terminálu aktualizovat.

Poznámka

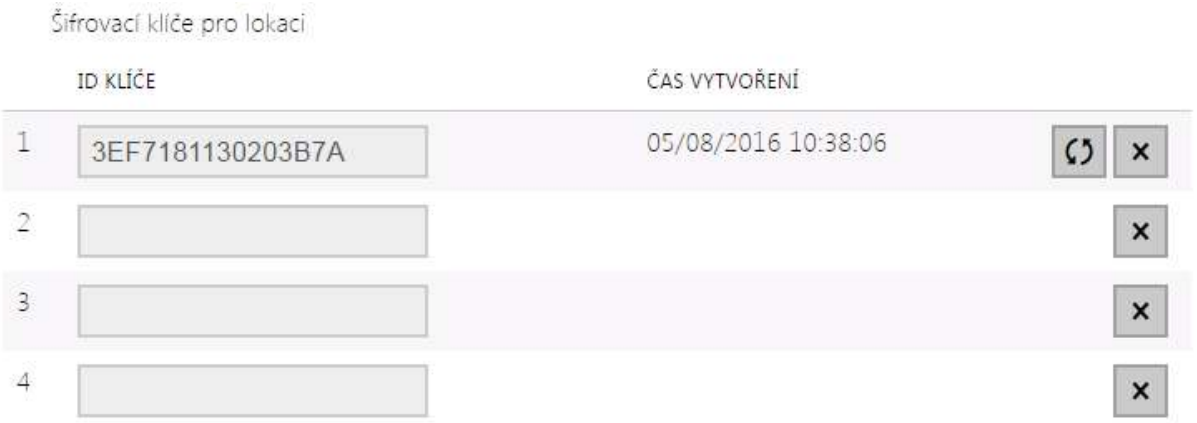
- Při prvním spuštění přístupového terminálu jsou automaticky vygenerovány šifrovací klíče a jsou uloženy do konfiguračního souboru přístupového terminálu. Pro větší bezpečnost doporučujeme tyto šifrovací klíče před prvním použitím ručně znovu vygenerovat.

Primární klíč je možné kdykoli znovu vygenerovat. Z původního primárního klíče se následně stane první sekundární klíč, z prvního sekundárního se stane druhý sekundární atd. Sekundární klíče lze kdykoli odstranit.

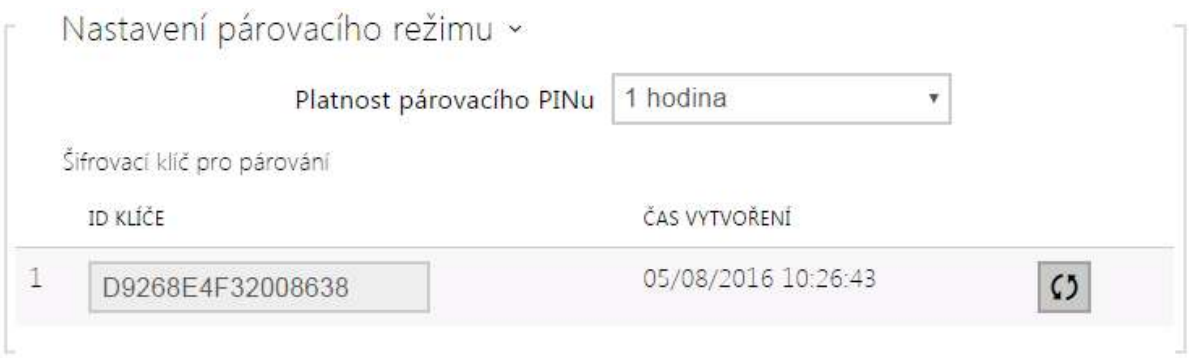
Po odstranění klíče se uživatelé aplikace 2N® Mobile Key, kteří tento klíč stále používají, nebudou moci autentizovat, pokud před smazáním klíče neaktualizují šifrovací klíče ve svém mobilním zařízení. Klíče v mobilním zařízení se aktualizují při každém použití aplikace 2N® Mobile Key.

Seznam parametrů

- ID lokace – jednoznačný identifikátor lokace, ve které platí sada nastavených šifrovacích klíčů.
- Tlačítko Export – exportuje identifikátor lokace a aktuální šifrovací klíče do souboru. Exportovaný soubor lze následně importovat do jiného zařízení. Zařízení se stejným názvem lokace a stejnými šifrovacími klíči tzv. lokaci.
- Tlačítko Import – importuje ID lokace a aktuální šifrovací klíče ze souboru exportovaného z jiného přístupového terminálu. Zařízení se stejným názvem lokace a stejnými šifrovacími klíči tzv. lokaci.



- **Tlačítko Obnovit primární klíč** – vygenerováním nového primárního šifrovacího klíče dojde k smazání nejstaršího sekundárního klíče. Uživatelé aplikace 2N® Mobile Key, kteří stále používají tento klíč, se nebudou moci autentizovat, pokud před touto operací neaktualizují šifrovací klíče ve svém mobilním zařízení. Klíče v mobilním zařízení se aktualizují při každém použití aplikace **2N® Mobile Key**.
- **Tlačítko Smazat primární klíč** – odstraněním primárního klíče se uživatelé, který tento klíč používají, nebudou moci autentizovat.
- **Tlačítko Smazat sekundární klíč** – uživatelé aplikace **2N® Mobile Key**, kteří stále používají tento klíč, se nebudou moci po smazání klíče autentizovat, pokud před touto operací neaktualizují šifrovací klíče ve svém mobilním zařízení. Klíče v mobilním zařízení se aktualizují při každém použití aplikace **2N® Mobile Key**.



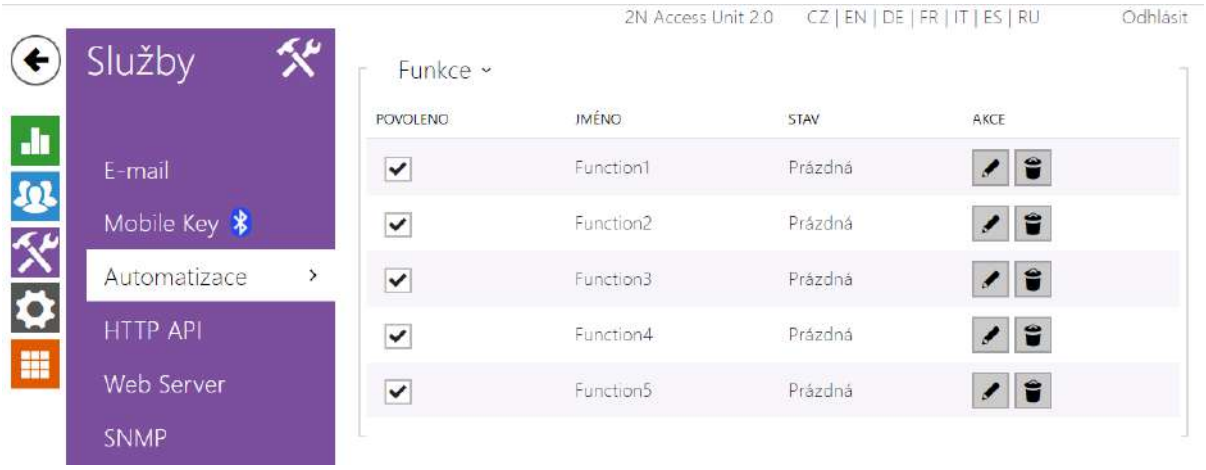
- **Platnost párovacího PINu** – doba platnosti autorizačního PINu pro párování mobilního zařízení uživatele s přístupovým terminálem.

Tip

- V případě nahlášení ztráty telefonu s uloženými přístupovými údaji doporučujeme následující postup:

1. Vymažte hodnotu Mobile Key Auth ID příslušného uživatele – čímž dojde k blokování ztraceného telefonu a znemožnění jeho zneužití.
2. Přegenerujte primární šifrovací klíč (volitelný krok) – čímž znemožníte případné zneužití šifrovacího klíče uloženého v mobilním zařízení.

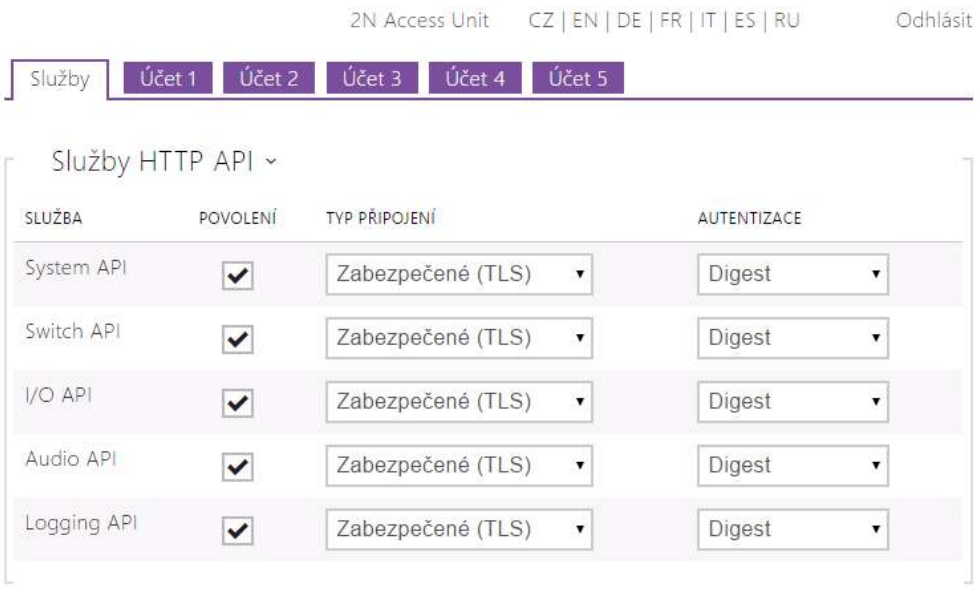
5.4.3 Automatizace



Přístupový terminál **2N Access Unit** poskytuje velmi flexibilní možnosti nastavení dle různorodých požadavků uživatele. Existují situace, kdy běžný rozsah nastavení (např. nastavení chování spínačů nebo volání) nedostačuje, a pro tyto případy poskytuje přístupový terminál **2N Access Unit** speciální programovatelné rozhraní **Automation**. Typické použití **Automation** je v aplikacích, které vyžadují složitější propojení se systémy třetích stran.

Detailní popis funkce a konfigurace **Automation** je k dispozici v manuálu Konfigurace **Automation**.

