Konfigurační manuál 2N Access Unit

v.2.46

www.2n.com

1. Popis produktu

Přístupové jednotky 2N zahrnují modely **2N Access Unit, 2N Access Unit 2.0, 2N Access Unit QR a 2N Access Unit M.** Přístupové jednotky 2N jsou schopny, spolu s doplňkovým software a případně interkomy 2N**,** nabídnout ucelené řešení přístupového systému do jakéhokoliv objektu.

Přístupové jednotky 2N lze v kombinaci s numerickou klávesnicí použít jako kódový zámek.

Přístupové jednotky 2N 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.

Přístupové jednotky 2N můžou být vybaveny reléovým spínačem (volitelně dalšími relé a výstupy), kterým lze ovládat elektrický zámek nebo jiná zařízení k nim připojená. Přístupové jednotky je možné velmi flexibilně nastavit, např. 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

Přihlášení do webového konfiguračního rozhraní

Zařízení se konfiguruje pomocí webového konfiguračního rozhraní. Pro přístup je potřeba znát IP adresu zařízení nebo doménové jméno zařízení. Zařízení musí být připojeno do lokální IP sítě a musí být napájeno.

Přihlášení pomocí doménového jména

K zařízení je možné se připojovat zadáním doménové adresy ve formátu *hostname.local* (např.: 2NAccessUnitM-00000001.local). Hostname nového zařízení se skládá z názvu zařízení a ze sériového čísla zařízení. Formáty názvů zařízení v hostname jsou uvedeny níže. Sériové číslo se do doménového jména zadává bez pomlček. Hostname je možné později změnit v sekci Systém > Síť.

Zařízení 2N	Název zařízení v hostname
2N Access Unit	2NAccessUnit
2N Access Unit 2.0	2NAccessUnit20
2N Access Unit M	2NAccessUnitM
2N Access Unit QR	2NAccessUnitQR

Přihlašování pomocí doménového jména má výhodu při používání dynamické IP adresy zařízení. Zatímco se dynamická IP adresa mění, doménové jméno zůstává stejné. Pro doménové jméno je možné vygenerovat certifikáty podepsané důvěryhodnou certifikační autoritou.

Přihlášení pomocí IP adresy

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

Přihlašovací údaje

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.

Nastavení připojení k lokální síti (platí pro 2N Access Unit, 2N Access Unit 2.0 a 2N Access Unit M)

IP adresu je možné zjistit buď přímo ze stavu DHCP serveru (podle MAC adresy uvedené na výrobním štítku), příp. ji může sdělit přímo zařízení pomocí hlasové funkce – viz Instalační manuál (odkaz níže).

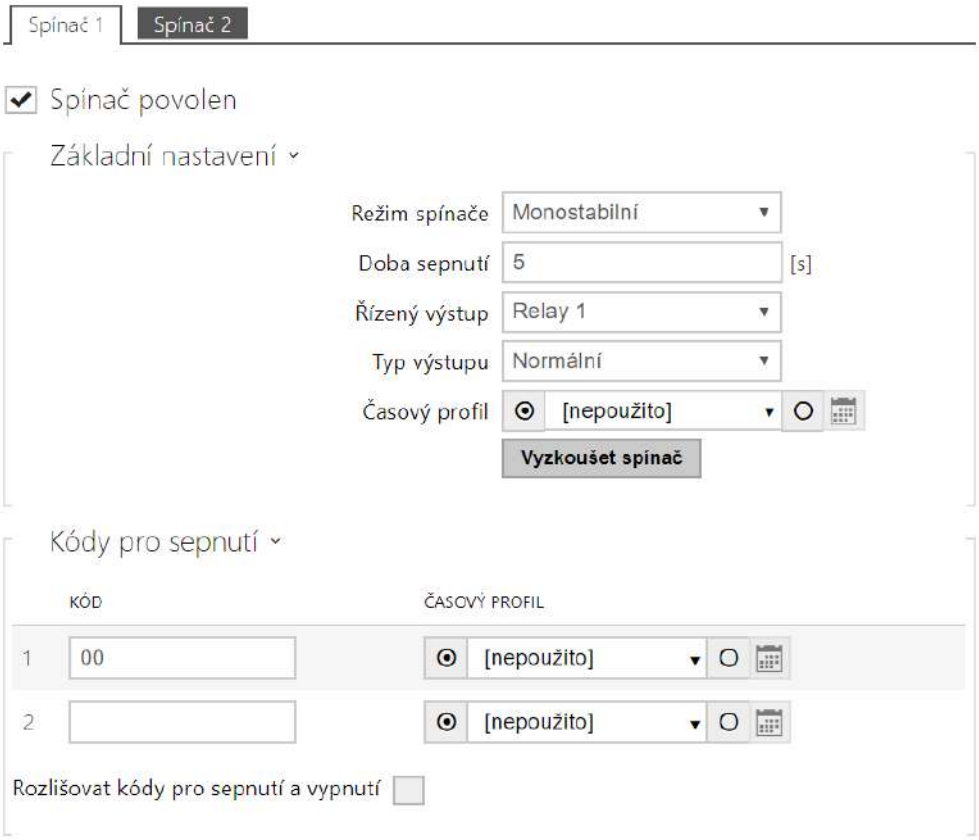
Pokud ve vaší síti není DHCP server, musíte nastavit zařízení na statickou IP adresu pomocí RESET tlačítka, viz Instalační manuál k příslušnému modelu. Vaše jednotka poté získá pevnou adresu **192.168.1.100**, kterou použijete pouze pro první přihlášení a poté ji můžete změnit.

Aktualizace firmware

Po prvním přihlášení /*/ doporučujeme zároveň aktualizovat firmware. Nejnovější firmware pro svoji jednotku naleznete na stránkách 2N.com. 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 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 zařízení, ke kterému je elektrický dveřní zámek připojen. Poté nastavte jeden nebo více kódů pro sepnutí spínače – elektrického dveřního zámku.

3. Licencované funkce

Přístupové jednotky 2N podporuje standardní licence, které jsou již součástí zařízení. Jedná se o Enhanced Integration, Enhanced Security a NFC licenci. NFC licenci lze použít pouze s **2N Access Unit** nebo **2N Access Unit 2.0**, která obsahuje 13.56 MHz čtečku karet.

Přehled licencí a jejich vlastností uvádí tabulka níže.

Licence	Vlastnosti	2N Access Unit 1.0	2N Access Unit 2.0	2N Access Unit M	2N Access Unit QR
Enhanced Integration (Standardní licence součástí zařízení)	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	✅	✅	✅	✅
	Řízení výtahu	✅	✅	✅	✅
Enhanced Security (Standardní licence součástí zařízení)	Podpora 802.1x	✅	✅	✅	✅
	Podpora SIPS (TLS)	✅	✅	✅	✅
	Blokování spínačů tamperem	✅	✅	✅	✅
	Podpora SRTP	❌	❌	❌	❌
	Tichý alarm	✅	✅	✅	✅
	Omezení neúspěšných pokusů o přístup	✅	✅	✅	✅
	Anti-Passback	✅	✅	✅	✅
	Promíchaná klávesnice	❌	⭐	❌	⭐
NFC (Standardní licence součástí zařízení)	Podpora NFC	✅	✅	✅	✅
Podpora řízení výtahů	Lift Control	✅	✅	✅	✅

✅ – Obsahuje z výroby

⭐ – Funkce dostupná pouze s připojením přídavného modulu displeje

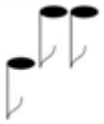
❌ – Nelze použít

4. Signalizace provozních stavů

Přístupové jednotky **2N** signalizují 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
	**Vnitřní aplikace spuštěna** Po zapnutí napájení nebo po restartu zařízení 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 zařízení 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 ze zařízení, 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 Instalačním manuálu zařízení.

5. Konfigurace pomocí webového rozhraní

Úvodní přehledová obrazovka

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

V záhlaví stránky se zobrazuje jméno zařízení (viz parametr Zobrazované jméno v nastavení **Služby > Web Server > Základní nastavení**). Pro výběr jazyka lze použít menu v pravém horním rohu webového rozhraní. Od zařízení se můžete odhlásit pomocí tlačítka Odhlásit v pravém horním rohu stránky, zobrazit si nápovědu pomocí ikony otazníku nebo pomocí bubliny poskytnout zpětnou vazbu.

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

Konfigurační menu

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

Upozornění

- V tomto konfiguračním manuálu jsou popsány veškeré funkce a parametry přístupových jednotek 2N. Zahrnují modely **2N Access Unit, 2N Access Unit 2.0, 2N Access Unit QR** a **2N Access Unit M.** Některé funkce nebo parametry nemusí být pro všechny modely přístupné.

Stav

- **Zařízení** – základní informace o zařízení
- **Služby** – informace o spuštěných službách a jejich stavu
- **Licence** – aktuální stav licence a dostupných funkcích zařízení
- **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 zařízení
- **Řízení výtahu** – nastavení pro přístup na jednotlivá patra výtahem

Služby

- **Řízení přístupu** – nastavení pravidel pro příchod a odchod
- **E-Mail** – umožňuje nastavit zasílání emailů například v případě neplatného pokusu o přístup
- **Mobile Key** – nastavení Bluetooth a správa připojených zařízení
- **Automatizace** – flexibilní nastavení zařízení dle specifických požadavků uživatele
- **HTTP API** – aplikační rozhraní pro ovládání vybraných funkcí zařízení
- **Web server** – nastavení web serveru a přístupového hesla
- **SNMP** – funkcionalita umožňující vzdálený dohled zařízení v síti pomocí protokolu SNMP

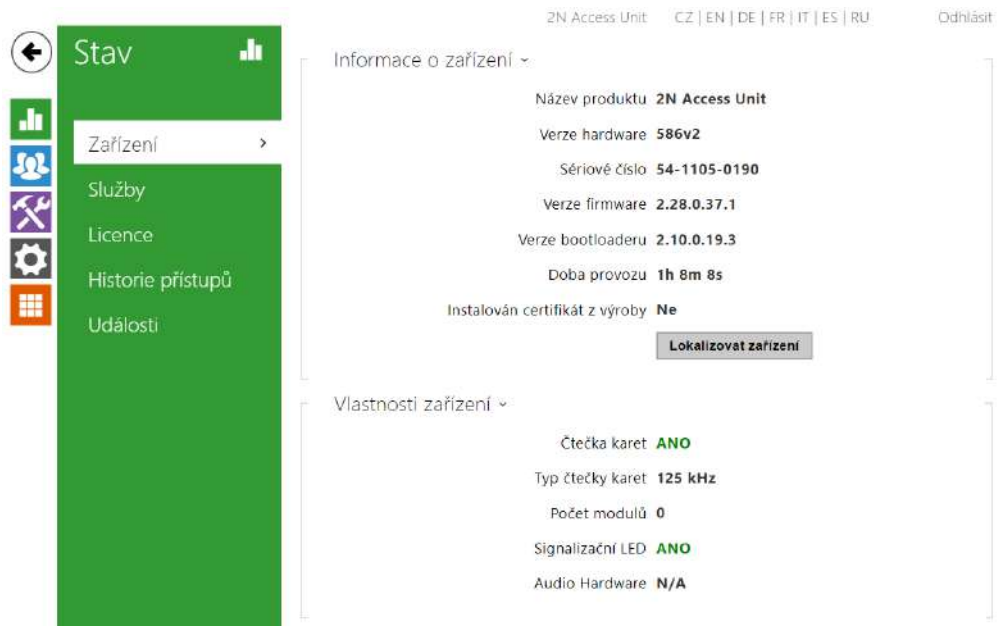
Systém

- **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

Upozornění

Varování
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.com/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.

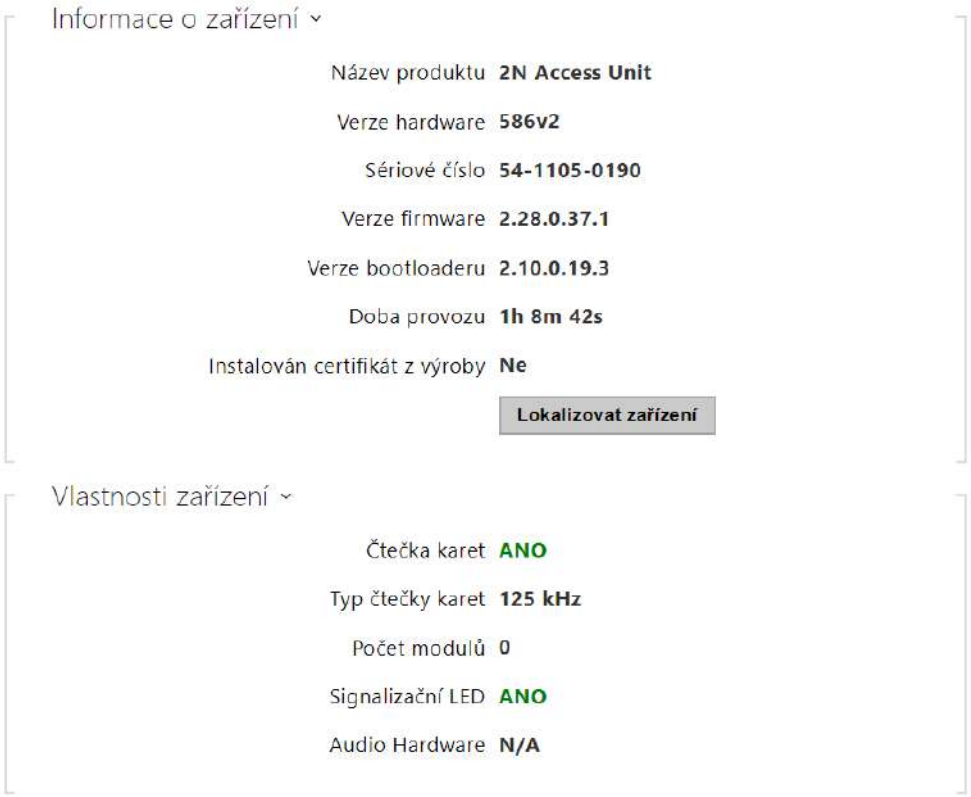
5.1 Stav



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 Historie přístupů

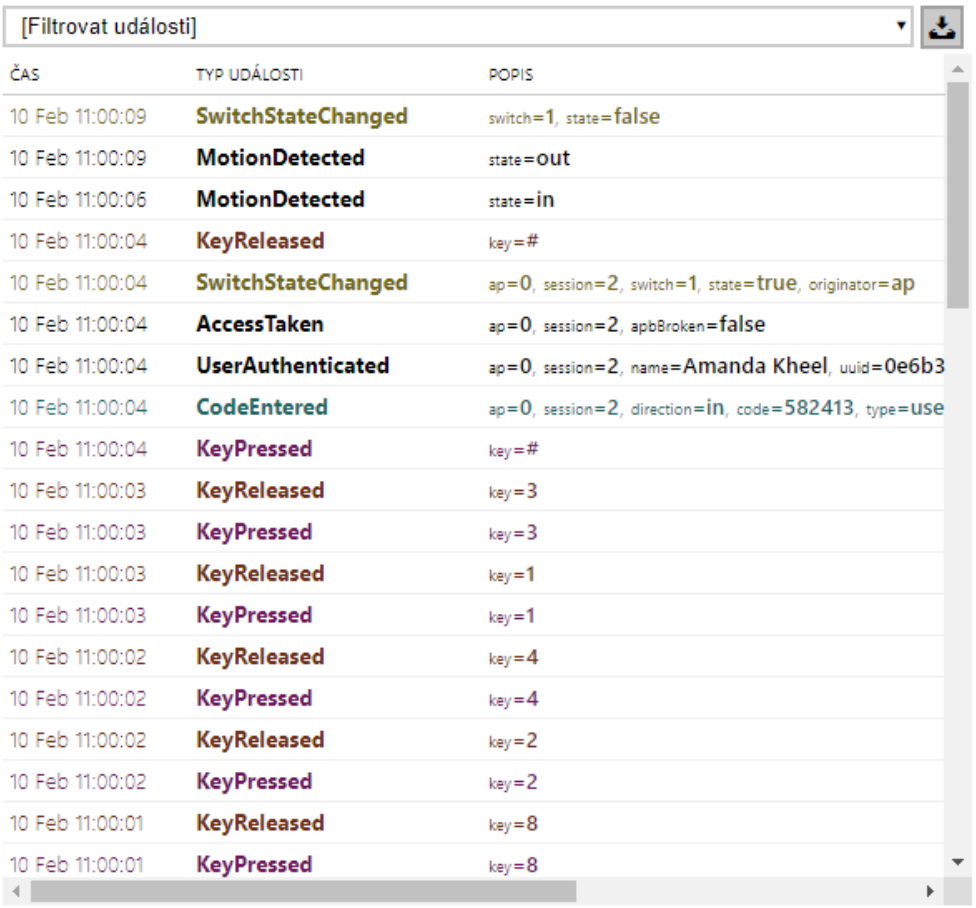
Na záložce **Historie přístupů** se zobrazuje posledních 10 záznamů o přiložených kartách. Každý záznam obsahuje čas přiložení karty, její ID, typ a popis obsahující informaci, zda je karta platná, příp. kterému uživateli byla přiřazena.


Záznamy

	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

V této záložce je možné vidět posledních 500 událostí, které zařízení zaznamenalo. Každá událost obsahuje čas a datum zachycení, typ události a popis více specifikující událost. Události lze filtrovat v rozbalovacím menu nad vlastním záznamem událostí podle typu události.



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

Událost	Význam
AccessLimited	Událost, která nastane po zadání 5 neúspěšných pokusů o autentizaci uživatele (karta, kód, otisk prstu). Přístupový modul bude zablokován po dobu 30 sekund i v případě, že následná autentizace by byla správná.
ApiAccessRequested	Událost, kdy byl zaslán požadavek na /api/accesspoint/grantaccess s výsledkem "success" : true.
AccessTaken	Při přiložení karty v Anti-passback oblasti.
CardHeld	Při přiložení karty, které trvá 4 s a déle.

Událost	Význam
CardEntered	Při přiložení karty.
CodeEntered	Po zadání kódu na numerické klávesnici ukončeném znakem *.
DeviceState	Indikace stavu zařízení, jako je například spuštění.
DoorOpenTooLong	Detekce dlouho otevřených dveří, nastavitelné v Hardware / Dveře / Dveře.
DoorStateChanged	Detekuje otevření/zavření dveří. Nastavení lze provést v Hardware / Dveře / Dveře.
FingerEntered	Autorizace pomocí otisku prstu.
InputChanged	Signalizuje změnu logického vstupu.
KeyPressed	Při stisku tlačítka (číslice jsou 0, 1, 2 ..., 9 a tlačítka rychlé volby jsou %1, %2 atd.).
KeyReleased	Při puštění tlačítka (číslice jsou 0, 1, 2 ..., 9 a tlačítka rychlé volby jsou %1, %2 atd.).
LiftFloorsEnabled	Přístup na patro pomocí výtahu.
LiftStatusChanged	Detekce připojení/odpojení Lift Control modulu.
LoginBlocked	Při zadání 3 špatných loginů do Webu, zařízení. Obsahuje údaje o IP adrese těchto přístupů.
MobKeyEntered	Autorizace pomocí bluetooth.
OutputChanged	Signalizuje změnu stavu logického výstupu.
RexActivated	Událost při aktivaci vstupu, která je nastavena na tlačítko REX.

Událost	Význam
SilentAlarm	Událost tichého alarmu po zadání kódu, který je o jedničku vyšší než správný kód. Tzn. kód pro otevření je 123 a kód tichého alarmu je 124. Nebo po přiložení prstu k modulu čtečky otisků prstů, který je označený pro použití k aktivaci tichého alarmu.
SwitchesBlocked	Spínače blokovány neplatným zadáním přístupu.
SwitchOperationChanged	Změna fungování spínače (signalizuje stav uzamčení nebo přidržení spínače, nastartování i restartování časovače nebo jeho ukončení – přechodu do trvalého přidržení).
SwitchStateChanged	Změna stavu spínače, nastavení v Hardware / Spínače.
TamperSwitchActivated	Signalizuje aktivaci ochranného spínače – otevření krytu zařízení. Funkce ochranného spínače musí být nakonfigurována v menu Digitální vstupy / Ochranný spínač.
UnauthorizedDoorOpen	Detekce neautorizovaného otevření dveří, nastavitelné v Hardware / Dveře / Dveře.
UserAuthenticated	Signalizuje autentizaci uživatele a následné otevření dveří.
UserRejected	Neplatné ověření uživatele.

5.2 Adresář

Zde je přehled toho, co v kapitole naleznete:

5.2.1 Uživatelé

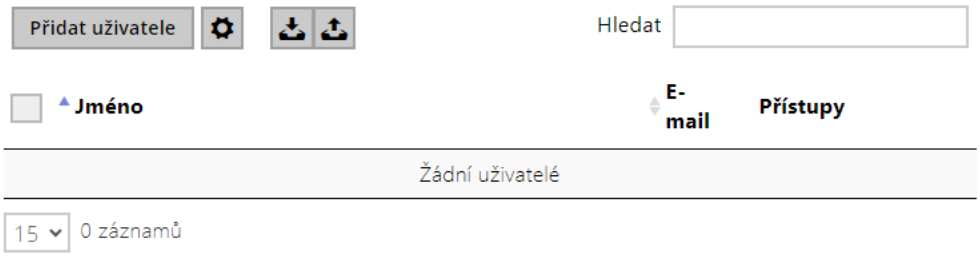
Seznam uživatelů je jednou z nejdůležitějších částí konfigurace zařízení. Seznam uživatelů obsahuje důležité informace o uživatelích, které zpřístupňují funkce zařízení, jako je otvírání dveří pomocí RFID karet, spínání kódového zámku, informování uživatele o přístupech pomocí e-mailů apod.

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 zařízení 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 zařízení – 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 zařízení 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 zařízení.

Po přiložení karty k RFID čtečce je ID karty porovnáno s databází karet v zařízení. 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.



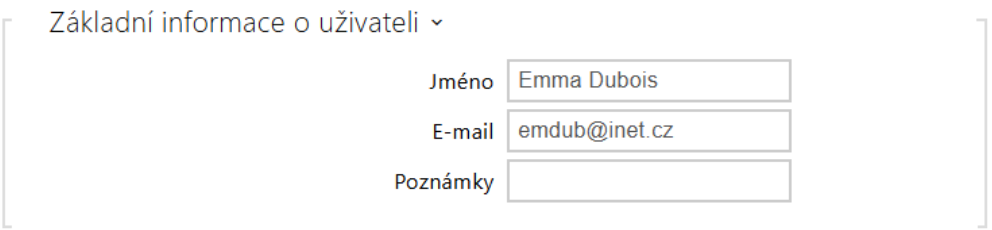
Funkce Vyhledávání v seznamu uživatelů funguje jako fulltextové vyhledávání ve jméně a emailu. Vyhledává všechny shody v celém seznamu. Nový Uživatel se přidává pomocí tlačítka nad tabulkou. Pro zobrazení detailu nastavení uživatele slouží ikona . Pro nastavení zobrazení sloupců tabulky slouží ikona , 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.

Ze/do zařízení je pomocí ikony / umožněno exportovat/importovat CSV soubor se seznamem uživatelů. Pokud je adresář prázdný, vyexportuje se soubor pouze s hlavičkou (v angličtině), který může sloužit jako šablona pro importování uživatelů. Pokud se importuje prázdný soubor pouze s hlavičkou a zvolí se varianta **Nahradit adresář**, dojde ke smazání celého adresáře. Import umožňuje nahrát až 10 000 uživatelů, v závislosti na typu zařízení.

Upozornění

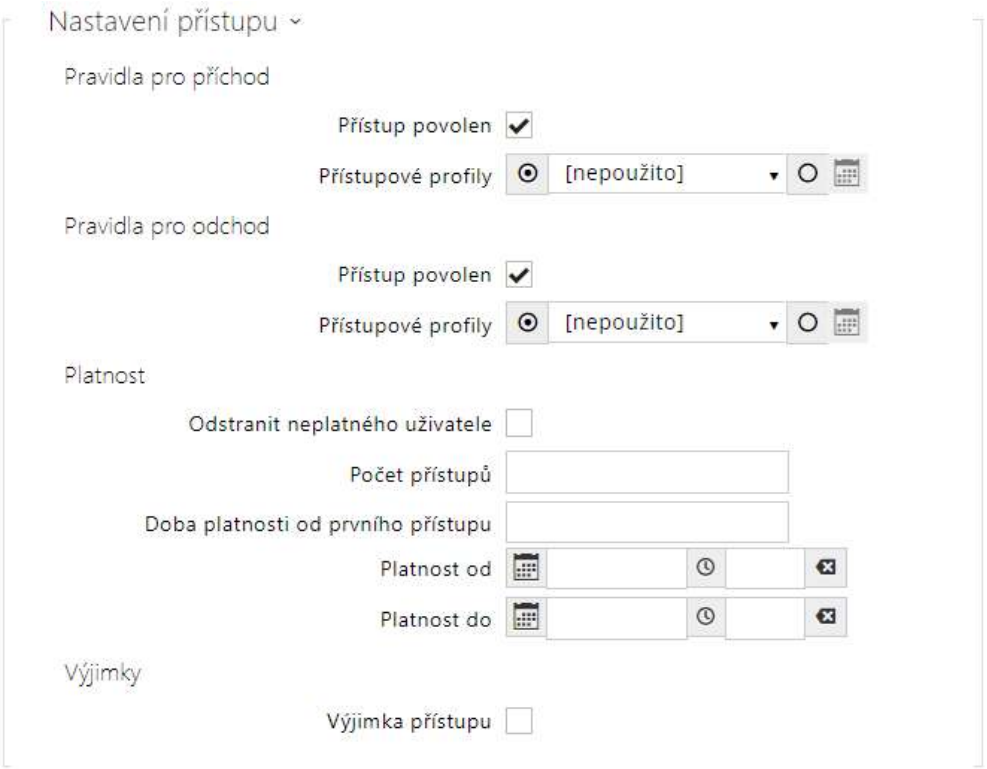
- Speciální uživatelé, například ti vytvoření službou **My2N** či systémem **2N Access Commander**, nejsou součástí exportu adresáře.
- Při úpravách CSV souboru pomocí Microsoft Excelu je třeba soubor uložit ve formátu CSV UTF-8 (s oddělovači).

Každý záznam v seznamu uživatelů obsahuje následující údaje:



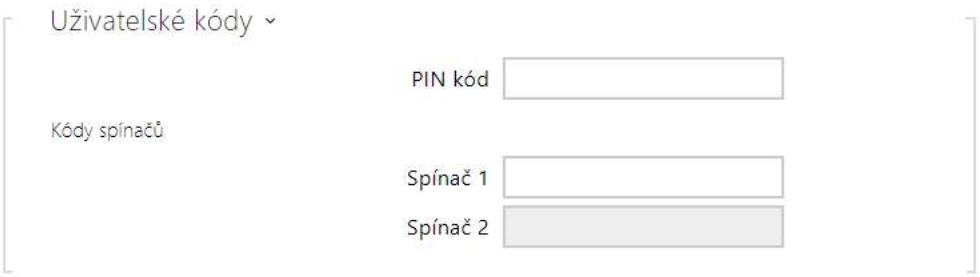
- **Jméno** – nepovinný údaj sloužící pro lepší orientaci v seznamu, např. při vyhledávání uživatelů.

- **E-mail** – emailová adresa uživatele sloužící pro odeslání informací pomocí e-mailu, např. o přístupu uživatele do objektu nebo při využití 2N Automation. Je možné přidat více e-mailových adres oddělených čárkou nebo středníkem.
- **Poznámky** – slouží k přidání vlastních poznámek ke kontaktu. Do poznámky je možné vepsat metadata, která se využívají při integraci se systémy třetích stran. S obsahem poznámky lze pracovat v bloku Comparator v Automatizaci, viz 2N Automation manuál.



- **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.
- **Platnost**
  - **Odstranit neplatného uživatele** – volí, zda je uživatel odstraněn ze zařízení, jakmile je neplatný (tj. uplynula doba jeho platnosti nebo počet jeho povolených přístupů je 0).
  - **Počet přístupů** – nastavuje počet povolených přístupů pro tohoto uživatele. Ponechte prázdné pro nastavení neomezeného počtu přístupů.

  - **Doba platnosti od prvního přístupu** – nastavuje čas, po který bude uživatel platný od první úspěšné autorizace. Ponechte prázdné pro žádné relativní období platnosti. Relativní platnost může zkrátit dobu platnosti, ale nikdy ji neprodlouží. Čas je nastaven ve formátu HH:MM, např. 06:09.
  - **Platnost od** – umožňuje nastavit začátek platnosti nastaveného přístupu. Ponechte prázdné, aby nebyl začátek omezen. Platnost od musí předcházet Platnost do.
  - **Platnost do** – umožňuje nastavit konec platnosti nastaveného přístupu. Ponechte prázdné, aby nebyl konec omezen. Platnost do musí být po Platnost od.
- **Výjimka přístupu** – povoluje tomuto uživateli obejít pravidla Blokování přístupu a Anti-Passback.



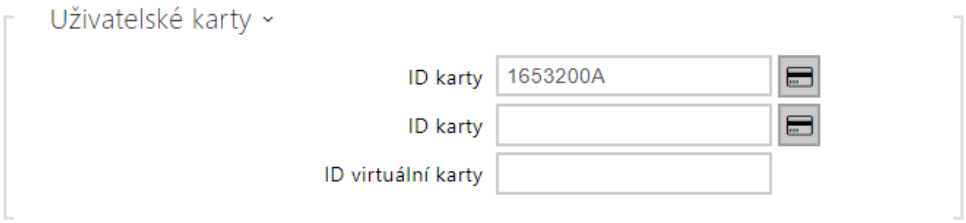
Každý z uživatelů může mít přiřazen vlastní soukromý kód pro sepnutí spínače. Uživatelské kódy spínačů lze libovolně kombinovat s univerzálními kódy spínačů zadanými v menu **Hardware > Spínače**.

Upozornění

- Pokud se kódy překrývají s jinými kódy již zadanými v konfiguraci interkomu, pak se u takto kolidujících kódů objeví značka .
- Při určování unikátnosti kódu jsou ignorovány počáteční nuly. To znamená, že dva kódy lišící se POUZE v počtu počátečních nul, jsou považovány za identické.

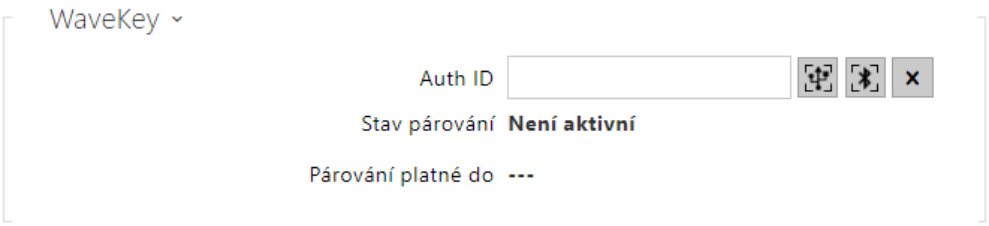
- **PIN kód** – umožňuje nastavit osobní numerický přístupový kód uživatele. Kód musí obsahovat alespoň dva znaky.
  - vygeneruje obrázek QR kódu. Kódy kratší než 4 číslice není možné z bezpečnostních důvodů zadávat pomocí načtení QR kódu. Kódy musí obsahovat pouze číslice. Při potřebě autentizace pomocí hexadecimálního QR kódu, je potřeba tento kód před zadáním převést do decimálního formátu. Akceptovaný hexadecimální rozsah: 1000 až FFFFFFFF.
- **Spínač** – 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 zařízení a minimálně jeden znak pro odemknutí dveří pomocí DTMF z telefonu.

- vygeneruje obrázek QR kódu. Kódy kratší než 4 číslice není možné z bezpečnostních důvodů zadávat pomocí načtení QR kódu. Kódy musí obsahovat pouze číslice. Při potřebě autentizace pomocí hexadecimálního QR kódu, je potřeba tento kód před zadáním převést do decimálního formátu. Akceptovaný hexadecimální rozsah: 1000 až FFFFFFFF.



Každý z uživatelů zařízení 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 (Služby > Řízení přístupu) nastaveno odesílání identifikátorů na Wiegand.



Tato sekce se zobrazuje pouze při připojení Bluetooth modulu.

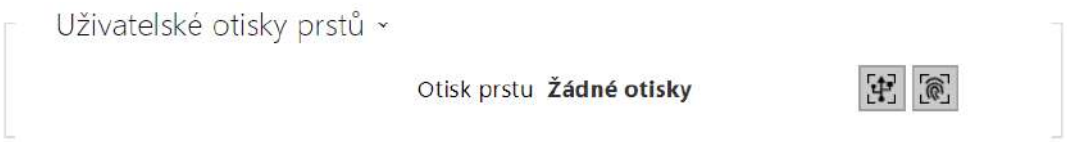
- **Auth ID** – unikátní identifikační číslo WaveKey pro řízení přístupu. Během párovacího procesu je uloženo do mobilního zařízení. Auth ID se skládá z 32 hexadecimálních znaků.
- **Párování platné do** – datum a čas konce platnosti vygenerovaného autorizačního PINu.
  - spárovat přes USB čtečku
  - spárovat přes toto zařízení

- smazat Auth ID

Párování pomocí Bluetooth modulu v zařízení

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.

Podrobný postup, jakým způsobem nahrát otisky prstů uživatele, je popsán v podkapitole 5.2.1.1 Pokyny pro nastavení uživatelských otisků prstů.

Zařízení umožňuje využít rozpoznané registrační značky vozidel zaslané v HTTP požadavku kamerami od firmy AXIS vybavené doplňkovou aplikací VaxALPR na api/lpr/licenseplate (více HTTP API manuál pro IP interkomy).

V případě, že je funkce zapnuta, dojde po přijetí platného HTTP požadavku k zaznamenání události do historie pod událostí LicensePlateRecognized.

Pokud je v rámci HTTP požadavku zaslán i obrázek (např. výřez fotografie nebo celá fotografie scény při detekci registrační značky), uloží se. V paměti zařízení je uloženo pět posledních fotografií, které je možné ze zařízení vyčíst pomocí HTTP požadavku zaslaného na api/lpr/image a které jsou k dispozici v systému **2N Access Commander**.

Pro korektní funkci je vhodné, aby byla každá registrační značka přiřazena právě jednomu záznamu v adresáři. Při vícenásobně zadaných registračních značkách dochází k tomu, že není možné jednoznačně přiřadit záznam v adresáři, který má registrační značku nakonfigurovanou (je vybrán první záznam, který má danou registrační značku nakonfigurovanou, a jeho přístupová pravidla se uplatní).

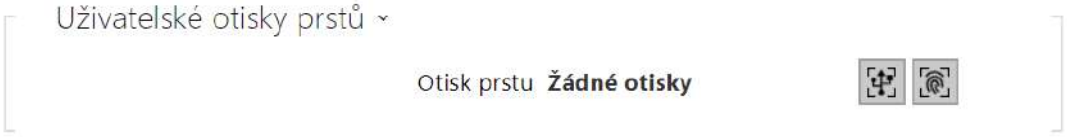
- **Registrační značky** – nastavuje registrační značky vozidel daného záznamu v adresáři. Záznamu je možné přiřadit více registračních značek oddělených čárkami (maximálně 20). Zadané registrační značky jsou využity ve funkci rozpoznávání registračních značek z obrazu externí kamery (pro více informací viz Interoperability manuál). Jedna registrační značka může mít maximálně 10 znaků. Délka zadaného řetězce je omezena na 255 znaků.

- **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.

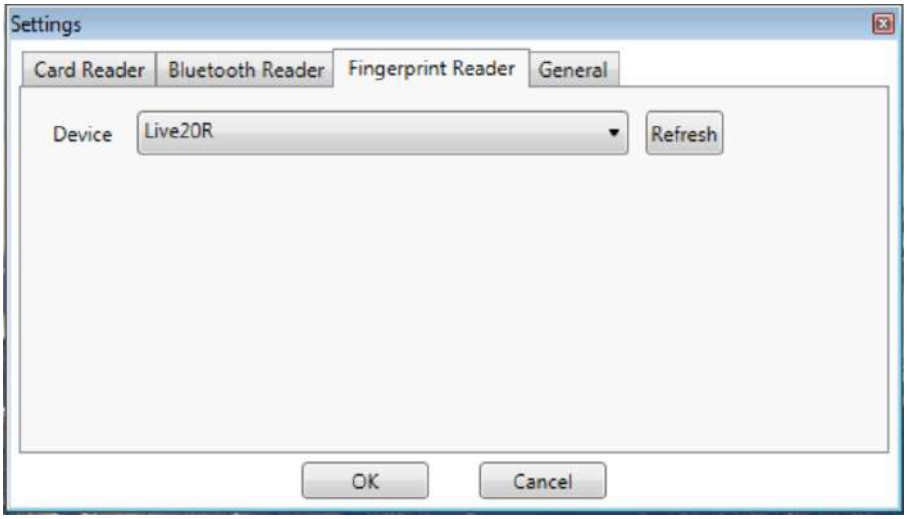
5.2.1.1 Pokyny pro nastavení uživatelských otisků prstů

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.

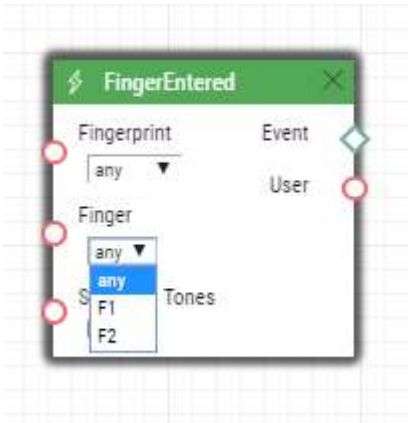
4) Přiložte vámi vybraný prst na externí USB čtečku. Pro vyšší přesnost se tento proces opakuje, celkem třikrát.

V případě neshody načtení otisků prstů proces opakujte.

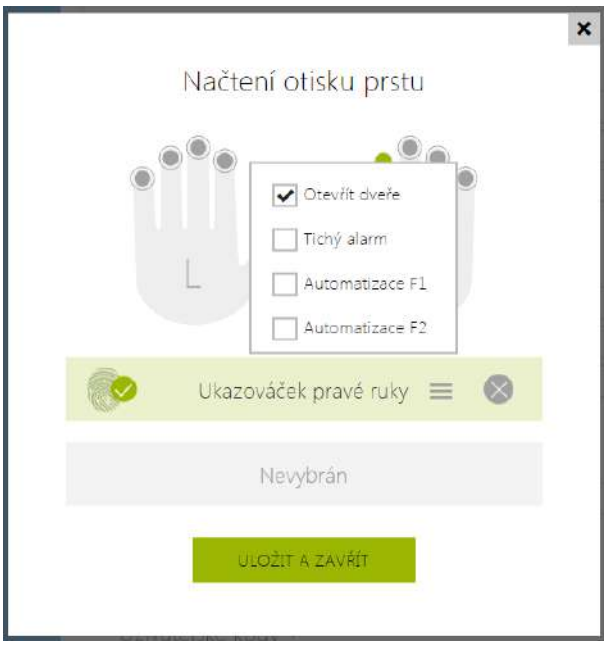
5) Pokud skenování prstů proběhlo v pořádku, nastavení potvrďte kliknutím na tlačítko HOTOVO.

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.

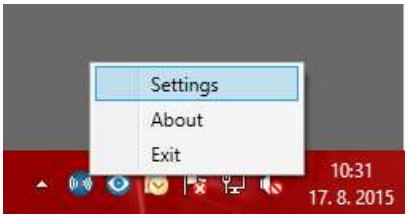


6) V záložce Uživatelé je možné zkontrolovat aktuální nastavení.

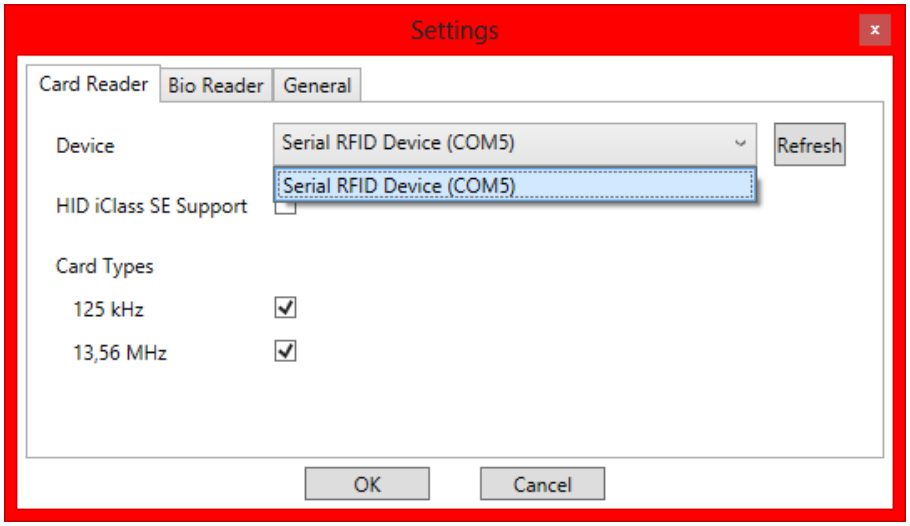
5.2.1.2 USB RFID čtečka karet

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

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

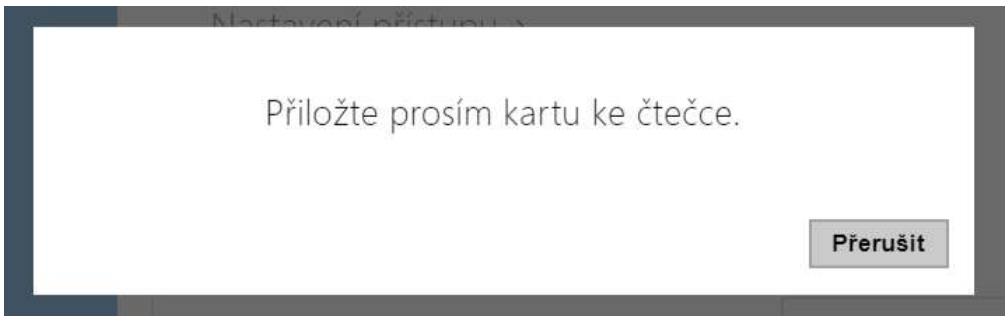


2. Nastavte COM port připojené čtečky



3. Na webu u uživatele zmáčkněte tlačítko načtení karty

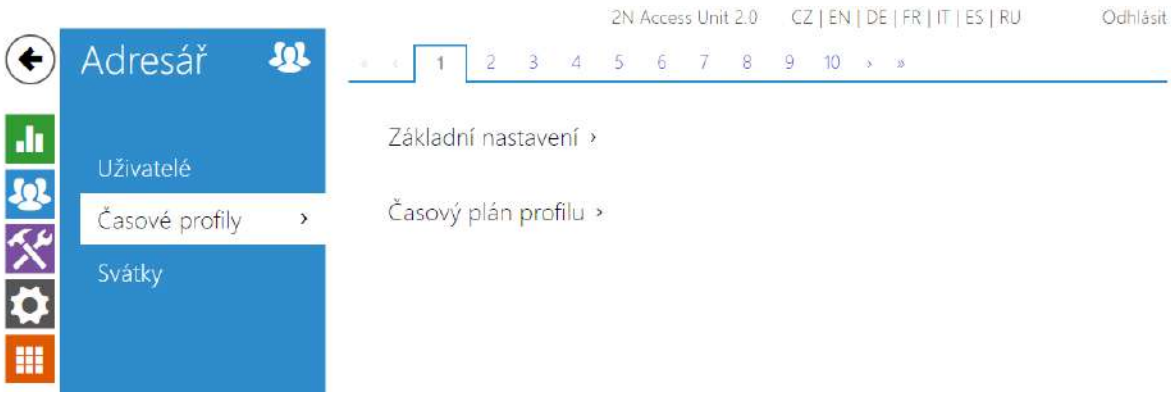
Přiložte kartu na čtečku



4. Karta je načtená

5. Nezapomeňte konfiguraci uložit.

5.2.2 Časové profily



Vybrané funkce přístupové jednotky 2N, 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

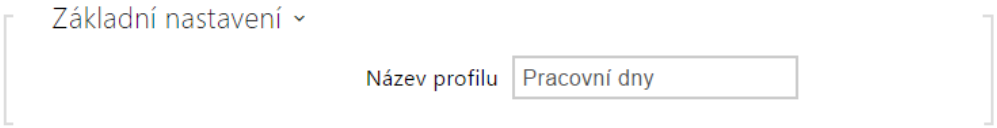
- blokovat sepnutí spínače mimo vyhrazený čas

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. Zařízení umožňuje vytvořit až 20 různých časových profilů. Dané funkci můžete přiřadit libovolný vytvořený časový profil, viz nastavení Uživatelé, Přístupové karty, Spínače.

