



2N[®] Access Unit

Access Control



Konfigurační manuál

Verze: 2.16

www.2n.cz

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



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



2N[®] je registrovaná ochranná známka společnosti 2N TELEKOMUNIKACE a.s. Jména výrobků a jakákoli jiná jména zde zmíněná jsou registrované ochranné známky a/nebo ochranné známky a/nebo značky chráněné příslušným zákonem.



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



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



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

Obsah:

- 1. Popis produktu
- 2. Expresní průvodce základním nastavením
- 3. Licencované funkce
- 4. Signalizace provozních stavů
- 5. Konfigurace přístupového terminálu
 - 5.1 Stav
 - 5.2 Adresář
 - 5.3 Hardware
 - 5.4 Služby
 - 5.5 Systém
- 6. Doplnkové informace
 - 6.1 Řešení problémů
 - 6.2 Směrnice, zákony a nařízení
 - 6.3 Obecné pokyny a upozornění

1. Popis produktu

Dveřní přístupový systém 2N[®] Access Unit je schopen, spolu s doplňkovým software a případně interkomu 2N Helios IP, nabídnout ucelené řešení přístupového systému do jakéhokoliv objektu.

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

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

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

V manuálu jsou použity následující symboly a piktogramy.

Nebezpečí úrazu

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

Varování

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

 **Upozornění**

- **Důležité upozornění.** Nedodržení pokynů může vést k nesprávné funkci zařízení.

 **Tip**

- **Užitečné informace** pro snazší a rychlejší používání nebo nastavení.

 **Poznámka**

- Postupy a rady pro efektivní využití vlastností zařízení.

2. Expresní průvodce základním nastavením

Nastavení připojení k lokální síti

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

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

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

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

 **Tip**

- Instalační manuál: **2.3 Elektrická instalace**

Aktualizace firmware

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

Nastavení spínání elektrického zámku

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

Spínač povolen

Základní nastavení ▾

Režim spínače

Doba sepnutí [s]

Časový profil

Rozlišovat kódy pro sepnutí a vypnutí

Nastavení výstupu ▾

Řízený výstup

Typ výstupu

Kódy pro sepnutí ▾

	KÓD	ČASOVÝ PROFIL
1	<input type="text" value="123"/>	<input type="text" value="[nepoužito]"/>
2	<input type="text"/>	<input type="text" value="[nepoužito]"/>

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

3. Licencované funkce




2N[®] Access Unit má pouze jednu licencovanou funkci a to je NFC.






4. Signalizace provozních stavů

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

Poznámka

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

Tóny	Význam
	<p>Uživatel aktivován</p> <p>Po vložení aktivačního kódu uživatele. Aktivační kód slouží k aktivaci uživatele (pozice v seznamu uživatelů). Nastavení aktivačního kódu je popsáno v kap. Uživatelé.</p>
	<p>Uživatel deaktivován</p> <p>Po vložení deaktivčního kódu uživatele. Deaktivační kód slouží k deaktivaci uživatele (pozice v seznamu uživatelů). Na neaktivního uživatele není možné volat, ale hovor může být případně přesměrován na následníka uživatele, pokud je nastaven. Nastavení deaktivčního kódu je popsáno v kap. Uživatelé.</p>
	<p>Profil aktivován</p> <p>Slouží pro aktivování profilu. Může být například využito k zapnutí vyzvánění celé skupiny uživatelů na telefonní čísla přímo v kanceláři. Nastavení aktivačního kódu je popsáno v kap. Profily.</p>