5.4.4 HTTP API



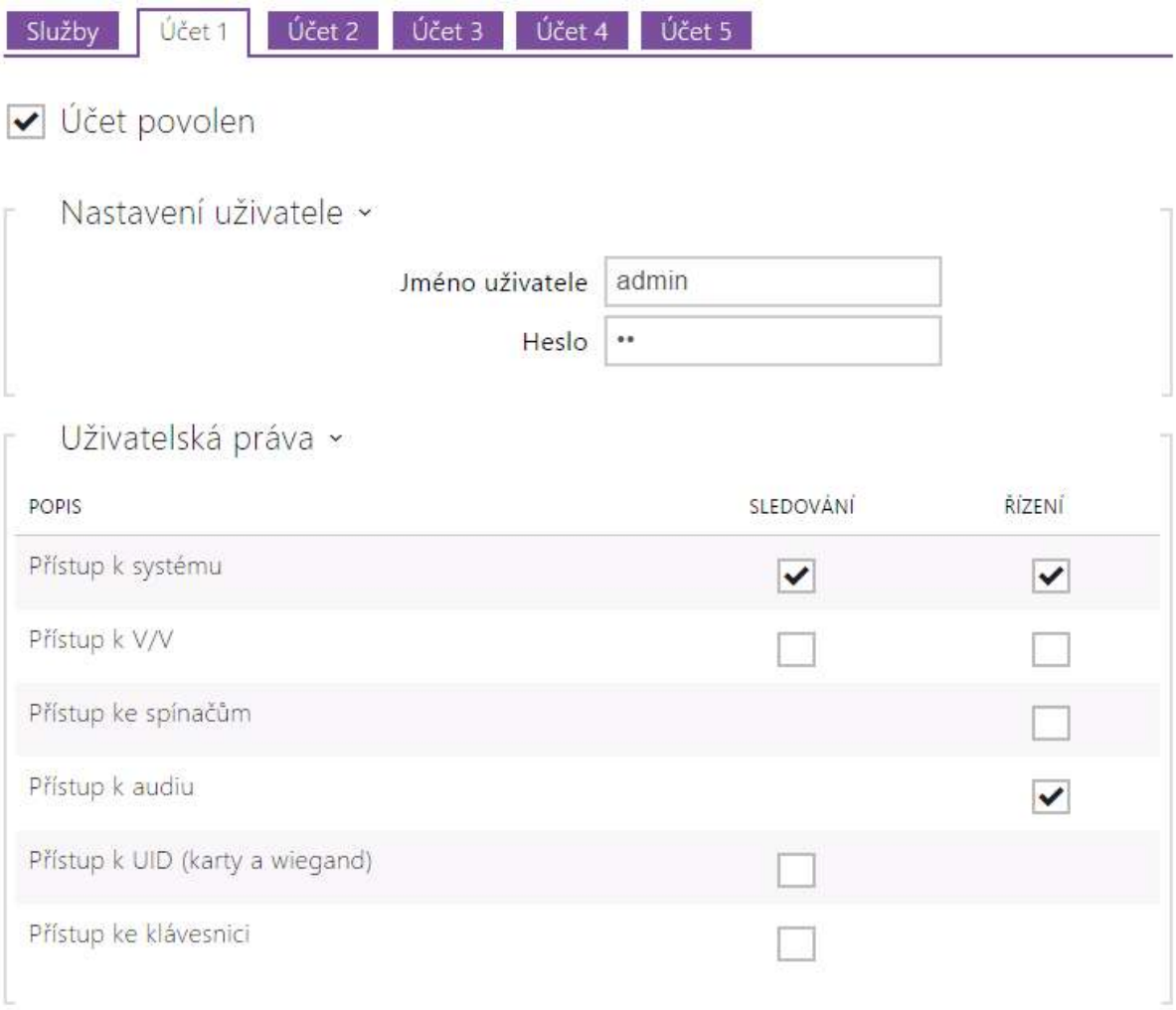
2N HTTP API je aplikační rozhraní pro ovládání vybraných funkcí interkomu pomocí HTTP protokolu. Toto rozhraní umožňuje jednoduše integrovat 2N IP interkomy s produkty třetích stran, např. systémy domácí automatizace, zabezpečovací a monitorovací systémy budov apod.

2N HTTP API je podle funkce rozděleno do následujících služeb:

- System API – umožňuje změny konfigurace, získání stavu a upgrade interkomu.
- Switch API – umožňuje řízení a sledování stavu spínačů, např. otvírání dveřních zámků apod.
- I/O API – umožňuje řízení a sledování logických vstupů a výstupů interkomu.
- Audio API – umožňuje změnu nastavení zvuku.
- Logging API – Logging API

Pro každou službu lze nastavit transportní protokol (HTTP nebo HTTPS) a způsob autentizace (žádná, Basic nebo Digest). V konfiguraci HTTP API lze vytvořit až pět uživatelských účtů (s vlastním jménem a heslem) s možností detailního řízení přístupu k jednotlivým službám a funkcím.

Detailní popis funkce a nastavení HTTP API je k dispozici v manuálu 2N HTTP API.


Služby
Účet 1
Účet 2
Účet 3
Účet 4
Účet 5
Účet povolen
Nastavení uživatele
Jméno uživatele
admin
Heslo
Uživatelská práva
POPIS
SLEDOVÁNÍ
ŘÍZENÍ
Přístup k systému
Přístup k V/V
Přístup ke spínačům
Přístup k audiu
Přístup k UID (karty a wiegand)
Přístup ke klávesnici

5.4.5 Web server

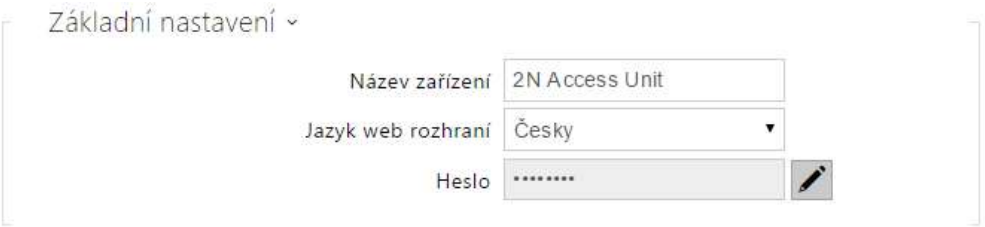
Přístupové terminály **2N Access Unit** lze konfigurovat pomocí běžného prohlížeče, který přistupuje k web serveru integrovanému v přístupovém terminálu. Pro komunikaci mezi prohlížečem a přístupovým terminálem se používá zabezpečený protokol HTTPS. Pro přihlášení k přístupovému terminálu je nutné zadat přihlašovací jméno a heslo. Výchozí jméno a heslo pro přihlášení je **admin** a **2n**. Výchozí heslo doporučujeme co nejdříve změnit.

Služba web server je využívána i dalšími funkcemi interkomu:

1. a. HTTP příkazy pro ovládání spínačů, viz kapitola Spínače
   b. Událost Event.HttpTrigger ve **2N Automation**, viz příslušný manuál.

Pro tyto speciální případy lze pro komunikaci použít nezabezpečený HTTP protokol.

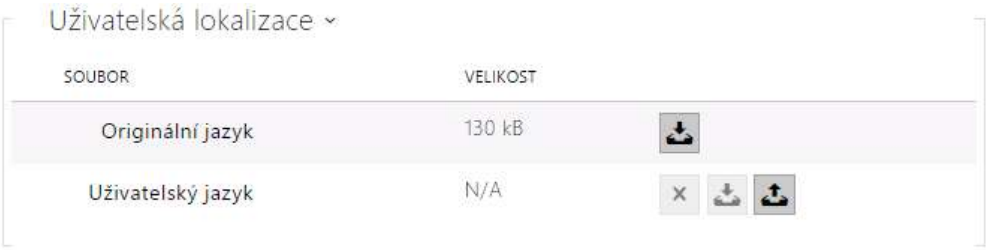
Seznam parametrů



- **Název zařízení** – nastavuje název zařízení zobrazovaný v pravém horním rohu webového rozhraní, v přihlašovacím okně a případně v dalších aplikacích (**2N® IP Manager**, **2N® IP Network Scanner** apod.)
- **Jazyk web rozhraní** – nastavuje výchozí jazyk po přihlášení k administračnímu web serveru. Jazyk webového rozhraní můžete kdykoli dočasně změnit pomocí tlačítek v horní liště stránky.

- **Přístupové heslo** – nastavuje heslo pro přihlášení k přístupovému terminálu. Ke změně hesla použijte tlačítko . Heslo musí obsahovat minimálně 8 znaků, z toho jedno malé písmeno abecedy, jedno velké písmeno abecedy a alespoň jednu číslici.

- **HTTP port** – nastavuje komunikační port web serveru pro komunikaci pomocí nezabezpečeného protokolu HTTP. Změna portu se projeví až po restartu interkomu.
- **HTTPS port** – nastavuje komunikační port web serveru pro komunikaci pomocí zabezpečeného protokolu HTTPS. Změna portu se projeví až po restartu interkomu.
- **Nejnižší povolená verze TLS** – určuje nejnižší verzi TLS, která bude povolena pro připojení k zařízením.
- **HTTPS osobní certifikát** – nastavuje uživatelský certifikát a privátní klíč, pomocí kterých se provádí šifrování komunikace mezi HTTP serverem interkomu a webovým prohlížečem na straně uživatele. Lze zvolit jednu ze tří sad uživatelských certifikátů a privátních klíčů, viz kapitola Certifikáty, nebo ponechat nastavení **Self Signed**, kdy se použije automaticky vygenerovaný certifikát vytvořený při prvním spuštění zařízení.
- **Povolit vzdálený přístup** – umožňuje povolit vzdálený přístup k web serveru interkomu z IP adres mimo lokální síť.



- **Originální jazyk** – umožňuje stáhnout ze zařízení originální soubor obsahující všechny texty uživatelského rozhraní v anglickém jazyce. Soubor je ve formátu XML viz níže.
- **Uživatelský jazyk** – umožňuje nahrát, stáhnout a případně odstranit uživatelský soubor s vlastními překlady textů uživatelského rozhraní.

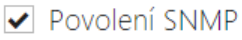
```
<?xml version="1.0" encoding="UTF-8"?>
<strings language="English" languageshort="EN">
  <!-- Global enums-->
  <s id="enum/error/1">Invalid value!</s>
  <s id="enum/bool_yesno/0">NO</s>
  <s id="enum/bool_yesno/1">YES</s>
  <s id="enum/bool_user_state/0">ACTIVE</s>
  <s id="enum/bool_user_state/1">INACTIVE</s>
  <s id="enum/bool_profile_state/0">ACTIVE</s>
  <s id="enum/bool_profile_state/1">INACTIVE</s>
  ..
  ..
  ..
</strings>
```

Při překladu modifikujte pouze hodnoty elementů **<s>** a neupravujte hodnoty atributů **id**. Jméno jazyka dané atributem **language** elementu **<strings>** bude uvedeno ve volbách parametru Jazyk web rozhraní. Zkratka jména jazyka daná atributem **languageshort** elementu **<strings>** bude uvedena v seznamu jazyku v horním pravém rohu okna a bude sloužit k rychlému přepínání mezi jazyky.

5.4.6 SNMP

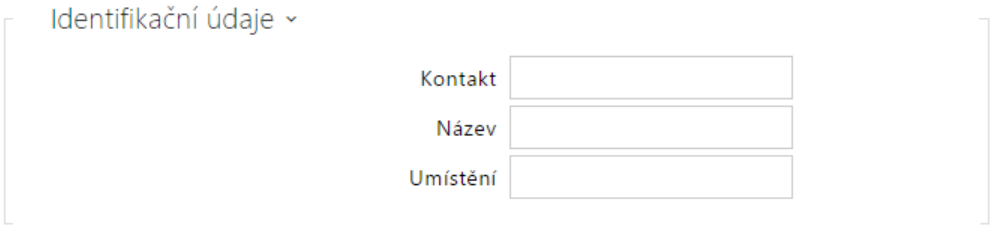
Přístupové terminály **2N Access Unit** integrují funkcionalitu umožnující vzdálený dohled přístupových terminálu v sítí pomocí protokolu SNMP. Interkomy podporují SNMP protokol verze 2c.