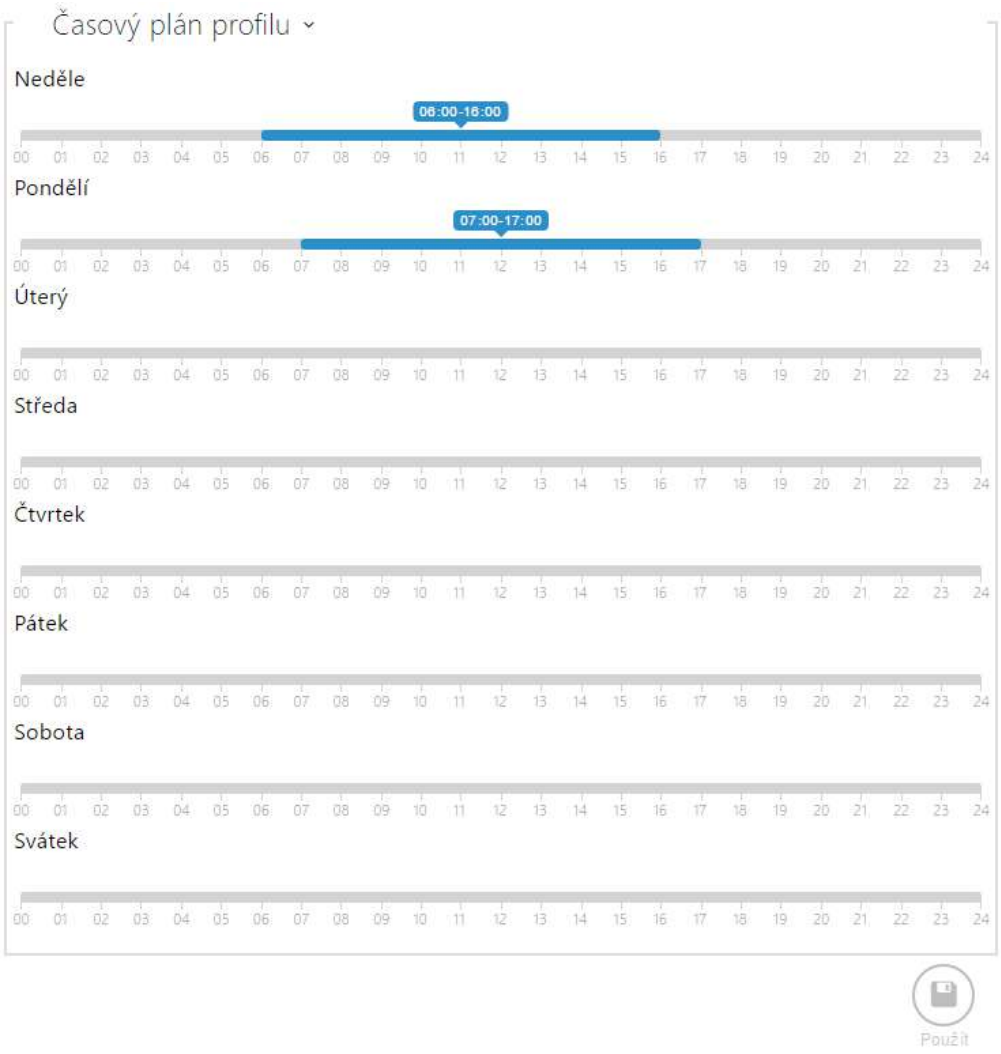
Platnost časového profilu můžete řídit nejen nastavením týdenního kalendáře, ale i pomocí speciálních aktivačních a deaktivačních kódů přiřazených danému profilu. Aktivační a deaktivační kódy lze kdykoli zadat pomocí numerické klávesnice zařízení. Tímto způsobem lze manuálně aktivovat příp. deaktivovat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

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

Seznam parametrů



- **Název profilu** – zadejte název časového profilu, abyste ho mohli snadno identifikovat při jeho výběru ve spínačích, řízení přístupu, telefonních číslech atd.



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

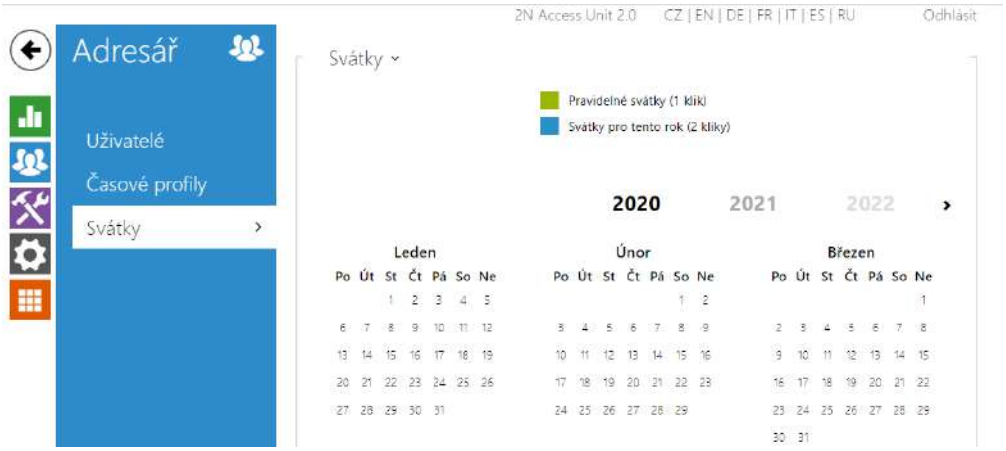
V případě, že daný den je označen jako svátek (viz nastavení **Adresář > Svátky**), pak se bez ohledu na to, jaký je den v týdnu, uplatní poslední řádek tabulky označený jako Svátek.

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

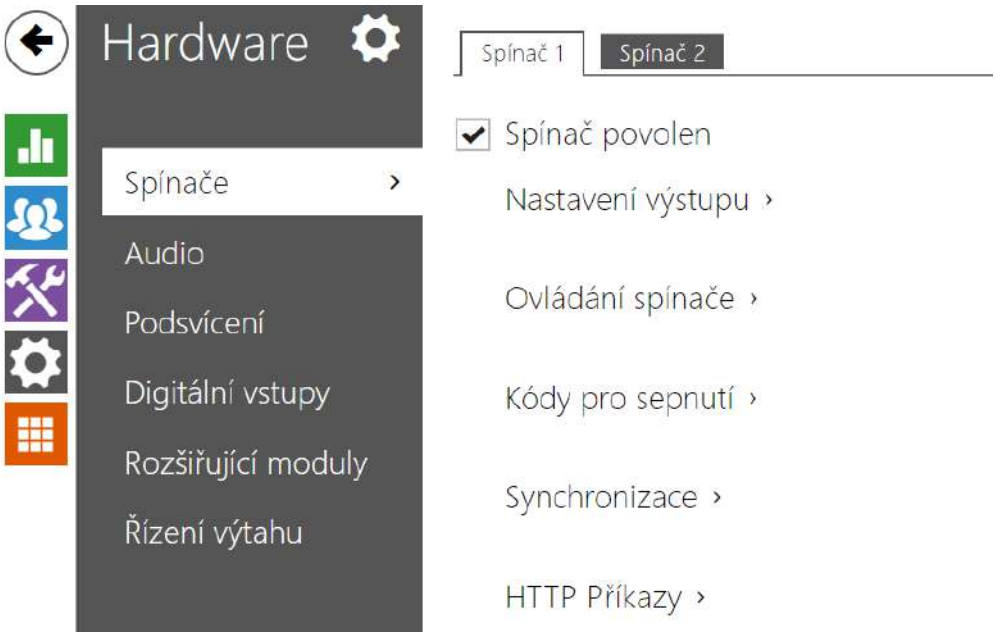


Na této stránce se nastavují dny, na které připadá svátek (příp. den pracovního klidu). Pro dny, na které připadá svátek, lze v časovém profilu nastavit odlišné časové intervaly než pro ostatní dny.
Svátky lze nastavit až na následujících 10 let dopředu (rok lze zvolit kliknutím na číslo roku v horní 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 zařízení (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,
- přiložením platné RFID karty ke čtečce,
- s definovaným zpožděním od sepnutí jiného spínače,
- časovým profilem *),
- přijetím HTTP příkazu z jiného zařízení v síti,
- pomocí automatizace pomocí akce Action.ActivateSwitch *).

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

> **Upozornění**
>
> - Možnosti označené *) vyžadují příslušné aktivní licence.

Uzamčení a přidržení spínače
Podmínky spínání spínače je možné modifikovat pomocí dvou funkcí. Jednou z nich je uzamčení, druhou je přidržení spínače. V případě, že je spínač uzamčen, je trvale ve stavu "vypnuto" a není možné s ním manipulovat, dokud není odemčen (uzamčení má vyšší prioritu než přidržení – v případě, že je spínač zároveň uzamčen a přidržen, uplatňuje se uzamčení). V případě, že je spínač přidržen, je trvale ve stavu "sepnuto" a není s ním možné manipulovat, dokud není uvolněn.
Uzamčení i přidržení je možné řídit mimo jiné pomocí časových profilů. U funkce uzamčení není

doporučeno časový profil využívat (ovládání uzamčení pomocí časového profilu je v zařízení přítomno z důvodu zpětné kompatibility), neboť v takovém případě na konci časového profilu dojde k odemčení spínače i přesto, že byl spínač uzamčen manuálně.
Aktuální kombinaci těchto dvou funkcí zobrazuje parametr **Aktuální fungování spínače** (Normální – uzamčení i přidržení je vypnuto; Přidržen – uzamčení je vypnuto a přidržení zapnuto; Uzamčen – uzamčení je zapnuto, nebere se ohled na nastavení přidržení).
Po restartu zařízení zkontroluje, zda je uzamčení či přidržení ovlivňováno časovým profilem. V případě, že ano, je příslušná funkce aktivována či deaktivována s ohledem na nastavení časového profilu. V případě, že ne, je nastaven poslední stav uzamčení před vypnutím zařízení, respektive je přidržení nastaveno do neaktivního stavu (spínač není přidržen).

Pokud je spínač aktivní, lze nastavit:

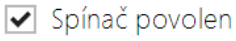
- sepnutí libovolného logického výstupu přístupového terminálu (relé, výkonový výstup)
- sepnutí výstupu, na který je připojen modul **2N Bezpečnostní relé**
- odeslání HTTP příkazu jinému zařízení

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.

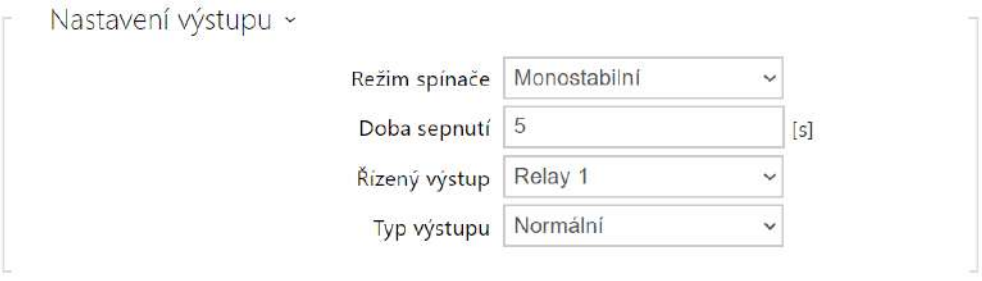
Spínač může signalizovat svůj stav pomocí:

- konfigurovatelného pípnutí
- signalizační LED diodou

Záložka Spínač 1–2



- **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 hovorem ani tlačítkem rychlé volby.



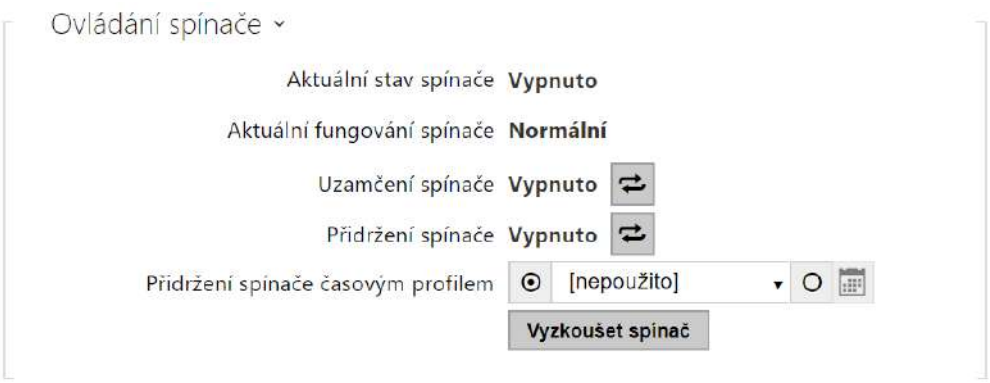
- **Režim spínače** – nastavuje monostabilní nebo bistabilní režim spínače. V monostabilním režimu je spínač automaticky vypnut po nastavené době sepnutí. V bistabilním režimu se spínač první aktivací zapne a druhou vypne.
- **Doba sepnutí** – nastavuje dobu sepnutí spínače v monostabilním režimu. V bistabilním režimu spínače se nastavená doba sepnutí neuplatní.
- **Řízený výstup** – přiřazuje spínači fyzický výstup. Lze vybrat mezi všemi dostupnými výstupy – relé, aktivní výstup, výstup na rozšiřujícím modulu apod. Pokud zvolíte volbu Žádný, spínač nebude ovládat žádný fyzický výstup, ale stále může ovládat externí zařízení pomocí HTTP příkazů.
- **Typ výstupu** – Pokud používáte Bezpečnostní relé, nastavte typ výstupu na **Security**. V režimu **Security** výstup pracuje v Inverzním režimu, tj. je stále sepnutý a ovládá Bezpečnostní relé pomocí specifické sekvence pulzů. Pokud používáte reverzní zámek dveří (tj. dveře jsou při přivedení napětí na zámek uzamčeny), nastavte typ výstupu na hodnotu **Inverzní**. V případě, že více spínačů je nastaveno na stejný výstup, ale mají rozdílné typy výstupů, budou řízeny podle následující priority: 1. Security, 2. Inverzní, 3. Normální.

Poznámka

- *Pro typ výstupu: **Security** lze nastavit dobu sepnutí spínače pouze hodnota vyšší jak 1 s. Pro typ výstupu: **Normální, Inverzní** lze nastavit dobu sepnutí na hodnotu 0.1 s a vyšší.*

Bezpečnost

- 12V výstup slouží k připojení zámku. Pokud je ovšem zařízení (2N IP Interkom, přístupové jednotky 2N) na místě (plášť budovy), kde hrozí neoprávněné vniknutí do zařízení, je silně doporučeno použít 2N Bezpečnostní relé (obj. č. 9159010) pro maximální bezpečnost instalace.



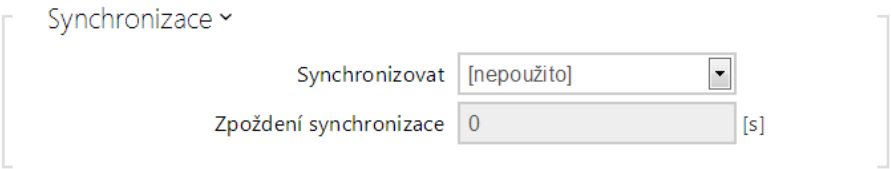
- **Aktuální stav spínače** – zobrazuje aktuální stav spínače (Zapnuto či Vypnuto).
- **Aktuální fungování spínače** – zobrazuje aktuální fungování spínače.
  - **Normální**: spínač není uzamčen ani přidržen.
  - **Přidržen**: spínač je přidržen a není uzamčen.
  - **Uzamčen**: spínač je uzamčen (v tomto případě na přidržení spínače nezáleží, uzamčení má prioritu).
- **Uzamčení spínače** – přepíná mezi odemčeným a zamčeným stavem. Když je spínač zamčený (ZAPNUTO), jeho logický stav je 0 a nelze jej ovládat, dokud není odemčen.
- **Přidržení spínače** – zapnuto: spínač je trvale v pozici 1 a není možné ho ovládat, dokud nedojde k jeho uvolnění (v případě, že je zároveň aktivní podržení i zamčení, je spínač uzamčen. Vypnuto: spínač není podržen v pozici 1.
- **Přidržení spínače časovým profilem** – umožňuje přiřadit spínači předdefinovaný časový profil nebo manuálně nastavit časový profil, který povoluje sepnutí spínače. Pokud přiřazený časový profil není aktivní, lze spínač aktivovat přiložením platné RFID karty nebo zadáním kódu/*/.
- **Tlačítko „Vyzkoušet spínač“** – umožňuje ručně aktivovat spínač pro ověření jeho funkce, například elektrického zámku nebo jiného připojeného zařízení.

Upozornění

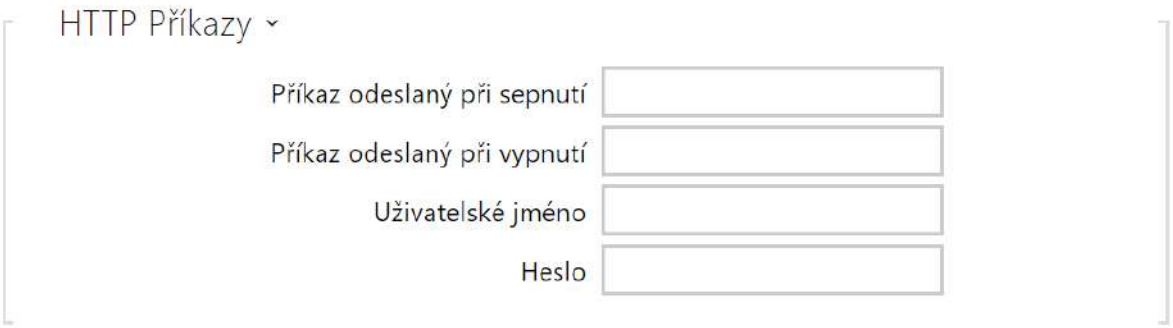
- V případě, že je spínač uzamčen a dojde k vypnutí a opětovnému zapnutí zařízení, bude spínač po zapnutí zařízení nadále uzamčen. Stejným způsobem se spínač chová v případě, že je zakázán a následně povolen.
- V případě, že je spínač přidržen a dojde k vypnutí a opětovnému zapnutí zařízení, nebude spínač po zapnutí přidržen. Spínač je po zapnutí zařízení přidržen jen v případě, že je nastaven časový profil pro přidržení spínače a tento profil je ve chvíli zapnutí zařízení aktivní. Stejným způsobem se spínač chová v případě, že je zakázán a následně povolen.

Seznam univerzálních kódů, pomocí kterých lze z klávesnice zařízení 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 zařízení 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, jsou vyhrazeny pro otevírání pomocí DTMF a z klávesnice nebudou akceptovány. 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** – nastavuje, zda budou v bistabilním režimu kódy na lichých řádcích (1, 3, ...) použity k aktivaci spínače a kódy na sudých řádcích (2, 4, ...) k deaktivaci.



- **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** – nastavuje URL pro HTTP nebo HTTPS GET požadavek odeslaný při aktivaci spínače. Příkaz musí být ve tvaru http://ip_adresa/cesta. Nap ř. http://2.2.2.1/relay1=on.
- **Příkaz odeslaný při vypnutí** –Nastavuje URL pro HTTP nebo HTTPS GET požadavek odeslaný při deaktivaci spínače. Příkaz musí být ve tvaru http://ip_adresa/cesta. Nap ř. http://192.168.1.50/relay1=off.
- **Uživatelské jméno** – nastavuje uživatelské jméno pro HTTP příkazy zaslané při aktivaci a deaktivaci spínače. Vyžadováno pouze v případě, že je vyžadována autentizace.
- **Heslo** – nastavuje heslo pro HTTP příkazy odeslané při aktivaci a deaktivaci spínače. Vyžadováno pouze v případě, že je vyžadována autentizace.

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)

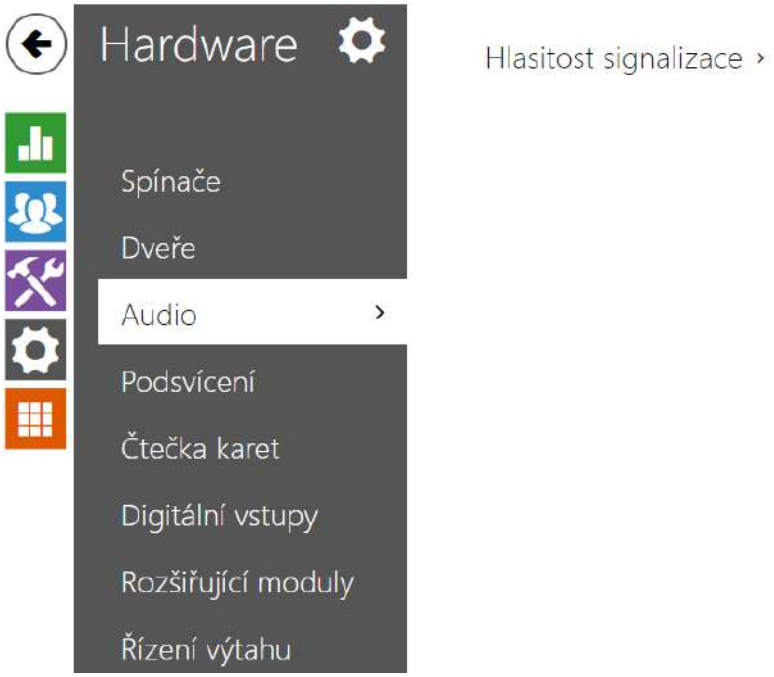
V případě použití externího relé **obj.č.: 9137411E** jsou použity následující HTTP příkazy (znak X v příkazech je třeba nahradit číslem relé):

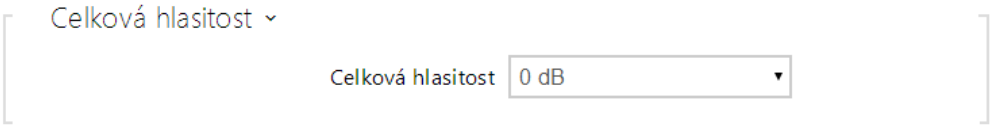
- **Pro trvalé sepnutí** – http://ip_adresa/state.xml?relayXState=1 (např.: http://192.168.1.10/state.xml?relay1State=1)
- **Pro sepnutí na předdefinovaný čas (defaultně 1,5 s)** – http://ip_adresa/state.xml?relayXState=2 (např.: http://192.168.1.10/state.xml?relay1State=2)
- **Pro vypnutí** – http://ip_adresa/state.xml?relayXState=0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

Záložka Pokročilé

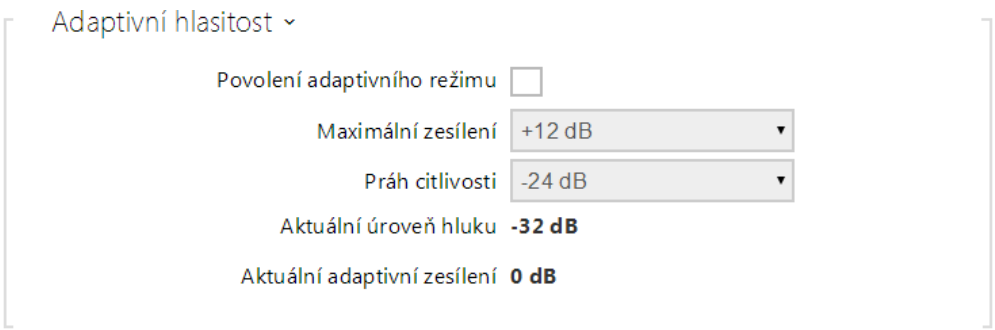
- **Maximální příkon výstupu 1** – nastavuje maximální hodnotu příkonu výstupu 1.

5.3.2 Audio



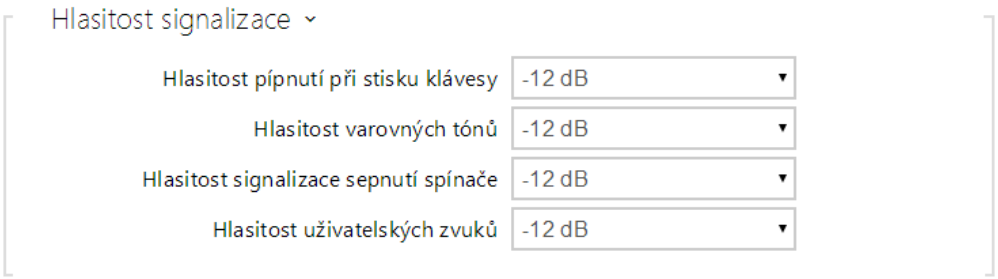


- **Celková hlasitost** – nastavuje celkovou hlasitost podle požadované hlasitosti hovoru a poté přizpůsobte ostatní hlasitosti podle potřeby. Toto nastavení ovlivňuje hlasitost všech zvuků.

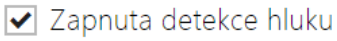


- **Povolení adaptivního režimu** – povoluje režim adaptivní hlasitosti, který postupně zvyšuje hlasitost zařízení na základě rozdílu mezi aktuální naměřenou úrovní hluku a vybraným prahem citlivosti, až do nastavené maximální hodnoty zesílení. Toto nastavení dále zvyšuje celkovou hlasitost.
- **Maximální zesílení** – nastavuje maximální zesílení, které lze aplikovat na celkovou hlasitost, jakmile aktuální úroveň hluku překročí práh citlivosti.

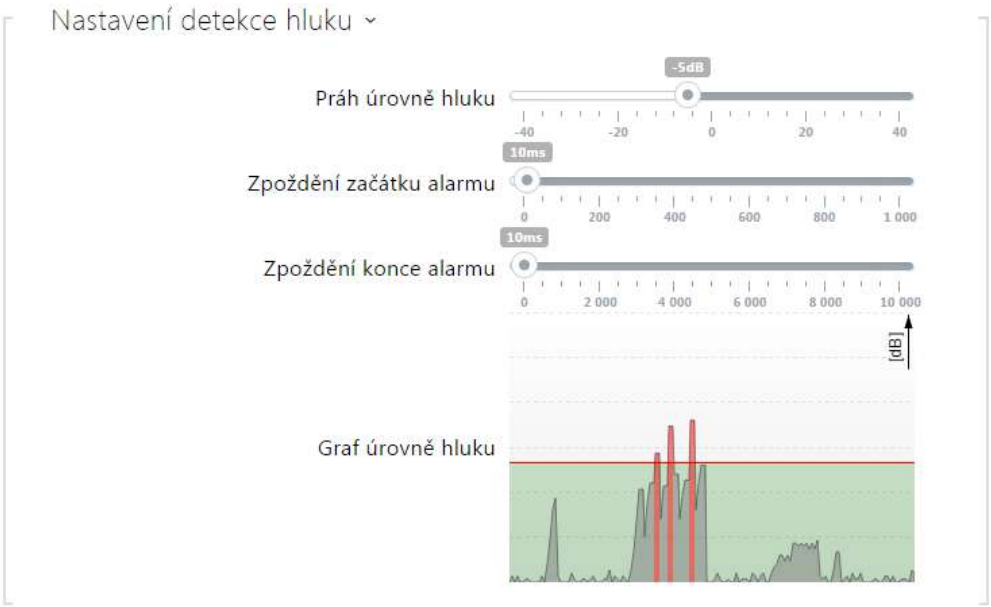
- **Práh citlivosti** – nastavuje práh okolního hluku, který určuje, kdy se začne zvyšovat hlasitost.
- **Aktuální úroveň hluku** – zobrazuje aktuálně naměřenou úroveň okolního hluku.
- **Aktuální adaptivní zesílení** – zobrazuje aktuálně aplikované zesílení celkové hlasitosti. Hodnota je daná rozdílem Aktuální úrovně hluku a nastaveného prahu citlivosti a nikdy nepřekročí nastavené maximální zesílení.



- **Hlasitost stisku tlačítka** – nastavuje hlasitost stisknutá tlačítka. Hodnota je relativní k celkové hlasitosti.
- **Hlasitost varovných tónů** – nastavuje hlasitost varovných a signalizačních tónů popsaných v kapitole Signalizace provozních stavů. Hodnota je relativní k celkové hlasitosti.
- **Hlasitost signalizace sepnutí spínače** – nastavuje hlasitost tónu sepnutého spínače. Hodnota je relativní k celkové hlasitosti.
- **Hlasitost uživatelských zvuků** – nastavuje hlasitost uživatelských zvuků přehrávaných automatizací. Hodnota je relativní k celkové hlasitosti.

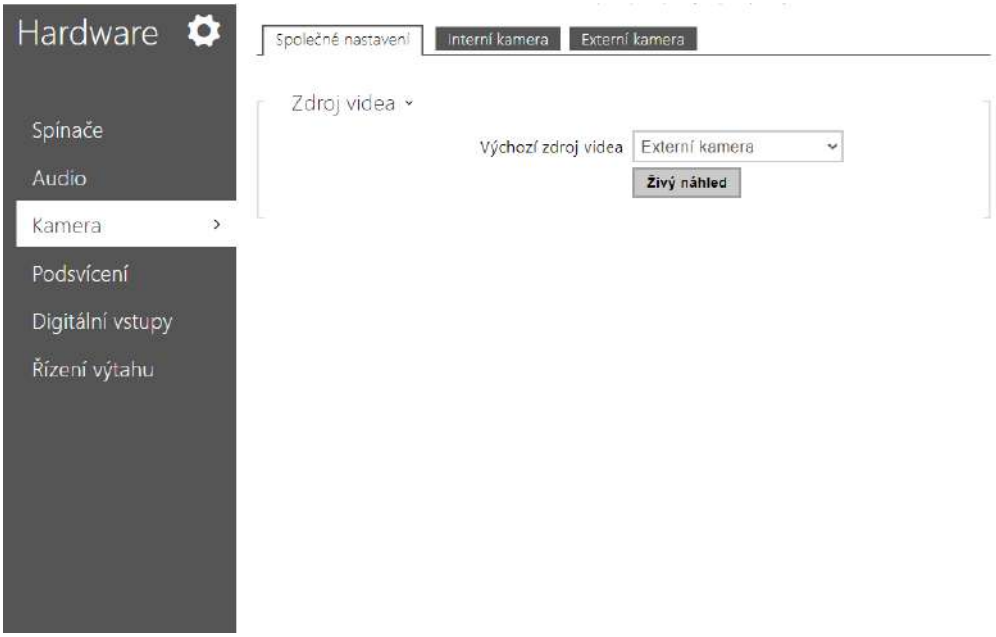


- **Zapnuta detekce hluku** – zapíná automatickou detekci hluku resp. překročení nastaveného prahu úrovně signálu mikrofonu. Alarm vyvolaný překročením prahové hodnoty lze zpracovat pomocí události automatizace **Event.NoiseDetected** a navázat jej na další uživatelské akce.



- **Práh úrovně hluku** – nastavuje práh úrovně signálu z mikrofonu, po jehož překročení bude vyvolán alarm.
- **Zpoždění začátku alarmu** – nastavuje dobu, po kterou musí být signál nad prahovou hodnotou, tak aby byl vyvolán alarm.
- **Zpoždění konce alarmu** – nastavuje dobu, po kterou musí být signál pod prahovou hodnotou, tak aby byl ukončen alarm.
- **Graf úrovně hluku** – zobrazuje historii úrovně měřeného signálu. Červeně jsou označeny okamžiky, kdy je aktivován alarm.

5.3.3 Kamera



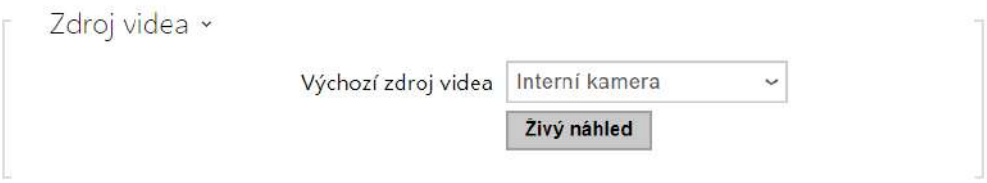
Toto menu je dostupné pouze u přístupových jednotek 2N, které jsou vybaveny interní kamerou nebo umožňují připojit externí kameru. Signál z kamery lze odesílat pomocí e-mailů, streamovat pomocí ONVIF/RTSP protokolu na jiné zařízení (např. video surveilance) nebo jednoduše stahovat ze zařízení jako JPEG snímky pomocí HTTP protokolu.

Jako zdroj video signálu může být použita:

- interní integrovaná kamera,
- běžná externí IP kamera podporující RTSP stream s kodeky MJPEG (max. rozlišení 640 x 480) nebo H.264 (max. rozlišení 640 x 480 Base Line Profile). Maximální doporučená snímková frekvence je v obou případech 15 snímků za sekundu. Při vyšších snímkových frekvencích může docházet k nežádoucím efektům (snížení plynulosti přehrávání).

V menu Kamera se nastavují parametry kamery, jako je jas, sytost barev, příp. přihlašovací údaje pro externí IP kameru. Parametry související se streamováním videa se nacházejí v menu **Služby > Streamování** a **Služby > E-Mail**.

Záložka Společné nastavení

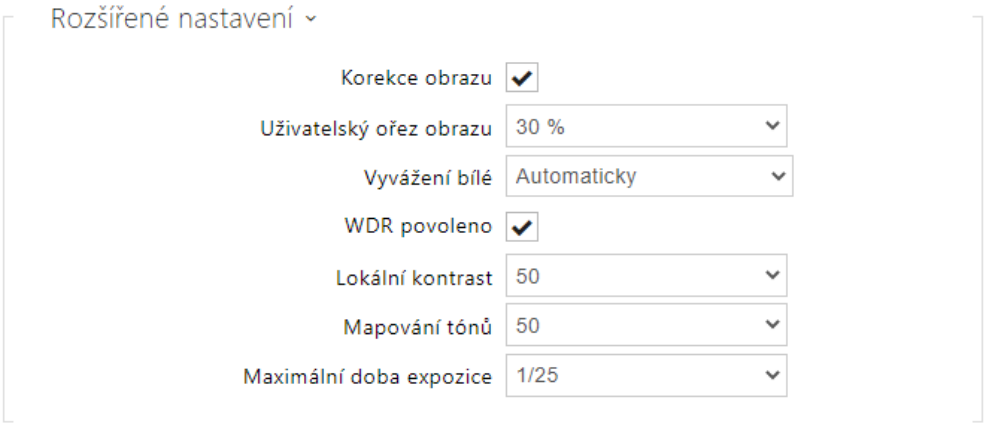


- **Výchozí zdroj videa** – nastavuje výchozí zdroj obrazu. Lze volit mezi interní kamerou (nebo analogovou kamerou připojenou k interkomu) nebo externí kamerou. Změna výchozího zdroje video signálu se uplatní u RTSP streamu a při použití HTTP API. V aplikaci **2N IP Eye** je nutné externí kameru vybrat ručně. V případě, že externí kamera není správně připojena nebo nastavena, zobrazují se znaky N/A na modrém pozadí.
- **Živý náhled** – zobrazí okno s živým náhledem ze zvolené kamery.

Záložka Interní kamera

- **Úroveň jasu** – nastavuje jas obrazu kamery. Toto nastavení umožňuje celkově zesvětlit nebo ztmavit obraz.
- **Úroveň expozice** – nastavuje jas obrazu kamery. Toto nastavení umožňuje celkově zesvětlit nebo ztmavit obraz.
- **Kontrast** – nastavuje kontrast obrazu kamery.
- **Saturace barev** – nastavuje sytost barev obrazu kamery.
- **Režim kamery** – nastavte vhodnou kombinaci expozičního režimu a frekvence napájení, pokud je v obrazu kamery viditelné blikání. V případě vnitřní instalace lze volit mezi různými způsoby potlačení blikání obrazu způsobeného zdroji umělého světla. V případě venkovní instalace lze nastavit režim potlačení přímého slunečního světla.
- **Živý náhled** – zobrazí okno s živým náhledem z kamery zařízení ve zvoleném režimu.

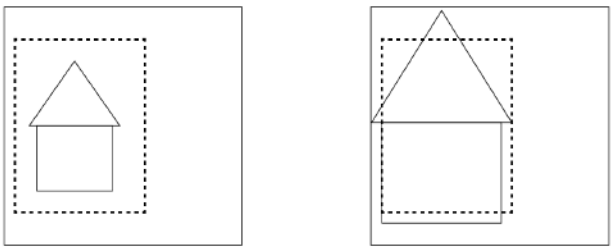
Skupina funkcí *Pokročilá nastavení* je platná pro 2N Access Unit QR.

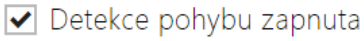


- **Korekce obrazu** – zapíná korekci rybího oka.
- **Uživatelský ořez obrazu** – nastavuje výchozí centrované oříznutí obrazu (okraje jsou rovnoměrně ořezány).
- **Vyvážení bílé** – nastavení fixního vyvážení bílé dle převládajícího zdroje světla je vhodné v případě, že nestačí automatické vyvážení bílé (nevhodně zvolená varianta vyvážení bílé vede k nežádoucímu zabarvení obrazu).
- **WDR povoleno** – WDR (Wide Dynamic Range) je vhodné zapnout v případě, že jsou ve scéně velmi temná a zároveň velmi osvětlená místa. WDR zajistí, že bude vidět celá scéna.
- **Lokální kontrast** – nastavením vyšší úrovně dojde ke zvýraznění kontrastu rozhraní světlých a tmavých částí scény.
- **Mapování tónů** – nastavením vyšší úrovně dojde ke zvýraznění obrazu a zlepšení viditelnosti (obraz může mít v takovém případě zkreslenou barevnost).
- **Maximální doba expozice** – nastavuje maximální dobu, po kterou je exponován a vytvářen jednotlivý snímek. Když je k dispozici více světla, nemusí být závěrka otevřena po celou dobu a kamera si automaticky nastaví kratší aktuální dobu expozice.

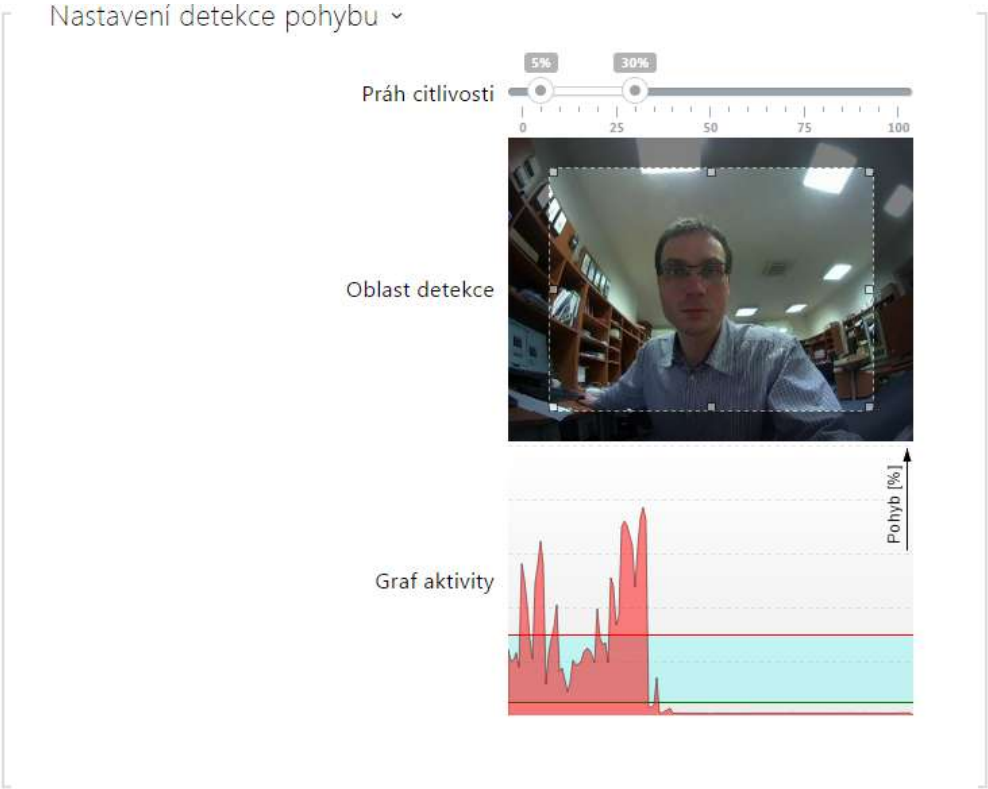
Upozornění

- Po změně nastavení parametru ***Uživatelské oříznutí scény*** u zařízení s procesorem ARTPEC-7 je nutné zkontrolovat vymezení oblasti pro oblast detekce pohybu a oblast ochrany soukromí, která se prostorově změní, viz ilustrace.



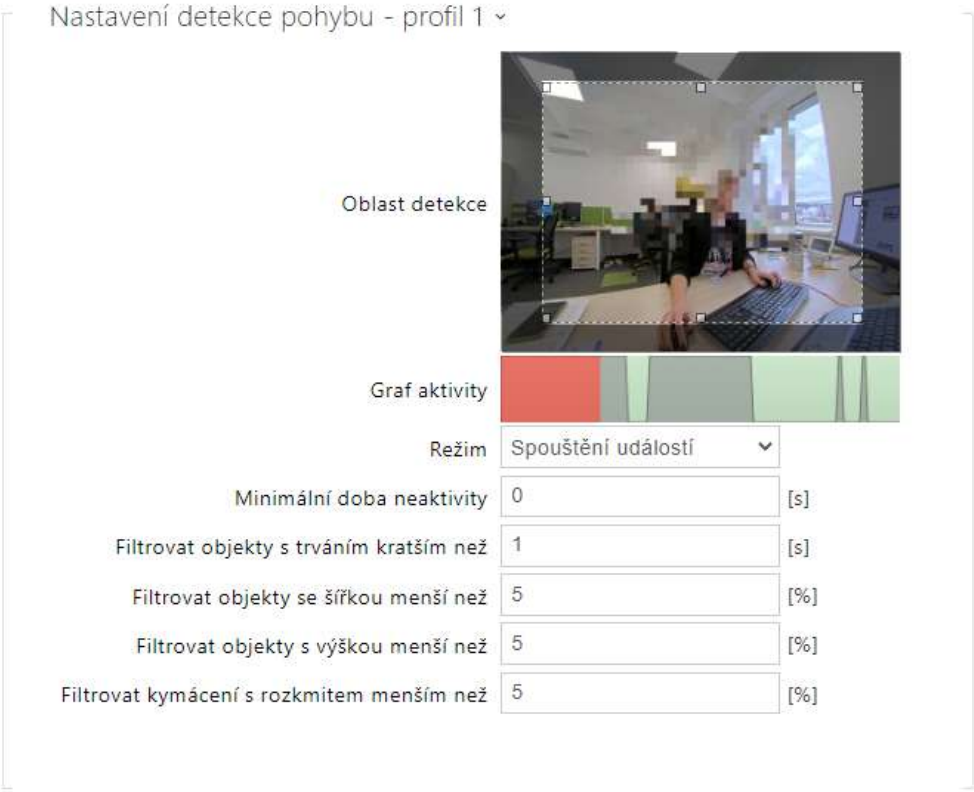


- **Detekce pohybu zapnuta** – umožňuje zapnout automatickou detekci pohybu z obrazu interní kamery. Pohyb je detekován pomoci sledování změny jasové složky ve vybrané části obrazu v čase. Při pohybu objektů v záběru kamery dochází ke změně určité části obrazu – aktivitě, kterou lze vyjádřit v procentech. Pokud aktivita překročí nastavený horní práh citlivosti je indikován pohyb. Pohyb je indikován tak dlouho, dokud aktivita neklesne pod nastavený dolní práh citlivosti. Prahy citlivosti lze nastavit podle požadavků, konkrétní instalace a stejně tak lze nastavit oblast detekce (výřez, ve kterém je sledovaná aktivita).



- **Práh citlivosti** – umožňuje nastavit dolní a horní práh citlivosti a hysterezi algoritmu detekce pohybu.
- **Oblast detekce** – umožňuje nastavit obdélníkový výřez obrazu, ve kterém se provádí detekce pohybu.
- **Graf aktivity** – zobrazuje historii detekované aktivity (změny jasové složky obrazu) společně s nastaveným dolním a horním prahem citlivosti.

- **Detekce pohybu – profil 1/2 zapnuta** – umožňuje zapnout automatickou detekci pohybu z obrazu interní kamery. Pohyb je detekován pomocí sledování změny jasové složky ve vybrané části obrazu v čase. Při pohybu objektů v záběru kamery dochází ke změně určité části obrazu. Pokud aktivita překročí horní práh citlivosti, je indikován pohyb. Pohyb je indikován tak dlouho, dokud aktivita neklesne pod dolní práh citlivosti.