Seznam parametrů

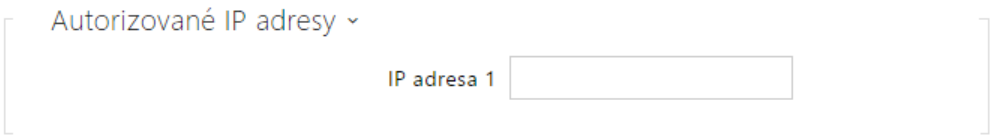


- **Povolení SNMP** – umožňuje zapnutí této funkce

- **Identifikátor komunity** – textový řetězec reprezentující přístupový klíč pro přístup k objektům v MIB tabulce
- **IP adresa pro trapy** – IP adresa, na kterou budou odesílaný SNMP trapy
- **Stáhnout soubor MIB** – umožňuje stáhnout aktuální definici MIB tabulky ze zařízení



- **Kontakt** – umožňuje zadat kontakt na správce zařízení (např. jméno, e-mail apod.)
- **Název** – umožňuje zadat název zařízení
- **Umístění** – umožňuje zadat popis umístění zařízení (např. 1. patro).

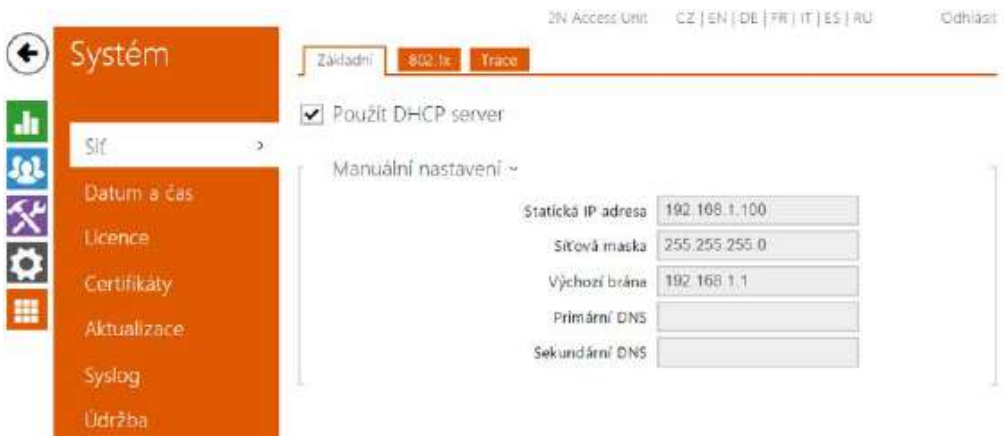


- **IP Adresa** – umožňuje zadat až 4 IP platné adresy pro přístup k SNMP agentu. Přístup z ostatních adres bude blokován. Pokud pole zůstane nevyplněné, lze k zařízení přistupovat z libovolné IP adresy.

5.5 Systém

Zde je přehled toho, co v kapitole naleznete:

5.5.1 Síť



Přístupový terminál **2N Access Unit** se připojuje do lokální sítě a pro správnou funkci musí mít nastavenou platnou IP adresu, příp. může IP adresu získat z DHCP serveru v této síti. IP adresa a nastavení DCHP se konfiguruje v záložce Síť.

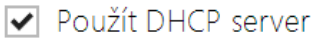
Tip

- *Pokud chcete zjistit aktuální IP adresu svého přístupového terminálu, můžete využít aplikaci **2N® IP Network Scanner**, která je volně ke stažení na stránkách **www.2n.cz** nebo můžete použít mechanismus popsaný v instalačním manuálu k příslušnému přístupovému terminálu – přístupový terminál vám sdělí svou IP adresu sám pomocí hlasové funkce.*

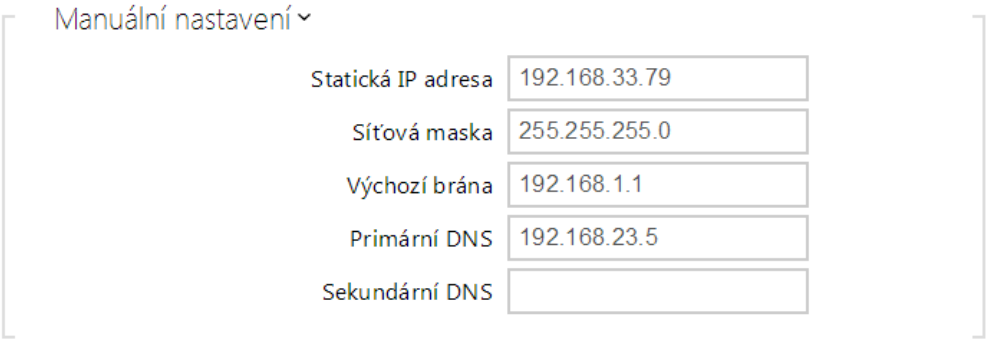
Jestliže ve své síti používáte RADIUS server a mechanismus ověřování připojených zařízení založený na protokolech 802.1x, můžete interkom nakonfigurovat tak, aby používal autentizaci EAP-MD5 nebo EAP-TLS. K nastavení této funkce slouží záložka 802.1x.

V záložce Trace můžete spustit zachytávání příchozích a odchozích paketů na síťovém rozhraní přístupového terminálu. Soubor se zachycenými pakety lze stáhnout a dále zpracovat např. pomocí aplikace Wireshark (**www.wireshark.org).**

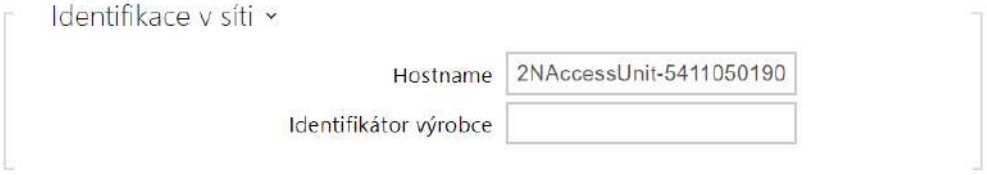
Seznam parametrů



- **Použít DHCP server** – povoluje automatické získání IP adresy z DHCP serveru v lokální síti. Pokud ve vaší síti DHCP server není nebo jej nelze použít z jiného důvodu, použijte manuální nastavení sítě.

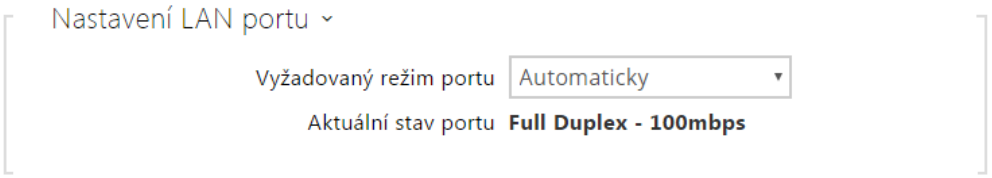


- **Statická IP adresa** – statická IP adresa přístupového terminálu. Adresa je použita společně s parametry níže, pokud není nastaven parametr Použít DHCP server.
- **Maska sítě** – nastavuje masku sítě.
- **Výchozí brána** – adresa výchozí brány, která umožňuje komunikaci se zařízeními mimo lokální síť.
- **Primární DNS** – adresa primárního DNS serveru pro překlad doménových jmen na IP adresy. V případě obnovení továrního nastavení zařízení bude primární DNS server nastaven na adresu 8.8.8.8.
- **Sekundární DNS** – adresa sekundárního DNS serveru, který je použit v případě, kdy primární DNS server není dostupný. V případě obnovení továrního nastavení zařízení bude sekundární DNS server nastaven na adresu 8.8.4.4.



- **Hostname** – nastavení identifikace 2N IP interkomu v síti.
- **Identifikátor výrobce** – nastavuje identifikátor výrobce jako znakový řetězec pro DHCP Option 60.

- **VLAN povolena** – zapíná podporu virtuální sítě (VLAN podle doporučení 802.1q). Pro správnou funkci je potřeba nastavit také ID virtuální sítě.
- **VLAN ID** – zvolené ID virtuální sítě v rozsahu 1-4094. Zařízení bude přijímat pouze pakety označené tímto ID. V případě nevhodného nastavení může dojít ke ztrátě připojení a následné je nutné zařízení uvést do výchozího stavu pomocí továrního nastavení.

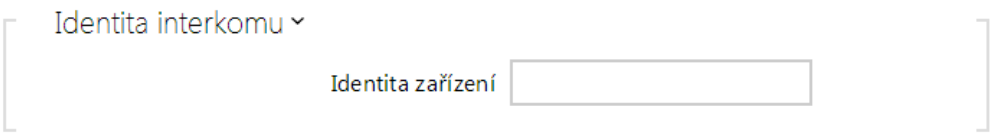


- **Vyžadovaný režim portu** – preferovaný režim portu síťového rozhraní (Automaticky nebo Half Duplex – 10 mbps). Umožňuje snížit přenosovou rychlost na 10 mbps v případě, že použitá síťová infrastruktura (kabeláž) není spolehlivá pro 100 mbps provoz.
- **Aktuální stav portu** – aktuální stav portu síťového rozhraní (Half nebo Full Duplex – 10 mbps nebo 100 mbps).

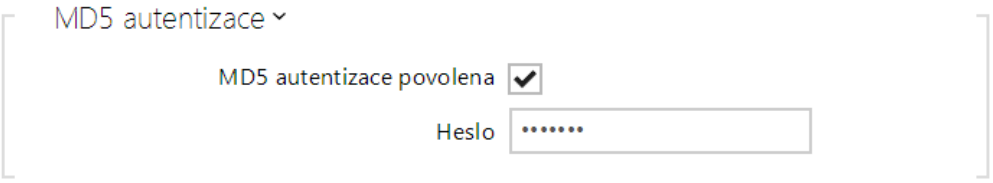
- **Ověřit dostupnost adresy v síti** – slouží k ověření dostupnosti dané adresy v síti jako příkaz „Ping“ v běžných operačních systémech. Po stisknutí tlačítka „Ping“ se zobrazí dialog, ve kterém je možno zadat IP adresu nebo doménové jméno a tlačítkem „Ping“ odeslat zkušební data na tuto adresu. Pokud je zadaná IP adresa nebo doménové jméno neplatné, je zobrazeno upozornění a tlačítko „Ping“ je neaktivní, dokud není zadávaná adresa platná. V dialogu se dále zobrazuje stav provádění funkce a výsledek. Stav „Selhal“ („Failed“) může znamenat buď nedostupnost zadané adresy do 10 vteřin, nebo nemožnost přeložit doménové jméno na adresu. Jestliže je přijata platná odpověď, je zobrazena IP adresa, ze které tato odpověď přišla, a délka čekání na odpověď v milisekundách. Novým stisknutím tlačítka „Ping“ je odeslán další dotaz na stejnou adresu.

Záložka 802.1x

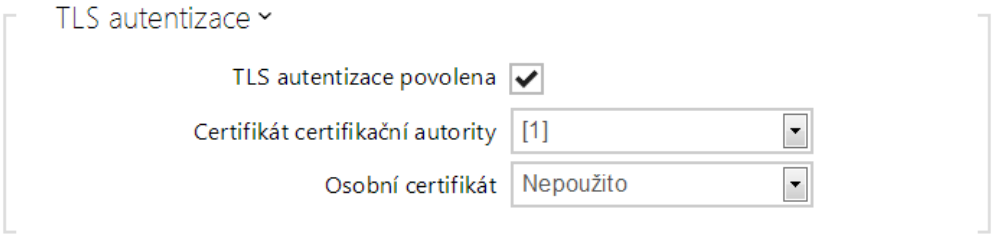
Záložka se nezobrazuje pro 2N Access Unit 2.0, která nepodporuje protokol 802.1x.



- **Identita zařízení** – jméno uživatele (identita) pro autentizaci pomocí metod EAP-MD5 a EAP-TLS.



- **MD5 autentizace povolena** – povoluje použití autentizace zařízení v síti pomocí protokolu 802.1x EAP-MD5. V případě, že vaše síť 802.1x nepodporuje, tuto funkci nezapínejte. V opačném případě se interkom stane nedostupným.
- **Heslo** – přístupové heslo použité pro autentizaci pomocí metody EAP-MD5.

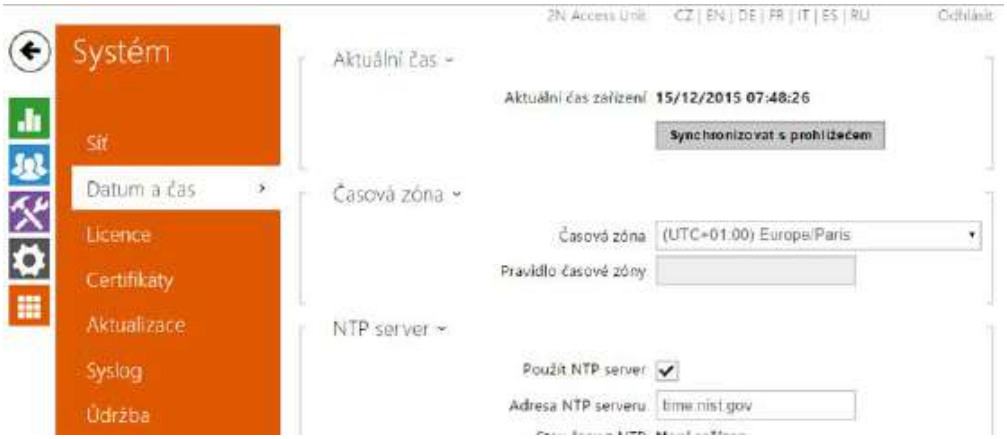


- **TLS autentizace povolena** – povoluje použití autentizace zařízení v síti pomocí protokolu 802.1x EAP-TLS. V případě, že vaše síť 802.1x nepodporuje, tuto funkci nezapínejte. V opačném případě se přístupový terminál stane nedostupným.
- **Certifikát certifikační autority** – specifikuje sadu certifikátů certifikačních autorit pro ověření platnosti veřejného certifikátu RADIUS serveru. Lze zvolit jednu ze tří sad certifikátů, viz kapitola Certifikáty. Pokud není certifikát certifikační autority uveden, veřejný certifikát RADIUS serveru se neověřuje.
- **Osobní certifikát** – specifikuje uživatelský certifikát a privátní klíč, pomocí kterých se ověřuje oprávnění přístupového terminálu komunikovat v lokální síti na portu síťového prvku zabezpečeném pomocí 802.1x. Lze zvolit jednu ze tří sad uživatelských certifikátů a privátních klíčů, viz kapitola Certifikáty.

Záložka Trace

V záložce Trace můžete spustit zachytávání příchozích a odchozích paketů na síťovém rozhraní přístupového terminálu. Zachycené pakety se ukládají do bufferu o velikosti 4 MB. Po zaplnění bufferu dochází automaticky k přepisu nejstarších uložených paketů. Při zachytávání paketů doporučujeme snížit přenosovou rychlost video streamu pod hodnotu 512 kbps. Zachytávání můžete spustit pomocí tlačítka  , zastavit pomocí tlačítka  a soubor se zachycenými pakety stáhnout pomocí tlačítka  .

5.5.2 Datum a čas



Pokud používáte nastavení časových profilů pro kódy pro spínání zámku apod., je nezbytné, aby měl přístupový terminál správně nastavené interní datum a čas.

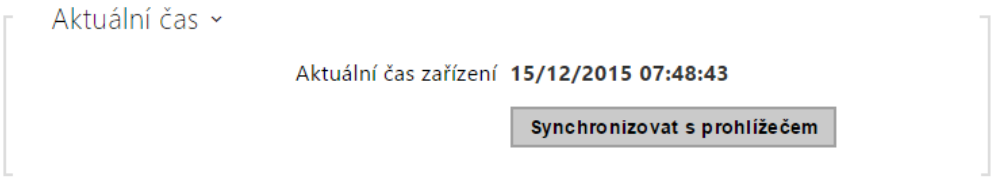
Přístupové terminály 2N® Access Unit jsou vybaveny zálohovanými hodinami reálného času, které umožňují překonat výpadek napájení po dobu až několika dnů. Čas v přístupovém terminálu můžete kdykoli synchronizovat s aktuálním časem ve svém PC pomocí tlačítka Synchronizovat.

Poznámka

- *Správné nastavení data a času není pro základní funkci přístupového terminálu nezbytné. Aktuální datum a čas jsou potřeba pro správnou funkci časových profilů a pro správné zobrazení času událostí v různých seznamech (Syslog, záznamy o přiložených kartách, log zařízení stahovaný pomocí 2N HTTP API apod.)*

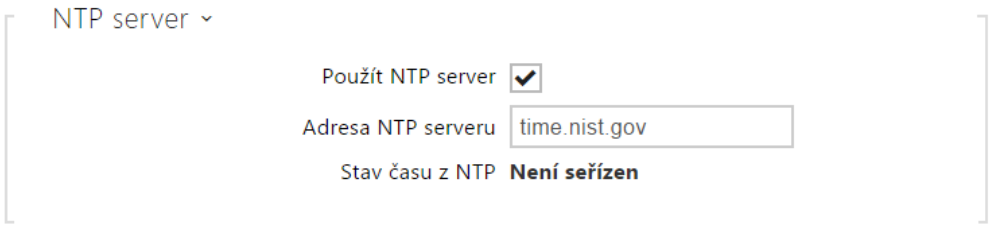
V běžných provozních podmínkách je přesnost obvodu reálného času v interkomu přibližně ±0,005 %, což může znamenat chybu až ±2 minuty/měsíc. Pro maximální přesnost a spolehlivost doporučujeme vždy synchronizovat čas s NTP serverem. Přístupový terminál provádí v pravidelných intervalech dotaz na tento server a aktualizuje svůj vlastní čas

Seznam parametrů



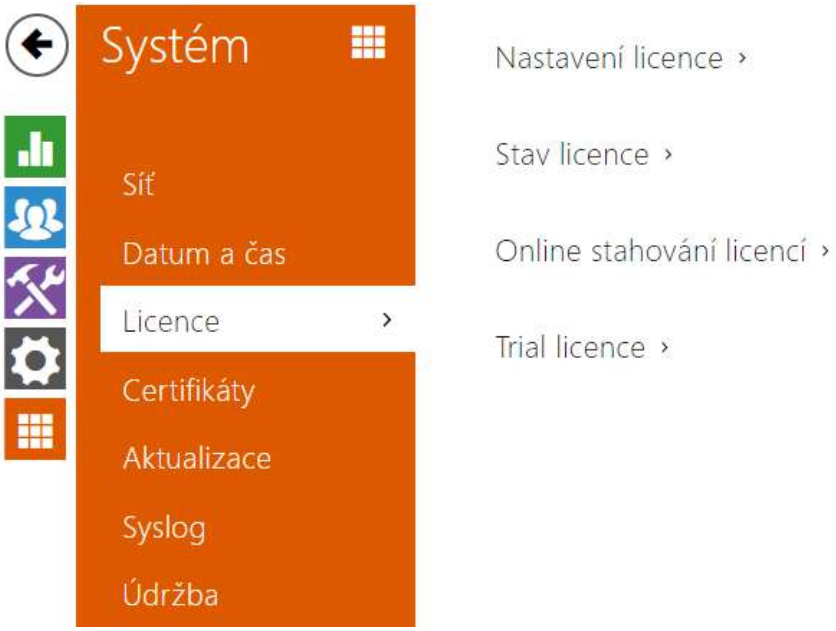
Synchronizovat – pomocí tlačítka můžete kdykoli synchronizovat čas v přístupovém terminálu s aktuálním časem ve svém PC.

- Časová zóna – nastavuje časovou zónu pro místo instalace přístupového terminálu. Nastavení určuje časový posun a přechody mezi letním a zimním časem.
- Pravidlo časové zóny – pokud je přístupový terminál nainstalován v lokalitě, která není uvedena v seznamu parametru Časová zóna, lze nastavit pravidlo časové zóny manuálně. Pravidlo časové zóny se uplatní pouze tehdy, jestliže je parametr Časová zóna nastaven na hodnotu ručně specifikovat časový posun a přechody mezi letním a zimním časem. Parametr Časová zóna musí být nastaven na hodnotu Manuální nastavení.



- Použít NTP server – povoluje použití NTP serveru pro synchronizaci vnitřního času přístupového terminálu.
- Adresa NTP serveru – nastavuje IP adresu nebo doménové jméno NTP serveru, podle kterého interkom synchronizuje vnitřní čas.

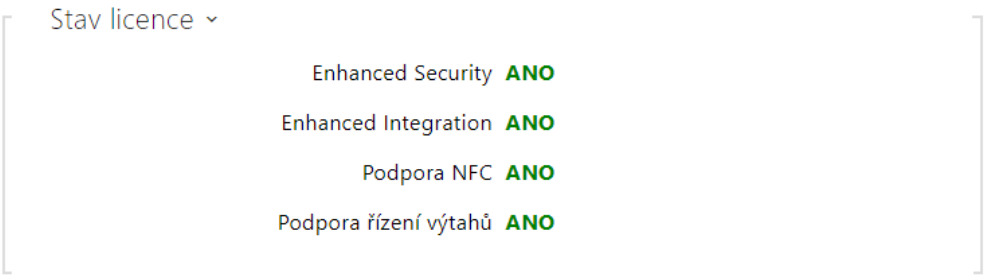
5.5.3 Licence



Některé funkce 2N Access Unit jsou dostupné pouze po zadání platného licenčního klíče. Seznam možností licencování přístupových terminálů naleznete v kapitole Licencované funkce.

Seznam parametrů

- Sériové číslo – zobrazuje sériové číslo zařízení, pro které je licence platná.
- Licenční klíč – umožňuje vložit platný licenční klíč.
- Platný licenční klíč – zobrazuje, zda vložený licenční klíč je platný.