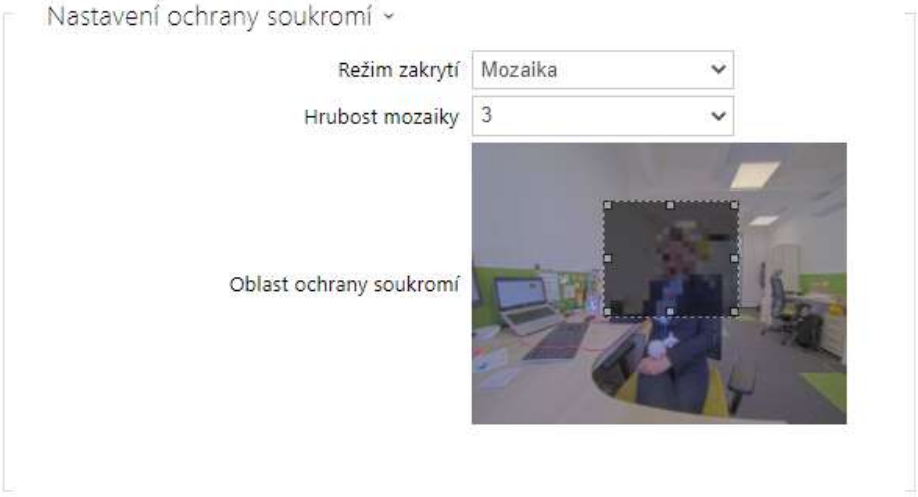
- **Oblast detekce** – umožňuje nastavit obdélníkový výřez obrazu, ve kterém se provádí detekce pohybu.
- **Graf aktivity** – zobrazuje historii detekované pohybové aktivity na časové ose. Zelená znamená žádný pohyb, šedá znamená detekovaný pohyb, ale nesplňuje podmínky filtrů, červená znamená detekovaný pohyb, který splňuje podmínky.
- **Režim** – volí způsob detekce pohybu, která generuje zápis pohybové události. Každý režim je určen pro specifické scénáře a účely.
  - **Spouštění událostí** – zachycuje okamžité, jednorázové pohyby. Příkladem použití je pořizování snímku, když někdo vstoupí do místnosti nebo se nějaký objekt pohne poblíž zařízení. Pomocí níže filtrů níže je možné definovat pohyby, které má kamera ignorovat.
  - **Nahrávání** – při detekci pohybu generuje pohybovou událost, která je automaticky prodloužena o 30 sekund. Pokud dojde k další pohybové události během těchto přidaných 30 sekund, budou tyto detekce pohybu sloučeny do jedné události. Tento

režim zajišťuje nepřetržité pokrytí a brání generování více krátkých událostí. Tento režim je vhodný pro bezpečnostní nebo monitorovací účely (ONVIF).
  - **Detekce přítomnosti obličejů** – detekuje a zaznamená pohyb, pokud se v oblasti detekce objeví obličej. Tento režim může generovat pohybové události, i když se v oblasti objeví statické obrázky obličeje.
  - **Detekce příchozích osob** – detekuje a zaznamená pohybující se osoby. Tento režim eliminuje pohybové události generované detekcí statického obrázku obličeje.
- **Minimální doba neaktivity** – nastavuje minimální dobu mezi dvěma událostmi detekce pohybu. Toto zabraňuje vzniku mnoha událostí v rychlém sledu za sebou.
- **Filtrovat objekty s trváním kratším než** – nastavuje minimální dobu, po kterou musí být nepřetržitě detekován pohyb, aby byla vygenerována událost detekce pohybu. Rozsah nastavení je od 1 do 5 s, 0 tento filtr zakazuje. Pohyb musí splňovat i ostatní podmínky nastavené v této sekci.
- **Filtrovat objekty se šířkou menší než** – nastavuje minimální šířku objektů relativně vůči celkové šířce obrazu kamery, kterou musí detekovaný objekt mít, aby došlo k vyhlášení události. Rozsah nastavení je od 1 do 100 %, 0 tento filtr zakazuje. Pohyb musí také splňovat další podmínky nastavené v této sekci.
- **Filtrovat objekty s výškou menší než** – nastavuje minimální výšku objektů relativně vůči celkové výšce obrazu kamery, kterou musí detekovaný objekt mít, aby došlo k vyhlášení události. Rozsah nastavení je od 1 do 100 %, 0 tento filtr zakazuje. Pohyb musí také splňovat další podmínky nastavené v této sekci.
- **Filtrovat objekty s kymácením menším než** – nastavuje rozsah pohybu, který když kymácející se objekt překročí, dojde k detekci pohybu. Rozsah je určen vůči celé šířce a výšce obrazu kamery. Nastavení nemá vliv na nekymácející se objekty. Rozsah nastavení je 1 až 20 %. 0 tento filtr zakazuje. Pohyb musí splňovat i ostatní podmínky nastavené v této sekci.

⚠ Upozornění

- U zařízení s procesorem ARTPEC-7 jsou pohybující se objekty vyhodnocovány i mimo aktivní oblast, a to včetně nastavených filtrů (v případě použití ***Uživatelského ořezu obrazu*** budou objekty vyhodnocovány i v částech obrazu, které jsou oříznuty a uživatel je nevidí v náhledu). Objekty, které vstoupí do aktivní zóny, spustí následně událost detekovaného pohybu. Například při nastavení časového filtru na 5 s objekt, který se pohybuje mimo aktivní oblast po dobu 10 s, spustí událost detekovaného pohybu okamžitě po vstupu do aktivní oblasti, protože podmínku filtru již splnil mimo aktivní oblast. Objekt je nadále detekován i při opuštění aktivní zóny a při opětovném vstupu do aktivní oblasti aktivuje událost okamžitě (pokud úplně neopustí oblast obrazu z kamery a není 'zapomenut').

- **Ochrana soukromí povolena** – povoluje funkci ochrany soukromí, která vymaskuje část obrazu zvolenou barvou nebo mozaikou.



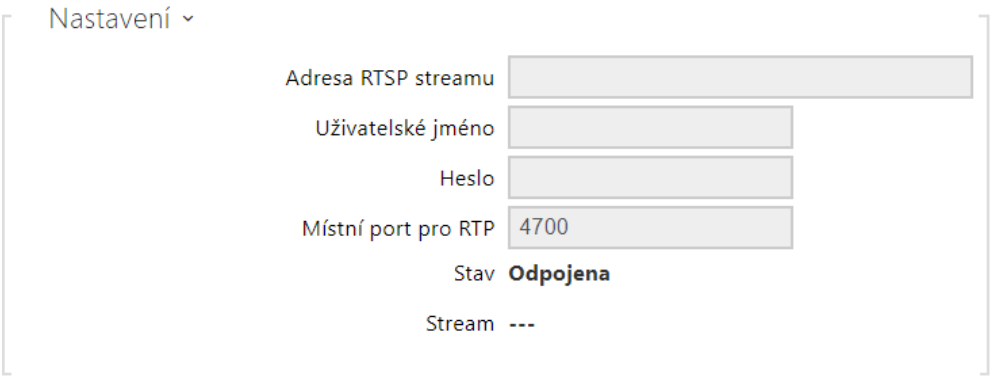
- **Režim zakrytí** – nastavuje barvu či mozaiku zakryté oblasti.
- **Hrubost mozaiky** – nastavuje hrubost mozaiky v oblasti ochrany soukromí.
- **Oblast ochrany soukromí** – nastavuje pozici a velikost oblasti ochrany soukromí.

Upozornění

- Ochrana soukromí může omezovat činnost jiných funkcí, např. **čtení QR kódů** nebo detekci pohybu. **Nedoporučujeme** používat ochranu soukromí s uvedenými funkcemi zároveň.

Záložka Externí kamera

- **Kamera povolena** – povoluje stahování RTSP streamu z externí IP kamery. Pro správnou funkci je nutné vyplnit platnou adresu RTSP streamu, příp. uživatelské jméno a heslo.



- **Adresa RTSP streamu** – adresa RTSP streamu IP kamery ve formátu rtsp://ip_adresa_kamera/parametr1=hodnota&parametr*2=hodnota*, viz tabulka parametrů níže. Parametry jsou specifické pro daný model připojené IP kamery. Pokud jako externí kameru používáte jiný interkom **2N IP**, použijte adresu ve tvaru http://ip_adresa/mjpeg_stream nebo http://ip_adresa/h264_stream.

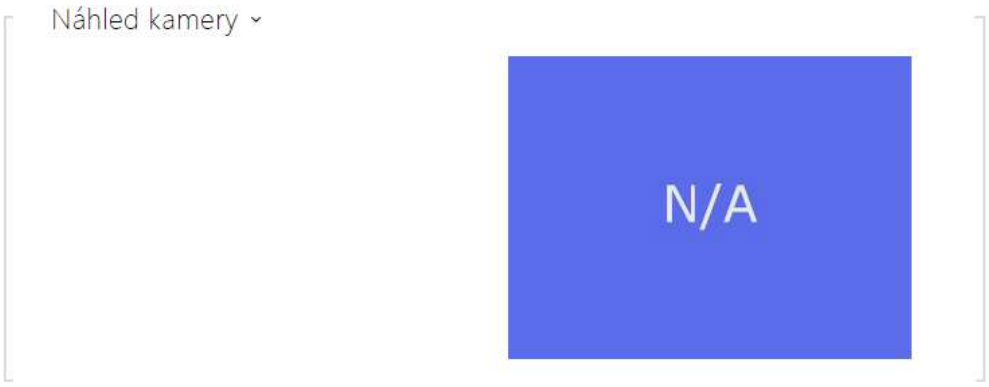
parametr	popis	příklad / hodnoty
vcodec	video kodek	vcodec=h264 pro kodek H.264 vcodec=mjpeg pro kodek MJPEG
vres	rozlišení videa	vres=1920x1080 pro FullHD
fps	snímková frekvence	fps=15 (1 až 30 fps, maximální možná hodnota pro video kodek MJPEG je 15 fps)
vbr	přenosová rychlost	vbr=768 pro 768 kbps
audio	audio	• audio=1 (povoleno) • audio=0 (zakázáno)

parametr	popis	příklad / hodnoty
zipstream	zipstream	• zipstream=off (zakázáno) • zipstream=low • zipstream=medium • zipstream=high • zipstream=higher

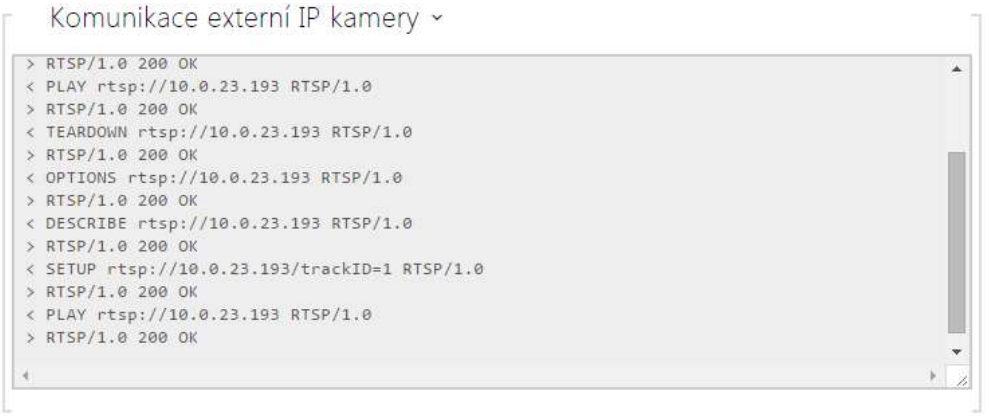
- **Uživatelské jméno** – jméno uživatele pro autentizaci připojení k externí IP kameře. Parametr je povinný pouze tehdy, pokud externí IP kamera vyžaduje autentizaci.
- **Heslo** – heslo pro autentizaci připojení k externí IP kameře. Parametr je povinný pouze tehdy, pokud externí IP kamera vyžaduje autentizaci.
- **Lokální port pro RTP** – nastavuje místní UDP port příjem RTP streamu.

Tip

- FAQ: Externí kamera – Jak ji nastavit na interkomu 2N IP?

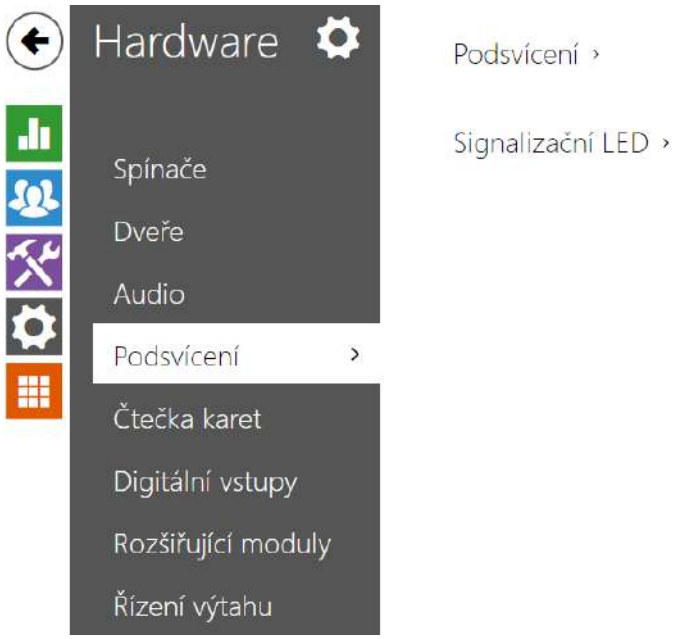


V okně náhled kamery se zobrazuje aktuální obraz přijímaný z externí kamery. V případě, že externí kamera není správně připojena nebo nastavena, zobrazují se znaky N/A na modrém pozadí.



V okně Komunikace externí IP kamery se zobrazuje průběh RTSP komunikace s nastavenou externí IP kamerou včetně případných chyb a poruchových stavů.

5.3.4 Podsvícení



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

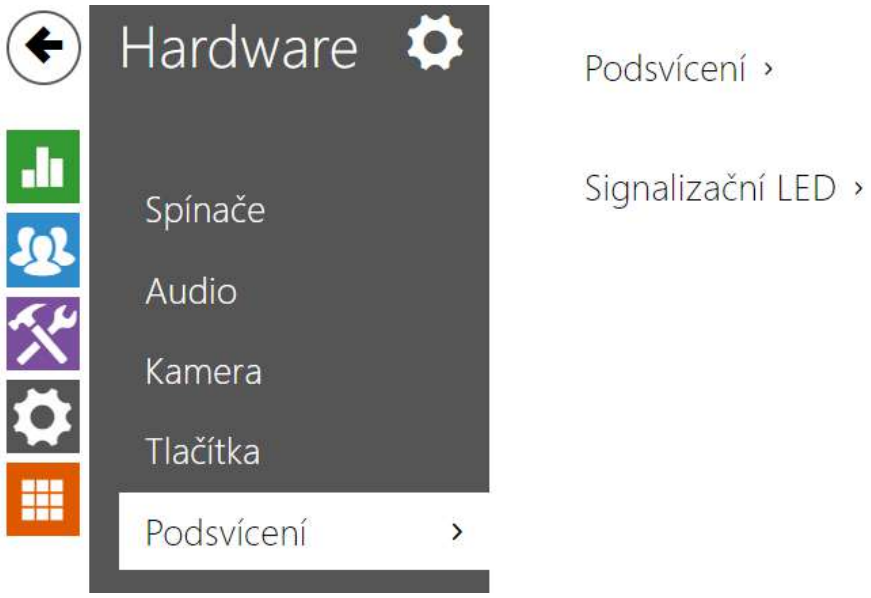
- **Podsvícení** – nastavuje hodnotu jasu podsvícení ve dne. Hodnota se udává v procentech z maximálního možného jasu LED.

- **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 zařízením, zároveň obecně zvyšuje spotřebu zařízení. Nízký jas signalizační led při použití zařízení na přímém slunci vede ke snížení kontrastu mezi zhasnutou a rozsvícenou LED a obtížné rozpoznání stavu LED.

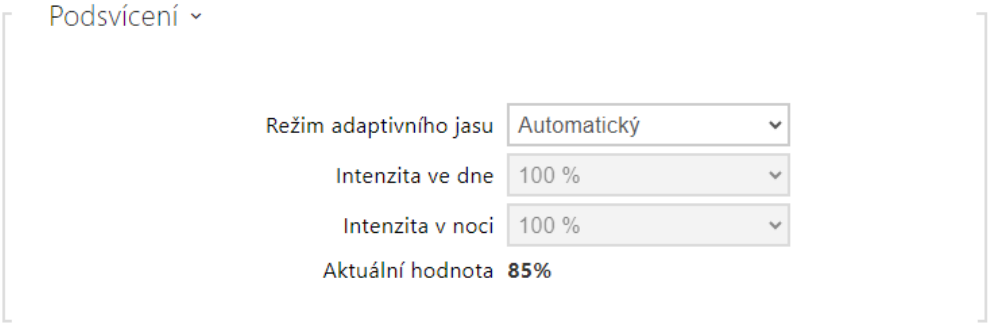
5.3.4.1 Podsvícení (2N Access Unit QR)



Na této záložce lze nastavit nezávisle úroveň svitu signalizačních LED.

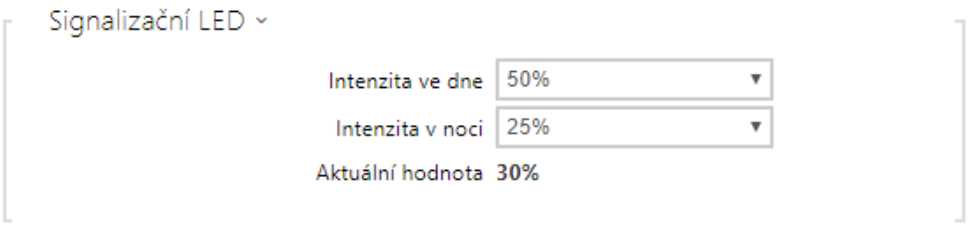
V případě, že je zařízení vybaveno senzorem úrovně okolní světla, automaticky zvolí vhodnou úroveň podsvícení v rozsahu nastavených hodnot. Viz tabulky níže:

Vlastnost	2N Access Unit QR
Řízení úrovně podsvícení	**Ano**
Senzor úrovně okolního světla	**Ano**



Nastavení parametrů ve skupině Podsvícení jsou platná pro podsvícení hlavní jednotky a přídavných modulů.

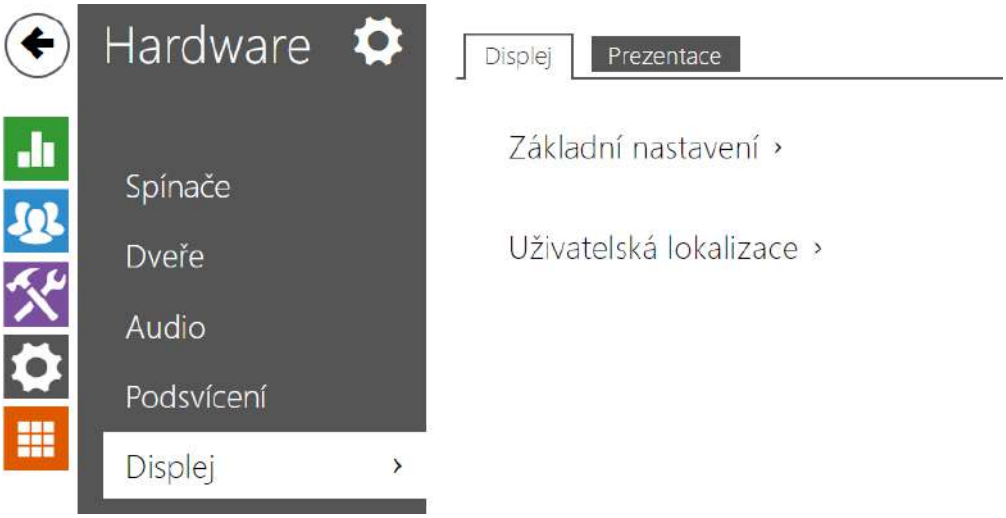
- **Režim adaptivního jasu** – Vybírá režim funkce adaptivního jasu. Když je tato funkce povolena, intenzita podsvícení všech LED a displejů se řídí automaticky.



Nastavení parametrů v bloku Signalizační LED jsou platná pro signalizační LED rozšiřujících modulů.

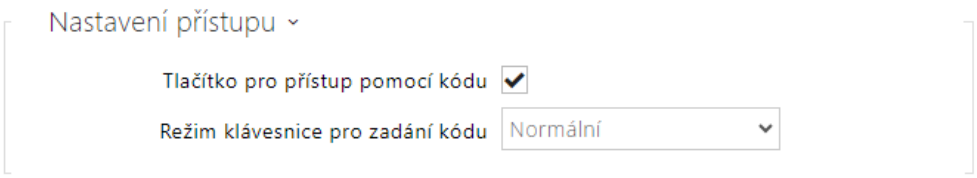
- **Intenzita ve dne** – nastavuje hodnotu intenzity podsvícení ve dne. Hodnota se udává v procentech z maximálního možného jasu LED.
- **Intenzita v noci** – nastavuje hodnotu jas LED v noci. Hodnota se udává v procentech z maximálního možného jasu LED. V případě, kdy jsou parametru Intenzita ve dne a Intenzita v noci nastaveny na stejnou hodnotu, úroveň okolního světla se nebere v potaz.
- **Aktuální hodnota** – zobrazuje aktuálně automaticky zvolenou hodnotu intenzity LED dle aktuální detekované úrovně okolního světla.

5.3.5 Displej

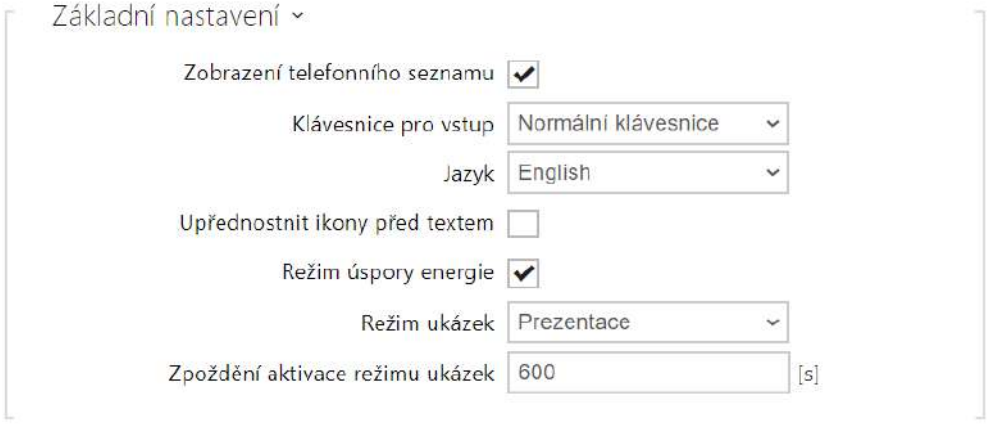


Přístupové jednotky 2N (modely **2N Access Unit 2.0** a **2N Access Unit QR)** lze rozšířit o modul displeje. Barevný LCD displej nabízí funkci dotykové klávesnice a zobrazuje stav zařízení (např. otevření dveří, odmítnutí přístupu atd.) a nebo může zároveň pracovat v režimu Prezentace, kdy se po nastavené době nečinnosti může na displeji zobrazovat prezentace v podobě sady nahraných obrázků. Mezi jednotlivými obrázky se automaticky přepíná a dobu zobrazení jednoho obrázku lze nastavit.

Záložka Displej

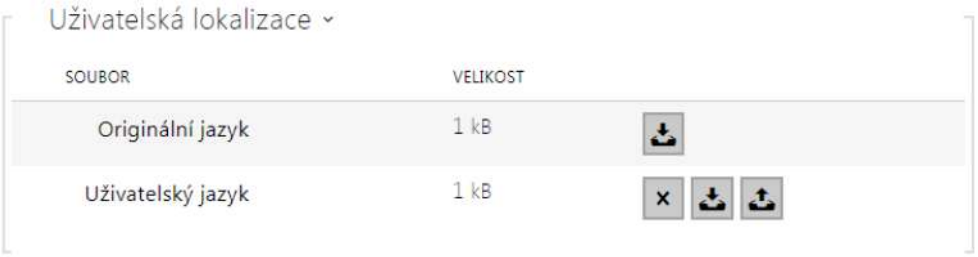


- **Tlačítko pro přístup pomocí kódu** – volí, zda má být na domovské obrazovce zobrazeno tlačítko Zadat PIN pro otevření numerické klávesnice.
- **Režim klávesnice pro zadání kódu** – vyberte mezi normálním a promíchaným uspořádáním numerické klávesnice, kde se po každém potvrzení změní poloha čísel pro zvýšení bezpečnosti. Toto nastavení se rovněž použije při vícenásobné autentizaci.



- **Zobrazení telefonního seznamu** – umožňuje zapnout a vypnout funkci telefonního seznamu na displeji.
- **Klávesnice pro vstup** – nastavuje povolení a druh klávesnice
  - **Vypnuto** – klávesnice pro vstup není k dispozici
  - **Normální klávesnice** – nastaví zobrazení běžného typu klávesnice
  - **Promíchaná klávesnice** – tato funkce náhodně promíchá pořadí tlačítek numerické klávesnice před každým novým zobrazením na displeji. Funkce znesnadňuje odpozorování zadávaného kódu další osobou.
- **Jazyk** – nastavuje jazyk textů zobrazovaných na displeji. Lze vybrat jeden z předdefinovaných jazyků.
- **Upřednostnit ikony před textem** – ikony na displeji budou upřednostněny před textem.
- **Režim úspory energie** – umožňuje aktivaci úsporného režimu, kdy se jas displeje sníží. Pokud nenastane žádná událost po dobu dvou Zpoždění aktivace prezentace, aktivace úsporného režimu proběhla úspěšně. Úsporný režim je vypnutý v případě hodnoty 0 uvedené v kolonce pro Zpoždění aktivace prezentace. Pohybem před kamerou zařízení či jakékoliv události na displeji (např. aktivace zámku dveří nebo dotyk na displeji) přejde displej do plného jasu.

- **Režim ukázek** – nastavuje, zda zařízení při nečinnosti přechází do režimu ukázek. Je možné volit různé chování v režimu ukázek (Prezentace, Logo společnosti, Adresa).
- **Zpoždění aktivace režimu ukázek** – nastavuje čas nečinnosti, po kterém zařízení přechází do režimu ukázek v rozsahu 1 až 600 vteřin.

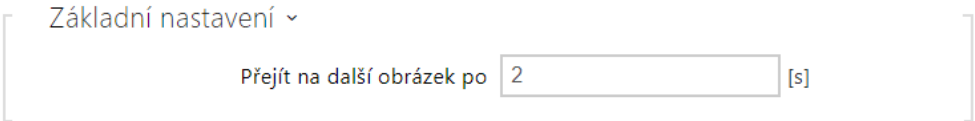


- **Originální jazyk** – umožňuje stáhnout šablonu lokalizačního souboru pro vlastní překlad. Jedná se o XML soubor se všemi texty zobrazovanými na displeji.
- **Uživatelský jazyk** – umožňuje nahrát, odstranit a stáhnout vlastní lokalizační soubor.

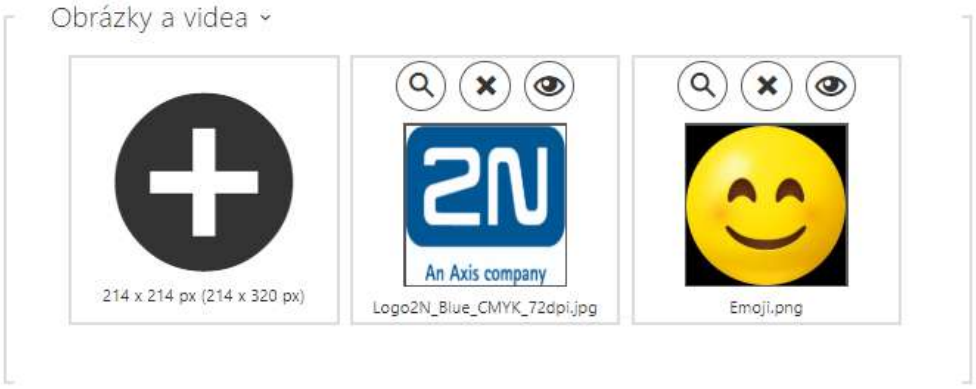
ⓘ Pokud vám nevyhovuje ani jeden z předefinovaných jazyků displeje, postupujte následovně:
- stáhněte originální jazykový soubor (je v angličtině),
- upravte soubor pomocí textového editoru (anglické texty nahraďte vlastními),
- nahrajte upravený lokalizační soubor zpět do zařízení,
- nastavte parametr **Nastavení jazyka / Jazyk** na hodnotu **vlastní**,
- zkontrolujte texty přímo na displeji zařízení a případně je upravte.

Záložka Prezentace

Na této záložce se nastavuje seznam obrázků zobrazovaných v režimu prezentace. Lze nahrát až 8 obrázků, které se postupně s nastaveným zpožděním přepínají.



- **Přejít na další obrázek po** – nastavuje dobu zobrazení jednoho obrázku prezentace, než dojde k přepnutí na další obrázek.



Rozměry nahrávaných obrázků by měly být 214 x 214 pixelů . V opačném případě budou automaticky přizpůsobeny rozlišení displeje.

Pro náhled nahraného obrázku slouží ikona lupy, odstranit obrázek lze ikonou, ikona umožňuje skrýt zobrazení vybraného obrázku nebo videa na displeji zařízení.

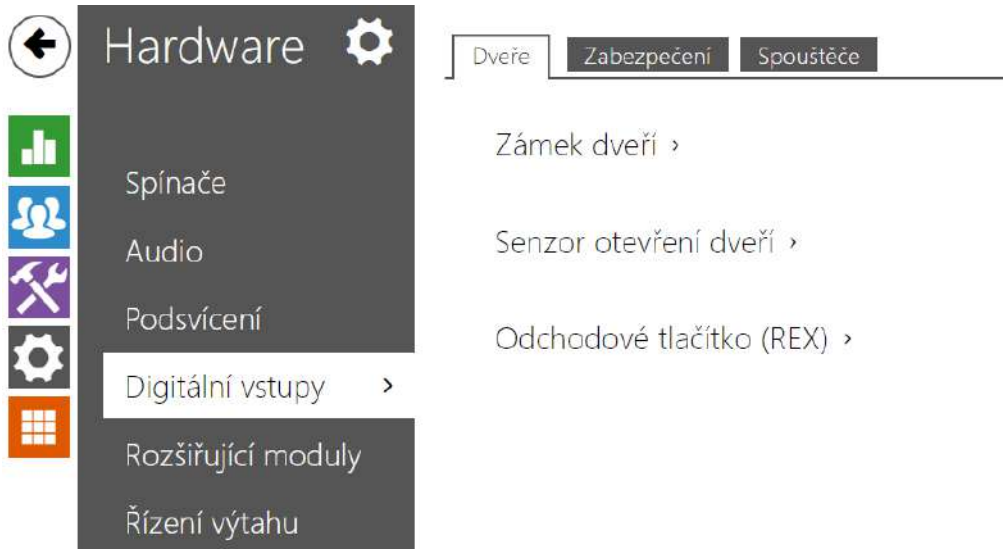
Pokud není nahrán žádný obrázek, režim prezentace se nikdy neaktivuje.

Tip

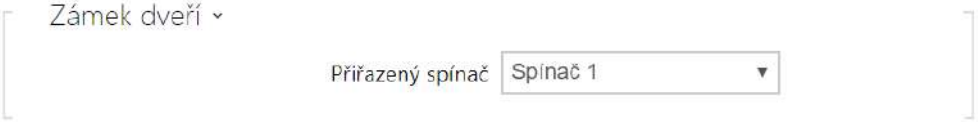
- Pro skrytí zobrazované části "Začněte dotykem" na displeji je potřeba nahrát obrázek o rozlišení 214 x 320 px.

5.3.7 Digitální vstupy

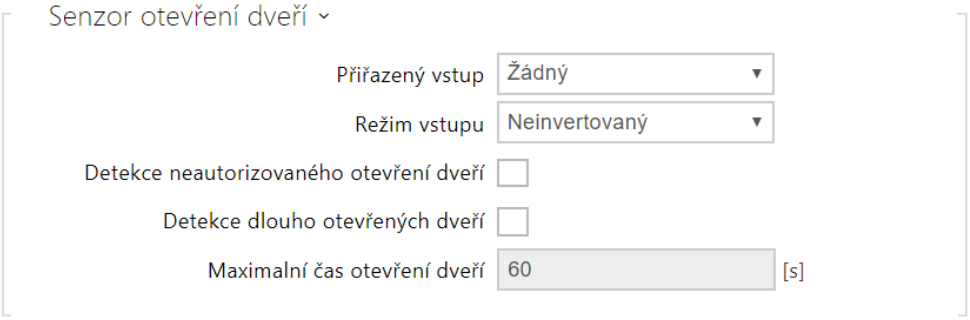
V této části konfigurace můžete nastavit parametry související s digitálními vstupy a jejich propojení s dalšími funkcemi.



Záložka Dveře

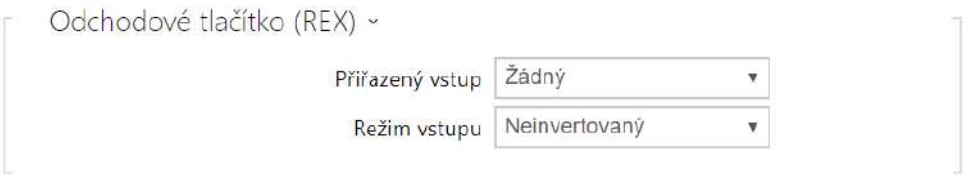


- **Přiřazený spínač** – umožňuje vybrat spínač určený pro ovládání zámku dveří. Podle stavu tohoto spínače se řídí signalizace odemknutí dveří (zelený symbol dveří, zelená LED).



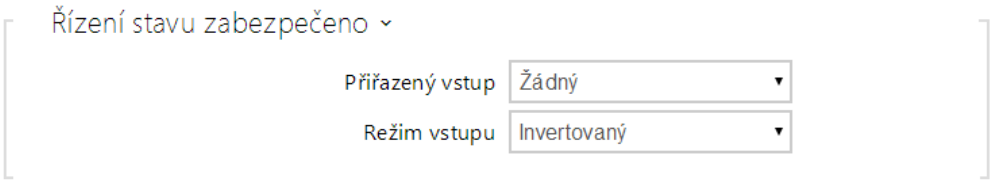
- **Přiřazený vstup** – umožňuje určit jeden z logických vstupů (příp. žádný vstup) pro detekci otevřených dveří.
- **Režim vstupu** – umožňuje nastavit aktivní úroveň (polaritu) vstupu. Neinvertovaný / Invertovaný.
- **Detekce neautorizovaného otevření dveří** – umožňuje detekovat, že dveře byly otevřeny, aniž by byl nejdříve aktivován spínač přiřazený dveřím.
- **Detekce dlouho otevřených dveří** – umožňuje detekovat dlouho otevřené dveře.

- **Maximální čas otevření dveří** – doba, po kterou mohou dveře zůstat otevřené, než se vyvolá událost Door Open Too Long.

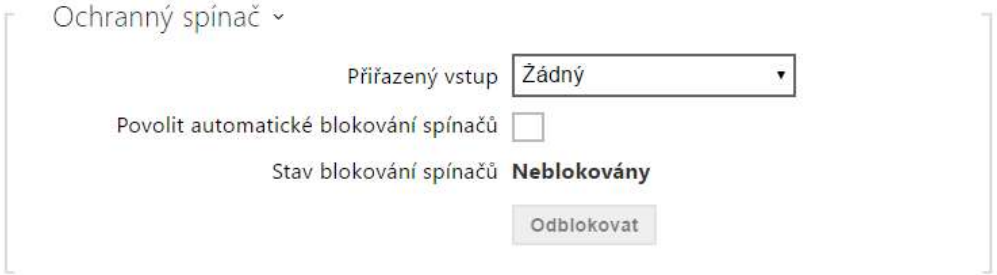


- **Přiřazený vstup** – volí logický vstup pro funkci odchodového tlačítka. Aktivace vstupu odchodového tlačítka aktivuje přiřazený spínač zámku dveří, jehož doba sepnutí a režim jsou konfigurovány v nastavení vybraného spínače.
- **Režim vstupu** – umožňuje nastavit aktivní úroveň (polaritu) vstupu. Neinvertovaný / Invertovaný.

Záložka Zabezpečení



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



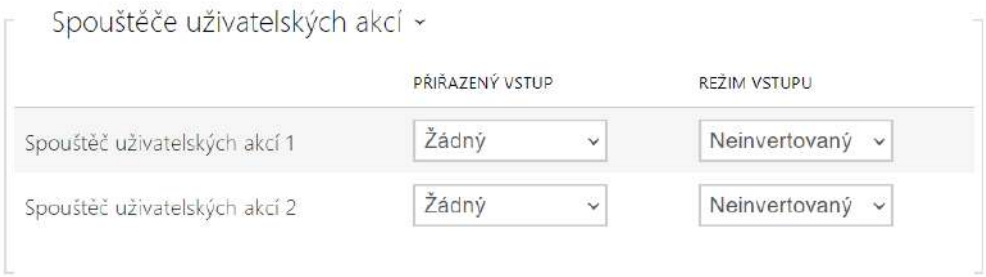
Modely vybavené ochranným spínačem umožňují detekovat otevření krytu zařízení a signalizovat tuto situaci jako událost **TamperSwitchActivated**. Události jsou zapisovány do logu, který lze vyčítat pomocí HTTP API (viz manuál **2N HTTP API**).

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**.
- **Automatické blokování spínačů** – zablokuje ostatní spínače aktivací ochranného spínače na dobu 30 minut.
- **Stav blokování spínačů** – zobrazuje a umožňuje nastavení blokování spínačů.

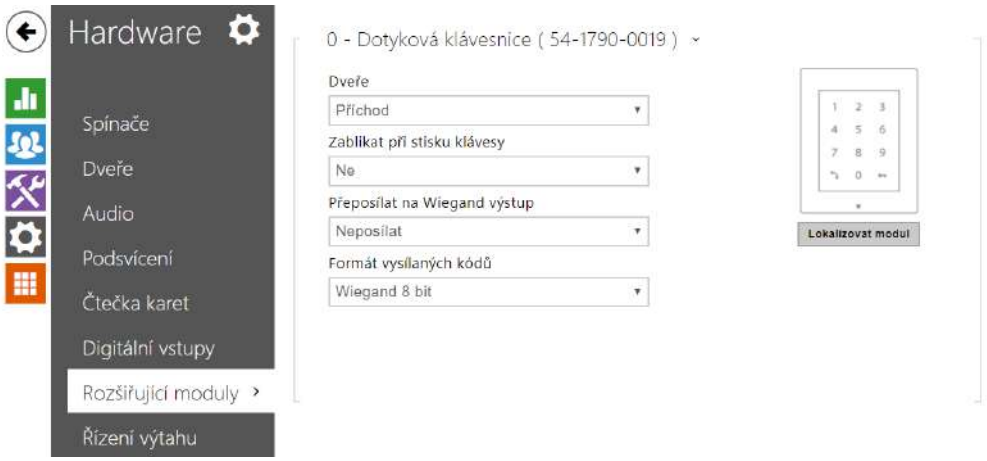
> **Poznámka**
>
> Platí pro model **2N Access Unit**:
> - Od PCB verze 599v2 jsou všechna zařízení vybavena optickým ochranným spínačem.
> - Od PCB verze 599v2 přiřazený vstup je nově signalizován podsvícením piktogramu na modulu. U nižších verzí PCB je signalizován rozsvícením LED diody na pravé straně modulu.

Záložka Spouštěče



- **Spouštěč uživatelských akcí 1, 2**
  - **Přiřazený vstup** – umožňuje zvolit logický vstup, který bude plnit funkci uživatelské akce. V případě, že je funkce aktivována, je do seznamu událostí v zařízení zapsána událost UserActionActivated s parametrem state=in (deaktivace funkce je indikována state=out). Na základě této události mohou například nadřazené systémy vyhlásit poplach, uzamknout celou budovu či provést jinou libovolnou akci.
  - **Režim vstupu** – volí, zda bude uživatelská akce vyhodnocována na základě inverzní hodnoty přiřazeného vstupu, či normální hodnoty.

5.3.8 Rozšiřující moduly



2N Access Unit, 2N Access Unit 2.0 a 2N Access Unit QR lze rozšiřovat pomocí tzv. rozšiřujících modulů připojených přes VBUS sběrnici. K dispozici jsou moduly uvedené v Instalačním manuálu zařízení. Dokud není připojen rozšiřující modul, tato sekce se ve webovém konfiguračním rozhraní nezobrazuje. Pro zobrazení sekce je po připojení rozšiřujícího modulu doporučeno restartovat zařízení.

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.

Upozornění

- Detekce připojeného modulu neprobíhá automaticky. Pro zobrazení připojeného modulu v seznamu rozšiřujících modulů zařízení restartujte.
- V případě, že verze firmwaru připojovaného modulu a hlavní jednotky nejsou kompatibilní, nebude modul detekován. Proto je nutné po připojení modulů aktualizovat firmware zařízení. Aktualizovat firmware lze pomocí webového rozhraní zařízení v části **Systém > Údržba**.

Upozornění

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

- Po připojení modulu se čtečkou karet k zařízení, ve kterém jsou nahrané čtecí klíče **2N PICard**, je nutné modul se zařízením spárovat. Bez spárování nebude mít modul čtečky přístup ke čtecím klíčům a nebude moct zašifrované karty načíst. Spárování modulu se provede pomocí tlačítka **Spárovat modul**.

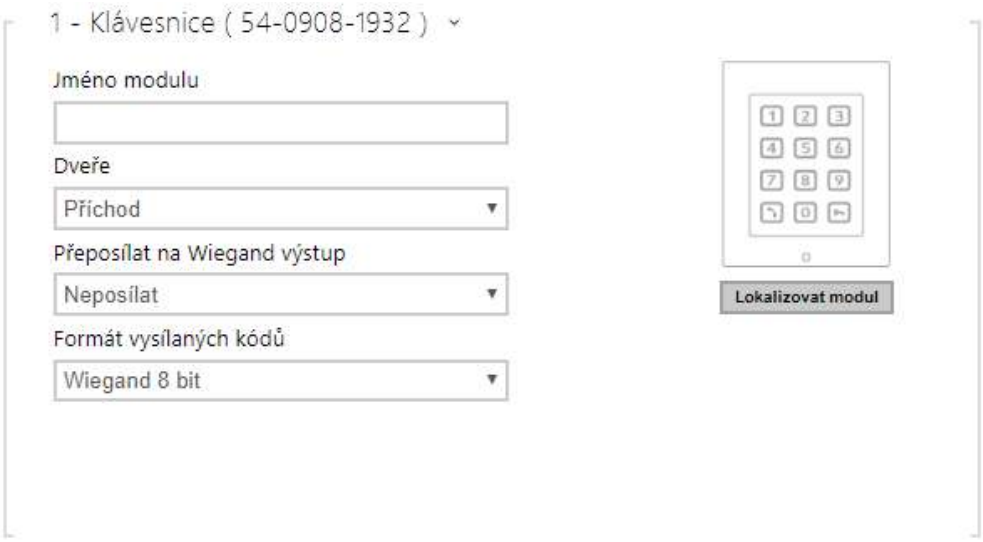
Upozornění

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

Tip

- Umístěním kurzoru myši na obrázek modulu se zobrazí jeho základní výrobní a softwarové informace.