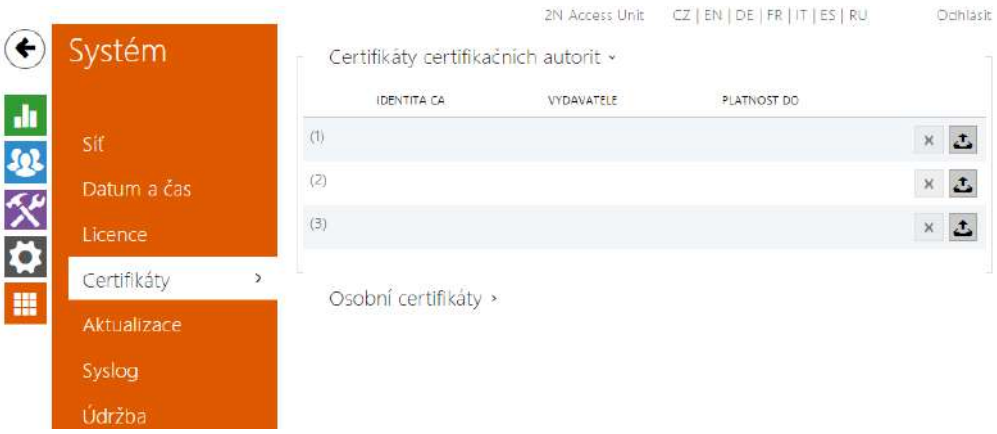


- **Enhanced Security** – zobrazuje, zda jsou k dispozici funkce aktivované licencí Enhanced Security.
- **Enhanced Intergration** – zobrazuje, zda jsou k dispozici funkce aktivované licencí Enhanced Integration.
- **Podpora NFC** – zobrazuje, zda je k dispozici funkce NFC.
- **Podpora řízení výtahů** – zobrazuje, zda je k dispozici funkce aktivované Lift Module licence.

- **Automatická aktualizace** – zařízení aktualizuje licenční klíč z Licenčního serveru 2N.
- **Ruční aktualizace** – manuální dotaz na ověření dostupnosti licence.
- **Stav ruční aktualizace** – probíhá, aktualizováno, nespecifikováno, chyba: licence není dostupná.

- **Stav trial licence** – zobrazuje stav trial licence (neaktivována, aktivována, platnost vypršela).
- **Zbývající doba platnosti trial licence** – zobrazuje zbývající dobu platnosti trial licence.

5.5.4 Certifikáty



Některé síťové služby přístupového terminálu **2N Access Unit** využívají pro komunikaci s ostatními zařízeními v síti zabezpečený protokol TLS. Tento protokol zamezuje třetím stranám odposlouchávat příp. modifikovat obsah komunikace. Při navazování spojení pomocí TLS protokolu probíhá jednostranná příp. oboustranná autentizace, která vyžaduje certifikáty a privátní klíče.

Služby přístupového terminálu, které využívají protokol TLS:

1. Web server (protokol HTTPS)
2. E-mail (protokol SMTP)
3. 802.1x (protokol EAP-TLS)
4. SIPs

Přístupové terminály **2N Access Unit** umožňují nahrát až 3 sady certifikátů certifikačních autorit, které slouží k ověřování identity zařízení, se kterým interkom komunikuje, a zároveň nahrát 3 osobní certifikáty a privátní klíče, pomocí kterých se šifruje komunikace.

Každé službě přístupového terminálu vyžadující certifikáty můžete přiřadit jednu ze sad certifikátů, viz kapitoly **Web Server**, **E-mail** a **Streaming**. Certifikáty mohou být sdíleny více službami současně.

2N Access Unit akceptuje certifikáty ve formátech DER (ASN1) a PEM.

Při prvním připojení napájení k přístupovému terminálu se automaticky vygeneruje tzv. **Self Signed certifikát** a **privátní klíč**, který lze použít pro službu **Web server** a **E-mail** bez nutnosti nahrát vlastní certifikát a privátní klíč.

Poznámka

- *V případě, že používáte Self Signed certifikát pro šifrování komunikace mezi web serverem přístupového terminálu a prohlížečem, komunikace je zabezpečena, ale prohlížeč vás upozorní, že nemůže ověřit důvěryhodnost certifikátu přístupového terminálu.*

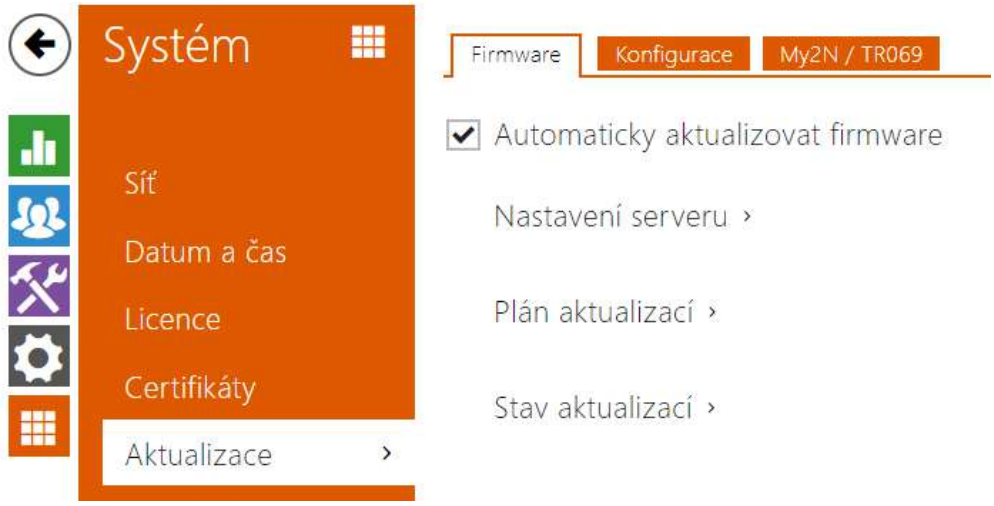
Aktuální přehled nahraných certifikátů certifikačních autorit a osobních certifikátů se zobrazuje ve dvou tabulkách:

Stiskem tlačítka  můžete do zařízení nahrát certifikát uložený ve vašem PC. V dialogovém okně vyberte soubor s certifikátem (příp. privátním klíčem) a stiskněte tlačítko **Nahrát**. Stiskem tlačítka  certifikát z interkomu odstraníte.

Upozornění

- V případě použití certifikátů založených na eliptických křivkách je možné použít pouze křivky secp256r1 (aka prime256v1 aka NIST P-256) a secp384r1 (aka NIST P-384).

5.5.5 Aktualizace



2N Access Unit umožňuje kromě manuální aktualizace firmware a konfigurace také automaticky stahovat a aktualizovat firmware a konfiguraci podle stanovených pravidel z úložiště na vámi definovaném TFTP nebo HTTP serveru.

Adresa TFTP a HTTP serveru může být nakonfigurována manuálně. 2N Access Unit podporuje automatické zjištění adresy pomocí místního DHCP serveru (tzv. Option 66).

Záložka Firmware

Na této záložce se nastavuje automatické stahování firmware z vámi definovaného serveru. Přístupový terminál v nastavených intervalech porovnává soubor na serveru s aktuálním firmware a v případě, že firmware na serveru je novější, provede automatickou aktualizaci včetně restartu přístupového terminálu (cca 30 s). Doporučujeme proto nastavit časově aktualizaci tak, aby probíhala v době minimálního využívání interkomu (např. v noci).

2N Access Unit očekává na serverech soubory s názvy:

1. MODEL-firmware.bin – firmware přístupového terminálu
2. MODEL-common.xml – společná konfigurace všech přístupových terminálů daného modelu
3. MODEL-MACADDR.xml – specifická konfigurace pro jeden přístupový terminál

MODEL v názvu souboru specifikuje model interkomu:

1. au – 2N Access Unit

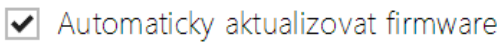
MACADDR je MAC adresa interkomu ve formátu 00-00-00-00-00-00. MAC adresu přístupového terminálu naleznete na výrobním štítku nebo přímo ve webovém rozhraní v záložce Stav.

Příklad:

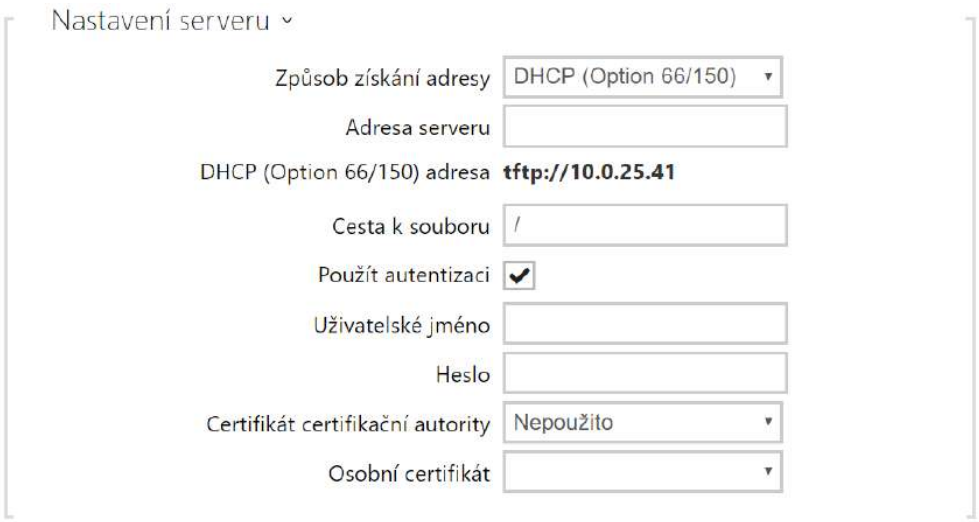
2N Access Unit s MAC adresou 00-87-12-AA-00-11 bude stahovat z TFTP serveru soubory s těmito názvy:

- au-firmware.bin
- au-common.xml
- au-00-87-12-aa-00-11.xml

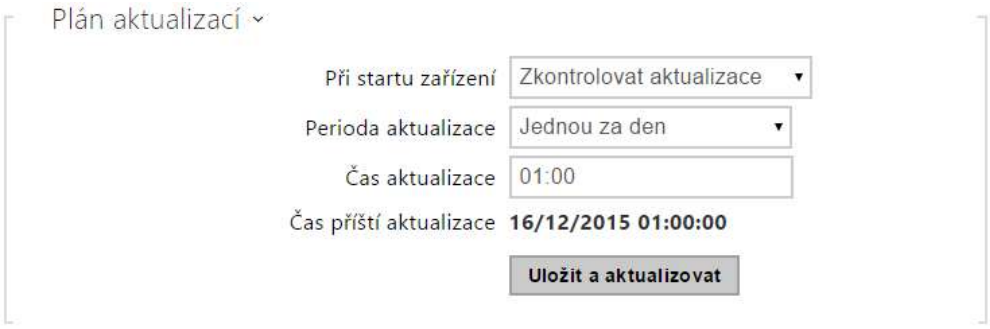
Seznam parametrů



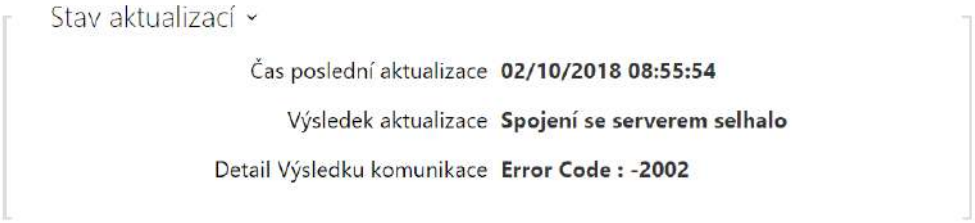
- Automaticky aktualizovat firmware/konfiguraci – povoluje automatické stahování firmware/konfigurace z TFTP/HTTP serveru.