Konfigurace modulu klávesnice

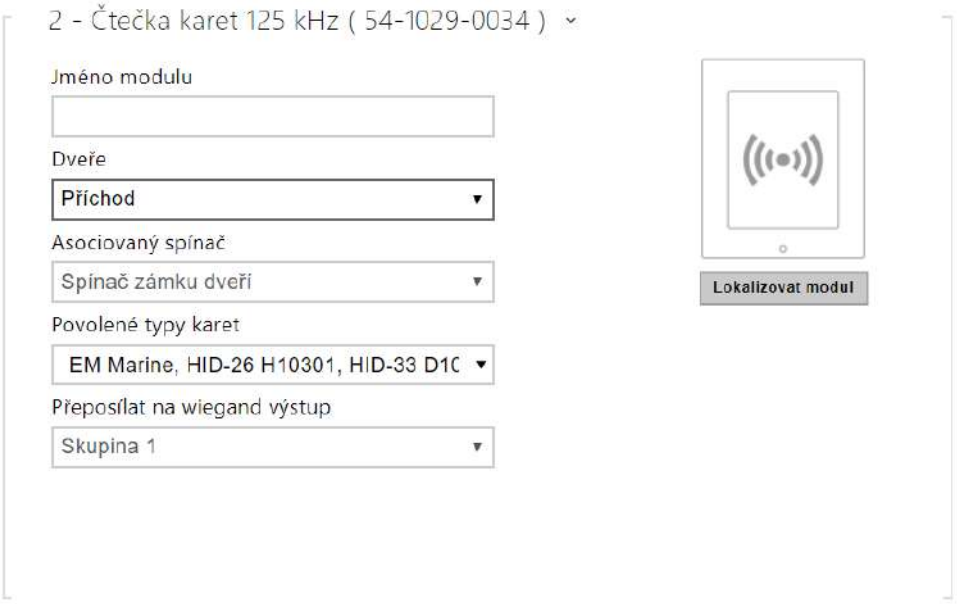


- **Název modulu** – nastavuje název modulu. Název modulu se používá při logování událostí z klávesnice.
- **Dveře** – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směru je využíván docházkovým systémem.
- **Přeposílat na Wiegand výstup** – nastavuje skupinu and výstupů, na 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



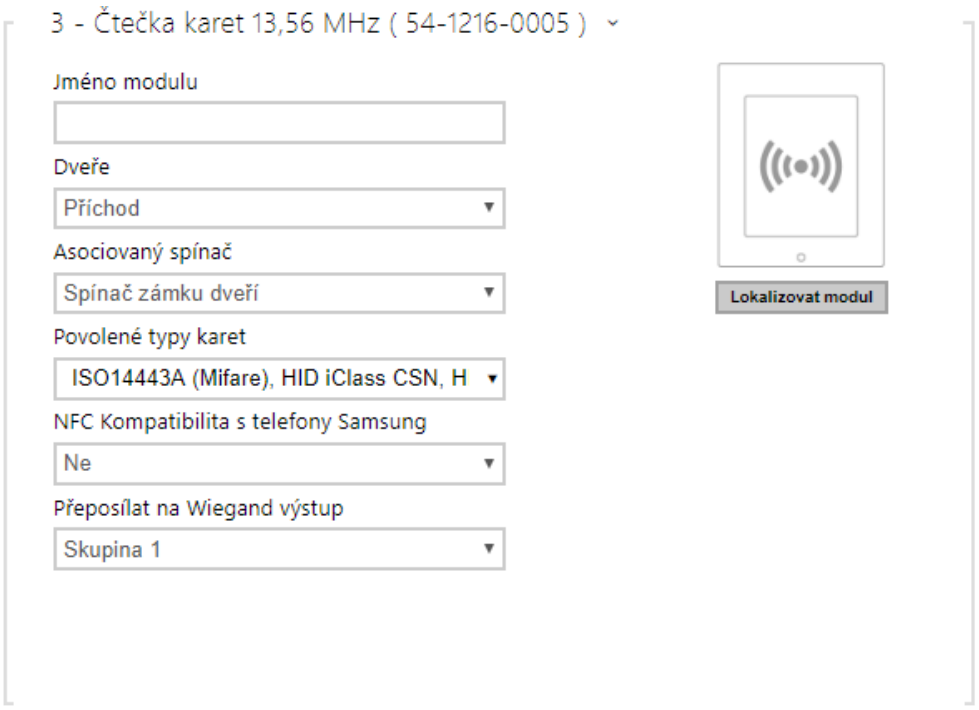
- **Název modulu** – nastavuje název modulu. Název modulu se používá při logování událostí čtečky karet.
- **Dveře** – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směr je využíván docházkovým systémem.

- **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



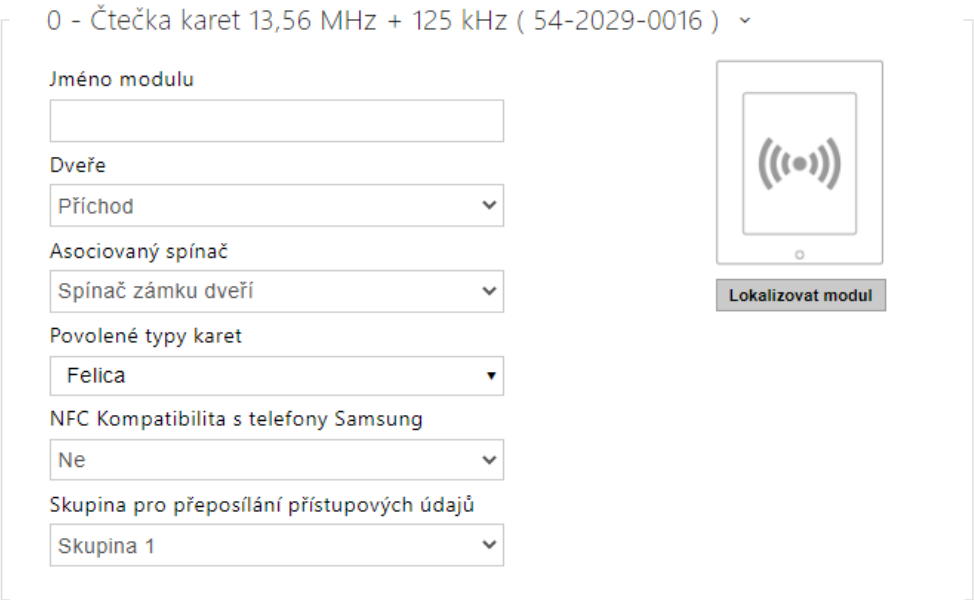
- **Název modulu** – nastavuje název modulu. Název modulu se používá při logování událostí čtečky karet.
- **Dveře** – nastavuje směr průchodu při použití čtečky (Nespecifikováno, Příchod, Odchod). Parametr směr je využíván docházkovým systémem.
- **Asociovaný spínač** – nastavuje číslo spínače aktivovaného 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



- **Název 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 2 m.
  - **Velký** – dosah je maximálně možný.
- **Spustit autentizaci** – nastavuje způsob autentizace pomocí mobilního telefonu:
  - **Na zařízení** – autentizaci je nutné potvrdit dotykem na čtečce za přítomnosti telefonu se spárovanou **2N Mobile Key** aplikací.
  - **V aplikaci** – autentizaci je nutné potvrdit klepnutím na ikonu ve spuštěné aplikaci na mobilním telefonu.
  - **Detekcí pohybu** – autentizace bude spuštěna detekcí pohybu za přítomnosti telefonu se spárovanou **2N Mobile Key** aplikací.

Varování

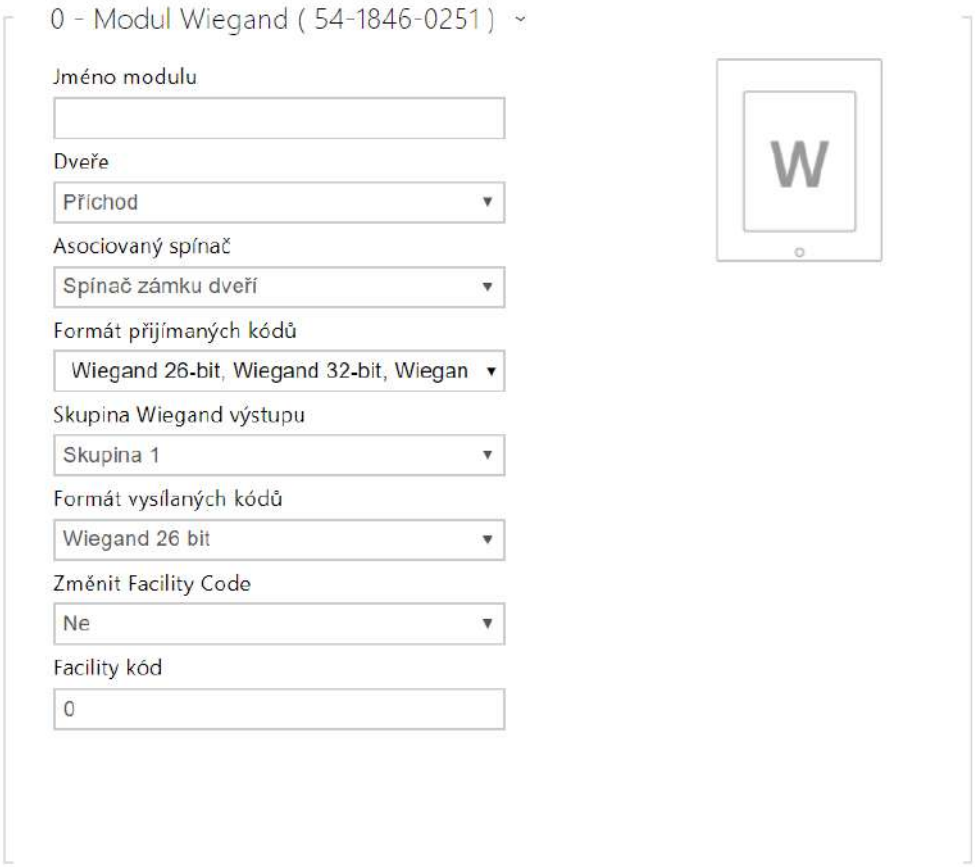
- S upgradem na verzi 2.30 dojde k upgradu i v bluetooth modulech. Při downgradu na verzi 2.29 a nižší může dojít k jejich nefunkčnosti.

Konfigurace modulu vstupů a výstupů I/O

- **Název modulu** – nastavuje název modulu. Název modulu se používá při specifikaci vstupu nebo výstupu v objektech SetOutput, GetInput a InputChanged v nastavení **2N Automation**.

Konfigurace modulu Wiegand

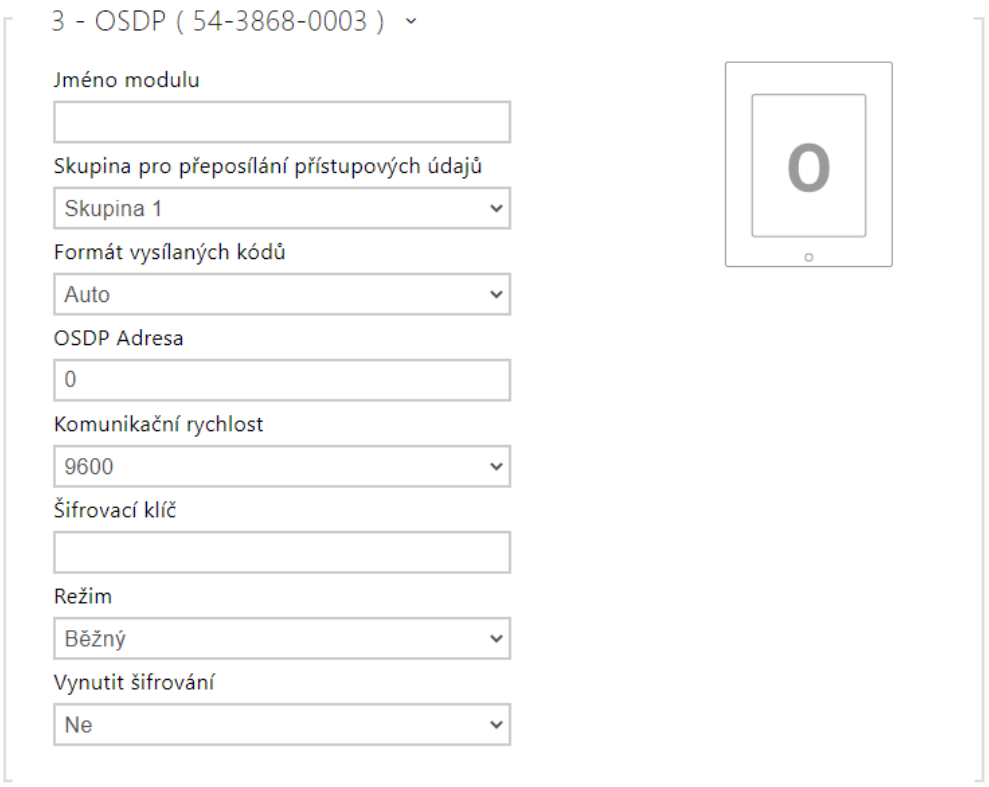
Modul Wiegand je vybaven vstupním a výstupním Wiegand rozhraním, které jsou na sobě nezávislé, mají nezávislé nastavení a mohou přijímat a vysílat kódy současně. Vstupní Wiegand rozhraní lze použít pro připojení externích zařízení, jako jsou čtečky RFID karet, biometrické čtečky apod. Pomocí výstupního Wiegand rozhraní lze zařízení 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 **2N Automation**.



- **Název modulu** – nastavuje název modulu. Název modulu se používá při specifikaci vstupu nebo výstupu v objektech SetOutput, GetInput a InputChanged v nastavení **2N 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 OSDP

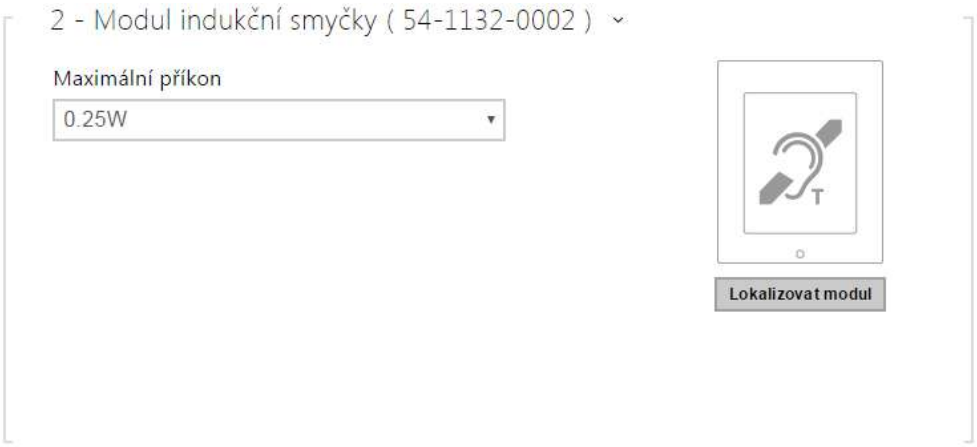


- **Název modulu** – nastavuje název modulu. Název modulu se používá při specifikaci vstupu nebo výstupu v nastavení **Automation**.
- **Skupina pro přeposílání přístupových údajů** – přiřazuje OSDP výstupu do skupiny, na kterou mohou být přeposílány kódy z připojených čteček karet, příp. OSDP vstupů.
- **Formát vysílaných kódů** – nastavuje formát vysílaných kódů.
- **OSDP Adresa** – adresa OSDP modulu v rozmezí 0–126 na OSDP lince.
- **Komunikační rychlost** – nastavení komunikační rychlosti v souladu s připojeným zařízením.
- **Šifrovací klíč** – vlastní klíč pro šifrovanou komunikaci.
- **Režim** – pro vzdálené nastavení šifrovacího klíče na periferii, pokud je to umožněno, je možné využít instalační režim. Po přijetí šifrovacího klíče dojde k automatickému

přepnutí do běžného režimu. Instalační režim je signalizován rychlým blikáním signalizační LED na OSDP modulu.
- **Vynutit šifrování** – nastavení vynuceného šifrování pouze pro šifrovanou komunikaci.

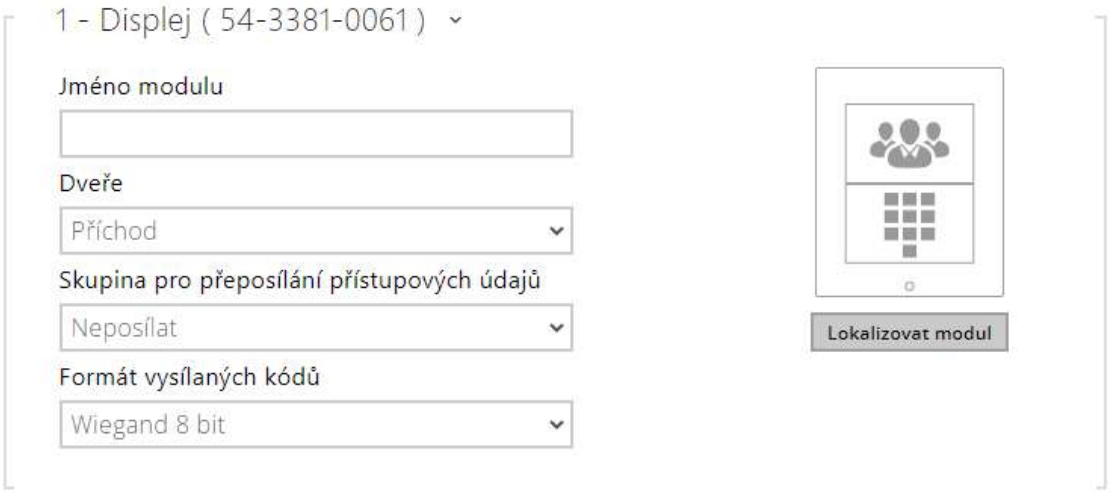
> **Upozornění**
>
> - Pokud dojde po nastavení vynuceného šifrování ke komunikaci ze strany zařízení OSDP v nešifrované formě, bude tato komunikace odmítnuta.

Konfigurace modulu indukční smyčky (není kompatibilní s 2N Access Unit QR)



- **Název modulu** – nastavuje název modulu. Název modulu se používá při logování událostí indukční smyčky.
- **Maximální příkon** – nastavuje maximální vysílací výkon antény indukční smyčky. Vyšší vysílací výkon znamená vyšší dosah, avšak méně výkonu pro ostatní funkce zařízení. Za běžných okolností by měla být vyhovující výchozí hodnota 0,25 W.

Konfigurace modulu displeje



- **Název 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.
- **Skupina pro přeposílání přístupových údajů** – nastavuje skupinu, na kterou budou přeposílány všechny zadané přístupové kódy.
- **Formát vysílaných kódů** – 4bit nebo 8bit (vyšší bezpečnost) formát vysílaných kódů.

Upozornění

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

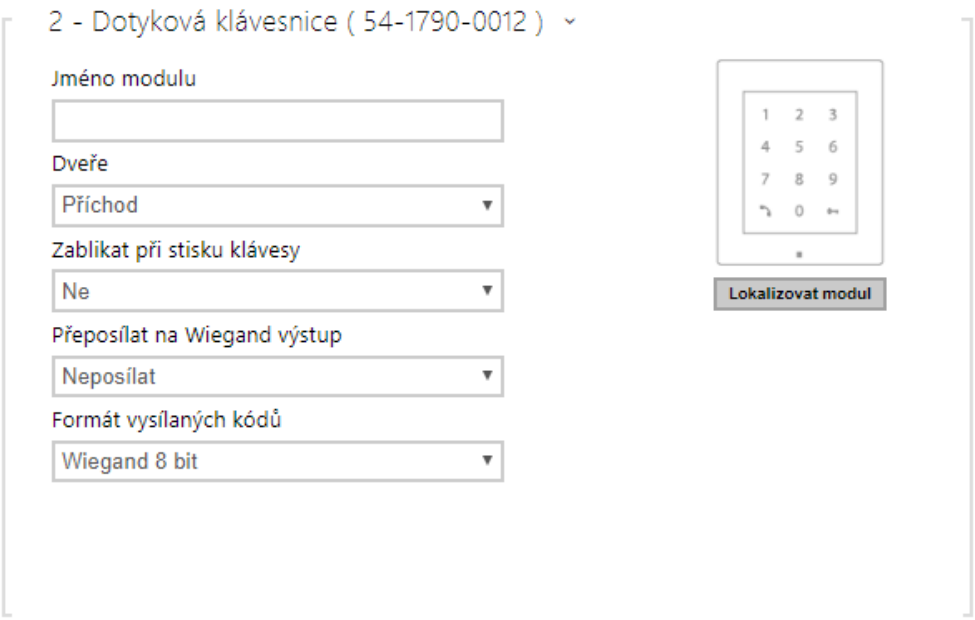
Konfigurace modulu čtečky otisků prstů

- **Název 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.
- **Režim citlivosti na sluneční světlo** – povolením se předchází chybovému chování čtečky, která je vystavena přímému slunečnímu záření. Pro změnu nastavení je nutné zařízení restartovat. Režim může způsobit sníženou citlivost čtení.

Poznámka

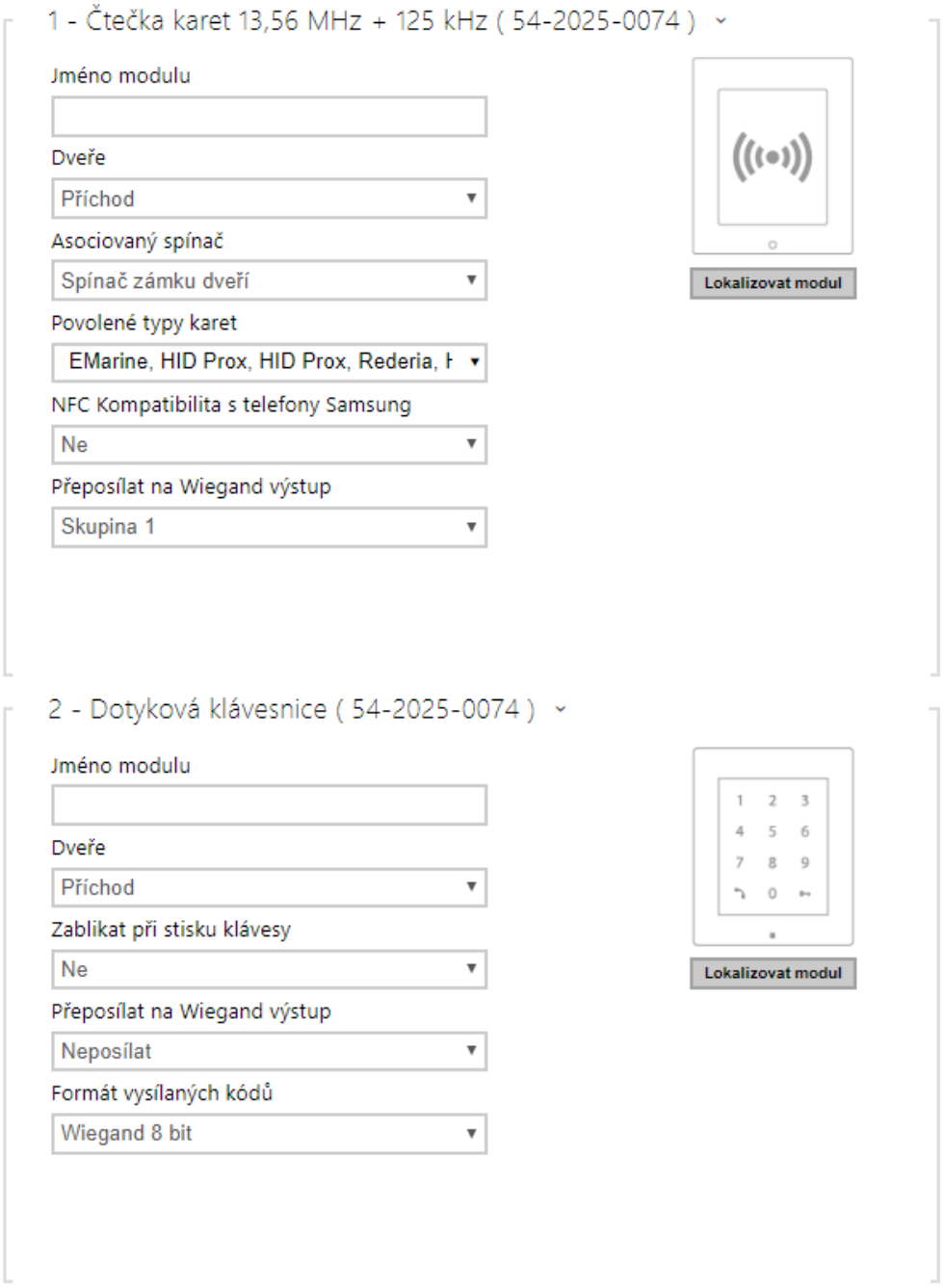
- Při odpojení modulu čtečky otisků prstů bude po restartu zařízení v profilu uživatele skryta část Uživatelské otisky prstů, která zobrazuje, kolik otisků má uživatel nahraných v paměti zařízení. Po opětovném připojení jakéhokoliv modulu čtečky otisků prstů se část konfigurace uživatele opět zobrazí.

Konfigurace modulu dotykové klávesnice



- **Název 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.
- **Blikat 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)

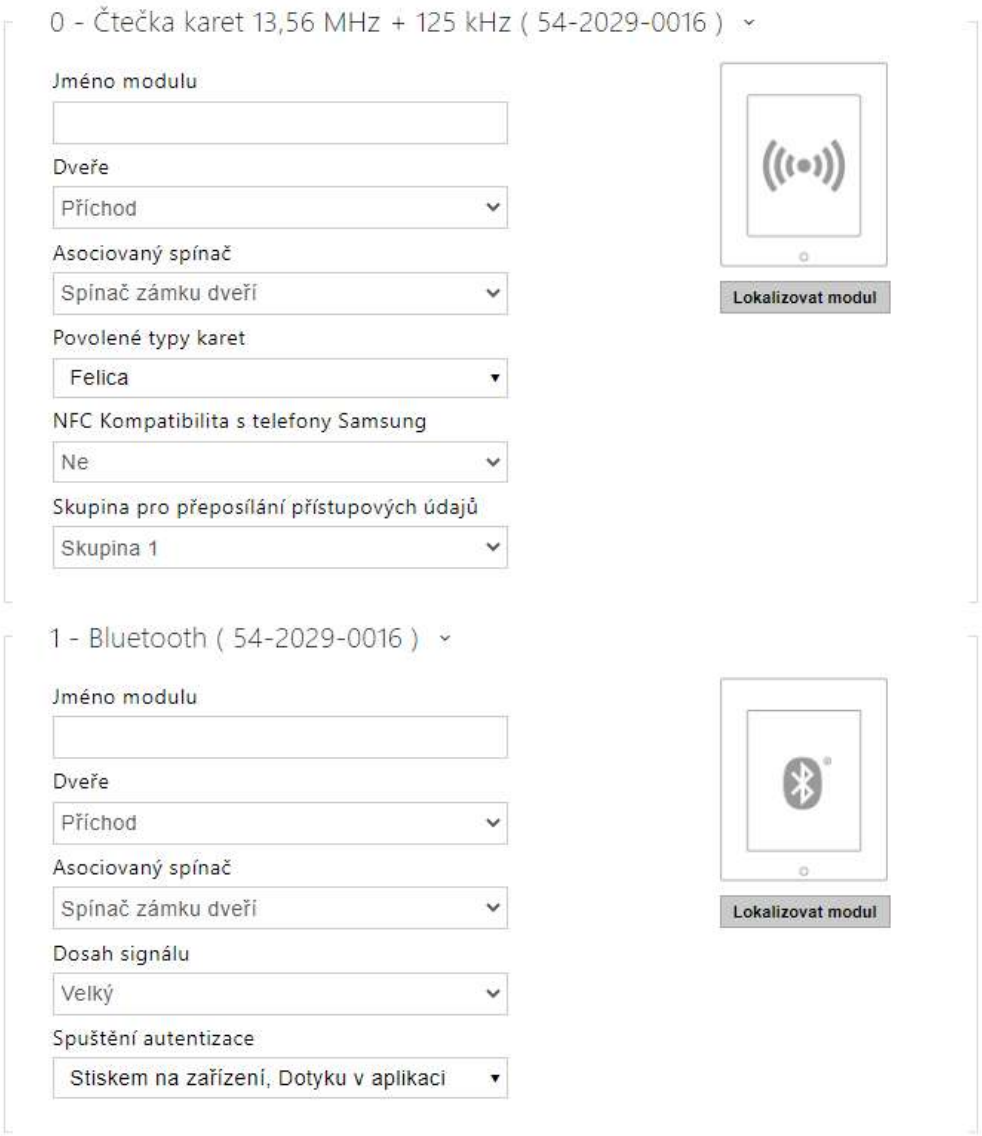
- **Název modulu** – nastavuje název modulu. Název modulu se používá při logování událostí z modulu čtečky karet.
- **Dveře** – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směr je využíván docházkovým systémem.

- **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)

- **Název 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.
- **Blikat 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, 13.56MHz, NFC



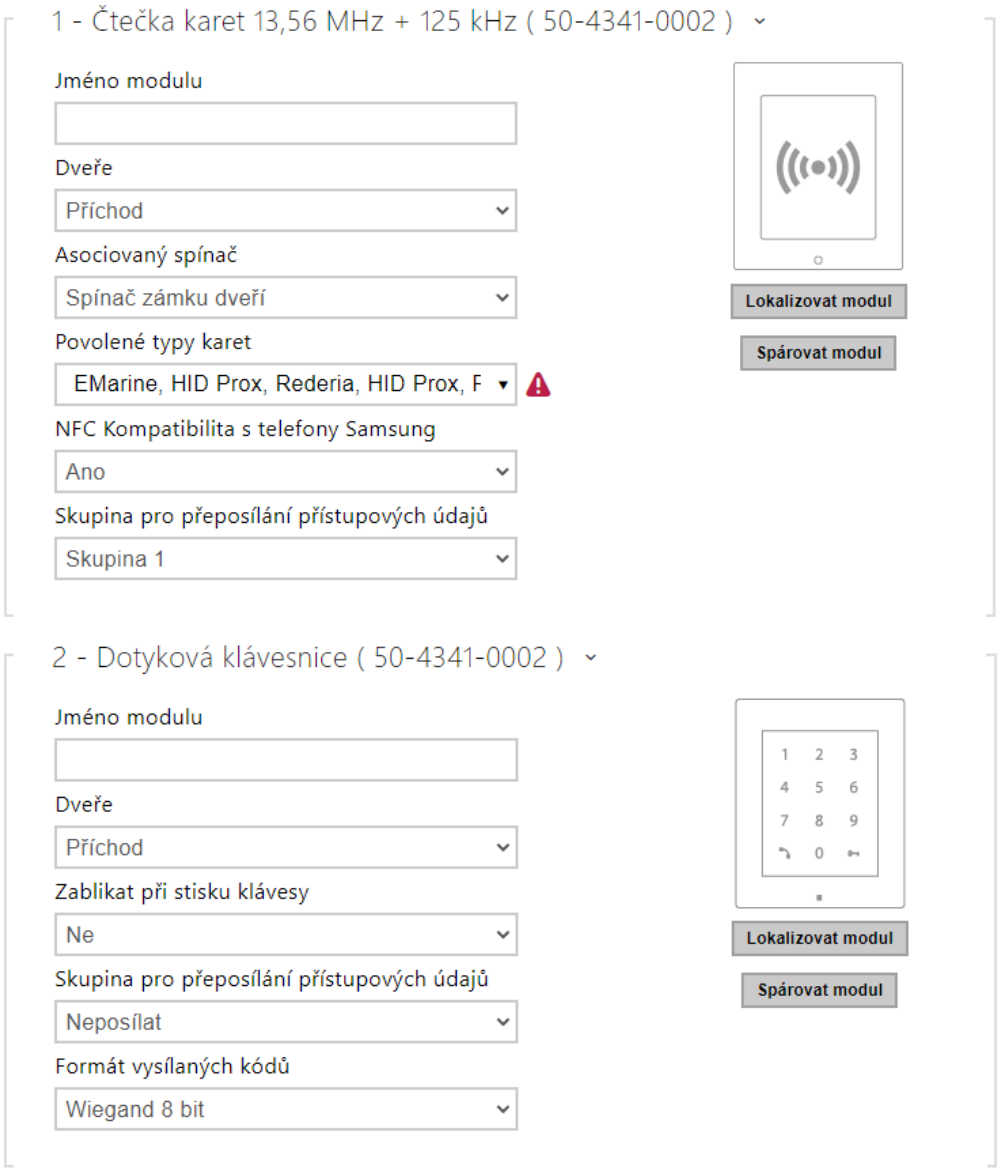
Čtečka karet 13,56 MHz (125 kHz)

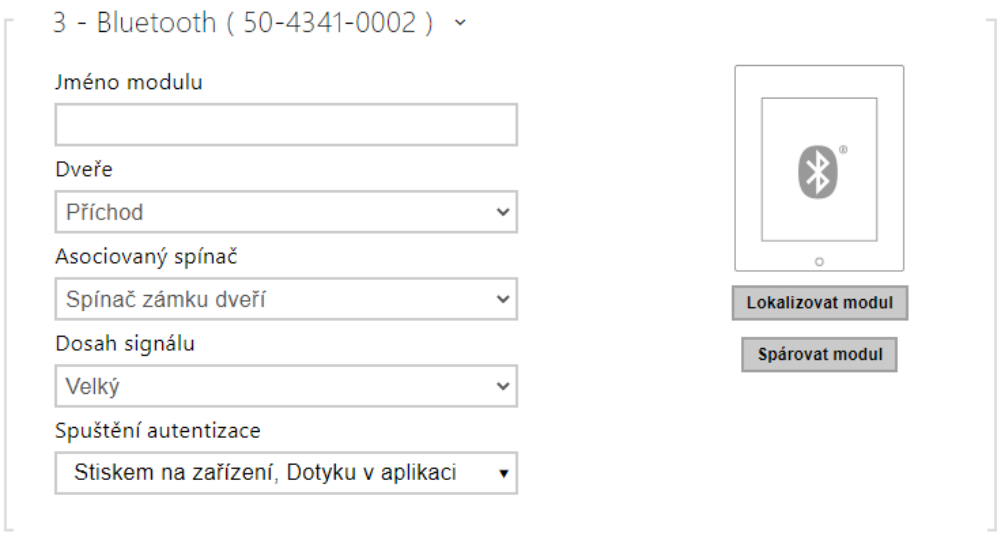
- **Název modulu** – nastavuje název modulu. Název modulu se používá při logování událostí z modulu čtečky karet.
- **Dveře** – nastavuje směr průchodu při použití čtečky (Příchod, Odchod). Parametr směr je využíván docházkovým systémem.
- **Asociovaný spínač** – nastavuje číslo spínače aktivovaného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

- **Název 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 2 m.
  - **Velký** – dosah je maximálně možný.
- **Spustit autentizaci** – nastavuje způsob autentizace pomocí mobilního telefonu:
  - **Na zařízení** – autentizaci je nutné potvrdit dotykem na čtečce za přítomnosti telefonu se spárovanou **2N Mobile Key** aplikací.
  - **V aplikaci** – autentizaci je nutné potvrdit klepnutím na ikonu ve spuštěné aplikaci na mobilním telefonu.
  - **Detekcí pohybu** – autentizace bude spuštěna detekcí pohybu za přítomnosti telefonu se spárovanou **2N Mobile Key** aplikací.

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





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

- **Název 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 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.
- **Skupina pro přeposílání přístupových údajů** – umožňuje nastavit skupinu, na kterou budou přeposílány všechny přijaté přístupové kódy uživatelů.

Dotyková klávesnice (sériové číslo)

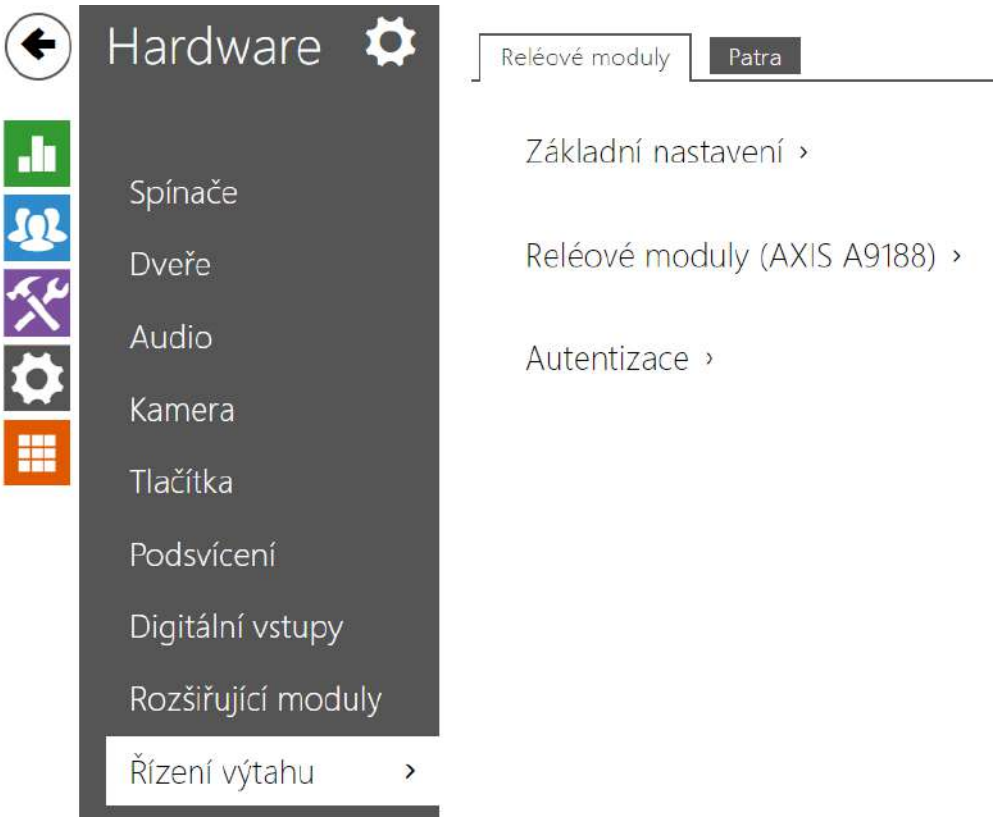
- **Název modulu** – nastavuje název modulu. Název modulu se používá při logování událostí z modulu dotykové klávesnice.
- **Dveře** – nastavuje směr průchodu při použití čtečky (Příchod / Odchod). Parametr směru je využíván docházkovým systémem.
- **Blikat při stisku klávesy** – nastavuje světelnou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

Bluetooth

- **Název 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 2 m.
  - **Velký** – dosah je maximálně možný.
- **Spustit autentizaci** – nastavuje způsob autentizace pomocí mobilního telefonu. Jednu, kombinaci dvou nebo všech tří.
  - **Na zařízení** – autentizaci je nutné potvrdit dotykem na čtečce za přítomnosti telefonu se spárovanou **2N Mobile Key** aplikací.
  - **V aplikaci** – autentizaci je nutné potvrdit klepnutím na ikonu ve spuštěné aplikaci na mobilním telefonu.
  - **Detekcí pohybu** – autentizace bude spuštěna detekcí pohybu za přítomnosti telefonu se spárovanou **2N Mobile Key** aplikací.

5.3.9 Řízení výtahu



Pomocí připojení reléového modulu AXIS A9188 k zařízení lze řídit přístup na jednotlivá patra v budově za použití výtahu. K jednomu zařízení je možné připojit max. 5 těchto reléových modulů, přičemž každý z modulů může ovládat 8 pater, dohromady tedy max. 64 pater.

Záložka Reléové moduly

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

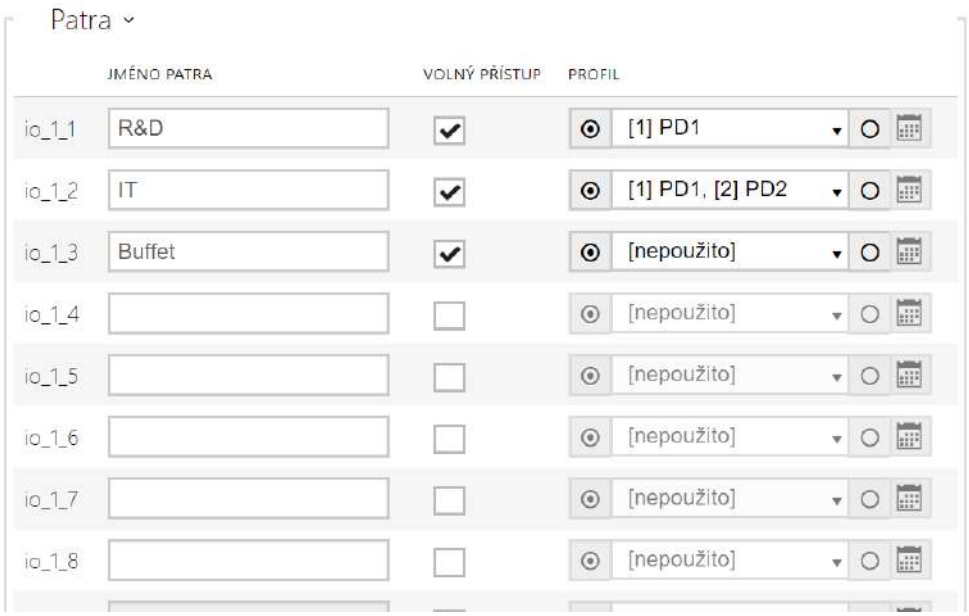
- **Zapnuto** – slouží k aktivaci a deaktivaci modulu AXIS A9188, který slouží ke kontrole řízení výtahu až na 8 patrech.
- **IP Adresa** – IP adresa AXIS A9188.
- **Stav** – zobrazuje stav připojeného modulu AXIS A9188 (Chyba/Přístup odepřen/ Připraveno/Zastaveno).
- **Sériové číslo** – sériové číslo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

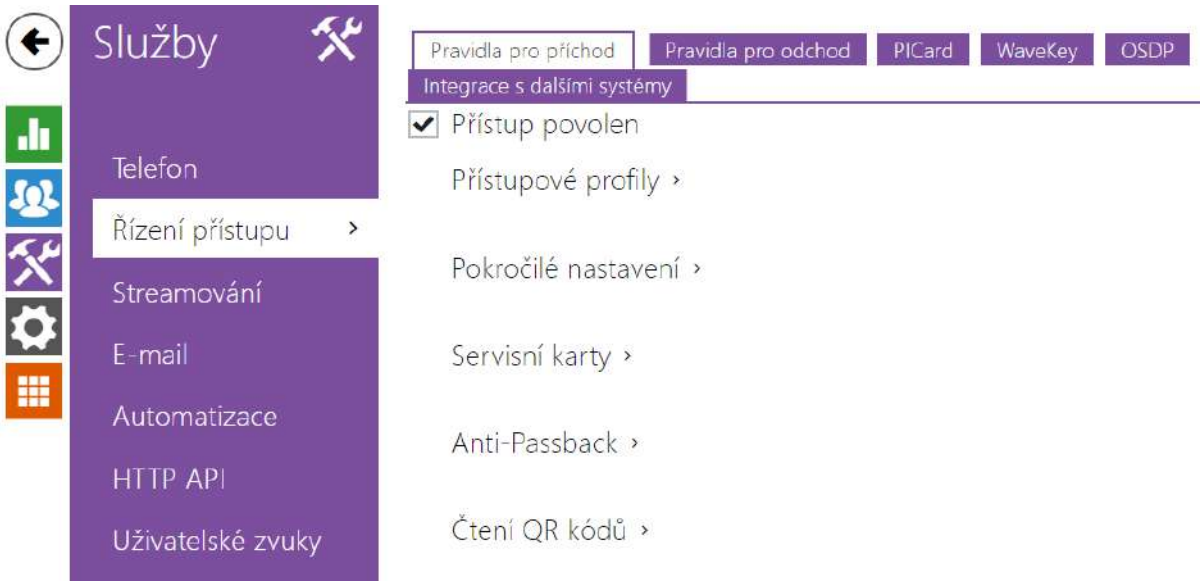
1. Vyhledejte reléový modul AXIS A9188 v lokální síti pomocí AXIS IP Utility.
2. Zadejte přihlašovací údaje root/root.
3. V menu vyberte **Preferences > Additional device configuration**.
4. Zobrazí se nové okno s konfigurací zařízení.
5. V menu vyberte **System Options > Security > Certificates**.
6. 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 zařízení, 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:

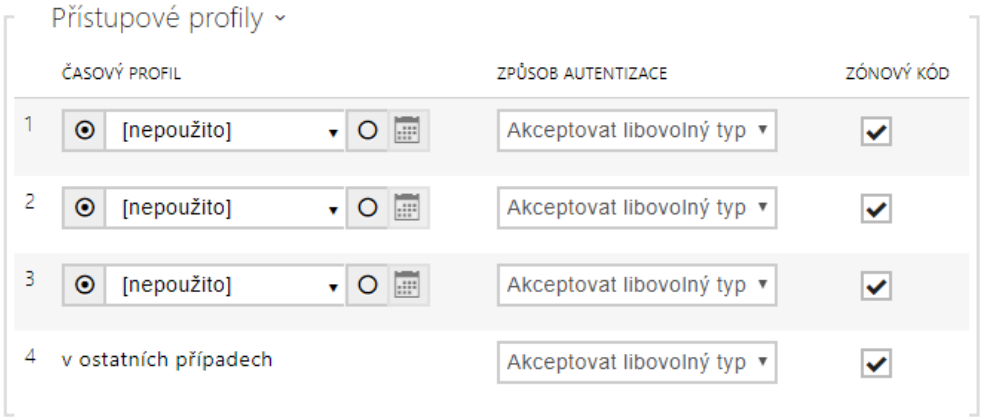
5.4.1 Řízení přístupu

Služba Řízení přístupu slouží pro správu přístupů a způsob ověřování autentizace uživatele.



Záložka Pravidla pro příchod

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

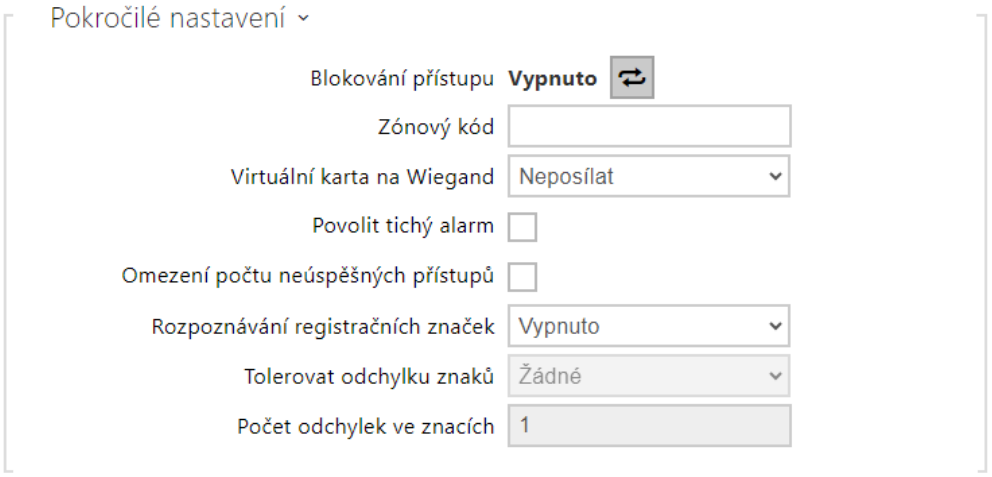


- **Časový profil** – nabízí výběr jednoho či více časových profilů zároveň, které se uplatní. Samotné nastavení časových profilů je možné v sekci Adresář > Časové profily.
  -  označením se volí globální profily z Adresář > Časové profily.
  -  označením se volí individuální časový profil jen pro tento prvek.

- **Způsob autentizace** – nastavuje způsob autentizace (Bluetooth, otisk prstu, přístupová karta, numerický kód nebo QR 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.



- **Blokování přístupu** – zobrazuje aktuální nastavení blokování přístupu. Odemknuto/ Uzamknuto.
- **Zónový kód** – umožňuje zadat numerický kód spínače. Kód musí obsahovat alespoň dva znaky, ale doporučujeme použít nejméně čtyři znaky.
- **Virtuální karta 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.

Upozornění

- V případě, že uživatel použije autentizaci pro spuštění tichého alarmu a tichý alarm není povolen, bude jeho přístup zamítnut a alarm nebude aktivován.

- **Omezení počtu neúspěšných přístupů** – povoluje omezení počtu neúspěšných pokusů o autentizaci. Po pěti neúspěšných pokusech o přístup (nesprávný numerický kód, neplatná karta atd.) bude přístupová jednotka 2N zablokována po dobu třiceti sekund i v případě, že autentizace by byla platná.
- **Rozpoznávání registračních značek** – volí scénář po rozpoznání registrační značky vozidla.

Upozornění

- Pro korektní funkci je vhodné, aby byla každá registrační značka přiřazena právě jednomu záznamu v adresáři. Při vícenásobně zadaných registračních značkách dochází k tomu, že není možné jednoznačně přiřadit záznam v adresáři, který má registrační značku nakonfigurovanou (je vybrán první záznam, který má danou registrační značku nakonfigurovanou, a jeho přístupová pravidla se uplatní).

  - **Vypnuto**
  - **Otevření značkou** – k otevření dveří dojde, pokud má uživatel s načtenou registrační značkou aktuálně právo příchodu či odchodu. Otevírání dveří (respektive závory apod.) po detekci platné registrační značky **funguje nezávisle** na ostatních Způsobech autentizace, které jsou nastaveny v Přístupových profilech.
  - **Multifaktor se značkou** – tato možnost je dostupná pouze při aktivování beta funkce Vícefaktorové ověřování registračních značek. Zapne trvalé blokování přístupu a trvale vypne způsob autentizace pomocí Bluetooth (WaveKey). Po načtení registrační značky bude uživateli s načtenou registrační značkou udělena dočasná výjimka s trváním 60 sekund a současně se na tuto dobu aktivuje funkce WaveKey. Přístup bude udělen pouze uživateli s načtenou registrační značkou, který se do 60 sekund autentizuje dalším způsobem autentizace (WaveKey/QR kód). Uživatelům s trvalou výjimkou je umožněn přístup po celou dobu trvalého blokování přístupu, ale pouze v čase 60 sekund od zaznamenání registrační značky se mohou autentizovat také pomocí WaveKey.
    Každá další přijatá registrační značka vozidla zruší předchozí dočasnou výjimku, a pokud existuje uživatel s nově přijatou registrační značkou, je přidělena dočasná výjimka tomuto uživateli.
- **Tolerovat odchylku znaků** – volí, zda je tolerována odchylka v rozpoznané registrační značce vozidla. Je možné si vybrat mezi nulovou tolerancí, tolerancí od začátku, tolerancí od konce nebo tolerancí jak od začátku, tak od konce. Při volbě tolerance znaků z obou stran je při načítání poznávací značky prvně tolerována odchylka znaků od začátku, a pokud nedojde k rozpoznání značky, tak při dalším načtení je tolerována odchylka od konce.

- **Počet odchylek ve znacích** – volí, zda je tolerována odchylka jednoho nebo dvou znaků. Odchylka znaků se týká začátku a/nebo konce dle nastavení parametru **Tolerovat odchylku znaků**. Při prvním načtení poznávací značky zařízení netoleruje žádnou odchylku. Pouze pokud nerozpozná poznávací značku uloženou v adresáři, bude při dalším načítání tolerovat odchylku v jednom znaku ve směrech nastavených výše. Pokud ani tak zařízení poznávací značku z adresáře neidentifikuje, bude zařízení při dalším načítání tolerovat odchylku ve dvou znacích.

Zařízení umožňuje využít rozpoznané registrační značky vozidel zaslané v HTTP požadavku kamerami od firmy AXIS vybavené doplňkovou aplikací VaxALPR na api/lpr/licenseplate (viz HTTP API manuál pro IP interkomy).

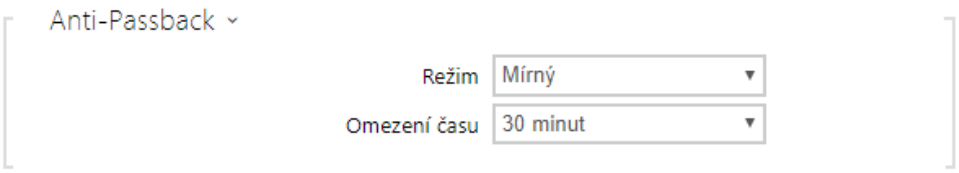
V případě, že je funkce zapnuta, dojde po přijetí platného HTTP požadavku k zaznamenání události do historie pod událostí LicensePlateRecognized. Pokud je v rámci HTTP požadavku zaslán i obrázek (např. výřez fotografie nebo celá fotografie scény při detekci registrační značky), uloží se. V paměti zařízení je uloženo pět posledních fotografií, které je možné ze zařízení vyčíst pomocí HTTP požadavku zaslaného na api/lpr/image a které jsou k dispozici v systému **2N Access Commander**.

Varování

- Softwarovým obnovením továrního nastavení nebo nahráním odlišné konfigurace nedojde ke změně nastavení blokování přístupu. Pouze hardwarové obnovení továrního nastavení pomocí tlačítka Reset na zařízení uvede parametr do výchozího nastavení.
  - Security relé zvyšuje zabezpečení instalace proti zneužití pomocí hardwarového resetu.

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.

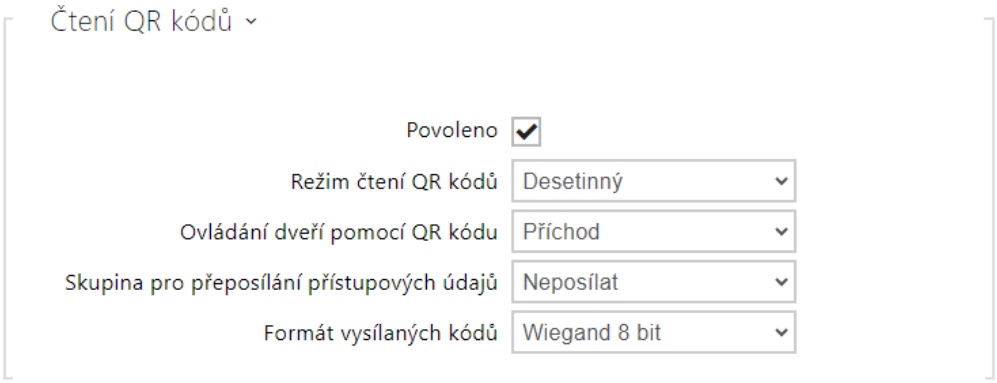
- **ID přidávací karty** – ID servisní karty určené pro přidávání do seznamu instalovaných karet. ID karty je sekvence 6–32 znaků z množiny 0–9, A–F.
- **ID odebírací karty** – ID servisní karty určené pro odebírání ze seznamu instalovaných karet. ID karty je sekvence 6–32 znaků z množiny 0–9, A–F.



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 **UserAuthenticated** s parametrem *apbBroken=**true***.

  - **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** s parametrem *apbBroken=**true***.
- **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.



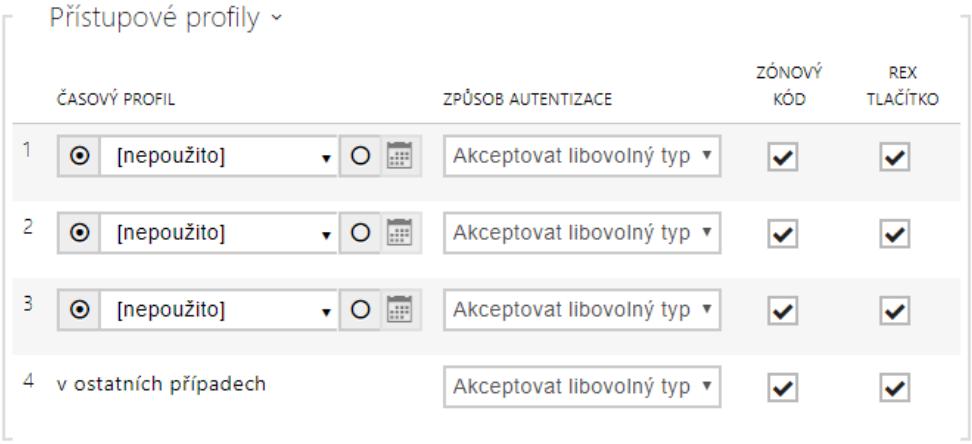
- **Povoleno** – zapíná/vypíná čtení QR kódů pomocí kamery zařízení. V případě, že je čtení QR kódů zapnuto, je možné zadávat PIN kódy a individuální kódy spínačů, které jsou del ší než deset číslic, pomocí ukázání QR kódu na kameru zařízení.
- **Režim čtení QR kódů** – V zařízení jsou vždy uložené desetinné kódy. V Desetinném režimu musí přečtené kódy odpovídat kódům (o délce 4 až 15 číslic) uloženým v zařízení. V Hexadecimálním režimu jsou kódy po přečtení převedeny na desetinné a porovnány s uloženými desetinnými kódy. Předřazené nuly jsou ignorovány. Akceptovaný hexadecimální rozsah: 1000 až FFFFFFFF.
- **Ovládání dveří pomocí QR kódu** – Povoluje nebo zakazuje ovládání dveří načtením QR kódu.
- **Skupina pro přeposílání přístupových údajů** – nastavuje skupinu, na kterou budou přeposílány všechny zadané přístupové kódy.
- **Formát vysílaných kódů** – 4bit nebo 8bit (vyšší bezpečnost) formát vysílaných kódů.

Upozornění

- Pro správnou činnost čtení QR kódů nepoužívejte současně funkci ochrany soukromí.
- Pro zvýšenou bezpečnost omezte počet neúspěšných přístupů v bloku Pokročilé nastavení výše.
- Funkce čtení QR kódů je dostupná pouze na modelech s procesorem ARTPEC-7 společnosti Axis.

Záložka Pravidla pro odchod

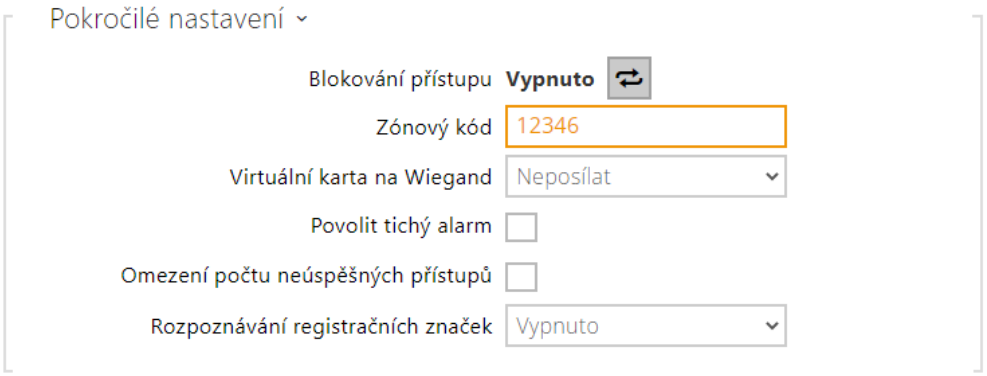
- **Přístup povolen** – povoluje jakýkoliv přístup z konkrétní strany dveří (příchod, odchod). Pokud není přístup povolen, není možno dveře z této strany otevřít.



- **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.



- **Blokování přístupu** – zobrazuje aktuální nastavení blokování přístupu. Odemknuto/ Uzamknuto.
- **Zónový kód** – umožňuje zadat numerický kód spínače. Kód musí obsahovat alespoň dva znaky, ale doporučujeme použít nejméně čtyři znaky.
- **Virtuální karta 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.

Upozornění

- V případě, že uživatel použije autentizaci pro spuštění tichého alarmu a tichý alarm není povolen, bude jeho přístup zamítnut a alarm nebude aktivován.

- **Omezení počtu neúspěšných přístupů** – povoluje omezení počtu neúspěšných pokusů o autentizaci. Po pěti neúspěšných pokusech o přístup (nesprávný numerický kód, neplatná karta atd.) bude přístupová jednotka 2N zablokována po dobu třiceti sekund i v případě, že by autentizace byla platná.
- **Rozpoznávání registračních značek** – volí scénář po rozpoznání registrační značky vozidla.

Upozornění

- Pro korektní funkci je vhodné, aby byla každá registrační značka přiřazena právě jednomu záznamu v adresáři. Při vícenásobně zadaných registračních značkách dochází k tomu, že není možné jednoznačně přiřadit záznam v adresáři, který má registrační značku nakonfigurovanou (je vybrán první záznam, který má danou registrační značku nakonfigurovanou, a jeho přístupová pravidla se uplatní).

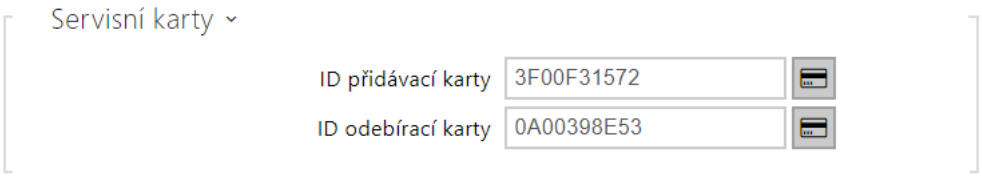
  - **Vypnuto**
  - **Otevření značkou** – k otevření dveří dojde, pokud má uživatel s načtenou registrační značkou aktuálně právo příchodu či odchodu. Otevírání dveří (respektive závory apod.) po detekci platné registrační značky **funguje nezávisle** na ostatních Způsobech autentizace, které jsou nastaveny v Přístupových profilech.
  - **Multifaktor se značkou** – tato možnost je dostupná pouze při aktivování beta funkce Vícefaktorové ověřování registračních značek. Zapne trvalé blokování přístupu a trvale vypne způsob autentizace pomocí Bluetooth (WaveKey). Po načtení registrační značky bude uživateli s načtenou registrační značkou udělena dočasná výjimka s trváním 60 sekund a současně se na tuto dobu aktivuje funkce WaveKey. Přístup bude udělen pouze uživateli s načtenou registrační značkou, který se do 60 sekund autentizuje dalším způsobem autentizace (WaveKey/QR kód). Uživatelům s trvalou výjimkou je umožněn přístup po celou dobu trvalého blokování přístupu, ale pouze v čase 60 sekund od zaznamenání registrační značky se mohou autentizovat také pomocí WaveKey.
    Každá další přijatá registrační značka vozidla zruší předchozí dočasnou výjimku, a pokud existuje uživatel s nově přijatou registrační značkou, je přidělena dočasná výjimka tomuto uživateli.
- **Tolerovat odchylku znaků** – volí, zda je tolerována odchylka v rozpoznané registrační značce vozidla. Je možné si vybrat mezi nulovou tolerancí, tolerancí od začátku, tolerancí od konce nebo tolerancí jak od začátku, tak od konce. Při volbě tolerance znaků z obou stran je při načítání poznávací značky prvně tolerována odchylka znaků od začátku, a pokud nedojde k rozpoznání značky, tak při dalším načtení je tolerována odchylka od konce.
- **Počet odchylek ve znacích** – volí, zda je tolerována odchylka jednoho nebo dvou znaků. Odchylka znaků se týká začátku a/nebo konce dle nastavení parametru **Tolerovat odchylku znaků**. Při prvním načtení poznávací značky zařízení netoleruje žádnou odchylku. Pouze pokud nerozpozná poznávací značku uloženou v adresáři, bude při dalším načítání tolerovat odchylku v jednom znaku ve směrech nastavených výše. Pokud ani tak zařízení poznávací značku z adresáře neidentifikuje, bude zařízení při dalším načítání tolerovat odchylku ve dvou znacích.

Zařízení umožňuje využít rozpoznané registrační značky vozidel zaslané v HTTP požadavku kamerami od firmy AXIS vybavené doplňkovou aplikací VaxALPR na api/lpr/licenseplate (viz HTTP API manuál pro IP interkomy).

V případě, že je funkce zapnuta, dojde po přijetí platného HTTP požadavku k zaznamenání události do historie pod událostí LicensePlateRecognized. Pokud je v rámci HTTP požadavku zaslán i obrázek (např. výřez fotografie nebo celá fotografie scény při detekci registrační značky), uloží se. V paměti zařízení je uloženo pět posledních fotografií, které je možné ze zařízení vyčíst pomocí HTTP požadavku zaslaného na api/lpr/image a které jsou k dispozici v systému **2N Access Commander**.

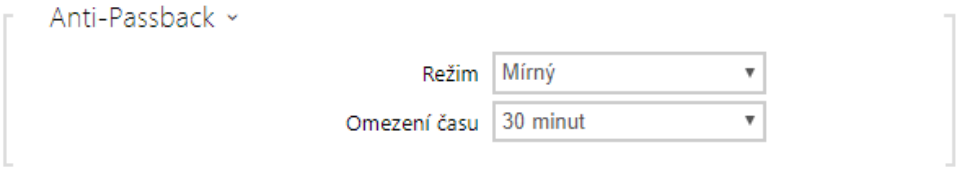
Varování

- Softwarovým obnovením továrního nastavení nebo nahráním odlišné konfigurace nedojde ke změně nastavení blokování přístupu. Pouze hardwarové obnovení továrního nastavení pomocí tlačítka Reset na zařízení uvede parametr do výchozího nastavení.
  - Bezpečnostní relé zvyšuje zabezpečení instalace proti zneužití pomocí hardwarového resetu.



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.

- **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 **UserAuthenticated** s parametrem *apbBroken=**true***.

  - **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** s parametrem *apbBroken=**true***.
- **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 PICard

Technologie **2N PICard** slouží k šifrování přihlašovacích údajů na přístupových kartách. Pro čtení přihlašovacích údajů potřebují zařízení 2N přístup k odpovídajícím klíčům, které generuje aplikace **2N PICard Commander**. Ty lze následně importovat do **2N Access Commanderu**, který zajistí distribuci do všech podporovaných zařízení 2N.

> **Upozornění**
>
> - Zařízení, na kterých lze číst karty s nahranou technologií PICard, jsou uvedena v Konfiguračním manuálu **2N PICard Commander**.

- **Název projektu** – název pro vytvořený šifrovací klíč.
- **Hash** – číselný identifikátor projektu.
- **Nahrát klíče PICard** – výběrem souboru s klíči a zadáním platného hesla bude nahrán klíč PICard.
- **Smazat** – smaže nahrané klíče PICard.

Záložka WaveKey

Zařízení 2N vybavená modulem Bluetooth umožňují autentizovat uživatele pomocí mobilní aplikace **2N Mobile Key** dostupné pro zařízení s operačními systémy iOS 12 a vyšší (telefony iPhone 4s a vyšší), příp. Android 6.0 Marshmallow a vyšší (telefony s podporou Bluetooth 4.0 Smart).

Identifikace uživatele (Auth ID)

Aplikace **2N Mobile Key** se na straně zařízení 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 zařízení 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 seznamu uživatelů zařízení. Auth ID lze přesunout k jinému uživateli, příp. zkopírovat do jiného zařízení. Po vymazání hodnoty pole dojde k blokování přístupu uživatele pomocí Mobile Key.

Šifrovací klíče a lokace

Komunikace mezi aplikací **2N Mobile Key** a zařízením je vždy šifrovaná. Bez znalosti šifrovacího klíče nemůže aplikace **2N Mobile Key** uživatele autentizovat. Primární šifrovací klíč je automaticky vygenerován při prvním spuštění zařízení 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 ze zařízení exportovat a následně importovat do dalších. 2N zařízení 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 zařízení 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 seznamu uživatelů zařízení na stránce příslušného uživatele. Párování lze fyzicky provést lokálně pomocí USB Bluetooth modulu připojeného k PC, příp. vzdáleně pomocí Bluetooth modulu integrovaného v zařízení. 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 zařízení a lze jej kdykoli přegenerovat.

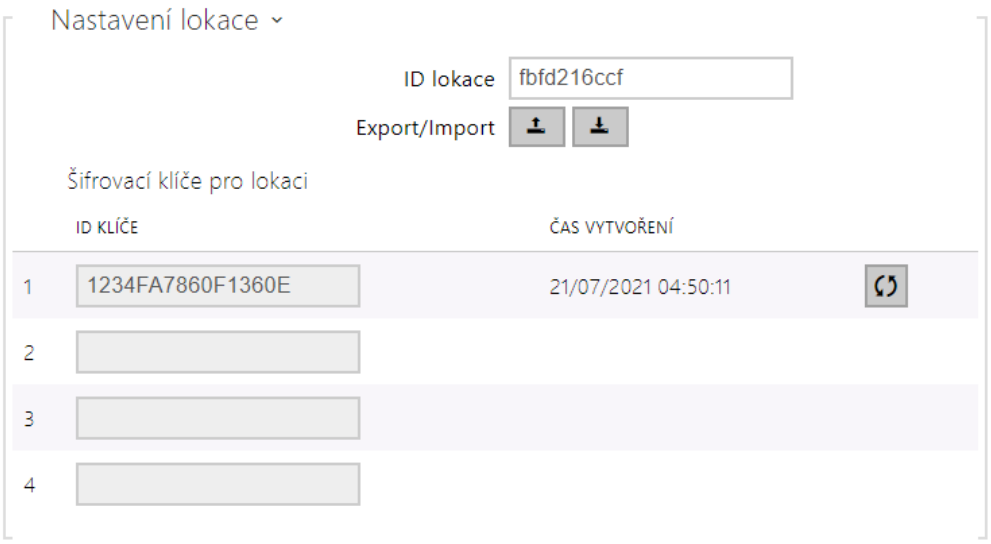
Správa šifrovacích klíčů

Zařízení 2N 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 zařízení 2N aktualizovat.

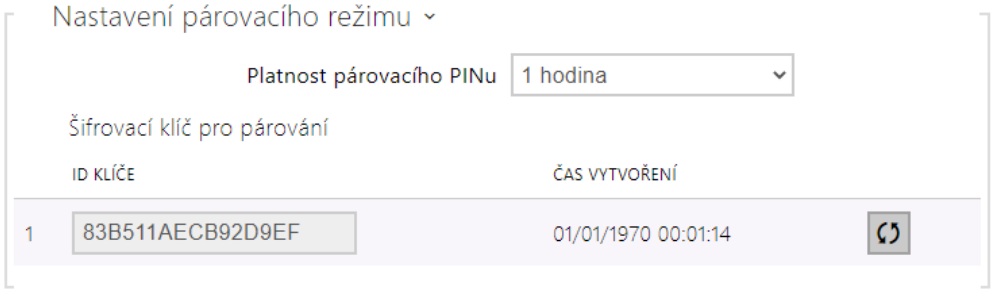
> **Poznámka**
>
> - Při prvním spuštění zařízení 2N jsou automaticky vygenerovány šifrovací klíče a jsou uloženy do konfiguračního souboru. Pro větší bezpečnost doporučujeme tyto šifrovací klíče před prvním použitím ručně znovu vygenerovat.

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**.



- **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.
- **Tlačítko Import** – importuje ID lokace a aktuální šifrovací klíče ze souboru exportovaného z jiného zařízení.
- **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 se zařízením.

Tip

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

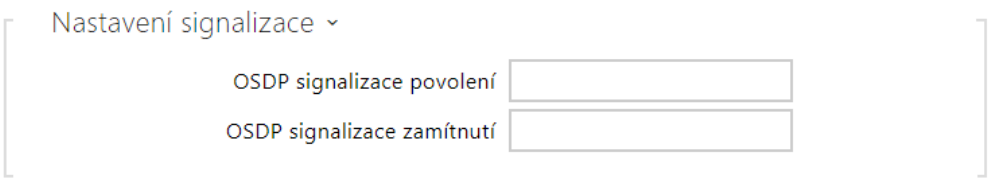
1. Vymažte hodnotu Mobile Key Auth ID příslušného uživatele – čímž dojde k blokování ztraceného telefonu a znemožnění jeho zneužití.
2. Přegenerujte primární šifrovací klíč (volitelný krok) – čímž znemožníte případné zneužití šifrovacího klíče uloženého v mobilním zařízení.

Varování

- S upgradem na verzi 2.30 dojde k upgradu v i Bluetooth modulech. Při downgradu na verzi 2.29 a nižší může dojít k jejich nefunkčnosti.

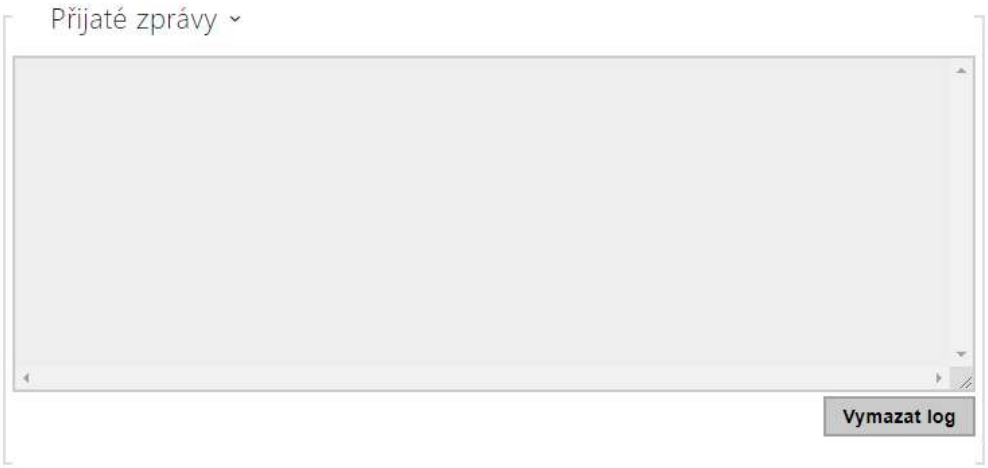
Záložka OSDP

OSDP protokol zajišťuje bezpečnou komunikaci pro zasílání přístupových údajů, jako je ID přístupové karty nebo PIN kódu mezi připojeným zařízením OSDP (control panelem, dveřním kontrolérem) a **zařízením 2N**. Cílem je umožnit aktivaci signalizace na zařízení na základě odpovědi z protistrany na zaslanou definici signalizace karty.



- **OSDP signalizace povolení** – definiční řetězec pro signalizaci povolení přístupu.
- **OSDP signalizace zamítnutí** – definiční řetězec pro signalizaci zamítnutí přístupu.

- V případě, že je do obou parametrů vložena stejná definice, dojde k vyhodnocení s audiovizuálními projevy, které budou odpovídat případu, jako by pro přístup těsně za sebou byl použit autorizovaný a neautorizovaný přístup.



Okno Přijaté zprávy slouží k získání definičního řetězce. Přiložením přístupové karty k zařízení je zobrazena definice signalizace OSDP zařízení protistrany pro autorizovaný nebo neautorizovaný přístup.
Přijatá zpráva se zobrazuje s časovým údajem ve formátu:

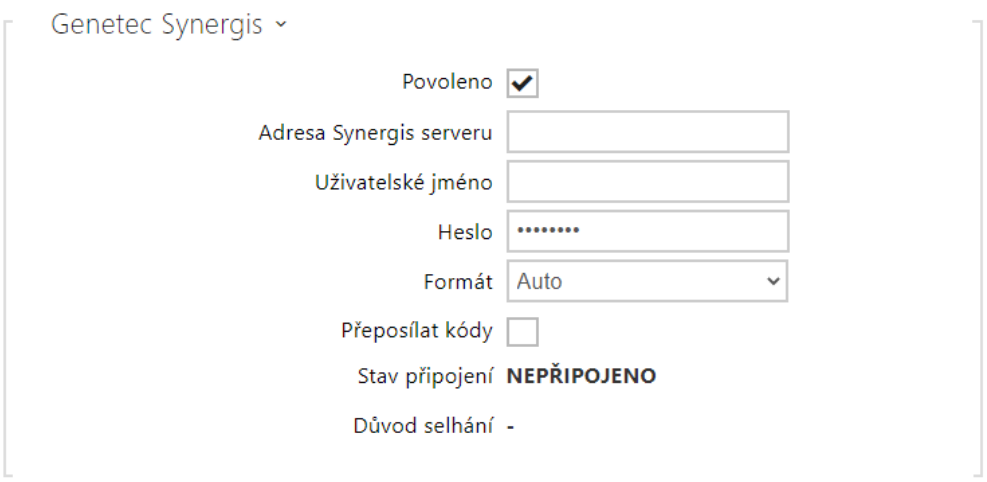
13:46:39] led(0,0,0,0,0,0,0,0,1,1,1,2,2)
13:46:39] buz(0,2,1,1,1)
13:46:42] led(0,0,0,0,0,0,0,0,1,1,1,1,1)
13:46:42] buz(0,1,0,0,0)

Jako definiční řetězec se použije část (bez časového údaje), přičemž jeho délka nesmí přesáhnout 255 znaků, např.: led(0,0,0,0,0,0,0,0,1,1,1,1,1) nebo buz(0,2,1,1,1). Při vyhodnocení shody na protistraně zařízení reaguje odpovídající signalizací. Libovolnou část definice je možné nahradit "*", tato část bude vyložena jako libovolný obsah zprávy (např. je tak možné dosáhnout toho, že signalizace bude aktivována na jakékoliv rozsvícení LED 0 na zařízení bez ohledu na ostatní parametry zprávy).

- **Vymazat log** – vymaže záznam přijaté zprávy.

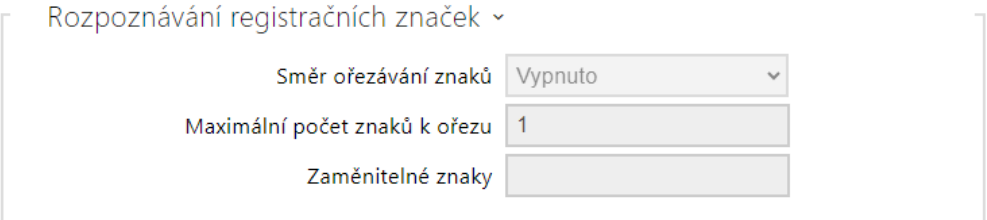
⚠
- Pro správné fungování je nutné mít v sekci **Hardware > Rozšiřující moduly** pro čtečku karet a klávesnici nastaven parametr Dveře/Nepoužito. Zařízení načtení karty potvrdí zvukovou signalizaci pípnutím, po vyhodnocení zařízení reaguje odpovídající signalizací.

Záložka Integrace s dalšími systémy



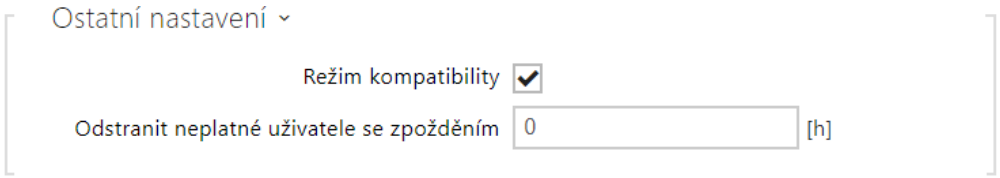
- **Povoleno** – povoluje spojení s externím bezpečnostním systémem Genetec Synergis.
- **Adresa Synergis serveru** – IP adresa nebo doménové jméno Synergis Serveru.
- **Uživatelské jméno** – uživatelské jméno používané při autentizaci.
- **Heslo** – heslo používané při autentizaci.
- **Formát** – nastavuje formát čtení karet pro zasílání ID karty do systému Genetec Synergis.
- **Přeposílat kódy** – nastavuje, zda se mají přeposílat zadané kódy. Kódy mohou mít maximálně 6 číslic a na konci je potřeba stisknout klávesu potvrzení.
- **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 Pokročilé



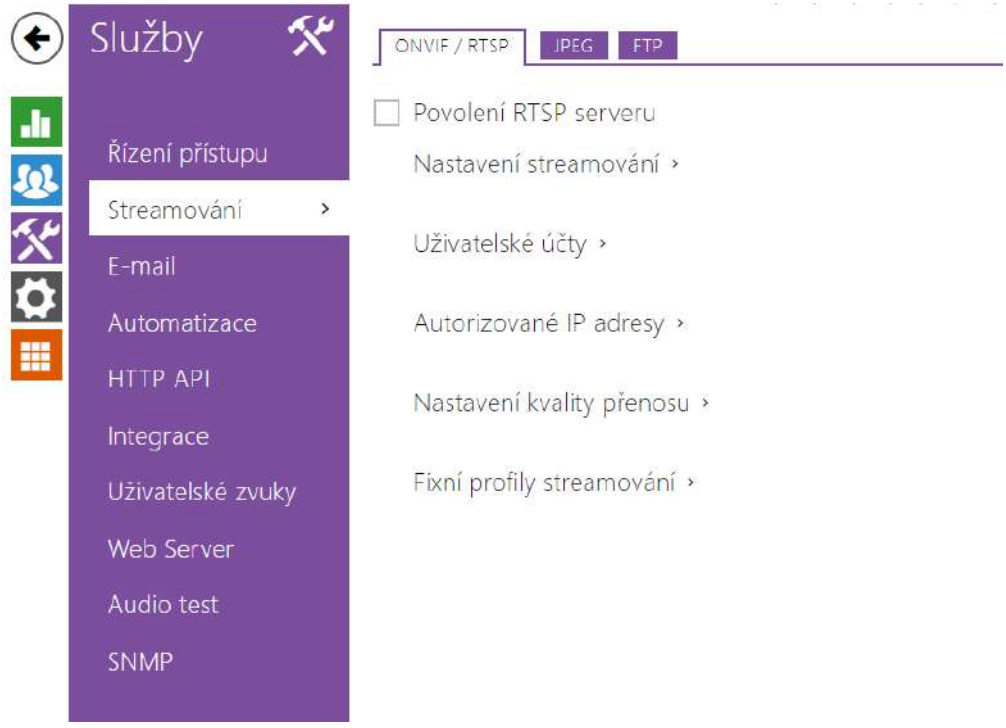
- **Směr ořezávání znaků** – volí, zda je povoleno ořezávání rozpoznaných registračních značek. Určete, z jakého směru může být ořezávání zkoušeno.
- **Maximální počet znaků k ořezu** – určuje maximální počet znaků k oříznutí – 1, nebo 2. Ořezávání znaků se provádí na začátku nebo na konci řetězce podle vybraného **Směru ořezávání znaků**.
- **Zaměnitelné znaky** – definuje vzájemně nahraditelné dvojice znaků pro účely funkce rozpoznávání registračních značek. První znak v páru bude nahrazen druhým znakem pro účely hledání shody s uloženými registračními značkami. Pomlčka odděluje znaky v páru.

Může být zadáno několik párů oddělených čárkou. Mezery jsou ignorovány. Např. O–0, I–1.



- **Režim kompatibility** – podpora starších režimů čtení karet. Nedoporučujeme používat v kombinaci s PICard kartami. Pokud je tento režim vypnut, musí se čísla karet pro úspěšnou autorizaci přesně shodovat.
- **Odstranit neplatné uživatele se zpožděním** – nastavuje zpoždění, po kterém jsou uživatelé s neplatným přístupem a povoleným automatickým odstraněním odstraněni z adresáře zařízení.

5.4.2 Streamování



2N Access Unit QR nabízí několik možností streamování audia a videa, viz následující tabulka:

Metoda přenosu	Popis
JPEG/HTTP	Stahování statických JPEG snímků. Viz záložka JPEG níže.

Metoda přenosu	Popis
MJPEG/HTTP	Série po sobě jdoucích JPEG snímků, metoda Server Push – multipart/x-mixed-replace. Viz záložka JPEG níže.
RTSP + RTP/UDP	RTSP se samostatnými audio a video streamy RTP/UDP. Podporováno pro audio (G.711) i video (H.264, H.263, MPEG-2 a MJPEG). Viz záložka RTSP níže.
RTP/RTSP	Tunelování RTP pomocí RTSP protokolu. Podporováno pro audio (G.711) i video (H.264, H.263, MPEG-2 a MJPEG). Viz záložka RTSP níže.
RTP/RTSP/HTTP	Tunelování RTSP protokolu pomocí HTTP. Podporováno pro audio (G.711) i video (H.264, H.263, MPEG-2 a MJPEG). Viz záložka RTSP níže.
RTP/UDP-Multicast	Neřízený multicast RTP paketů. Podporováno pouze pro audio (G.711). Viz záložka Multicast níže.

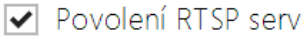
Vysvětlení pojmů

- **RTP (Real-Time Transport Protocol)** – protokol definující standardní formát paketů pro přenos audia a videa v IP sítích. Zařízení 2N využívají tento protokol pro přenos audio i video streamu. Transportním protokolem pro RTP bývá buď přímo UDP protokol, může jím však být i RTSP příp. HTTP protokol.
- **RTSP (Real-Time Streaming Protocol)** – síťový protokol pro řízení streamovacích serverů (řídí sestavování, spouštění a zastavování audio a video streamu).
- **HTTP (Hypertext Transfer Protocol)** – protokol umožňující přenášet prakticky libovolný obsah, používaný především internetovými prohlížeči pro komunikaci s web servery. Zařízení 2N umožňují pomocí protokolu HTTP přenášet statické JPEG snímky, příp. MJPEG stream způsobem nazývaným HTTP Server Push.
- **IP Multicast** – způsob odesílání paketů v IP sítích z jednoho zdroje na více stanic současně. Zařízení 2N využívají IP multicast pro vysílání a příjem audio streamu.
- **ONVIF (Open Network Video Interface Forum)** – sada specifikací pro vyhledávání, konfiguraci a správu videokamer v IP síti. Zařízení 2N jsou ONVIF kompatibilní zařízení a plně implementují tzv. ONVIF Profile T a Profile S.
- **JPEG** – standardní metoda ztrátové komprese obrazu.
- **MJPEG** – formát kódování video streamu, kde každý snímek je komprimován zvlášť pomocí metody JPEG. MJPEG kódování produkuje video vysoké kvality za cenu výrazně vyšší přenosové rychlosti oproti metodám uvedeným níže.

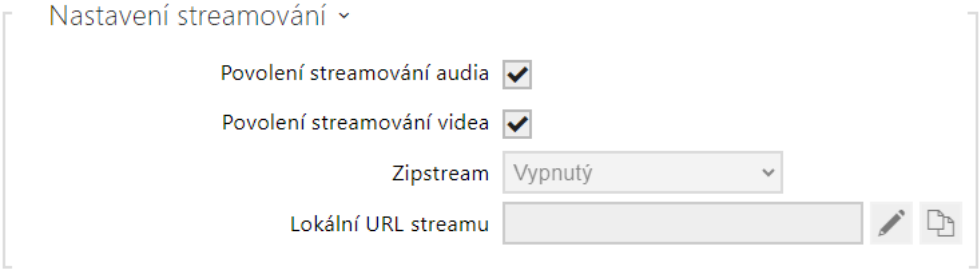
- **H.263** – standard pro kompresi video streamu používaný v telekomunikacích. Na rozdíl od metody MJPEG využívá rozdílové informace mezi po sobě jdoucími snímky a poskytuje výrazně vyšší stupeň komprese na úkor kvality video streamu.
- **H.263+** – jako H.263, pouze jiný způsob paketizace bitstreamu.
- **MPEG-4 part 2** – standard pro kompresi video streamu používaný spíše mimo oblast telekomunikací, ale velmi často podporovaný IP kamerami a video surveillance systémy. V případě **zařízení 2N** jsou stupeň komprese a kvalita obrazu srovnatelné se standardem H.263.
- **H.264** – standard pro kompresi video streamu. Na rozdíl od metod H.263 produkuje MPEG-4 přibližně stejně kvalitní video stream při poloviční přenosové rychlosti. Tento způsob komprese je někdy také nazýván MPEG-4 part 10.
- **G.711** – jeden z nejběžnějších standardů pro přenos audia v telekomunikačních sítích. Používá vzorkovací frekvenci 8 kHz a data jsou komprimována pomocí logaritmické komprese.

Záložka ONVIF/RTSP

Zařízení 2N integrují RTSP server, který se konfiguruje na této záložce. RTSP server umožňuje streamovat jak audio, tak video. Lze volit způsob přenosu dat, metodu a parametry komprese videa a další parametry související se zabezpečením a kvalitou přenosu.



- **Povolení RTSP serveru** – povoluje funkci RTSP serveru v zařízení.



- **Povolení streamování audia** – povoluje nabízení audio streamu při navazování spojení s RTSP serverem. Není-li streamování audia povolené, nebude se přenášet audio přes fixní profily streamování ani přes lokální URL stream.
- **Povolení streamování videa** – povoluje nabízení video streamu při navazování spojení s RTSP serverem. Není-li streamování videa povolené, nebude se přenášet video přes fixní profily streamování ani přes lokální URL stream.
- **Zipstream** – vybírá výchozí úroveň komprese Zipstream (pro H.264). AXIS Zipstream zachovává všechny důležité forenzní detaily, které potřebujete, a zároveň snižuje požadavky na datový přenos a úložiště v průměru o 50 %. Komprese Zipstream je dostupná pouze pro zařízení s procesorem Artpec-7 a pro kodek H.264.

- **Lokální URL stream** – uvádí poslední vygenerované a uložené URL streamu pro RTSP klienta. Editace a generování lokálního URL streamu lze provést v dialogovém okně, které se otevře kliknutím na ikonu tužky  .

  - **Video kodek** – výběr z dostupných video kodeků.
  - **Rozlišení videa** – výběr z možných rozlišení obrazu.
  - **Snímková frekvence** – nastavení snímkové frekvence (1 až 30 fps, maximální možná hodnota pro video kodek MJPEG je 15 fps).
  - **Bitrate** – výběr dostupné přenosové rychlosti.
  - **Audio** – povolení přenosu zvuku.
  - **Zipstream** (dostupné pouze pro H.264) – nastavení zipstreamu lokálního URL streamu, které má přednost před hodnotou zadanou v **Nastavení Streamování**.

Počet RTSP streamů je omezen na 4 souběžné streamy. Do tohoto počtu spadají i audio streamy bez videa, a zpětný kanál audia směřující na zařízení.

Pro správnou funkci ONVIF je nutné vytvořit alespoň jeden uživatelský účet a nastavit správnou úroveň přístupu (dle specifikace ONVIF a použité VMS). Bez nastavení uživatelských účtů jsou dostupné pouze základní funkce.