- **Způsob získání adresy** – umožňuje zvolit, zda adresa TFTP/HTTP serveru bude zadána manuálně nebo se použije adresa získaná automaticky z DHCP serveru pomocí parametru Option 66.
- **Adresa serveru** – umožňuje manuálně zadat adresu serveru TFTP (**tftp://ip_adresa**), HTTP (**http://ip_adresa**) nebo HTTPS (**https://ip_adresa**).
- **DHCP (Option 66) adresa** – zobrazuje adresu serveru získanou pomocí DHCP Option 66 nebo 150.
- **Cesta k souboru** – nastavuje adresář příp. předponu názvu souboru s firmware nebo konfigurací na serveru. Přístupový terminál očekává soubory s názvy au_firmware.bin, au-common.xml a au-MACADDR.xml.
- **Použít autentizaci** – umožňuje nastavit používání autentizaci pro přístup k HTTP serveru.
- **Uživatelské jméno** – uživatelské jméno použité pro autentizaci na serveru.
- **Heslo** – heslo pro použité pro autentizaci na serveru.
- **Certifikát certifikační autority** – specifikuje sadu certifikátů certifikačních autorit pro ověření platnosti veřejného certifikátu ACS serveru.
- **Osobní certifikát** – specifikuje uživatelský certifikát a privátní klíč, pomocí kterých se ověřuje oprávnění interkomu komunikovat se ACS serverem.



- **Při startu zařízení** – povoluje kontrolu anebo provedení aktualizace po každém startu přístupového terminálu.
- **Perioda aktualizace** – nastavuje periodu provádění aktualizace. Automatickou aktualizaci lze nastavit jednou za hodinu, den, týden, měsíc nebo periodu nastavit manuálně.
- **Čas aktualizace** – umožňuje nastavit čas ve formátu HH:MM, kdy se má aktualizace pravidelně provádět. Takto lze nastavit provádění aktualizace v době, kdy je přístupový terminál nejméně využíván. Parametr se neuplatní, pokud perioda aktualizace je nastavena na dobu kratší než jeden den.
- **Čas příští aktualizace** – zobrazuje čas naplánovaného provedení další aktualizace.



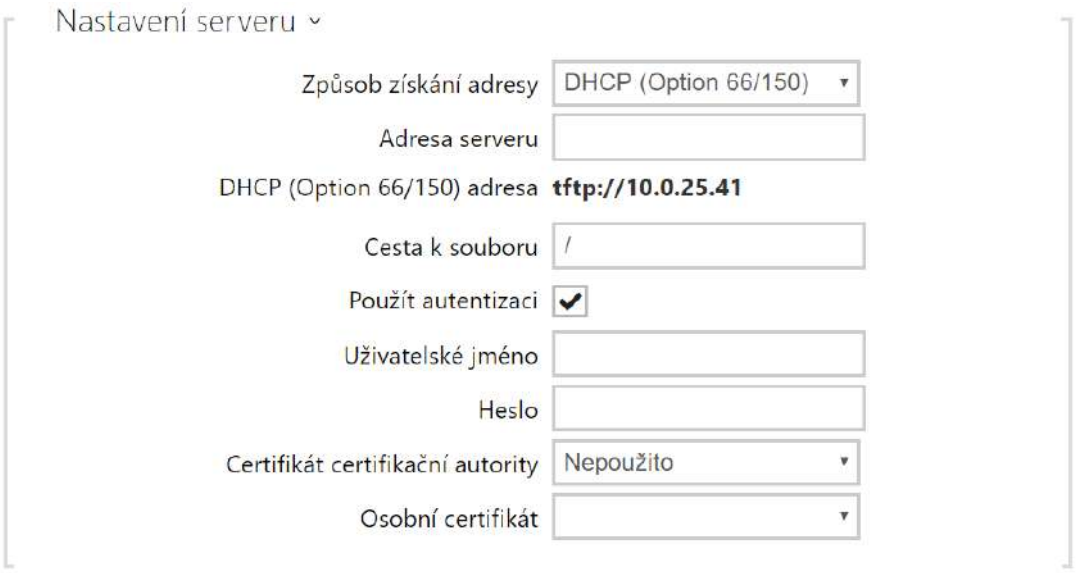
- **Čas poslední aktualizace** – zobrazuje čas naposledy provedené aktualizace.
- **Výsledek aktualizace** – zobrazuje výsledek naposledy provedené aktualizace. Možné hodnoty jsou následující: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Detail Výsledku komunikace** – chybný kód komunikace se serverem nebo status kód protokolu TFTP/HTTP.

Výsledek	Popis
Probíhá...	Aktualizace právě probíhá
Aktualizováno	Konfigurace/firmware byl bezchybně aktualizován. V případě stažení firmware dojde během několika sekund k restartu zařízení.
Firmware je aktuální	Byl proveden pokus o stažení nového firmware a bylo zjištěno, že firmware zařízení je aktuální.
Server není dostupný	Nepodařilo se načíst adresu serveru pomocí DHCP Option 66 nebo 150.
Neplatné doménové jméno	Doménové jméno serveru není platné, příp. DNS server je špatně nakonfigurován nebo není dostupný.
Server není dostupný	Dotazovaný HTTP/TFTP server neodpovídá.
Stahování selhalo	Při stahování souboru nastala dále nespecifikovaná chyba.
Soubor nenalezen	Soubor na serveru nebyl nalezen.
Soubor není platný	Stahovaný soubor je poškozen nebo není správného typu.

Záložka Konfigurace

Na této záložce se nastavuje automatické stahování konfigurace z vámi definovaného serveru. 2N Access Unit v nastavených intervalech stáhne soubor ze serveru a rekonfiguruje se. Při této aktualizaci nedochází k restartu přístupového terminálu.

- Automaticky aktualizovat konfiguraci – povoluje automatické stahování konfigurace z TFTP/HTTP serveru.

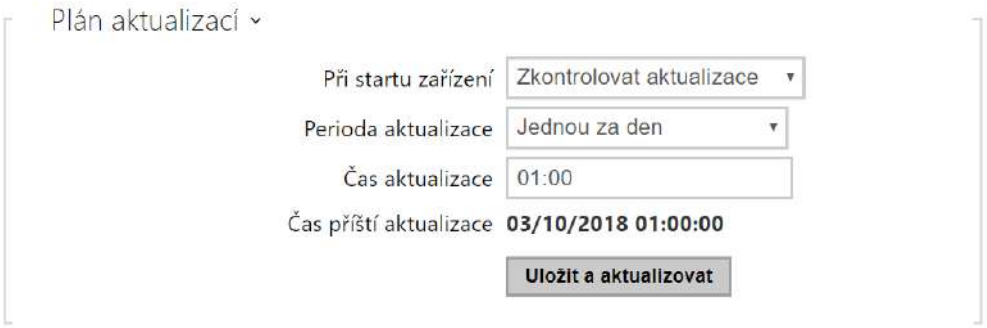


- Způsob získání adresy – umožňuje zvolit, zda adresa TFTP/HTTP serveru bude zadána manuálně nebo se použije adresa získaná automaticky z DHCP serveru pomocí parametru Option 66.
- Adresa serveru – umožňuje manuálně zadat adresu serveru TFTP (tftp://ip_adresa), HTTP (http://ip_adresa) nebo HTTPS (https://ip_adresa).
- DHCP (Option 66) adresa – zobrazuje adresu serveru získanou pomocí DHCP Option 66 nebo 150.
- Cesta k souboru – nastavuje adresář příp. předponu názvu souboru s firmware nebo konfigurací na serveru. Interkom očekává soubory s názvy XhipY_firmware.bin, XhipY-common.xml a XhipY-MACADDR.xml, kde X je předpona daná tímto parametrem a Y specifikuje model interkomu.
- Použít autentizaci – umožňuje nastavit používání autentizaci pro přístup k HTTP serveru.
- Uživatelské jméno – uživatelské jméno použité pro autentizaci na serveru.
- Heslo – heslo pro použité pro autentizaci na serveru.

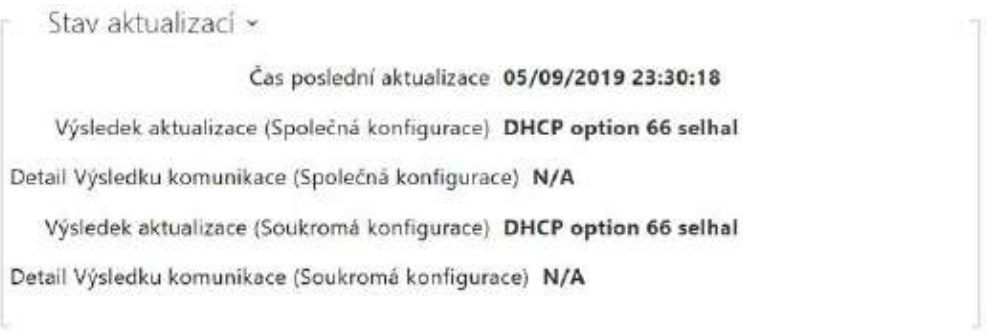
- **Certifikát certifikační autority** – specifikuje sadu certifikátů certifikačních autorit pro ověření platnosti veřejného certifikátu ACS serveru.
- **Osobní certifikát** – specifikuje uživatelský certifikát a privátní klíč, pomocí kterých se ověřuje oprávnění interkomu komunikovat se ACS serverem.

Info

- Intercom obsahuje Factory Cert certifikát, podepsaný certifikát, který je možné použít např. pro integraci s British Telecom.



- **Při startu interkomu** – povoluje kontrolu anebo provedení aktualizace po každém startu interkomu.
- **Perioda aktualizace** – nastavuje periodu provádění aktualizace. Automatickou aktualizaci lze nastavit jednou za hodinu, den, týden, měsíc nebo periodu nastavit manuálně.
- **Čas aktualizace** – umožňuje nastavit čas ve formátu HH:MM, kdy se má aktualizace pravidelně provádět. Takto lze nastavit provádění aktualizace v době, kdy je interkom nejméně využíván. Parametr se neuplatní, pokud perioda aktualizace je nastavena na dobu kratší než jeden den.
- **Čas příští aktualizace** – zobrazuje čas naplánovaného provedení další aktualizace.



- **Čas poslední aktualizace** – zobrazuje čas naposledy provedené aktualizace.