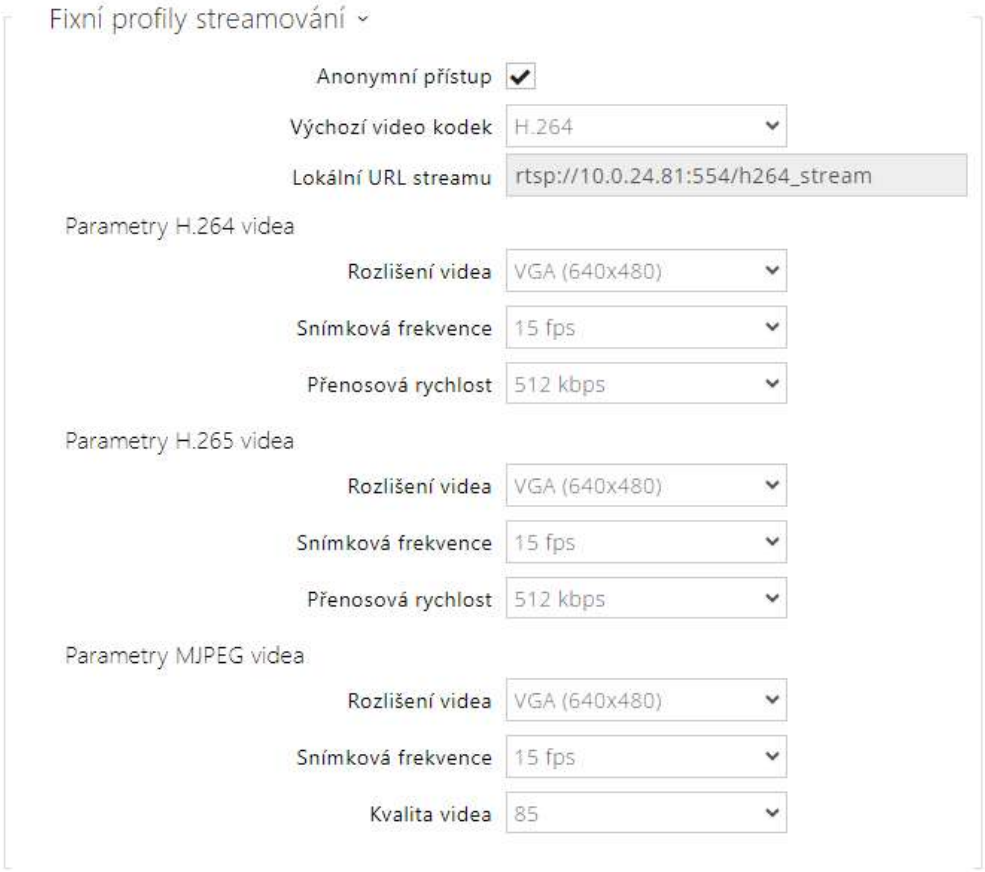
- **Jméno** – nastavuje uživatelské jméno pro přístup ke službě ONVIF.
- **Heslo** – nastavuje heslo pro přístup ke službě ONVIF.
- **Úroveň přístupu Onvif** – nastavuje úroveň přístupu uživatele ke službě ONVIF (Anonymous, User, Operator, Administrator)

- **IP adresa 1** – umožňuje nastavit autorizovanou IP adresu, ze kterých se lze přihlásit k RTSP serveru. Pokud není vyplněná, je možné připojit se z libovolné IP adresy.

- **Hodnota QoS DSCP** – nastavuje prioritu audio a video RTP paketů v síti. Nastavená hodnota se odesílá v poli TOS (Type of Service) v záhlaví IP paketu.
- **Povolení režimu UDP unicast** – povoluje režim odesílání dat audio a video streamu pomocí RTP/UDP protokolu. Pokud je tento režim vypnut, data audio a video streamu se přenáší vždy pouze pomocí RTP/RTSP protokolu.
- **Maximální délka paketu videa** – umožňuje nastavit maximální velikost video paketů odesílaných pomocí RTP/UDP protokolu.
- **Počáteční port pro RTP** – nastavuje počáteční lokální RTP port v rozsahu o délce 60 portů používaných při přenosu audia a videa. Výchozí hodnota je 4800 (tj. používaný rozsah je 4800–4859).
- **Jitter kompenzace** – nastavuje délku vyrovnávací paměti pro kompenzaci nerovnoměrnosti intervalů mezi příchody audio paketů. Nastavení delší vyrovnávací paměti zvýší odolnost příjmu za cenu většího zpoždění zvuku.

Tip

- FAQ: VLC player – Jak sledovat video z interkomu 2N IP
- FAQ: VLC player – Jak nahrát video z interkomu 2N IP



Poznámka

- Služba ONVIF media 1 nepodporuje profil H.265.

- **Anonymní přístup** – povoluje přístup k původním streamům RTSP serveru bez autorizace uživatele. Pokud toto pole není zaškrtnuté, RTSP klient se musí při přístupu k serveru autentizovat jako jeden z uživatelů služby ONVIF.
- **Výchozí video kodek** – výchozí nastavení nabízeného video kodeku při streamování pomocí RTSP.
- **Lokální URL streamu** – zobrazuje lokální URL streamu v závislosti na výběru kodeku.

- **Rozlišení videa** – nastavení rozlišení obrazu při streamování pomocí RTSP.
- **Snímková frekvence** – nastavení snímkové frekvence videa při streamování pomocí RTSP.
- **Přenosová rychlost** – nastavení přenosové rychlosti při streamování pomocí RTSP.
- **Kvalita videa** – nastavení úrovně komprese obraz (pouze MJPEG) v rozsahu 50 (nízká kvalita, nejnižší přenosová rychlost) – 95 (nejkvalitnější, největší přenosová rychlost).

Záložka JPEG

Na této záložce se konfiguruje nejjednodušší způsob streamování videa pomocí metod JPEG/HTTP a MJPEG/HTTP. Obrázky lze stahovat ze zařízení pomocí GET dotazu na adresu ve formátu:

- http://ip_adresa_interkomu/api/camera/snapshot?width= **W**&height=**H**

nebo (pro MJPEG, HTTP Server Push):

- http://ip_adresa_interkomu/api/camera/snapshot?width= **W**&height=**H**&fps=**N**

Hodnoty W a H specifikují rozlišení obrázku (jsou podporována rozlišení 160 x 120, 320 x 240, 640 x 480, 176 x 144, 322 x 272, 352 x 288, 1280 x 960 – pouze modely vybavené 1 MPix kamerou). Hodnota N specifikuje počet snímků za sekundu (lze volit mezi hodnotami 1 až 10).

V následující tabulce jsou uvedeny maximální počty souběžných MJPEG/HTTP streamů, při kterých ještě nedochází ke snížení frekvence odesílaných snímků za použití výchozí úrovně komprese JPEG.

Zařízení	Rozlišení	Počet streamů
2N Access Unit QR	640 x 480	8
2N Access Unit QR	1280 x 960	2

Poznámka

- *Metoda HTTP Server Push s obsahem multipart/x-mixed-replace není podporována všemi internetovými prohlížeči. Funkci můžete vyzkoušet např. v prohlížeči Firefox.*

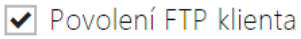
- **Úroveň JPEG komprese** – nastavuje úroveň JPEG komprese v rozsahu (1–99). Doporučená hodnota je 85. Parametr má vliv na velikost a kvalitu obrázku.

/*/

Záložka FTP

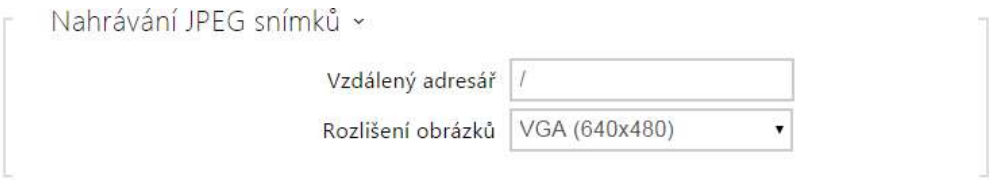
Na této záložce lze nastavit přístupové údaje k FTP(S) serveru, na který mohou být ukládány snímky z interní nebo externí kamery připojené k zařízení. Snímky jsou ukládány na FTP server ve formátu JPEG ve zvoleném rozlišení, název souboru snímku obsahuje datum a čas vytvoření snímku.

Snímky jsou na FTP server ukládány buď automaticky (periodicky /*/) příp. pomocí automatizace pomocí akce **Action.UploadSnapshotToFTP**.

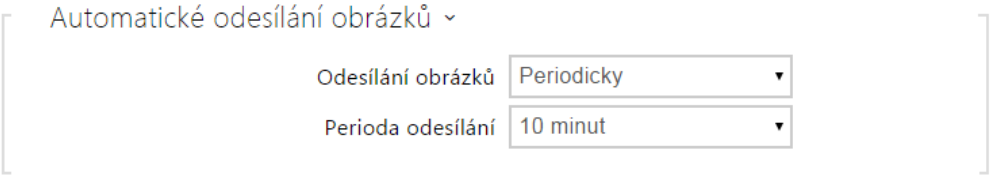


- **Povolení FTP klienta** – povoluje službu pro ukládání snímku z kamery na FTP server.

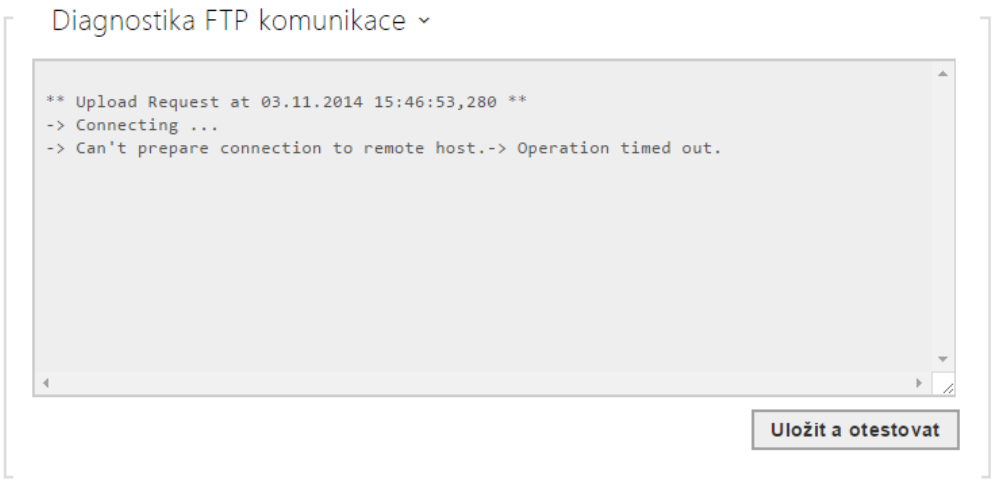
- **Adresa vzdáleného FTP serveru** – nastavuje adresu FTP serveru. Adresa musí být ve tvaru ftp://ip_adresa nebo ftps://ip_adresa.
- **Uživatelské jméno** – nastavuje jméno uživatele FTP serveru. Parametr je povinný, pokud FTP server vyžaduje autentizaci uživatele.
- **Heslo** – nastavuje heslo výše uvedeného uživatele FTP serveru.
- **Pasivní mód** – nastavuje pasivní režim přenosu (jako webový prohlížeč).



- **Vzdálený adresář** – nastavuje adresář na FTP serveru, do kterého budou snímky z kamery ukládány.
- **Rozlišení obrázků** – nastavuje rozlišení ukládaných obrázků.

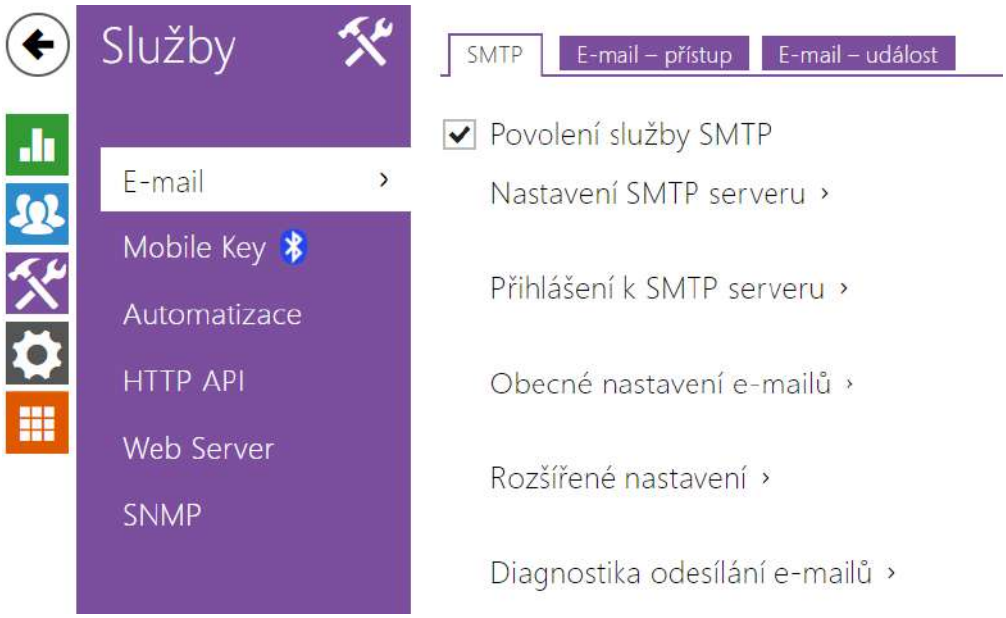


- **Odesílání obrázků** – umožňuje nastavit automatické odesílání obrázků na FTP server při začátku hovoru, příp. periodicky po uplynutí nastavené doby. Automatické odesílání obrázku lze vypnout (volba Automatizace), poté lze stále odesílat obrázky pomocí akce automatizace Action.UploadSnapshotToFtp.
- **Perioda odesílání** – nastavuje periodu automatického odesílání obrázků na FTP při nastavení parametru **Odesílaní obrázků** na hodnotu **Periodicky**. Periodu lze nastavit v několika krocích od 10 sekund do 30 minut.



Po stisku tlačítka **Uložit a otestovat** dojde k uložení aktuálně nastavené konfigurace FTP serveru, sejmutí obrázku z kamery a jeho uložení na FTP server. V průběhu ukládání obrázku se v okně výše zobrazuje detailní průběh komunikace s FTP serverem.

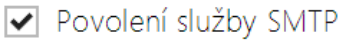
5.4.3 E-mail



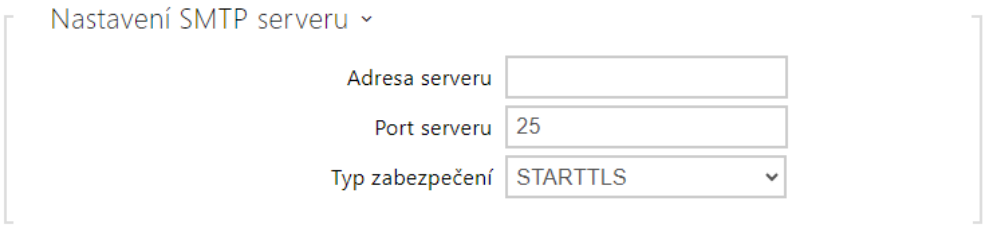
E-mailová adresa uživatele sloužící pro odeslání informací pomocí e-mailu, např. o přístupu uživatele do objektu nebo při využití 2N Automation. Můžete nastavit vlastní předmět a text zprávy e-mailu. Pokud je vaše zařízení vybaveno kamerou, může k e-mailu automaticky přiložit jeden nebo více snímků z kamery.
Zařízení 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**.

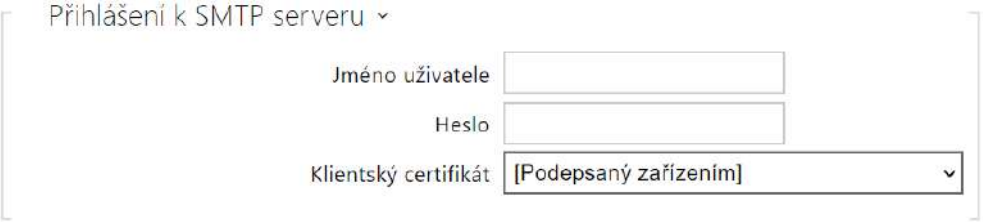
Záložka SMTP



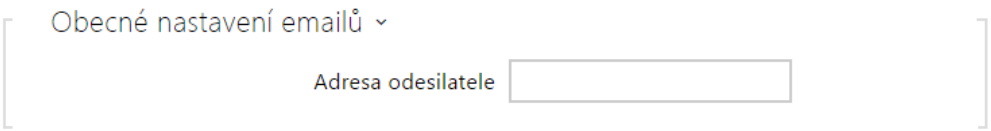
- **Povolení služby SMTP** – umožňuje povolit nebo blokovat službu odesílání e-mailů ze zařízení.



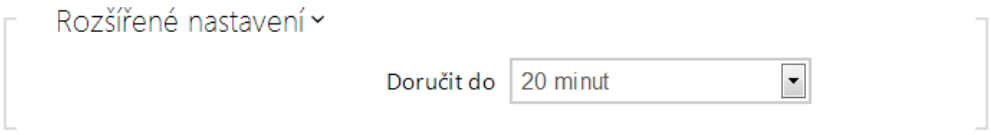
- **Adresa serveru** – adresa SMTP serveru, na který budou odesílány e-maily.
- **Port serveru** – port SMTP serveru. Upravte jen v případě nestandardního nastavení SMTP serveru. SMTP port bývá obvykle nastaven na hodnotu 25.
- **Typ zabezpečení** – volí typ zabezpečení pro komunikaci se SMTP serverem. Jaký typ zabezpečení server vyžaduje lze obvykle nalézt v jeho dokumentaci.



- **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 zařízení k SMTP serveru.
- **Klientský certifikát** – specifikuje klientský certifikát a privátní klíč, pomocí kterých se provádí šifrování komunikace mezi zařízením 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 zařízení.



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

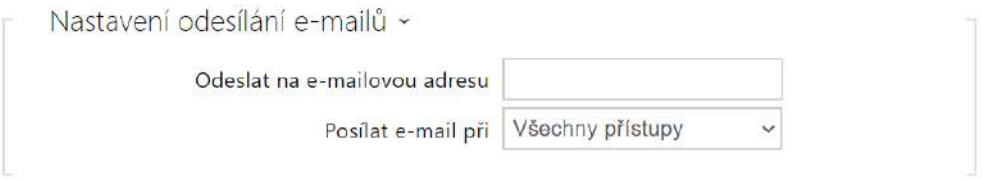


- **Doručit do** – nastavuje maximální dobu, po kterou se zařízení snaží doručit e-mail na nedostupný SMTP server.

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 zařízení, příp. jiným síťovým prvkem.

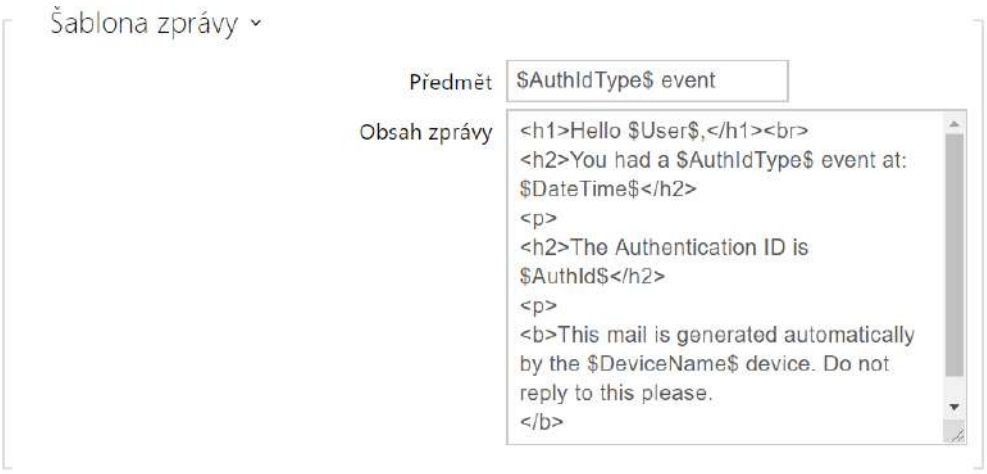
Záložka E-mail – přístup

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



- **Odeslat na e-mailovou adresu** – nastavení e-mailové adresy správce.
- **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.



- **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. Seznam zástupných symbolů vyskytujících se v šabloně je znázorněn v přehledové tabulce na konci této kapitoly.

Obsah zprávy

```
<p>Hello,
</p>
<p>User <b>$User$</b> generated a new access event on device <b>$DeviceName$</b> (IP:
<b>$Ip4Address$</b>)
</p>
<ul>
  <li>Authentication Type: <b>$AuthIdType$</b>
  </li>
  <li>Authentication ID: <b>$AuthId$</b>
  </li>
  <li>Validity: <b>$AuthIdValid$</b>
  </li>
  <li>Reason: <b>$AuthIdReason$</b>
  </li>
  <li>Direction: <b>$AuthIdDirection$</b>
  </li>
  <li>Date/Time: <b>$DateTime$</b>
```

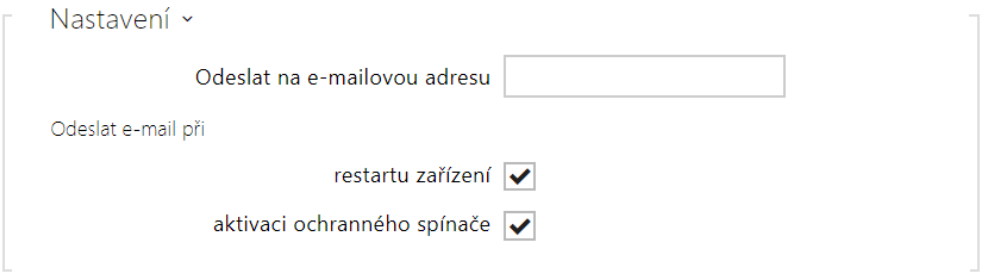
```
  </li>
</ul>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Upozornění

- Pro zástupné symboly $AuthIdType$ a $AuthIdValid$ je možno použít rozšířenou syntaxi, která slouží k náhradě vestavěných hodnot, například pro text v češtině: $AuthIdValid|Valid=platná|Invalid=neplatná$
- U neplatné hodnoty $AuthId$ je maskována první polovina ID, např.: ******11188, **********792d9044158891fa apod.
- U platné hodnoty $AuthId$ je maskováno celé ID ****.
- 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**

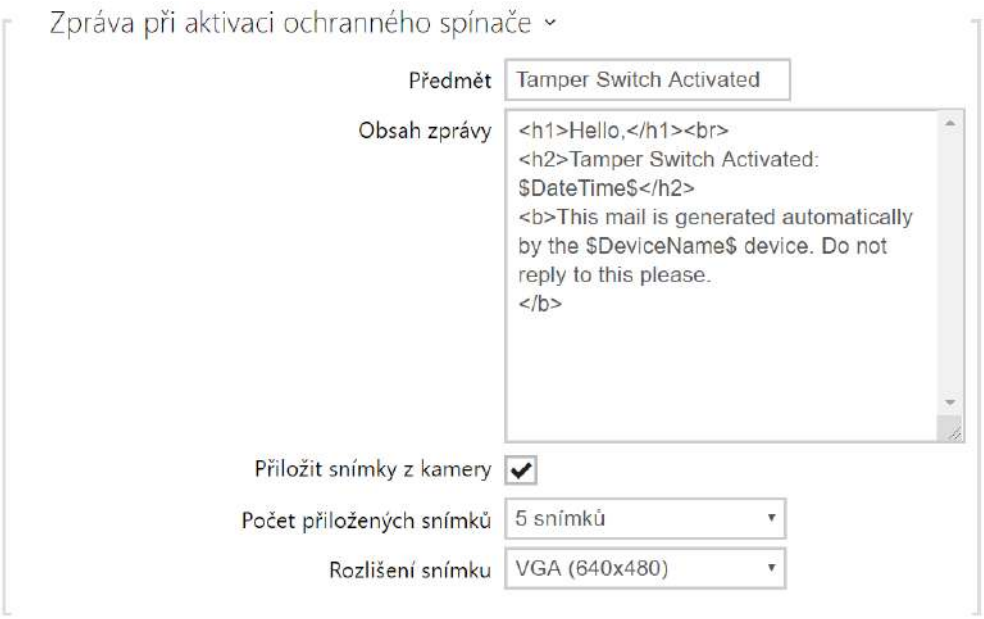
Zpráva při restartu zařízení – nastavení zprávy, která bude zaslána na uvedenou e-mailovou adresu při restartu zařízení.

- **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. Seznam zástupných symbolů vyskytujících se v šabloně je znázorněn v přehledové tabulce na konci této kapitoly.

Obsah zprávy

```
<p>Hello,
</p>
<p>Device <b>$DeviceName$</b> (IP: <b>$Ip4Address$</b>) rebooted on <b>$DateTime$</b>
</p>
<ul>
  <li>Reason: <b>$RebootReason$</b>
  </li>
  <li>Uptime: <b>$UpTime$</b>
  </li>
  <li>Firmware version: <b>$SoftwareVersion$</b>
  </li>
  <li>Build date: <b>$BuildTime$</b>
  </li>
</ul>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

⚠
- 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. Seznam zástupných symbolů vyskytujících se v šabloně je znázorněn v přehledové tabulce na konci této kapitoly.
- **Přiložit snímky** – povoluje odeslání přílohy s jedním nebo více snímky z kamery sejmutých v průběhu vyzvánění nebo hovoru.
- **Počet přikládaných snímků** – nastavuje počet snímků, které budou k e-mailu přiloženy.
- **Rozlišení snímků** – nastavuje rozlišení snímků odesílaných obrázků.

Obsah zprávy

```
<p>Hello,
</p>
<p>Tamper switch of device <b>$DeviceName$</b> (IP: <b>$Ip4Address$</b>) was
activated on <b>$DateTime$</b>
</p>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Upozornění

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

Upozornění

- Název pro zástupný symbol $DeviceName$ je přímo provázaný s hodnotou parametru *Název zařízení* v sekci Služby / Web Server / Základní nastavení. Doporučujeme použít takový název, který jasně definuje, o jaké zařízení se jedná.

Seznam zástupných symbolů

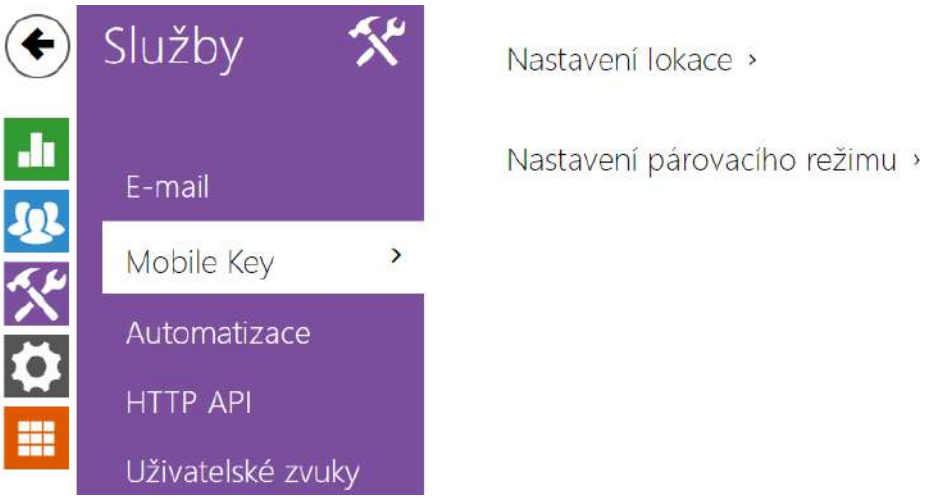
Výskyt	Zástupný symbol	Popis
Vždy	$DateTime$	aktuální datum a čas
	$DeviceName$	název zařízení
	$Ip4Address$	IP adresa zařízení
	$SoftwareVersion$	verze FW
	$BuildTime$	datum a čas sestavení
	$UpTime$	doba provozu zařízení
Závislý na konkrétním případu	$User$	uživatelské jméno
	$RebootReason$	důvod restartu
	$AuthId$	autentizační ID
	$AuthIdDirection$	směr (výstup/vstup)
	$AuthIdType$	typ ověření
	$AuthIdValid$	platný, neplatný
	$AuthIdReason$	důvod zamítnutí

Přehled zástupných symbolů v událostech

Zástupný symbol / Funkce	E-mail – přístup	E-mail – restart zařízení	E-mail – aktivace ochranného spínače	E-mail – zaslání diagnostiky	Automation
$DateTime$	*	*	*	*	*
$DeviceName$	*	*	*	*	*
$Ip4Address$	*	*	*	*	*
$SoftwareVersion$	*	*	*	*	*
$BuildTime$	*	*	*	*	*
$UpTime$	*	*	*	*	*
$User$	*			*	*
$RebootReason$		*			
$DialNumber$				• (odešle "E-Mail test")	CallStateChanged
$SipAccountNumber$					
$AuthId$	*				CardEntered, CardHeld
$AuthIdDirection$	*				CardEntered, CardHeld
$AuthIdType$	*				CardEntered, CardHeld
$AuthIdValid$	*				CardEntered, CardHeld

Zástupný symbol / Funkce	E-mail – přístup	E-mail – restart zařízení	E-mail – aktivace ochranného spínače	E-mail – zaslání diagnostiky	Automation
$AuthIdReason$	*				

5.4.4 Mobile Key



Přístupové jednotky 2N mohou být vybaveny modulem Bluetooth umožňujícím autentizovat uživatele pomocí mobilní aplikace **2N Mobile Key** dostupné pro zařízení s operačními systémy iOS 12 a vyšší (telefony iPhone 4S a vyšší) příp. Android 6.0 Marshmallow a vyšší (telefony s podporou Bluetooth 4.0 Smart).

Identifikace uživatele (Auth ID)

Aplikace **2N Mobile Key** se na straně zařízení 2N 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 přístupové jednotce 2N 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 parametru Mobile Key v seznamu uživatelů zařízení. Auth ID lze přesunout k jinému uživateli, příp. zkopírovat do jiného zařízení. Po vymazání hodnoty pole dojde k blokování přístupu uživatele.

Šifrovací klíče a lokace

Komunikace mezi aplikací **2N Mobile Key** a zařízením je vždy šifrovaná. Bez znalosti šifrovacího klíče nemůže aplikace **2N Mobile Key** uživatele autentizovat. Primární šifrovací klíč je automaticky vygenerován při prvním spuštění zařízení 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 ze zařízení exportovat a následně importovat do dalších zařízení. Zařízení 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 **zařízení 2N** 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 Adresáři zařízení na stránce příslušného uživatele. Párování lze fyzicky provést lokálně pomocí USB bluetooth modulu připojeného k PC, příp. vzdáleně pomocí bluetooth modulu integrovaného v zařízení. 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 zařízení a lze jej kdykoli přegenerovat.

Správa šifrovacích klíčů

Zařízení 2N 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 **zařízení 2N** aktualizovat.

> **Poznámka**

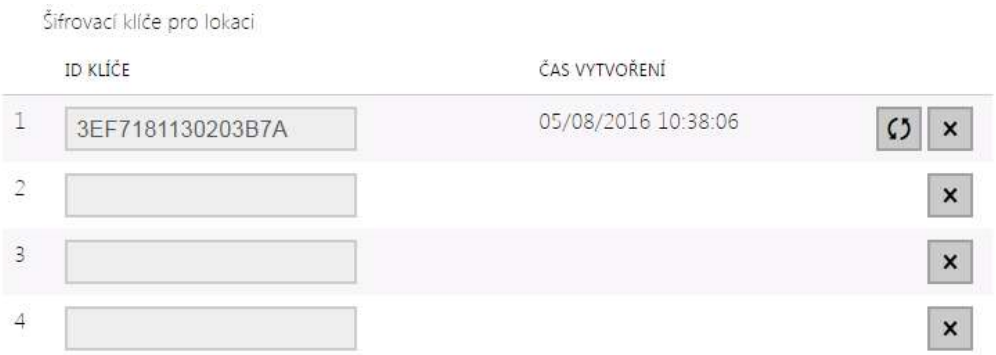
- Při prvním spuštění zařízení 2N jsou automaticky vygenerovány šifrovací klíče a jsou uloženy do konfiguračního souboru zařízení. Pro větší bezpečnost doporučujeme tyto šifrovací klíče před prvním použitím ručně znovu vygenerovat.

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.

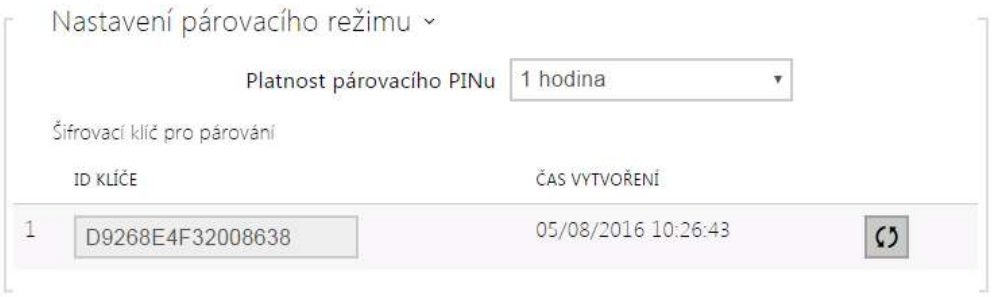
Po odstranění klíče se uživatelé aplikace **2N Mobile Key**, kteří tento klíč stále používají, nebudou moci autentizovat, pokud před smazáním klíče neaktualizují šifrovací klíče ve svém mobilním zařízení. Klíče v mobilním zařízení se aktualizují při každém použití aplikace **2N Mobile Key**.

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 zařízení. 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 se **zařízením 2N**.

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.

Varování

- S upgradem na verzi 2.30 dojde k upgradu v i bluetooth modulech. Při downgradu na verzi 2.29 a nižší může dojít k jejich nefunkčnosti.

5.4.5 Automatizace

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

Přístupové jednotky 2N poskytují 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 zařízení speciální programovatelné rozhraní **Automation**. Typické použití **Automation** je v aplikacích, které vyžadují složitější propojení se systémy třetích stran.

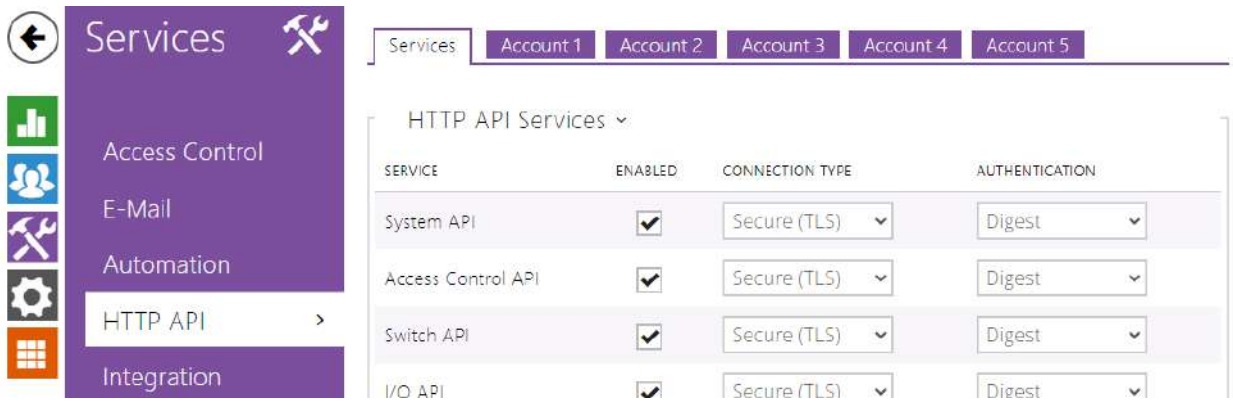
Do rozhraní Automation se vstupuje kliknutím na  u funkce, kterou chcete vytvořit nebo změnit.

Poznámka

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

5.4.6 HTTP API

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



Služby

HTTP API je podle funkce rozděleno do následujících služeb:

- **System API** – umožňuje změny konfigurace, získání stavu a upgrade zařízení.
- **Access Control API** – umožňuje řízení přístupů a způsob ověřování autentizace uživatele.
- **Switch API** – umožňuje řízení a sledování stavu spínačů, např. otvírání dveřních zámků apod.
- **I/O API** – umožňuje řízení a sledování logických vstupů a výstupů zařízení.
- **Display API** – umožňuje řízení displeje a zobrazování uživatelských informací na displeji.
- **E-Mail API** – umožňuje ze zařízení odesílat uživatelské e-maily.
- **Logging API** – umožňuje vyčítat zaznamenané události zařízen
- **Automation API** – umožňuje nastavit Secure/Unsecure komunikaci a požadavky autorizace.

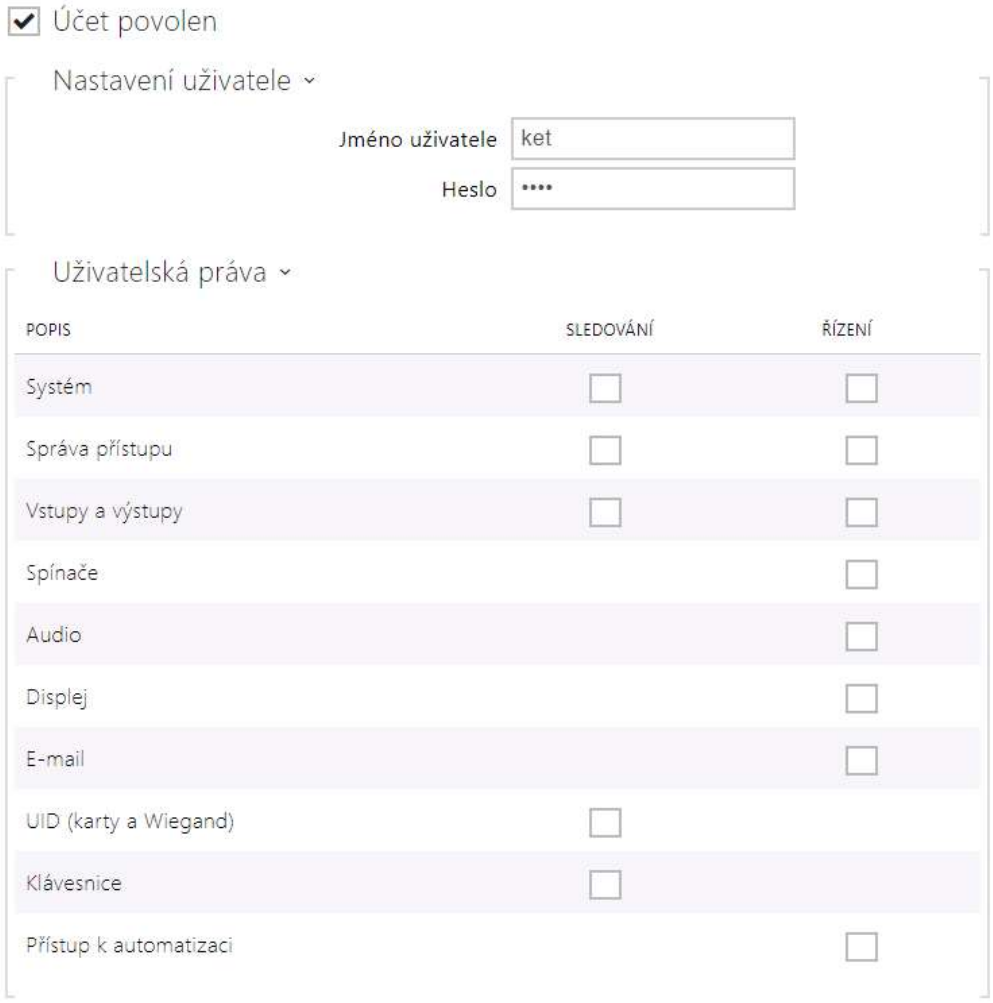
Pro každou službu lze nastavit transportní protokol (**HTTP** nebo **HTTPS**) a způsob autentizace (**žádná**, **Basic** nebo **Digest**). V konfiguraci **HTTP API** lze vytvořit až pět uživatelských účtů (s vlastním jménem a heslem) s možností detailního řízení přístupu k jednotlivým službám a funkcím.

U každé služby lze nastavit vyžadovaný způsob autentizace požadavků odesílaných na zařízení. Pokud autentizace není provedena, požadavek je odmítnut. Požadavky jsou autentizovány pomocí standardního autentizačního protokolu popsaného v **RFC-2617**. Je možné volit tyto tři metody autentizace:

- **Žádná** – služba nevyžaduje žádnou autentizaci. Služba je v tomto případě v lokální síti zcela nechráněná.
- **Basic** – služba vyžaduje autentizaci Basic podle **RFC-2617**. Služba v tomto případě vyžaduje heslo, to je však odesíláno v otevřeném formátu. Doporučujeme tuto volbu kombinovat s **HTTPS** protokolem, pokud je to možné.

- **Digest** – služba vyžaduje autentizaci Digest podle **RFC-2617**. Tato varianta je výchozí a z výše uvedených metod nejbezpečnější.

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

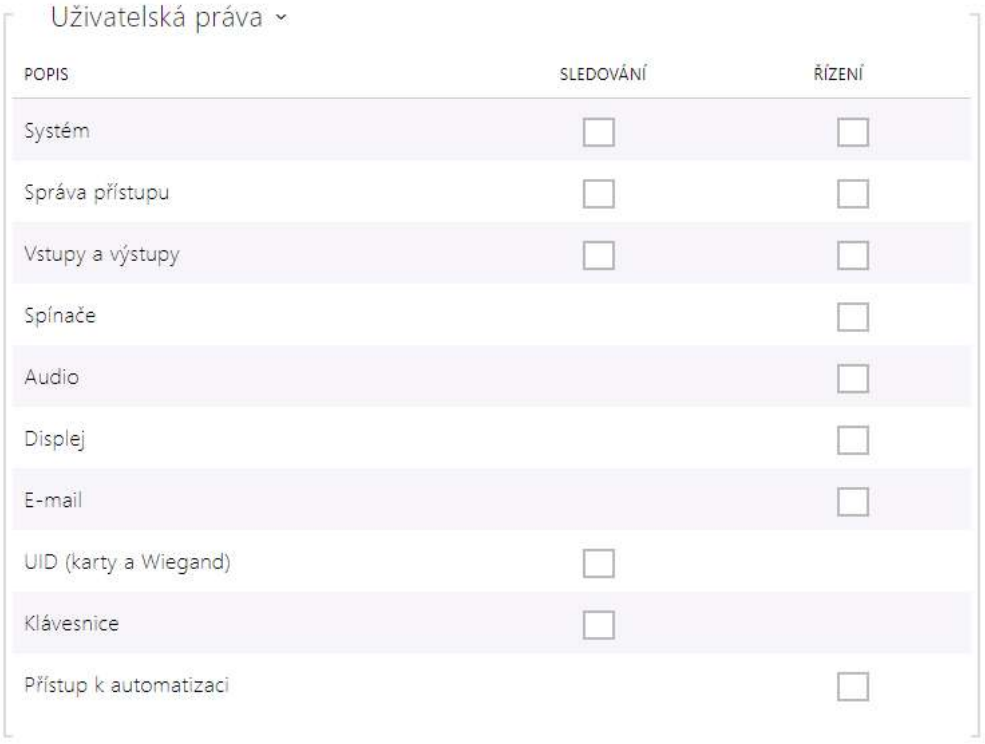


Záložka Účet 1–5

Zařízení umožňuje spravovat až pět uživatelských účtů určených pro přístup ke slu žbám **HTTP API**. Součástí uživatelského účtu je jméno a heslo uživatele a tabulka přístupových práv uživatele k jednotlivým službám **HTTP API**.

- **Účet povolen** – umožňuje povolit tento uživatelský účet.

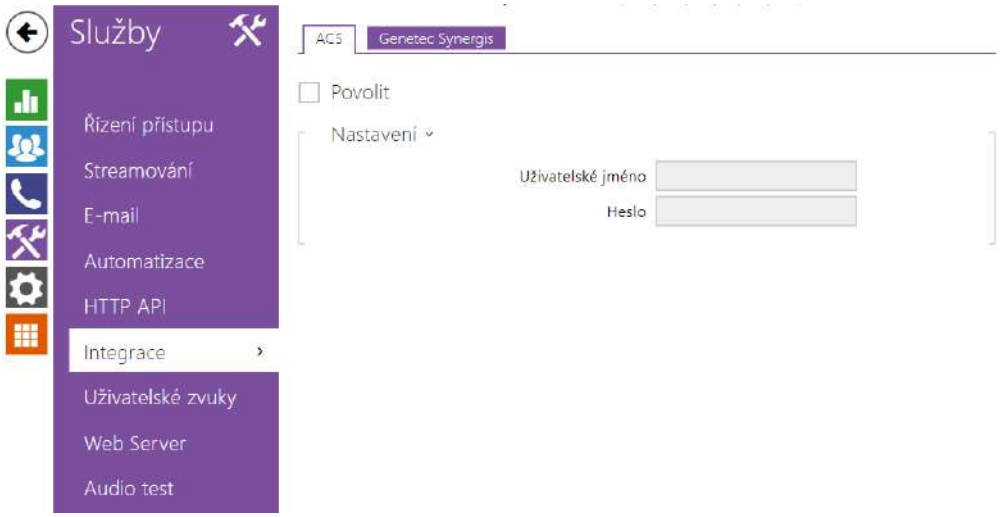
- **Jméno uživatele** – zadejte jméno uživatele pro autentizaci k HTTP API.
- **Heslo** – zadejte heslo pro autentizaci k HTTP API.



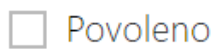
Pomocí tabulky přístupových práv lze řídit privilegia uživatelského účtu k jednotlivým službám.

5.4.7 Integrace

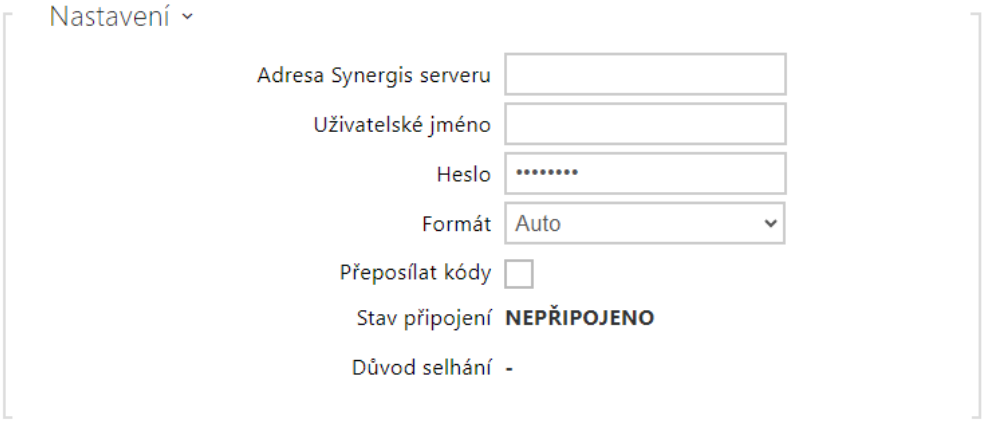
Služba Integrace umožňuje zařízením propojení se systémy třetích stran.



Záložka Genetec Synergis



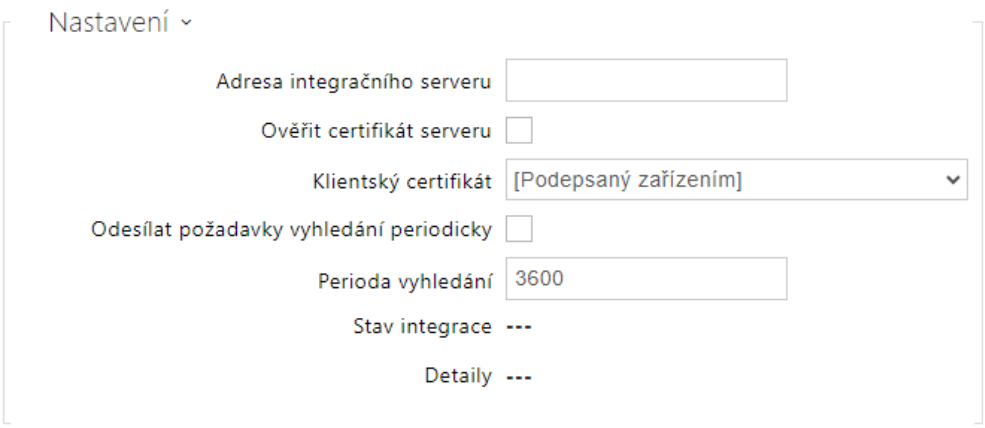
- **Povoleno** – povoluje spojení s externím bezpečnostním systémem Genetec Synergis.



- **Adresa Synergis serveru** – IP adresa nebo doménové jméno Synergis Serveru.
- **Uživatelské jméno** – uživatelské jméno používané při autentizaci.
- **Heslo** – heslo používané při autentizaci.

- **Formát** – formát vysílaných kódů.
- **Přeposílat kódy** – nastavuje, zda se mají přeposílat zadané kódy. Kódy mohou mít maximálně 6 číslic a na konci je potřeba stisknout klávesu potvrzení.

Záložka Discovery Service



- **Adresa integračního serveru** – nastavuje URL Služby vyhledání zařízení. Zařízení posílá HTTP požadavky se základními údaji při startu, při změně IP adresy a periodicky (v případě, že je to nakonfigurováno). Pokud je pole prázdné, požadavky nejsou odesílány.

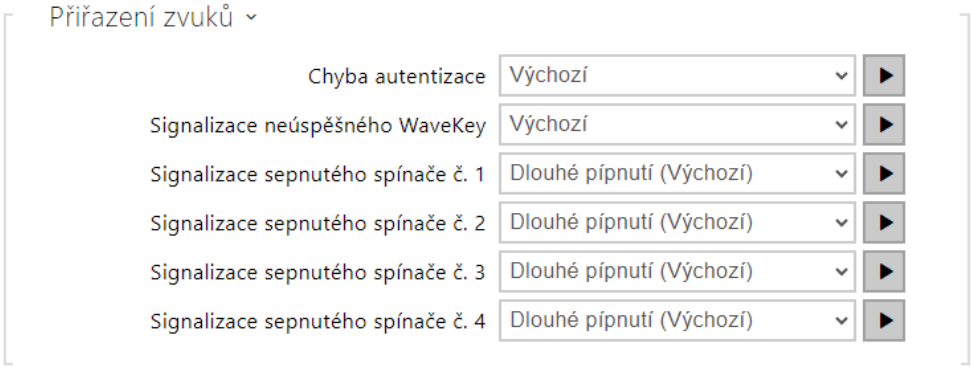
  > **Poznámka**
  >
  > Odesílaný JSON požadavek obsahuje následující informace o zařízení: MacAddress, Dhcp, IpAddress, NetMask, Gateway, SwVersion, SerialNumber, Variant, VariantId, Description, ProductName, CameraResolution (max.), HttpPort, HttpsPort.

- **Ověřit certifikát serveru** – povoluje ověření certifikátů intergračního serveru, což zajistí, že Discovery požadavky jsou zasílány důvěryhodnému serveru.
- **Klientský certifikát** – volí, který z nahraných certifikátů bude použit pro šifrovanou komunikaci s integračním serverem.
- **Odesílat požadavky vyhledání periodicky** – povoluje odesílání Discovery HTTP požadavků.
- **Perioda vyhledání** – nastavuje periodu odesílání HTTP požadavku na nakonfigurovanou URL v sekundách.
- **Stav integrace** – zobrazuje stav integrace na základě odpovědi od serveru.
- **Detaily** – zobrazuje detaily obsažené v odpovědi od serveru.

5.4.8 Uživatelské zvuky

Uživatelské zvuky umožňují nastavit typ zvukové signalizace sepnutého spínače zařízení, nebo ji úplně ztlumit. Povolení zvukové signalizace pro autentizaci je možné v sekci 5.4.1 Řízení přístupu.

- **Jazyk zvukových zpráv** – volí jazyk pro zvuková hlášení zařízení. Pokud je pro danou událost namapován soubor, pro který je k dispozici překlad, zpráva bude přehrána ve zvoleném jazyce. Není-li překlad k dispozici, bude přehráván anglicky nebo jako jazykově neutrální zvuk.



- **Chyba autentizace** – nastavuje zvuk přehrávaný při zamítnutí přístupu.
- **Signalizace neúspěšného WaveKey** – nastavuje zvuk, který se přehraje v případě, že žádný telefon neotevřel dveře během doby vyhledávání.
- **Signalizace sepnutého spínače 1–4** – nastavuje zvuk generovaný při sepnutí spínače. V nastavení jednotlivých spínačů je nutno signalizaci sepnutí upřesnit.

5.4.9 Web server

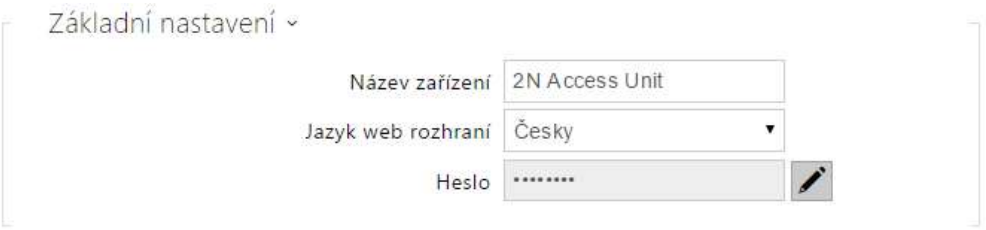
Přístupové jednotky 2N lze konfigurovat pomocí běžného prohlížeče, který přistupuje k web serveru integrovanému v zařízení. Pro komunikaci mezi prohlížečem a zařízením se používá zabezpečený protokol HTTPS. Pro přihlášení k zařízení je nutné zadat přihlašovací jméno a heslo. Výchozí jméno a heslo pro přihlášení je **admin** a **2n**. Výchozí heslo doporučujeme co nejdříve změnit.

Služba web server je využívána i dalšími funkcemi zařízení:

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

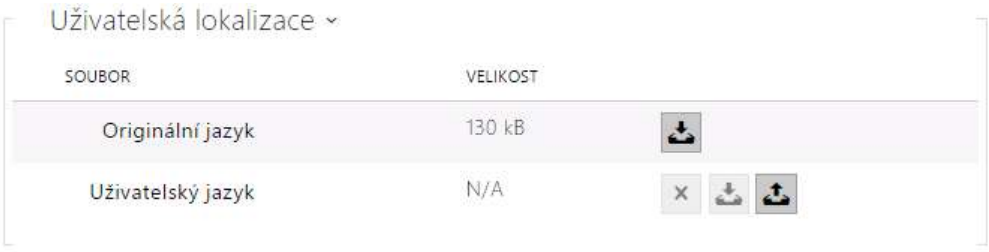
Pro tyto speciální případy lze pro komunikaci použít nezabezpečený HTTP protokol.

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 do webového konfiguračního rozhraní. Jazyk webového konfiguračního rozhraní můžete kdykoli dočasně změnit pomocí tlačítek v horní liště stránky.
- **Přístupové heslo** – nastavuje heslo pro přihlášení k zařízení. 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 zařízení.
- **HTTPS port** – nastavuje komunikační port web serveru pro komunikaci pomocí zabezpečeného protokolu HTTPS. Změna portu se projeví až po restartu zařízení.
- **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 zařízení 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 webovému konfiguračnímu rozhraní zařízení z IP adres mimo lokální síť.

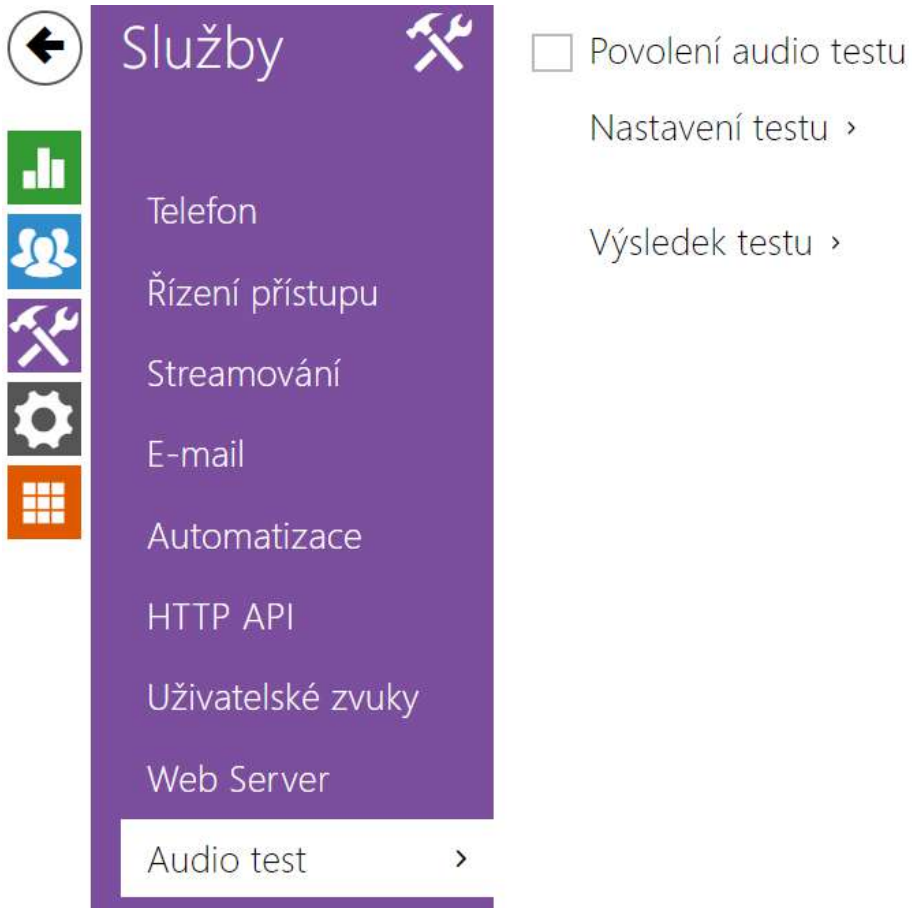


- **Originální jazyk** – umožňuje stáhnout ze zařízení originální soubor obsahující všechny texty uživatelského rozhraní v anglickém jazyce. Soubor je ve formátu XML viz níže.
- **Uživatelský jazyk** – umožňuje nahrát, stáhnout a případně odstranit uživatelský soubor s vlastními překlady textů uživatelského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

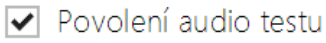
Při překladu modifikujte pouze hodnoty elementů **<s>** a neupravujte hodnoty atributů **id**. Jméno jazyka dané atributem **language** elementu **<strings>** bude uvedeno ve volbách parametru Jazyk webového konfiguračního rozhraní. Zkratka jména jazyka daná atributem **languageshort** elementu **<strings>**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

5.4.10 Audio test

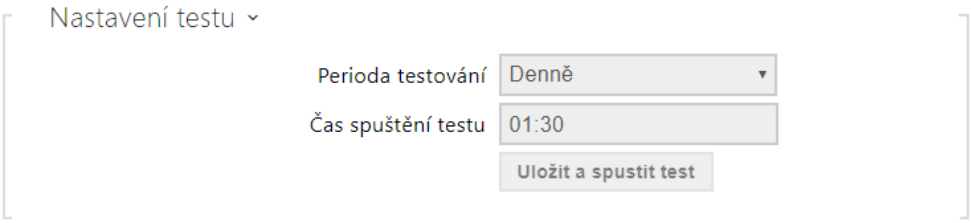


Model **2N Access Unit QR** umožňuje provádět pravidelnou kontrolu zabudovaného reproduktoru a mikrofonu. V průběhu testu generuje reproduktor v zařízení jeden nebo více krátkých tónů. Pomocí zabudovaného mikrofonu se snímá generovaný tón, a pokud je správně detekován, je test prohlášen za úspěšný. Doba trvání testu je přibližně 4 s. V případě, že test je neúspěšný (což může být způsobeno např. extrémním okolním hlukem), opakuje se ještě jednou za deset minut. Výsledek posledního testu je možné zobrazit v konfirmačním rozhraní zařízení anebo zpracovat pomocí **Automation**.

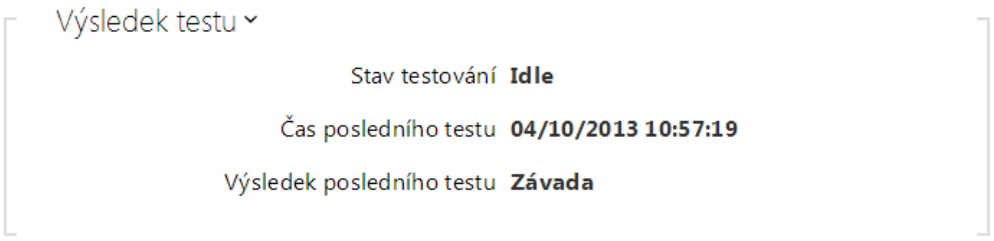
Seznam parametrů



- **Povolení audio testu** – povoluje automatické provádění audio testu.



- **Perioda testování** – umožňuje nastavit periodu provádění testu. Test lze automaticky spouštět jednou denně nebo jednou týdně.
- **Čas spuštění testu** – umožňuje nastavit čas, ve kterém se má test pravidelně provádět. Lze nastavit čas ve formátu HH:MM. Doporučujeme nastavit čas, kdy se očekává minimální využití zařízení.
- **Uložit a spustit test** – pomocí tlačítka můžete test spustit a uložit okamžitě, bez ohledu na aktuální nastavení.



- **Stav testování** – průběžně ukazuje stav průběhu testování.
- **Čas posledního testu** – zobrazuje čas naposledy provedeného testu.
- **Výsledek posledního testu** – zobrazuje výsledek naposledy provedeného testu.

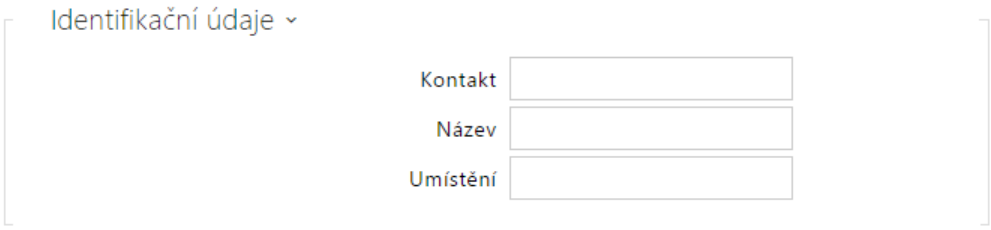
5.4.11 SNMP

Přístupové jednotky 2N integrují funkcionalitu umožňující vzdálený dohled zařízení v síti pomocí protokolu SNMP. Zařízení podporují SNMP protokol verze 2c.

Seznam parametrů

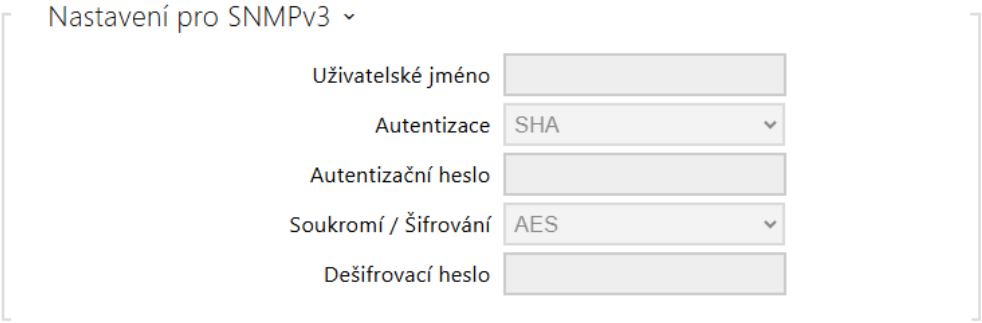
- **Povolení SNMP** – umožňuje zapnutí této funkce.

- **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.

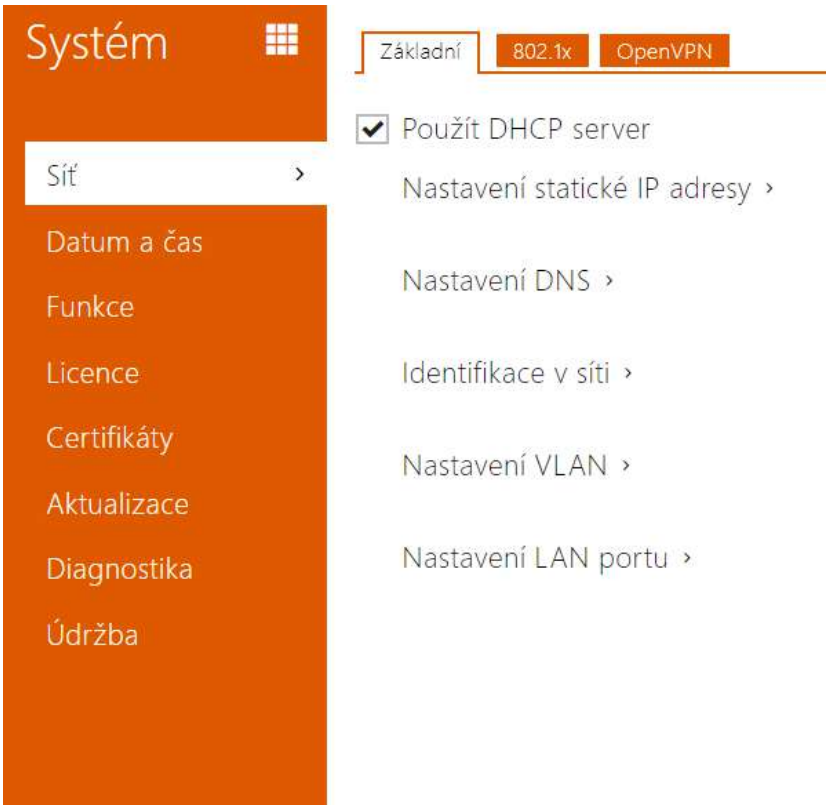


- **Uživatelské jméno** – nastavuje algoritmus, který je použit pro autentizaci SNMPv3 traps.
- **Autentizace** – nastavuje algoritmus, který se použije k dešifrování SNMPv3 traps.
- **Autentizační heslo** – nastavuje heslo pro autentizaci SNMPv3.
- **Soukromí / Šifrování** – nastavuje algoritmus, který se použije k dešifrování SNMPv3 traps.
- **Dešifrovací heslo** – nastavuje heslo pro dešifrování SNMPv3 traps.

5.5 Systém

Zde je přehled toho, co v kapitole naleznete:

5.5.1 Síť



Přístupové jednotky 2N se připojují do lokální sítě a pro správnou funkci musí mít nastavenou platnou IP adresu, příp. mohou IP adresu získat z DHCP serveru v této síti. IP adresa a nastavení DCHP se konfiguruje v záložce Síť.

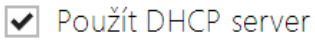
Tip

- *Pokud chcete zjistit aktuální IP adresu svého zařízení, můžete využít aplikaci **2N IP Network Scanner**, která je volně ke stažení na stránkách* 2N.com *nebo můžete použít mechanismus popsaný v Instalačním manuálu k příslušnému zařízení.*

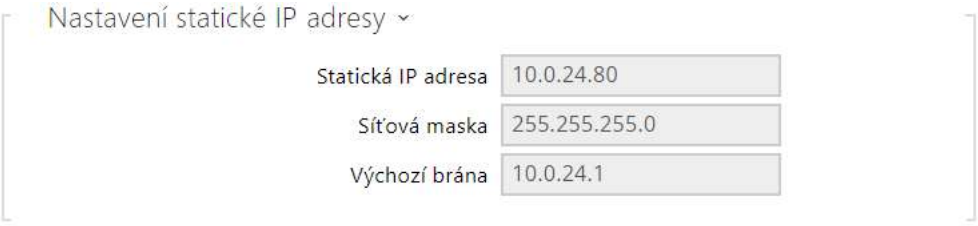
Jestliže ve své síti používáte RADIUS server a mechanismus ověřování připojených zařízení založený na protokolech 802.1x, můžete zařízení nakonfigurovat tak, aby používalo autentizaci EAP-MD5 nebo EAP-TLS. K nastavení této funkce slouží záložka 802.1x.

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

Seznam parametrů

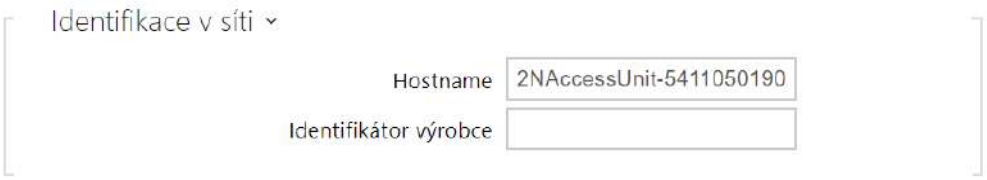


- **Použít DHCP server** – povoluje automatické získání IP adresy z DHCP serveru v lokální síti. Pokud ve vaší síti DHCP server není nebo jej nelze použít z jiného důvodu, použijte manuální nastavení sítě.

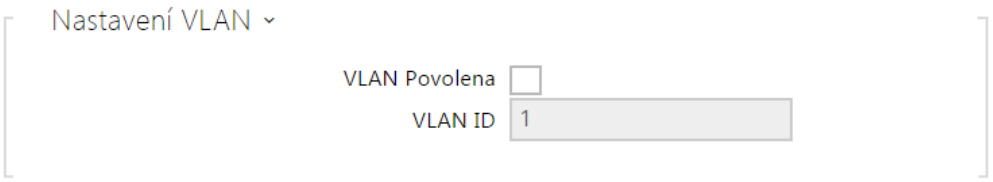


- **Statická IP adresa** – statická IP adresa zařízení. Adresa je použita společně s parametry níže, pokud není nastaven parametr Použít DHCP server.
- **Síťová maska** – nastavuje masku sítě.
- **Výchozí brána** – adresa výchozí brány, která umožňuje komunikaci se zařízeními mimo lokální síť.

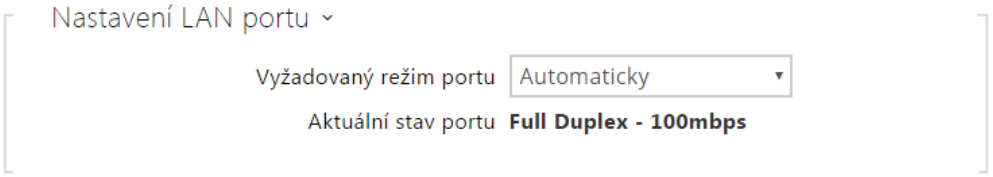
- **Primární DNS** – adresa primárního DNS serveru pro překlad doménových jmen na IP adresy. V případě obnovení továrního nastavení zařízení bude primární DNS server nastaven na adresu 8.8.8.8.
- **Sekundární DNS** – adresa sekundárního DNS serveru, který je použit v případě, kdy primární DNS server není dostupný. V případě obnovení továrního nastavení zařízení bude sekundární DNS server nastaven na adresu 8.8.4.4.



- **Hostname** – nastavení identifikace zařízení 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.

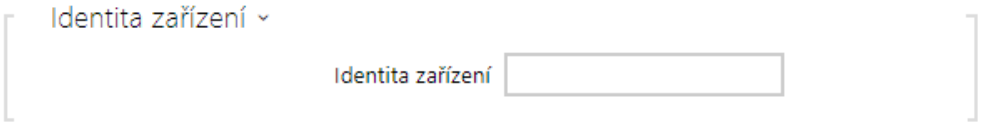


- **Vyžadovaný režim portu** – preferovaný režim portu síťového rozhraní (Automaticky nebo Half Duplex – 10 mbps). Umožňuje snížit přenosovou rychlost na 10 mbps v případě, že použitá síťová infrastruktura (kabeláž) není spolehlivá pro 100 mbps provoz.
- **Aktuální stav portu** – aktuální stav portu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

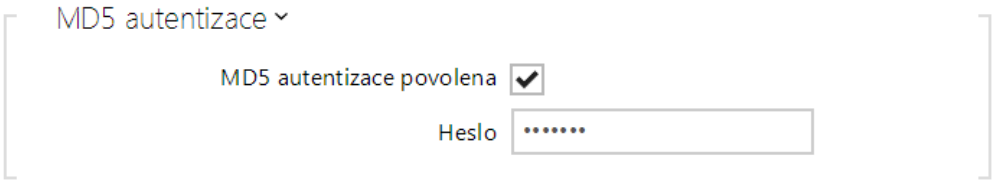
Záložka 802.1x

Upozornění

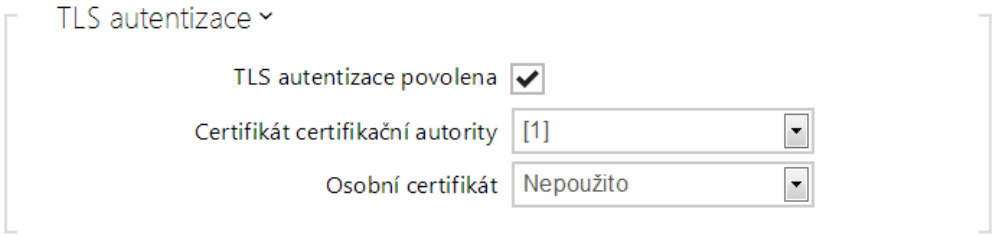
- Změny v nastavení autentizace se projeví po restartu zařízení.



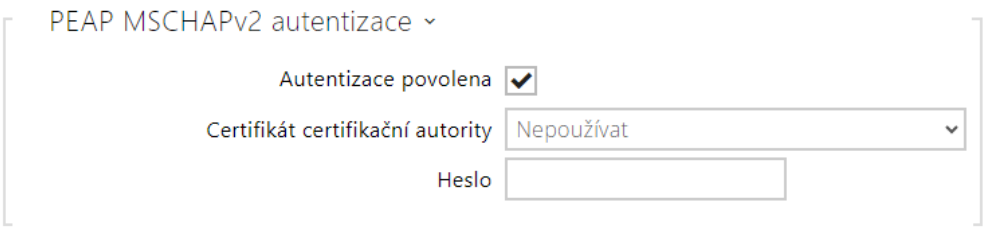
- **Identita zařízení** – jméno uživatele (identita) pro autentizaci pomocí metod EAP-MD5 a EAP-TLS.



- **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 zařízení 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 zařízení stane nedostupné.
- **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 zařízení 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.

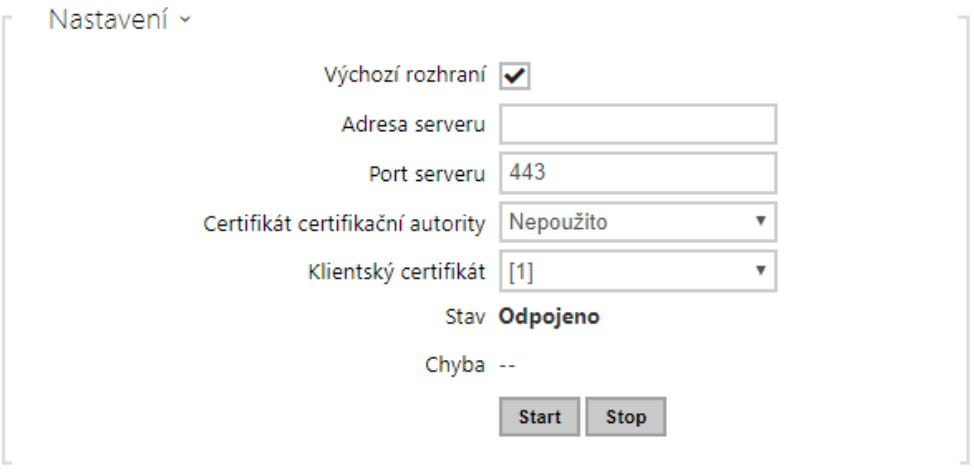


- **Autentizace povolena** – povoluje použití autentizace zařízení v síti pomocí protokolu 802.1x PEAP MSCHAPv2. V případě, že vaše síť 802.1x nepodporuje, tuto funkci nezapínejte. V opačném případě se zařízení stane nedostupným.
- **Certifikát certifikační autority** – specifikuje certifikát certifikační autority pro ověření platnosti veřejného certifikátu serveru RADIUS. Pokud není uveden, veřejný certifikát serveru RADIUS se neověřuje.
- **Heslo** – přístupové heslo použité pro autentizaci pomocí metody PEAP MSCHAPv2

Záložka OpenVPN

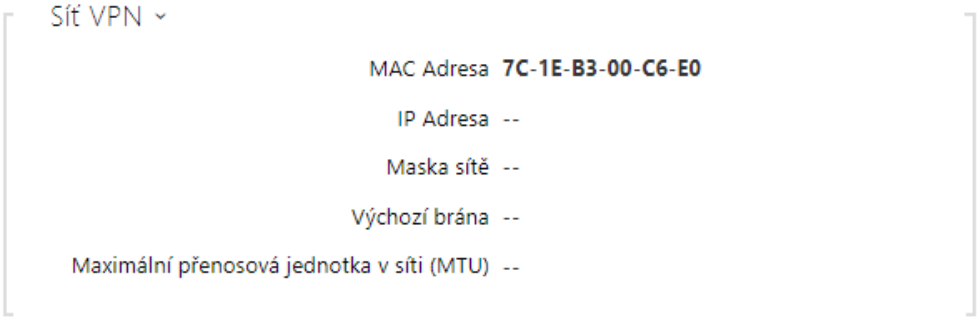
Pomocí OpenVPN lze připojit zařízení do jiné sítě.

- **Povoleno** – zapíná virtuální privátní síť (VPN).



- **Výchozí nastavení** – je-li povoleno, směřuje veškerý odchozí síťový provoz mimo masku lokální sítě na rozhraní VPN.
- **Adresa serveru** – adresa OpenVPN serveru.
- **Port serveru** – port serveru OpenVPN.
- **Certifikát certifikační autority** – specifikuje sadu certifikátů certifikačních autorit pro ověření platnosti veřejného certifikátu serveru OpenVPN. Lze zvolit jednu ze tří sad

certifikátů, viz sekce Certifikáty. Pokud není certifikát certifikační autority uveden, veřejný certifikát serveru OpenVPN se neověřuje.
- **Klientský certifikát** – specifikuje sadu klientských certifikátů pro ověření identity klienta serverem OpenVPN. Lze zvolit jednu ze tří sad certifikátů, viz sekce Certifikáty. Pokud není klientský certifikát uveden, identita klienta OpenVPN se neověřuje.
- **Stav** – zobrazuje stav připojení OpenVPN. Připojeno/Odpojeno.
- **Chyba** – zobrazuje, pokud je, typ chyby připojení OpenVPN.
- **Start** – připojí zařízení k OpenVPN.
- **Stop** – odpojí zařízení k OpenVPN.

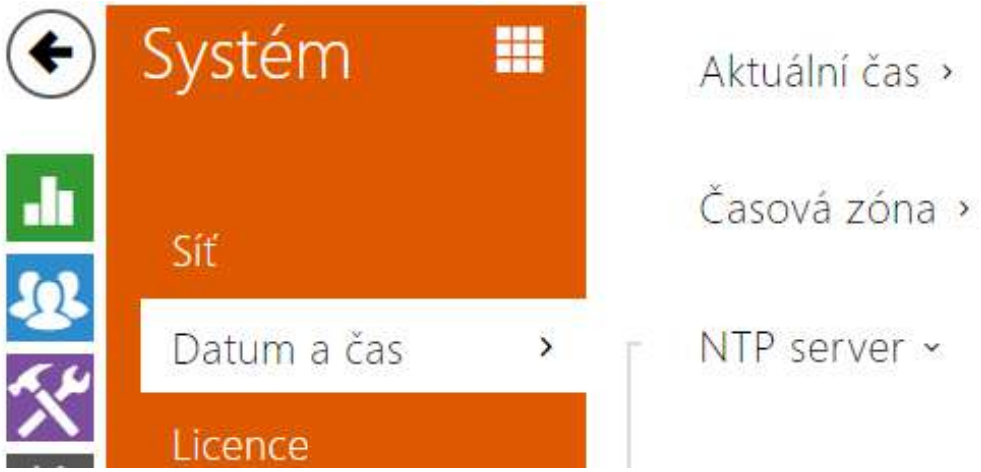


- **Síť VPN** – zobrazuje základní informace o VPN.

Tip

- Podrobné informace o nastavení OpenVPN serveru a klienta jsou k dispozici v sekci FAQ.

5.5.2 Datum a čas



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

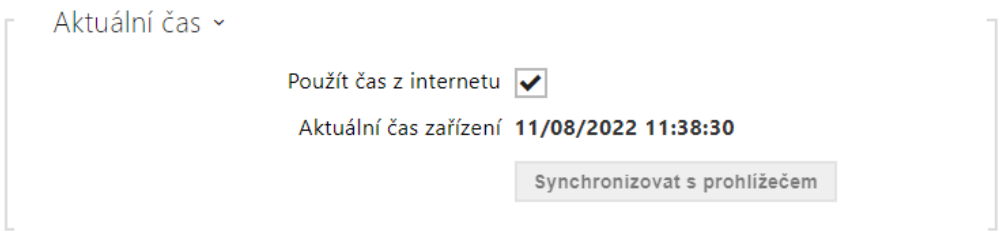
Přístupové jednotky 2N jsou vybaveny zálohovanými hodinami reálného času, které umožňují překonat výpadek napájení po dobu až několika dnů. Čas v zařízení můžete kdykoli synchronizovat s internetovým časem zaškrtnutím funkce **Použít aktuální čas z internetu** nebo s aktuálním časem ve svém PC pomocí tlačítka **Synchronizovat s prohlížečem**.

Poznámka

- *Správné nastavení data a času není pro základní funkci zařízení 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 zařízení přibližně ±0,005 %, což může znamenat chybu až ±2 minuty/měsíc. Pro maximální přesnost a spolehlivost doporučujeme vždy použití funkce **Použít aktuální čas z internetu**.

Seznam parametrů

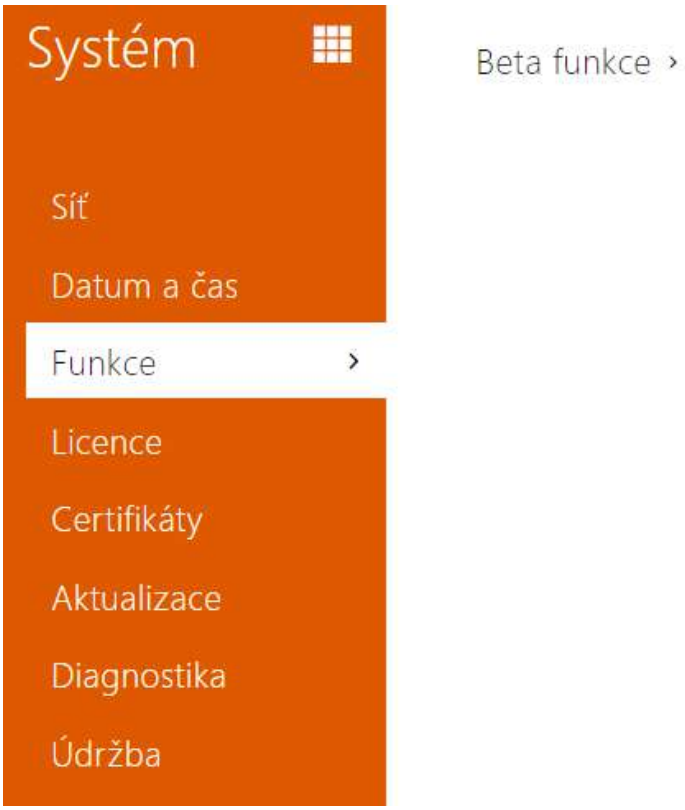


- **Použít čas z internetu** – Povoluje použití NTP serveru pro synchronizaci vnitřního času zařízení.
- **Synchronizovat s prohlížečem** – pomocí tlačítka můžete kdykoli synchronizovat čas v zařízení s aktuálním časem ve svém PC.

- **Automatická detekce** – nastavuje, zda bude časová zóna detekována automaticky ze služby My2N. V případě, že je automatická detekce vypnuta, je použito nastavení v parametru Manuální volba (ručně zvolená časová zóna nebo Vlastní pravidlo).