- **Výsledek aktualizace (Společná konfigurace)** – zobrazuje výsledek naposledy provedené společné aktualizace. Možné hodnoty jsou následující: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Detail Výsledku komunikace(Společná konfigurace)** – chybný kód komunikace se serverem nebo status kód protokolu TFTP/HTTP.
- **Výsledek aktualizace (Soukromé konfigurace)** – k soukromé konfiguraci dojde až po aktualizaci společné konfigurace. Zařízení se soukromou konfigurací se identifikuje podle MAC adresy. Z obrazuje výsledek naposledy provedené soukromé aktualizace. Možné hodnoty jsou následující: DHCP option 66 selhal, Firmware is up to date, Server connection failed, Running..., File not found.
- **Detail Výsledku komunikace(Soukromá konfigurace)** – chybný kód komunikace se serverem nebo status kód protokolu TFTP/HTTP.

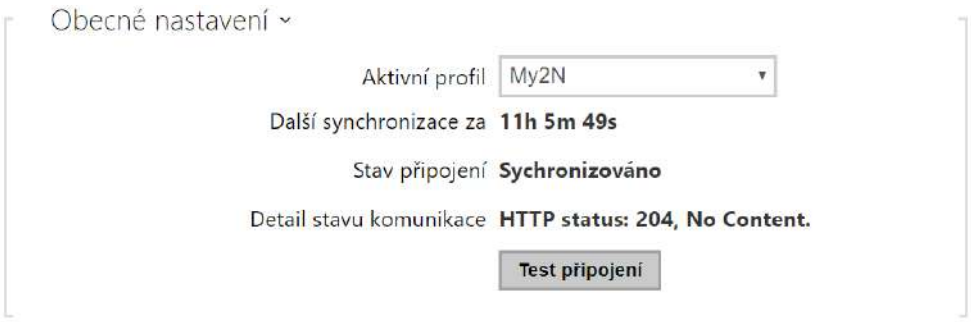
Záložka My2N / TR069

Na této záložce se povoluje a konfiguruje vzdálená správa interkomu pomocí protokolu TR-069.Protokol TR-069 umožňuje spolehlivě konfigurovat parametry interkomu, obnovit a zálohovat konfiguraci, příp. upradovat firmware zařízení.

Protokol TR-069 je využíván cloudovou službou My2N. Pro správnou funkci interkomu s My2N je nutné službu TR-069 povolit a parametr aktivní profil nastavit na hodnotu My2N. Poté se interkom bude periodicky přihlašovat ke službě My2N, která ho může konfigurovat.

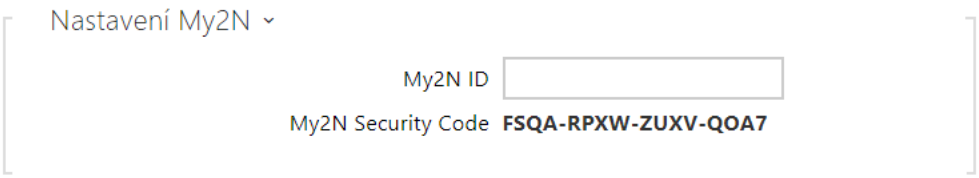
Tato funkce umožňuje připojit interkom k vašemu vlastnímu ACS (Auto Configuration Server). V takovém případě bude připojení ke službě My2N na interkomu vypnuto.

- **My2N / TR069 povoleno** – povoluje připojení ke službě My2N, příp. jinému ACS serveru.



- **Aktivní profil** – umožňuje vybrat jeden z přednastavených profilů (ACS serveru) příp. zvolit vlastní nastavení a připojení k ACS serveru nakonfigurovat ručně.

- **Další synchronizace za** – zobrazuje, za jak dlouho bude interkom kontaktovat vzdálený ACS server.
- **Stav připojení** – zobrazuje aktuální stav připojení k ACS serveru, příp. popis chybového stavu.
- **Detail stavu komunikace** – chybný kód komunikace se serverem nebo status kód protokolu TFTP/HTTP.
- **Test připojení** – testuje připojení ke službě TR069 dle nastaveného profilu, viz Aktivní profil. Výsledek testu se zobrazí v poli Stav připojení.

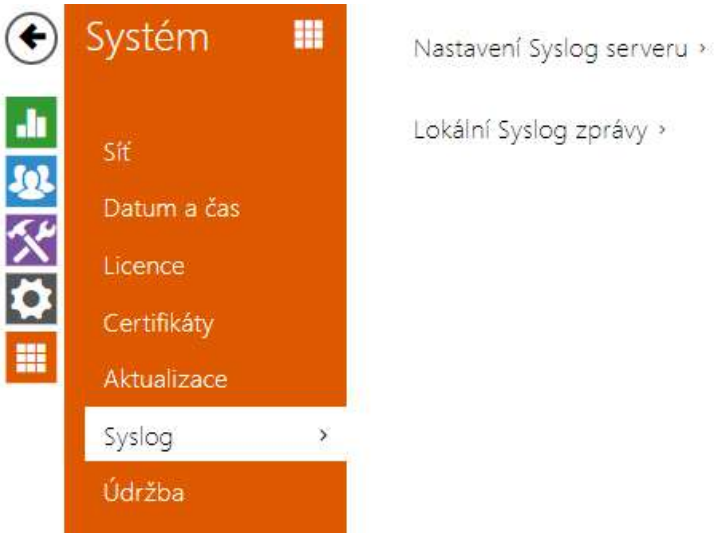


- **My2N ID** – unikátní identifikátor společnosti vytvořený pomocí My2N portálu.
- **My2N Security Code** – zobrazuje plné znění kódu sloužícího k aktivaci aplikace.

- **Adresa ACS serveru** – nastavuje adresu ACS serveru ve formátu ipadresa[: port], např. 192.168.1.1:7547
- **Uživatelské jméno** – nastavuje uživatelské jméno pro autentizaci interkomu na ACS serveru
- **Heslo** – nastavuje uživatelské heslo pro autentizaci interkomu na ACS serveru
- **Certifikát certifikační autority** – specifikuje sadu certifikátů certifikačních autorit pro ověření platnosti veřejného certifikátu ACS serveru. Lze zvolit jednu ze tří sad certifikátů, viz kapitola Certifikáty. Pokud není certifikát certifikační autority uveden, veřejný certifikát ACS serveru se neověřuje.
- **Osobní certifikát** – specifikuje uživatelský certifikát a privátní klíč, pomocí kterých se ověřuje oprávnění interkomu komunikovat se ACS serverem. Lze zvolit jednu ze tří sad uživatelských certifikátů a privátních klíčů, viz kapitola Certifikáty.

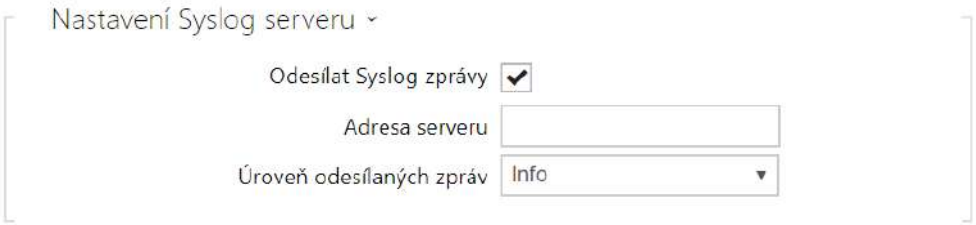
- **Povolení periodického přihlašování** – povoluje periodické přihlašování interkomu k ACS serveru.
- **Interval pro periodické přihlašování** – nastavuje interval periodického přihlašování k ACS serveru, pokud je povolen pomocí parametru **Povolení periodického přihlašování**.

5.5.6 Syslog

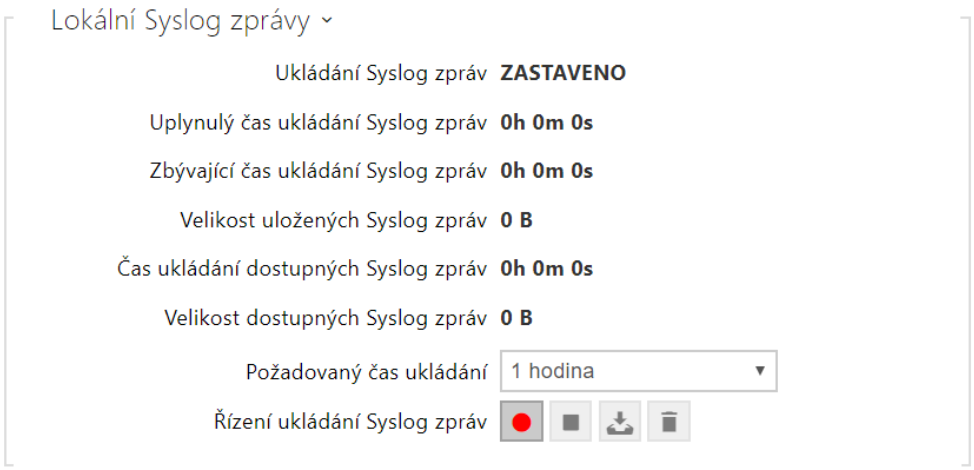


Přístupový terminál **2N Access Unit** umožňuje odesílat systémové zprávy obsahující důležité informace o stavu a procesech zařízení na syslog server, kde tyto zprávy mohou být zaznamenávány a použity pro další analýzu a audit sledovaného zařízení. V běžném provozu přístupového terminálu není nutné tuto službu konfigurovat.

Seznam parametrů

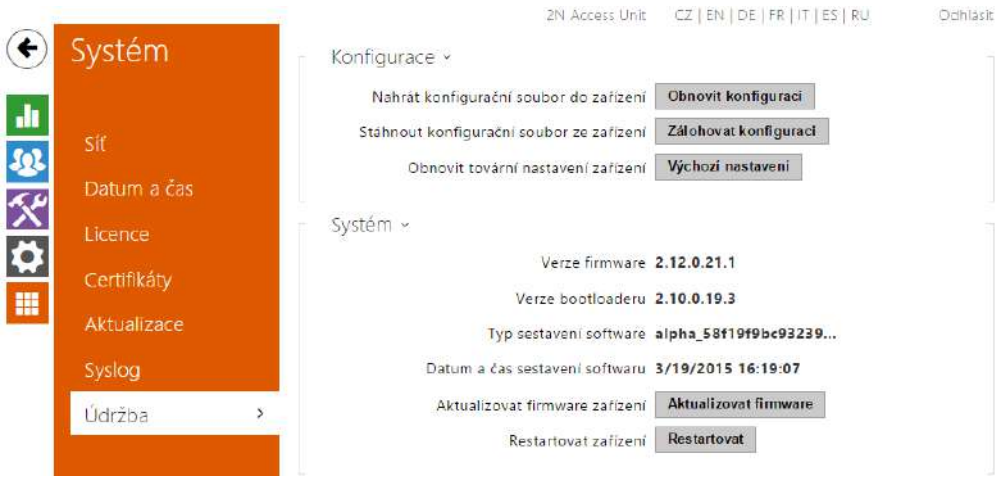


- **Odesílat Syslog zprávy** – povoluje odesílání systémových zpráv Syslog serveru. Pro správnou funkci musí být nastavena platná adresa serveru.
- **Adresa serveru** – IP/MAC adresa serveru, na kterém běží aplikace pro záznam systémových hlášení.
- **Úroveň odesílaných zpráv** – nastavuje úroveň podrobnosti odesílaných zpráv (Error, Warning, Notice, Info, Debug 1–3). Úroveň zpráv Debug 1–3 se doporučuje nastavit pouze v případě usnadnění lokalizace problému v zařízení, kterou vyžaduje technická podpora.