- **Detekovaná časová zóna** – zobrazuje automaticky zjištěnou časovou zónu. V případě, že služba není k dispozici nebo je vypnutá, zobrazuje N/A.
- **Manuální volba** – nastavuje časovou zónu pro místo instalace zařízení. Nastavení určuje časový posun a přechody mezi letním a zimním časem.
- **Vlastní pravidlo** – pokud je zařízení nainstalováno v lokalitě, která není uvedena v seznamu parametru Časová zóna, lze nastavit pravidlo časové zóny manuálně.

- **Použít NTP server** – povoluje použití NTP serveru pro synchronizaci vnitřního času zařízení. IP adresu serveru ani doménové jméno nelze nastavit při vypnutí funkce **Použít čas z internetu**.
- **Adresa NTP serveru** – nastavuje IP adresu nebo doménové jméno NTP serveru, podle kterého zařízení synchronizuje vnitřní čas.

5.5.3 Funkce



Zobrazuje seznam zveřejněných beta funkcí, které jsou určeny k testování uživateli.
Seznam uvádí:

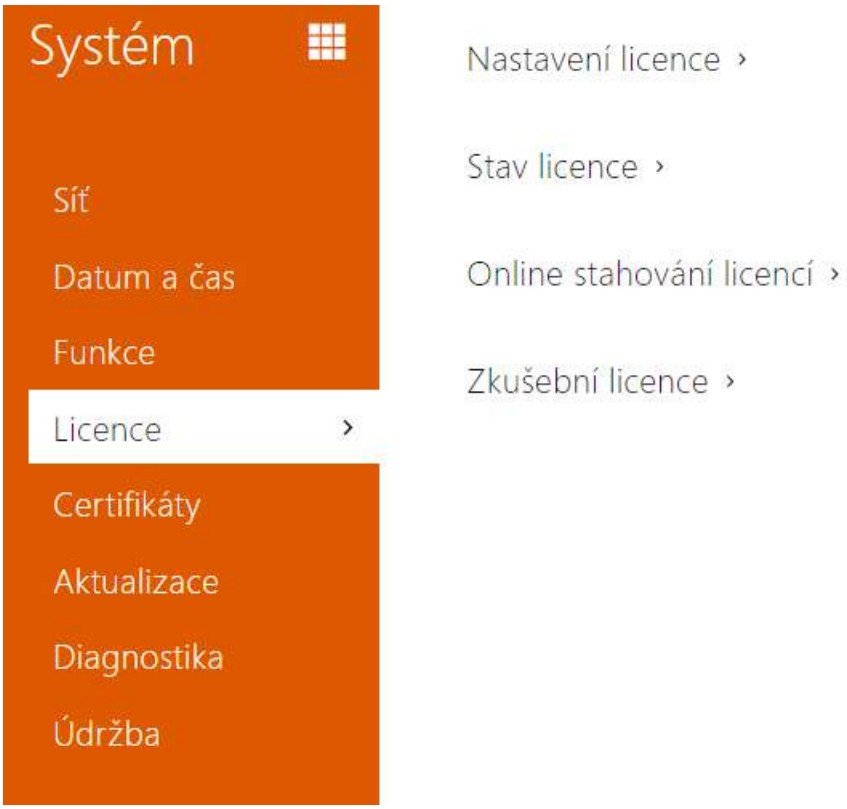
- název funkce,
- stav funkce indikující, zda je funkce spuštěna nebo zastavena,
- akci umožňující funkci spustit nebo zastavit.

Ke spuštění nebo zastavení funkce dojde až po restartu zařízení. Dokud není zařízení restartováno, je možné požadavek na změnu stavu zrušit akcí **Přerušit**.

> **Poznámka**
>
> - Na testovací funkce není poskytnuta záruka a společnost 2N TELEKOMUNIKACE a.s. nenese odpovědnost za funkční omezení a případné škody vzniklé v důsledku funkčních omezení beta funkcí. Beta funkce jsou poskytovány výhradně za účelem testování.

Název beta funkce	Popis
Konfigurační soubor chráněný heslem	Tato funkce umožňuje zašifrování konfiguračního souboru heslem během jeho zálohování (viz 5.5.8 Údržba). Při nahrání konfiguračního souboru do zařízení bude vyžadováno heslo, kterým je konfigurační soubor zabezpečen. Pokud heslo nesouhlasí, konfigurační soubor nebude nahrán do zařízení.
Vícefaktorové ověřování registračních značek	Po aktivaci této funkce se objeví volba Multifaktor v sekci Služby > Řízení přístupu > Pravidla pro příchod > Pokročilé nastavení > Rozpoznávání registračních značek. Přístup je povolen až po spojení nejméně dvou autentizačních metod v závislosti na nastavení přístupových pravidel. Při rozpoznání registrační značky je nezbytné do 60 sekund zadat další autentizační metodu.

5.5.4 Licence



Některé funkce přístupových jednotek 2N jsou dostupné pouze po zadání platného licenčního klíče. Seznam možností licencování přístupových jednotek 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.

- **Standardní licence** – zobrazuje seznam licencí, které jsou součástí zařízení z výroby.
  - **Enhanced Security** – zobrazuje, zda jsou k dispozici funkce aktivované licencí Enhanced Security.
  - **Podpora NFC** – zobrazuje, zda je k dispozici podpora identifikace uživatele pomocí telefonů vybavených technologií NFC.
  - **Enhanced Intergration** – zobrazuje, zda jsou k dispozici funkce aktivované licencí Enhanced Integration.
  - **Podpora řízení výtahů** – zobrazuje, zda je k dispozici funkce aktivované Lift Module licence.

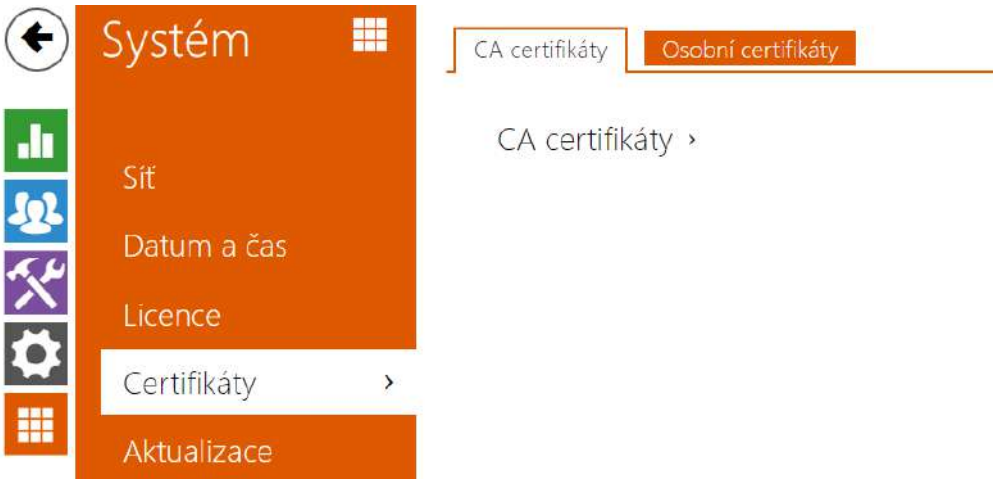
Tip

- Licencované funkce

- **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.

5.5.5 Certifikáty



Některé síťové služby přístupové jednotky 2N 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 přístupových jednotek, které využívají protokol TLS:

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

Přístupové jednotky 2N umožňují nahrát sady certifikátů certifikačních autorit, které slouží k ověřování identity zařízení, se kterým zařízení 2N komunikují, a zároveň nahrát 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.

Přístupové jednotky 2N:

- akceptují certifikáty ve formátech DER (ASN1) a PEM.
- podporují šifrování AES, DES a 3DES.
- podporují algoritmy:
  - RSA až 2048bitová velikost klíče pro certifikáty nahrané uživatelem; interně až 4096bitových klíčů (při připojování – přechodné a rovnocenné certifikáty)
  - Elliptic Curves

Upozornění

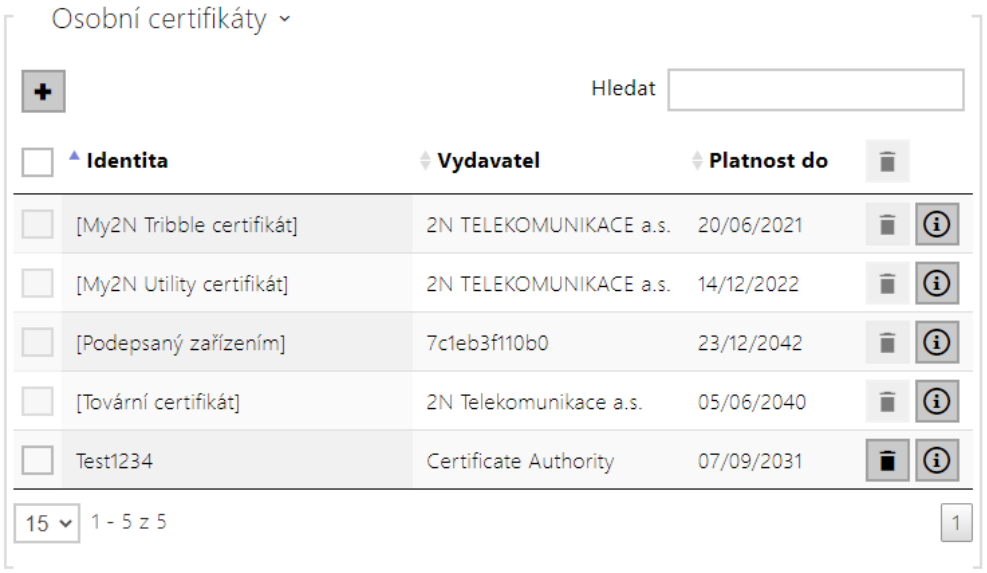
- CA certifikáty musí používat formát X.509 v3.

Při prvním připojení napájení k zařízení 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 zařízení a prohlížečem, komunikace je zabezpečena, ale prohlížeč vás upozorní, že nemůže ověřit důvěryhodnost certifikátu zařízení.*

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



Stiskem tlačítka + můžete do zařízení nahrát certifikát uložený ve vašem PC. V dialogovém okně lze vyplnit ID certifikátu pro identifikaci při jeho výběru, úpravě či mazání. ID může být maximálně 40 znaků dlouhé, může obsahovat malé a velké znaky abecedy, číslice a znaky '_' a '-'. ID není povinné. Vyberte soubor s certifikátem (příp. privátním klíčem) a stiskněte tlačítko **Nahrát**. Stiskem tlačítka 🗑 certifikát ze zařízení odstraníte. Stiskem tlačítka ⓘ zobrazíte informace o certifikátu.

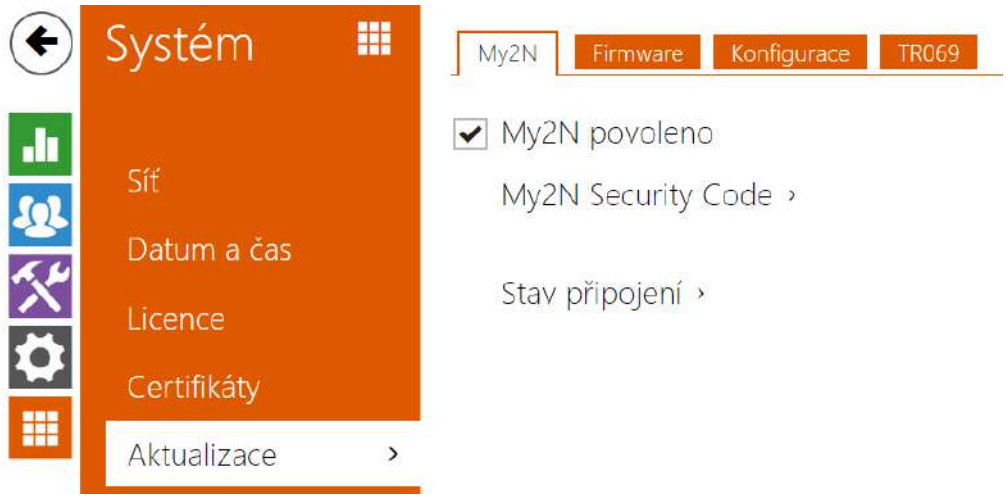
⚠ Upozornění

Po aktualizaci firmwaru nebo restartu změní zařízení **Self signed certifikát** na nový. Je třeba zkontrolovat a porovnat certifikát zobrazující se na zařízení s certifikátem na webu, zda-li jsou shodné.

⚠ 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).

5.5.6 Aktualizace



Přístupové jednotky 2N umožňují 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. Zařízení podporuje automatické zjištění adresy pomocí místního DHCP serveru (tzv. Option 66).

Upozornění

- Konfigurační soubor má v sobě uložené přihlašovací heslo. Pokud je heslo v souboru výchozím heslem 2n, bude nahrána pouze platná část konfigurace. To znamená, že se konfigurace nahraje, ale heslo zůstane původní a nezmění se na hodnotu uvedenou v souboru.

Záložka My2N

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

- **Sériové číslo** – zobrazuje sériové číslo zařízení, pro které je platný My2N kód.
- **My2N Security Code** – zobrazuje plné znění kódu sloužícího k aktivaci aplikace.
- **VYGENEROVAT NOVÝ** – aktuální My2N Security Code bude zneplatněn a bude vygenerován nový.

Zobrazuje informace o stavu připojení zařízení do My2N.

- **My2N ID** – unikátní identifikátor společnosti vytvořený pomocí My2N portálu.

Záložka Firmware

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

Zařízení 2N očekává na serverech soubory s názvy:

a. **MODEL**-firmware.bin – firmware zařízení
b. **MODEL**-common.xml – společná konfigurace všech zařízení daného modelu

c. **MODEL**-**MACADDR**.xml – specifická konfigurace pro jedno zařízení

MODEL v názvu souboru specifikuje model zařízení :

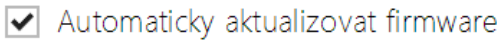
1. **au – 2N Access Unit**
2. **aug2 – 2N Access Unit 2.0**
3. **aum – 2N Access Unit M**
4. **auqr - 2N Access Unit QR**

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

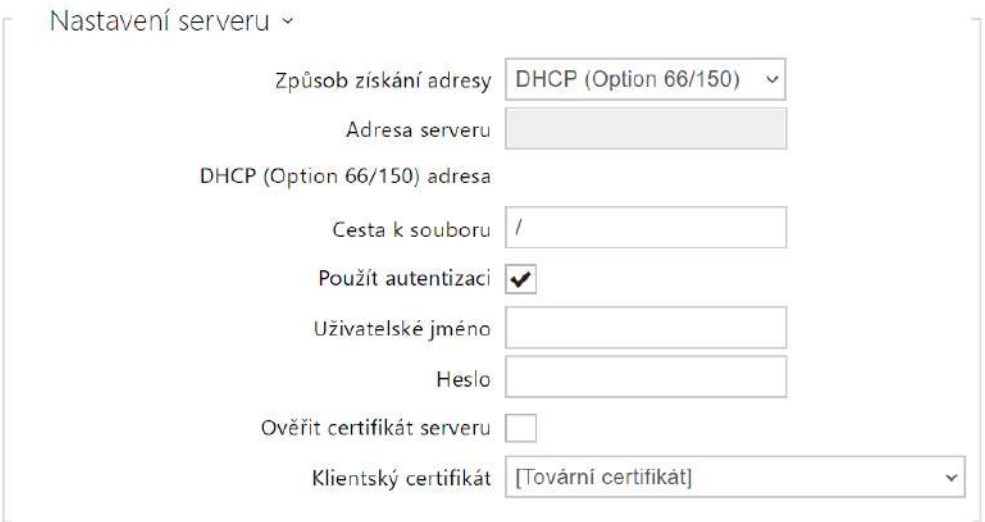
Příklad:

2N Access Unit 2.0 s MAC adresou 00-87-12-AA-00-11 bude stahovat z TFTP serveru soubory s těmito názvy:

- aug2-firmware.bin
- aug2-common.xml
- aug2-00-87-12-aa-00-11.xml



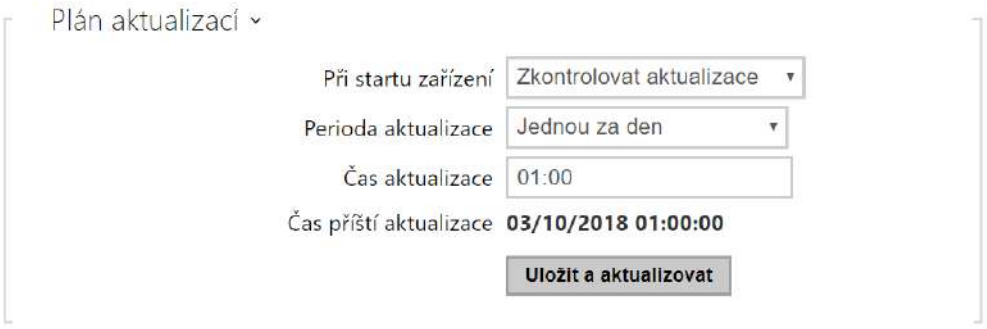
- **Automaticky aktualizovat firmware** – povoluje automatické stahování firmware z TFTP/ HTTP serveru.



- **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 66/150) adresa** – zobrazuje adresu serveru získanou pomocí DHCP Option 66 nebo 150.
- **Cesta k souboru** – nastavuje cestu ke složce s firmwarem. Zadejte / pro hledání model-firmware.bin (konkrétní model) v kořenovém adresáři serveru. Více informací o modelech apod. lze zobrazit v bočním panelu nápovědy (?).
- **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.
- **Ověřit certifikát serveru** – specifikuje sadu certifikátů certifikačních autorit pro ověření platnosti veřejného certifikátu ACS serveru.
- **Klientský certifikát** – specifikuje klientský certifikát a privátní klíč, pomocí kterých se ověřuje oprávnění zařízení komunikovat se ACS serverem.

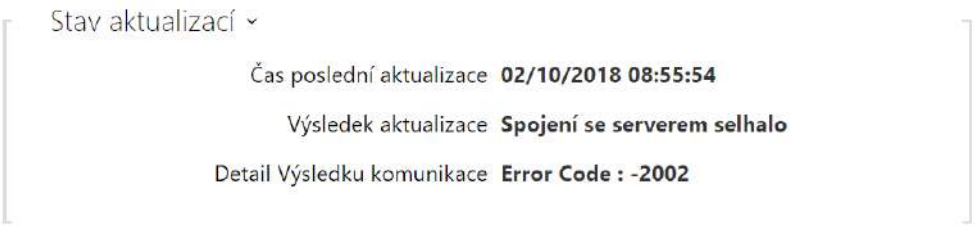
Info

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



- **Při startu zařízení** – povoluje kontrolu anebo provedení aktualizace po každém startu zařízení.
- **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 zařízení 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.



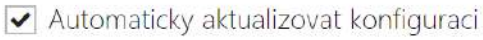
- **Čas poslední aktualizace** – zobrazuje čas naposledy provedené aktualizace.
- **Výsledek aktualizace** – zobrazuje výsledek naposledy provedené aktualizace. Možné hodnoty jsou následující: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Detail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

Výsledek	Popis
Adresa serveru je neplatná	Adresa serveru je neplatná.
Protokol není podporován	Protokol není podporován. Podporovány jsou jen protokoly HTTP(s) a TFTP.
Umístění souboru je neplatné	Umístění daného souboru je neplatné.
Funkce DHCP Option 66 selhala	Nahrávání adresy serveru přes protokol DHCP Option 66 nebo 150 selhalo.
Doménové jméno je neplatné	Doménové jméno serveru je neplatné kvůli nesprávné konfiguraci nebo nedostupnosti DNS serveru.
Server nenalezen	Požadovaný HTTP/TFTP server neodpovídá.
Autentizace selhala	Autentizační data HTTP nejsou správná.
Soubor nenalezen	Soubor nebyl na serveru nalezen.
Požadavek čeká ve frontě...	Žádost o aktualizaci čeká ve frontě.

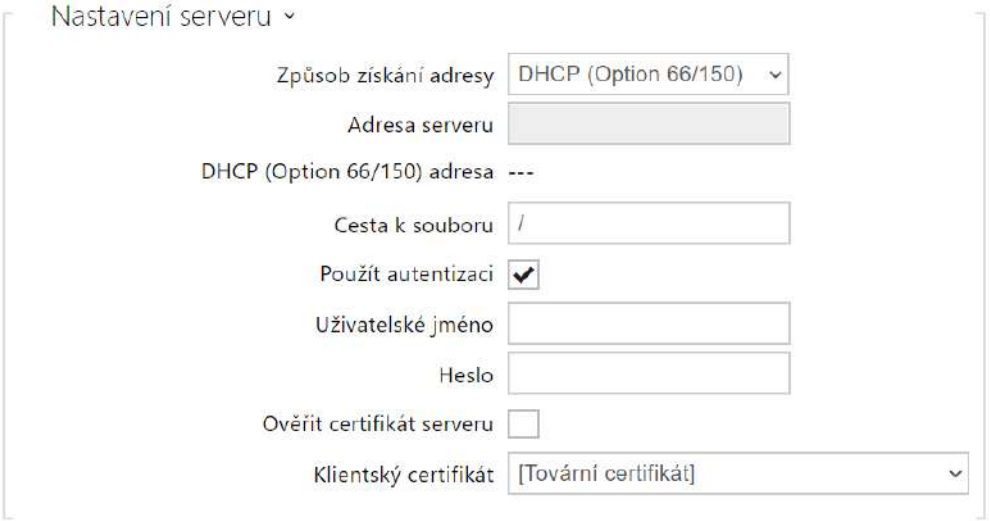
Výsledek	Popis
Probíhá...	Aktualizace probíhá.
Soubor je neplatný	Soubor ke stažení je poškozen nebo nesprávného typu.
Firmware je aktuální	Pokus o aktualizaci firmwaru ukázal, že byla nahrána nejnovější verze firmwaru.
Aktualizace proběhla úspěšně	Aktualizace konfigurace/firmwaru proběhla úspěšně. V případě aktualizace firmwaru bude zařízení za pár sekund restartováno.
Interní chyba	Při stahování souboru došlo k neidentifikované chybě.

Záložka Konfigurace

Na této záložce se nastavuje automatické stahování konfigurace z vámi definovaného serveru. Zařízení v nastavených intervalech stáhne soubor ze serveru a rekonfiguruje se. Při této aktualizaci nedochází k restartu zařízení.

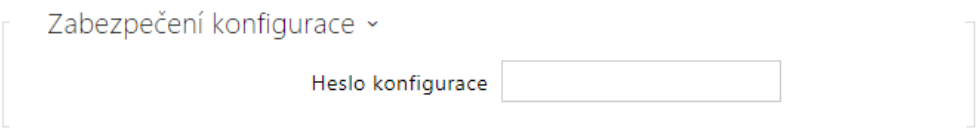


- **Automaticky aktualizovat konfiguraci** – povoluje automatické stahování konfigurace z TFTP/HTTP serveru.

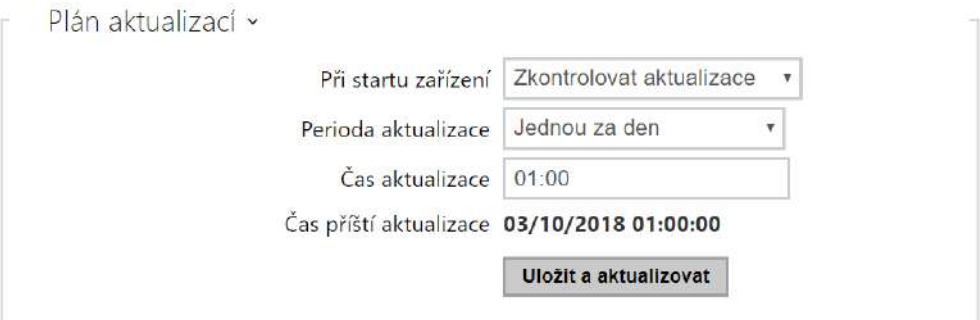


- **Způsob získání adresy** – umožňuje zvolit, zda adresa TFTP/HTTP serveru bude zadána manuálně nebo se použije adresa získaná automaticky z DHCP serveru pomocí parametru Option 66.
- **Adresa serveru** – umožňuje manuálně zadat adresu serveru TFTP (tftp://ip_adresa), HTTP (http://ip_adresa) nebo HTTPS (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. Zařízení 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 zařízení.
- **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.
- **Ověřit certifikát serveru** – specifikuje sadu certifikátů certifikačních autorit pro ověření platnosti veřejného certifikátu ACS serveru.
- **Klientský certifikát** – specifikuje klientský certifikát a privátní klíč, pomocí kterých se ověřuje oprávnění zařízení komunikovat se ACS serverem.

> **Info**
>
> - Zařízení obsahuje Factory Cert certifikát, podepsaný certifikát, který je možné použít např. pro integraci s British Telecom.

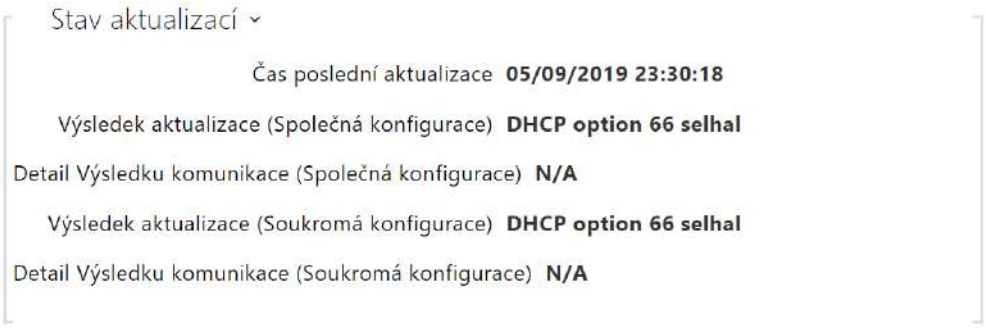


- **Heslo konfigurace** – nastavuje heslo použité pro rozšifrování konfigurace zabezpečené heslem.



- **Při startu zařízení** – povoluje kontrolu anebo provedení aktualizace po každém startu zařízení.

- **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 zařízení nejméně využíváno. 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. Zobrazuje 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.

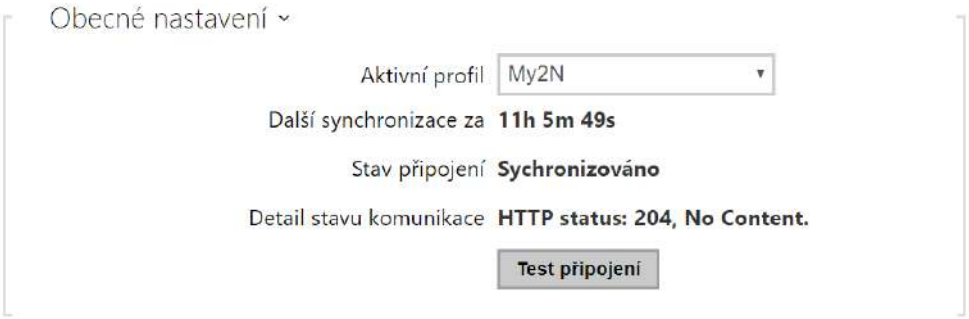
Záložka TR069

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

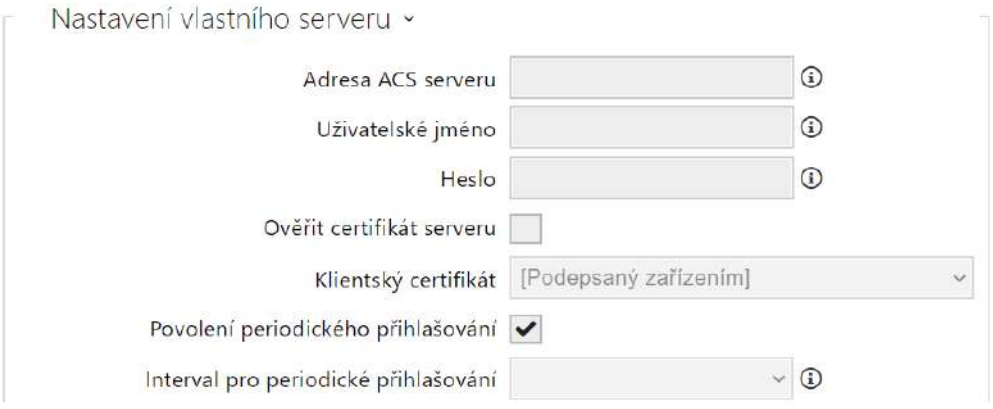
Protokol TR-069 je využíván cloudovou službou My2N. Pro správnou funkci zařízení s My2N je nutné službu TR-069 povolit a parametr aktivní profil nastavit na hodnotu My2N. Poté se zařízení bude periodicky přihlašovat ke službě My2N, která ho může konfigurovat.

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

- **My2N / TR069** – povoluje službu My2N / TR069.

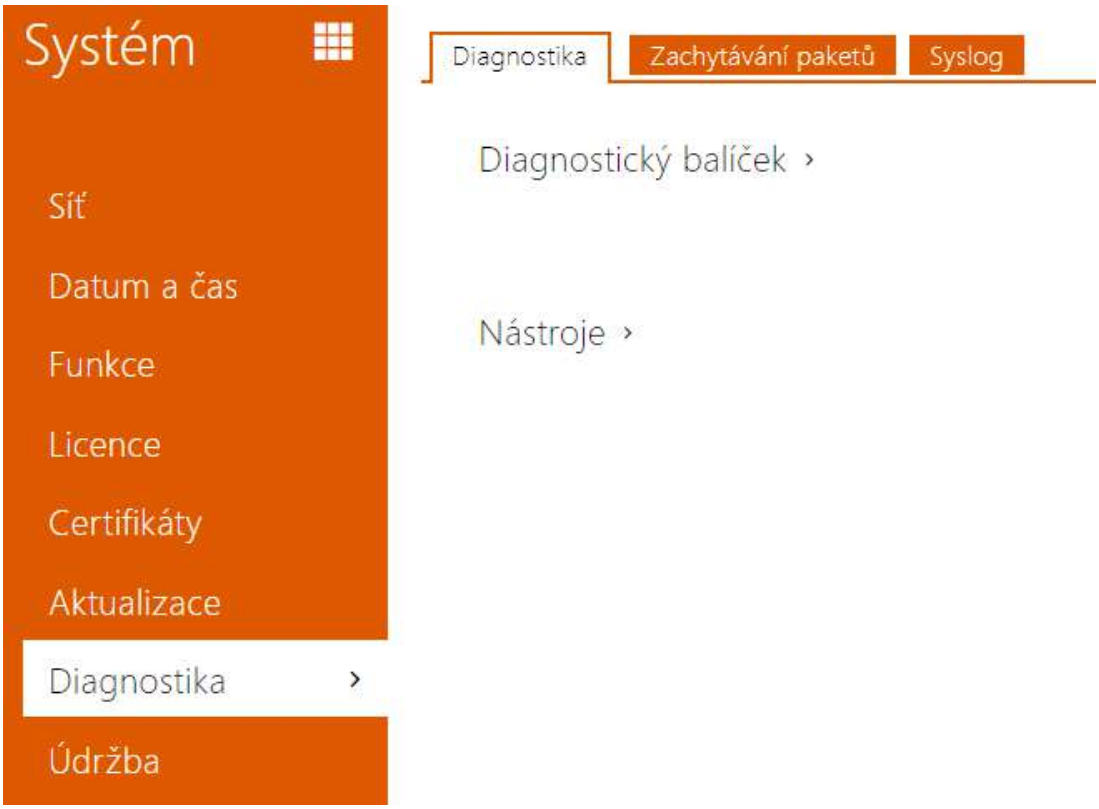


- **Aktivní profil** – umožňuje vybrat jeden z přednastavených profilů (ACS serveru) příp. zvolit vlastní nastavení a připojení k ACS serveru nakonfigurovat ručně.
- **Další synchronizace za** – zobrazuje, za jak dlouho bude zařízení kontaktovat vzdálený ACS server.
- **Stav připojení** – zobrazuje aktuální 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.



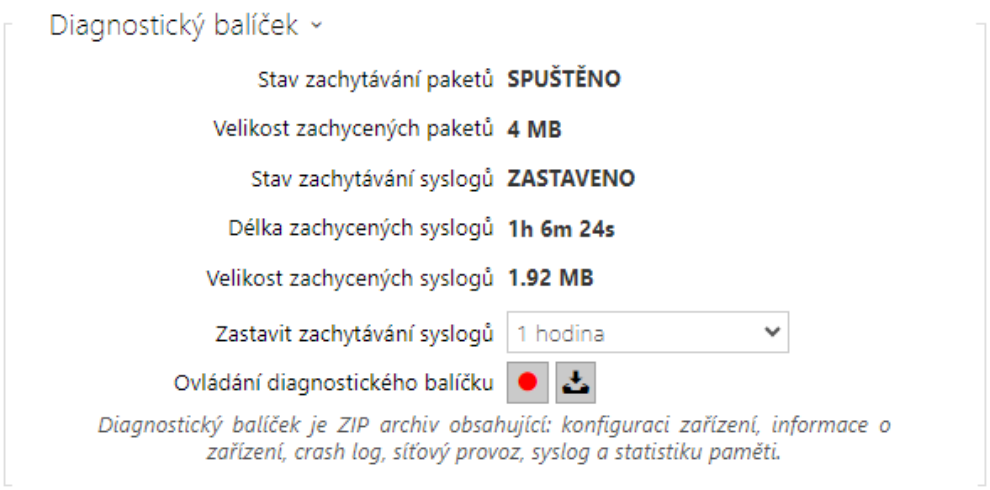
- **Adresa ACS serveru** – nastavuje adresu ACS serveru ve formátu ipadresa[: port], např. 192.168.1.1:7547
- **Uživatelské jméno** – nastavuje uživatelské jméno pro autentizaci zařízení na ACS serveru
- **Heslo** – nastavuje uživatelské heslo pro autentizaci zařízení na ACS serveru
- **Ověřit certifikát serveru** – 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.
- **Klientský certifikát** – specifikuje klientský certifikát a privátní klíč, pomocí kterých se ověřuje oprávnění zařízení komunikovat se ACS serverem. Lze zvolit jednu ze tří sad uživatelských certifikátů a privátních klíčů, viz kapitola Certifikáty.
- **Povolení periodického přihlašování** – povoluje periodické přihlašování zařízení k ACS serveru.
- **Interval pro periodické přihlašování** – nastavuje interval periodického přihlašování k ACS serveru, pokud je povolen pomocí parametru **Povolení periodického přihlašování**.

5.5.7 Diagnostika



Záložka Diagnostika

Rozhraní umožňuje spustit zachytávání diagnostických logů, které je možné následně stáhnout a odeslat Technické podpoře. Zachycené diagnostické logy pomáhají v identifikaci a řešení hlášených problémů. Logy obsahují informace o zařízení, o jeho konfiguraci, o síťovém provoze, crash log a statistiku paměti.



- **Stav zachytávání paketů** – ukazuje, zda je spuštěno zachytávání paketů v záložce Zachytávání paketů.
- **Velikost zachycených paketů** – ukazuje, jaké množství paketů je zachyceno.
- **Stav zachytávání syslogů** – ukazuje, zda je spuštěno zachytávání syslog zpráv v záložce Syslog.
- **Délka zachytávání syslogů** – ukazuje, jak dlouho se zachytávají syslog zprávy v záložce Syslog.
- **Velikost zachycených paketů** – ukazuje, jaké množství syslog zpráv je zachyceno.
- **Zastavit zachytávání syslogů** – nastavuje dobu, po kterou se budou data zachytávat.

Zachytávání se spustí pomocí tlačítka pro nahrávání  . Při opětovném stisku tlačítka pro nahrávání se zachytávání restartuje a začíná běžet znovu. Soubor se zachycenými pakety lze stáhnout pomocí tlačítka  .

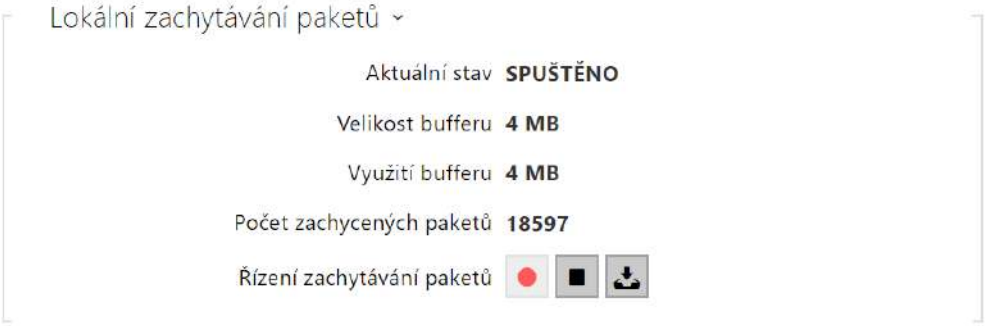
Upozornění

- Spuštění zachytávání diagnostických dat restartuje zachytávání paketů, pokud již běží.
- Pro zvýšení bezpečnosti zašifrujte soubor heslem. Toto heslo bude potřeba při obnově konfigurace k dešifrování souboru a přístupu k jeho obsahu. Ujistěte se, že heslo neztratíte a uložíte ho na bezpečné místo.

- **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 Zachytávání Paketů

V záložce můžete spustit zachytávání příchozích a odchozích paketů na síťovém rozhraní zařízení. Zachycené pakety se mohou ukládat lokálně do bufferu zařízení o velikosti 4 MB nebo vzdáleně do PC uživatele. Soubor se zachycenými pakety lze stáhnout a dále zpracovat např. pomocí aplikace Wireshark (www.wireshark.org).

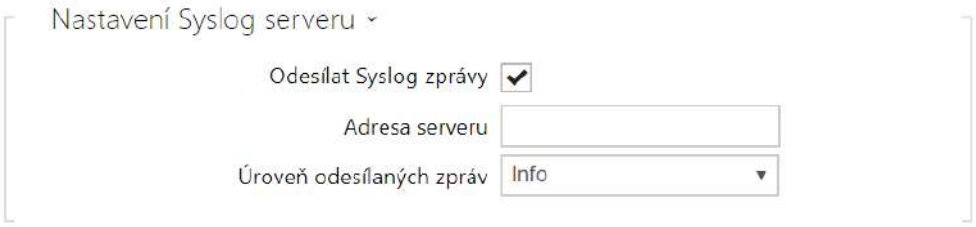


Po zaplnění bufferu při lokálním zachytávání dochází automaticky k přepisu nejstarších uložených paketů. Při lokálním zachytávání paketů doporučujeme snížit přenosovou rychlost video streamu pod hodnotu 512 kbps. Zachytávání můžete spustit pomocí tlačítka  , zastavit pomocí tlačítka  a soubor se zachycenými pakety stáhnout pomocí tlačítka  .

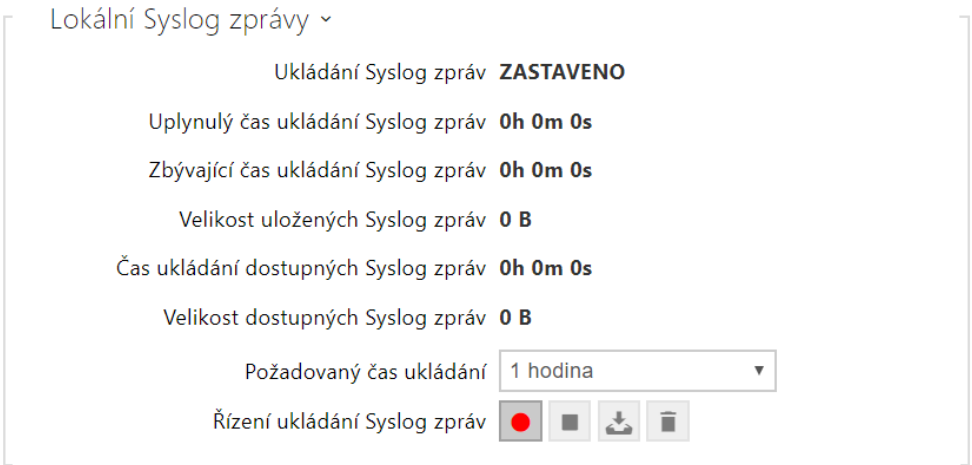
Vzdálené zachytávání můžete spustit pomocí tlačítka . Je potřeba upřesnit čas (s), během kterého se příchozí a odchozí pakety mají zachytávat. Po uplynutí nastavené časové hodnoty bude soubor se zachycenými pakety automaticky stažen do PC uživatele. Zastavit zachytávání lze pomocí tlačítka .

Záložka Syslog

Přístupové jednotky 2N 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 zařízení není nutné tuto službu konfigurovat.

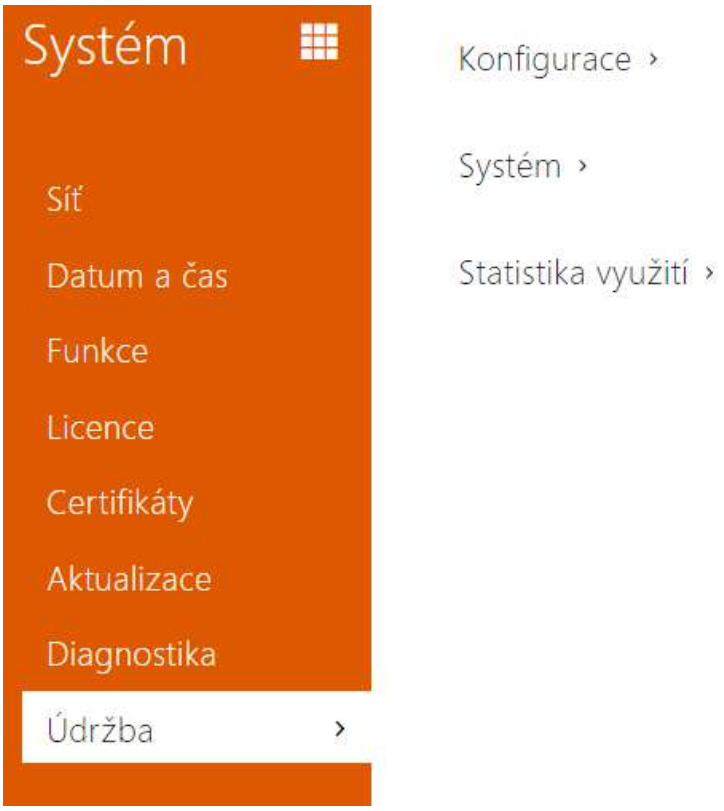


- **Odesílat Syslog zprávy** – povoluje odesílání systémových zpráv Syslog serveru. Pro správnou funkci musí být nastavena platná adresa serveru.
- **Adresa serveru** – nastavuje IP adresu ve formátu "IP[:port]" nebo MAC adresu serveru, na kterém běží aplikace pro záznam syslog zpráv.
- **Úroveň odesílaných 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.

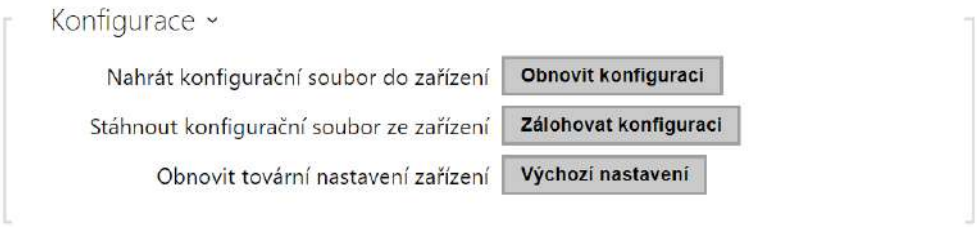


Všeobecný přehled o lokálních syslog zprávách.

5.5.8 Údržba



Toto menu slouží k údržbě konfigurace a firmwaru zařízení. Umožňuje zálohovat a obnovit nastavení všech parametrů, aktualizovat firmware zařízení, příp. nastavit všechny parametry zařízení 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 zařízení můžete zvolit, zda se z konfiguračního souboru mají uplatnit obecná nastavení, importovat nastavení sítě a certifikáty.

  Upozornění

  - Konfigurační soubor má v sobě uložené přihlašovací heslo. Pokud je heslo v souboru nezakódované nebo je nastaveno jako výchozí (2n v zakódované formě), bude nahrána pouze platná část konfigurace. To znamená, že se

konfigurace nahraje, ale heslo se nezmění na hodnotu uvedenou v souboru, ale původní heslo zůstane zachováno.
- Při obnově konfigurace ze zašifrovaného souboru je potřeba zadat heslo k jeho dešifrování.

- **Zálohovat konfiguraci** – slouží k záloze aktuální kompletní konfigurace zařízení. Po stisku tlačítka dojde ke stažení kompletní konfigurace, kterou můžete uložit na svém PC.

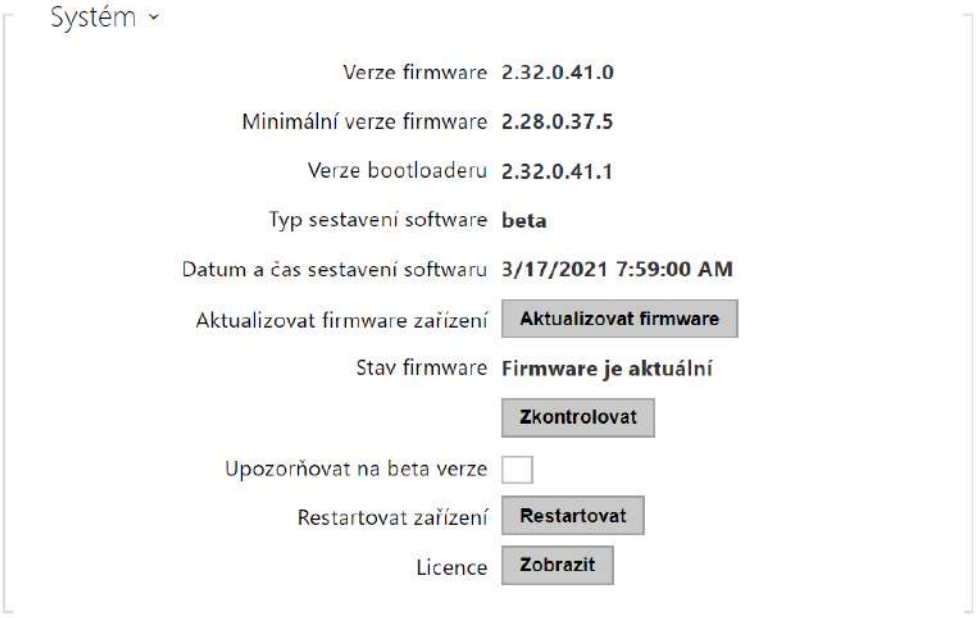
Upozornění

- Konfigurace zařízení může obsahovat citlivé informace, jako jsou údaje uživatelů a přístupová hesla, proto se souborem nakládejte obezřetně.
- Pro zvýšení bezpečnosti zašifrujte soubor heslem. Toto heslo bude potřeba při obnově konfigurace k dešifrování souboru a přístupu k jeho obsahu. Ujistěte se, že heslo neztratíte a uložíte ho na bezpečné místo.

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

Upozornění

- *Obnovení výchozího nastavení vymaže případný nahraný licenční klíč. Je vhodné si ho tedy uschovat zkopírováním na jiné úložiště pro pozdější potřebu.*
- *Licenční klíč není smazán v případě HW resetu (tedy resetu pomocí tlačítka na zařízení), pokud je povolena funkce automatické aktualizace (Systém > Licence), která aktualizuje licenční klíč z Licenčního serveru 2N. Softwarovým resetem dojde k obnovení všech parametrů do výchozího stavu s výjimkou certifikátů a nastavení sítě.*



Poznámka

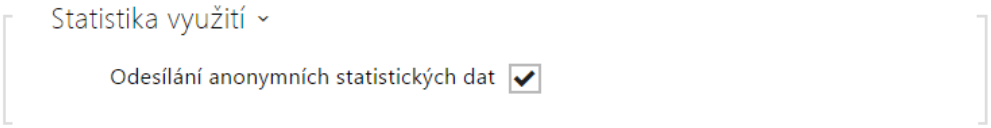
- Funkce, spolehlivost a zabezpečení zařízení jsou závislé na nainstalovaném firmwaru. Pravidelná aktualizace firmwaru na aktuální verzi je součástí podmínek používání výrobku. Chyby, které mohou být způsobeny používáním zastaralé verze firmwaru, nemohou být předmětem reklamace. Aktuální firmware implementuje zkušenosti zákazníků a požadavky v oblasti zabezpečení osobních dat.

- **Aktualizovat firmware** – slouží k nahrání nového firmwaru do zařízení. Po stisku tlačítka se zobrazí dialogové okno, ve kterém můžete vybrat soubor s firmwarem určeným pro dané zařízení. Po úspěšném uploadu firmwaru se zařízení automaticky restartuje. Po restartu je plně k dispozici s novým firmwarem. Celý proces aktualizace trvá necelou minutu. Aktuální verzi firmwaru pro svoje zařízení můžete získat na adrese 2N.com. Aktualizace firmwaru neovlivňuje konfiguraci. Zařízení kontroluje soubor firmwaru a neumožní nahrát nesprávný nebo poškozený soubor.
- **Restartovat** – provede restart zařízení. Celý proces restartu trvá asi 30 s. Po dokončení restartu, kdy zařízení získá IP vlastní adresu, se automaticky zobrazí přihlašovací okno.

Upozornění

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

- **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 je ve shodě s následujícími směrnicemi a předpisy:

- 2014/53/EU pro rádiová zařízení
- 2011/65/EU o omezení používání některých nebezpečných látek v elektrických a elektronických zařízeních
- 2012/19/EU o odpadních elektrických a elektronických zařízeních

Industry Canada

Tento přístroj třídy A je ve shodě s požadavky kanadské normy ICES/NMB-003.

FCC

Toto zařízení bylo certifikováno ve shodě s požadavky pro digitální přístroj třídy A, dle části 15 pravidel FCC.

POZN.: Účelem těchto požadavků je vytvořit rozumnou ochranu proti škodlivému rušení v rezidenčních instalacích. Toto zařízení generuje, používá a může vyzařovat vysokofrekvenční energii, a pokud není instalováno a používáno v souladu s instrukcemi, může škodlivě rušit rádiovou komunikaci.

Nelze však zaručit, že k rušení v dané instalaci nedojde. Pokud toto zařízení způsobí škodlivé rušení rádiového nebo televizního příjmu, což se dá zjistit vypnutím a zapnutím přístroje, může se uživatel toto rušení pokusit opravit některým z následujících způsobů:

- Přesměrovat nebo přemístit přijímací anténu či vedení
- Zvýšit vzdálenost mezi zařízením a přijímačem
- Připojit zařízení do výstupu jiného obvodu napájecí sítě, než do kterého je připojen přijímač
- Požádat o pomoc prodejce nebo zkušeného rádiového/televizního technika

Změny nebo úpravy této jednotky, které nejsou výslovně schváleny stranou odpovědnou za shodu, by mohly vést ke zneplatnění práva uživatele na provoz tohoto zařízení.

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.