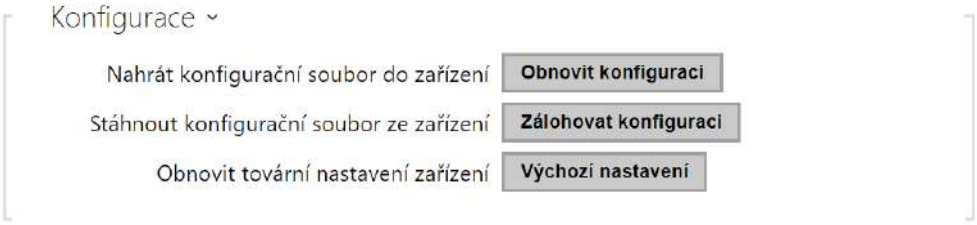


Všeobecný přehled o lokálních syslog zprávách.

5.5.7 Údržba



Toto menu slouží k údržbě konfigurace a firmwaru přístupového terminálu. Umožňuje zálohovat a obnovit nastavení všech parametrů, aktualizovat firmware přístupového terminálu příp. nastavit všechny parametry přístupového terminálu do výchozího stavu.



- **Obnovit konfiguraci** – slouží k obnově konfigurace z předchozí zálohy. Po stisku tlačítka se zobrazí dialogové okno, ve kterém můžete vybrat soubor s konfigurací a nahrát jej do zařízení. Před nahráním souboru do interkomu můžete zvolit, zda se z konfiguračního souboru má uplatnit adresář a nastavení síťových parametrů.
- **Zálohovat konfiguraci** – slouží k záloze aktuální kompletní konfigurace přístupového terminálu. Po stisku tlačítka dojde ke stažení kompletní konfigurace, kterou můžete uložit na svém PC.

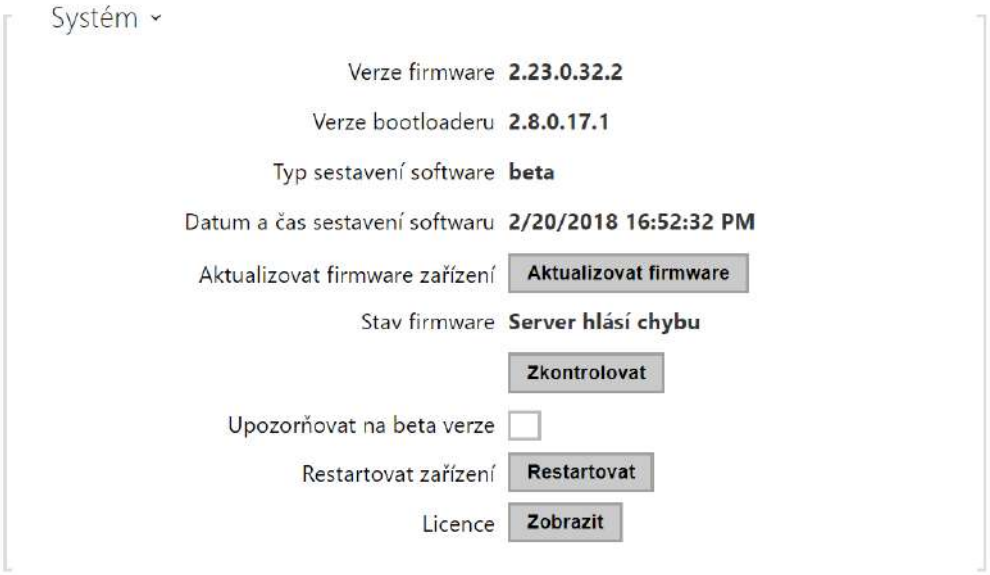
Upozornění

- *Konfigurace přístupového terminálu může obsahovat citlivé informace, jako jsou telefonní čísla uživatelů a přístupová hesla, proto se souborem nakládejte obezřetně.*

- Výchozí nastavení – slouží k nastavení všech parametrů přístupového terminálu do výchozího stavu s výjimkou parametrů nastavení sítě. Pokud chcete přístupový terminál uvést do úplného výchozího stavu, použijte příslušnou propojku nebo tlačítko reset, viz instalační manuál k přístupovému terminálu.

Upozornění

- *Obnovení výchozího nastavení vymaže případný nahraný licenční klíč. Je vhodné si ho tedy uschovat zkopírováním na jiné úložiště pro pozdější potřebu.*



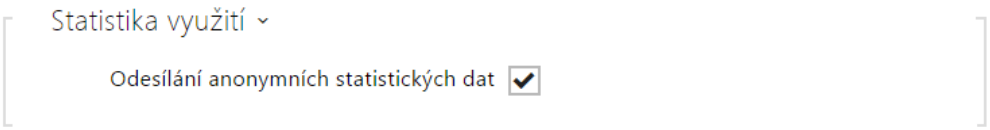
- Aktualizovat firmware – slouží k nahrání nového firmwaru do přístupového terminálu. Po stisku tlačítka se zobrazí dialogové okno, ve kterém můžete vybrat soubor s firmwarem určeným pro váš přístupový terminál. Po úspěšném uploadu firmwaru se přístupový terminál automaticky restartuje. Po restartu je plně k dispozici s novým firmwarem. Celý proces aktualizace trvá necelou minutu. Aktuální verzi firmwaru pro svůj přístupový terminál můžete získat na adrese www.2n.cz. Aktualizace firmwaru neovlivňuje konfiguraci. Interkom kontroluje soubor firmwaru a neumožní nahrát nesprávný nebo poškozený soubor.

- Restartovat – provede restart přístupového terminálu. Celý proces restartu trvá asi 30 s. Po dokončení restartu, kdy přístupový terminál získá IP vlastní adresu, se automaticky zobrazí přihlašovací okno.

Upozornění

Zápis změny konfigurace interkomu se provádí v časovém rozmezí 3–15 s v závislosti na velikosti příslušné konfigurace interkomu. Během této doby nerestartujte interkom.

- Licence – po kliknutí na tlačítko Zobrazit se otevře dialogové okno se seznamem použitých licencí a softwaru třetích stran. Také obsahuje link na dokument EULA.



- Odesílání anonymních statistických dat – povoluje odesílání anonymních statistických dat o využití zařízení výrobci. Tato data neobsahují žádné citlivé informace, jako např. hesla, přístupové kódy ani telefonní čísla. 2N TELEKOMUNIKACE a.s. používá tyto informace ke zlepšování kvality, spolehlivosti a výkonu software. Účast je dobrovolná a zasílání statistických údajů můžete kdykoliv zrušit.

6. Doplňkové informace

Zde je přehled toho, co v kapitole naleznete:

6.1 Řešení problémů

Nejčastěji řešené problémy najdete na stránkách **faq.2n.cz**.

6.2 Směrnice, zákony a nařízení

2N Access Unit splňuje všechny požadavky následujících směrnic, zákonů a nařízení:

2014/35/EU ze dne 26. února 2014 o harmonizaci právních předpisů členských států týkajících se dodávání elektrických zařízení určených pro používání v určitých mezích napětí na trh

2014/30/EU ze dne 26. února 2014 o harmonizaci právních předpisů členských států týkajících se elektromagnetické kompatibility

2011/65/EU ze dne 8. června 2011 o omezení používání některých nebezpečných látek v elektrických a elektronických zařízeních

2012/19/EU ze dne 4. července 2012 o odpadních elektrických a elektronických zařízeních (OEEZ).

6.3 Obecné pokyny a upozornění

Před použitím tohoto výrobku si prosím pečlivě přečtěte tento návod k použití a řiďte se pokyny a doporučeními v něm uvedenými.

V případě používání výrobku jiným způsobem, než je uvedeno v tomto návodu, může dojít k nesprávnému fungování výrobku nebo k jeho poškození či zničení.

Výrobce nenese žádnou odpovědnost za případné škody vzniklé používáním výrobku jiným způsobem, než je uvedeno v tomto návodu, tedy zejména jeho nesprávným použitím, nerespektováním doporučení a upozornění.

Jakékoliv jiné použití nebo zapojení výrobku, kromě postupů a zapojení uvedených v návodu, je považováno za nesprávné a výrobce nenese žádnou zodpovědnost za následky způsobené tímto počínáním.

Výrobce dále neodpovídá za poškození, resp. zničení výrobku způsobené nevhodným umístěním, instalaci, nesprávnou obsluhou či používáním výrobku v rozporu s tímto návodem k použití.

Výrobce nenese odpovědnost za nesprávné fungování, poškození či zničení výrobku důsledkem neodborné výměny dílů nebo důsledkem použití neoriginálních náhradních dílů.

Výrobce neodpovídá za ztrátu či poškození výrobku živelnou pohromou či jinými vlivy přírodních podmínek.

Výrobce neodpovídá za poškození výrobku vzniklé při jeho přepravě.

Výrobce neposkytuje žádnou záruku na ztrátu nebo poškození dat.

Výrobce nenese žádnou odpovědnost za přímé nebo nepřímé škody způsobené použitím výrobku v rozporu s tímto návodem nebo jeho selháním v důsledku použití výrobku v rozporu s tímto návodem.

Při instalaci a užívání výrobku musí být dodrženy zákonné požadavky nebo ustanovení technických norem pro elektroinstalaci. Výrobce nenese odpovědnost za poškození či zničení výrobku ani za případné škody vzniklé zákazníkovi, pokud bude s výrobkem nakládáno v rozporu s uvedenými normami.

Zákazník je povinen si na vlastní náklady zajistit softwarové zabezpečení výrobku. Výrobce nenese zodpovědnost za škody způsobené nedostatečným zabezpečením.

Zákazník je povinen si bezprostředně po instalaci změnit přístupové heslo k výrobku. Výrobce neodpovídá za škody, které vzniknou v souvislosti s užíváním původního přístupového hesla.

Výrobce rovněž neodpovídá za vícenáklady, které zákazníkovi vznikly v souvislosti s uskutečňováním hovorů na linky se zvýšeným tarifem.

Nakládání s elektroodpadem a upotřebenými akumulátory

Použitá elektrozařízení a akumulátory nepatří do komunálního odpadu. Jejich nesprávnou likvidací by mohlo dojít k poškození životního prostředí!

Po době jejich použitelnosti elektrozařízení pocházející z domácností a upotřebené akumulátory vyjmuté ze zařízení odevzdejte na speciálních sběrných místech nebo předejte zpět prodejci nebo výrobci, který zajistí jejich ekologické zpracování. Zpětný odběr je prováděn bezplatně a není vázán na nákup dalšího zboží. Odevzdávaná zařízení musejí být úplná.

Akumulátory nevhazujte do ohně, nerozebírejte ani nezkratujte.

An Axis company

2N TELEKOMUNIKACE a.s.

Modřanská 621, 143 01 Prague 4, Czech Republic

Phone: +420 261 301 500, Fax: +420 261 301 599

E-mail: sales@2n.cz

Web: www.2n.cz

v2.29