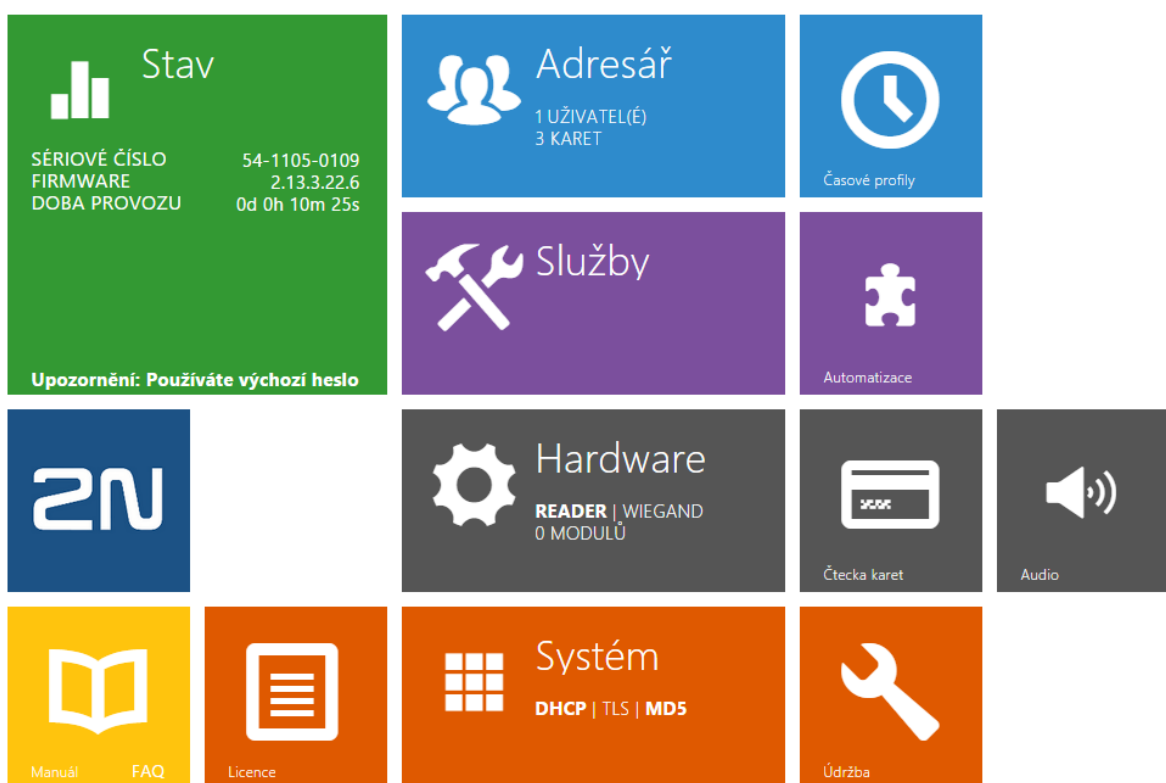
	<p>Profil deaktivován</p> <p>Slouží pro deaktivování profilu. Může být například využito k vypnutí vyzvánění na telefonních číslech v kanceláři a jejich případnému směrování buď na jedno telefonní číslo, např. na vrátnici, či na mobilní telefonní čísla účastníků. Nastavení deaktivčního kódu je popsáno v kap. Profily.</p>
	<p>Vnitřní aplikace spuštěna</p> <p>Po zapnutí napájení nebo po restartu 2N[®] Access Unit je zahájen start vnitřní aplikace 2N[®] Access Unit. Úspěšný start vnitřní aplikace je signalizován touto tónovou kombinací.</p>
	<p>Připojeno do lokální sítě, obdržena IP adresa</p> <p>Po startu vnitřní aplikace se 2N[®] Access Unit přihlašuje do lokální sítě. Úspěšné přihlášení do lokální sítě je signalizováno touto tónovou kombinací.</p>
	<p>Odpojeno od lokální sítě, IP adresa ztracena</p> <p>V případě, že dojde k odpojení UTP kabelu z 2N[®] Access Unit, je tento stav signalizován touto tónovou kombinací.</p>
	<p>Uvedení síťových parametrů do výchozího stavu</p> <p>Po zapnutí napájení je nastaven časový limit 30 sekund pro zadání kódu uvedení síťových parametrů do výchozího stavu. Uvedení síťových parametrů do výchozího stavu je popsáno v kap. Konfigurace zařízení v Instalačním manuálu 2N[®] Access Unit.</p>

5. Konfigurace přístupového terminálu

2N Access Unit CZ | EN | DE | FR | IT | ES | RU

Odhlásit

2N[®] Access Unit



Úvodní přehledová obrazovka

Úvodní stránka se zobrazí po přihlášení do webového rozhraní přístupového terminálu.

Kdykoli se k ní můžete vrátit pomocí tlačítka , umístěného v levém horním rohu dalších stránek webového rozhraní.

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

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

 **Tip**

- Video Tutoriál: **New web interface of 2N® Helios IP intercoms**

Konfigurační menu

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

Stav

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

Adresář

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

Hardware

- **Spínače** – nastavení spínání elektrického zámku, osvětlení apod.
- **Audio** – hlasitosti audia, signalizačních tónu apod.
- **Čtečka karet** – nastavení čtečky karet, Wiegand interface
- **Digitální vstupy** – řízení vstupů
- **Rozšiřující moduly** – nastavení rozšiřujících modulů 2N[®] Access Unit

Služby

- **E - Mail** - umožňuje nastavit zasílání emailů například v případě neplatného pokusu o přístup
- **Automatizace** - flexibilní nastavení přístupového terminálu dle specifických požadavků uživatele
- **HTTP API** - aplikační rozhraní pro ovládání vybraných funkcí interkomu
- **Web server** - nastavení web serveru a přístupového hesla
- **SNMP** - interkomy **2N Helios IP** integrují funkcionalitu umožňující vzdálený dohled interkomů v síti pomocí protokolu SNMP

System

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

5.1 Stav

2N Access Unit
CZ | EN | DE | FR | IT | ES | RU
Odhlásit

← Stav

Zařízení
>

Služby

Licence

Historie přístupů

Události

Informace o zařízení ▾

Název produktu **2N Access Unit**

Verze hardware **586v2**

Sériové číslo **54-0984-0032**

Verze firmware **2.14.0.23.2**

Verze bootloaderu **2.10.0.19.3**

Doba provozu **Od 0h 1m 52s**

Vlastnosti zařízení ▾

Čtečka karet **ANO**

Typ čtečky karet **13.56 MHz NFC**

Počet modulů **0**

Signalizační LED **ANO**

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.

Stav síťového rozhraní ▾

MAC Adresa **7C-1E-B3-01-1F-F6**

Stav DHCP **POUŽITO**

IP Adresa **10.0.27.46**

Maska sítě **255.255.255.0**

Výchozí brána **10.0.27.1**

Primární DNS **10.0.100.102**

Sekundární DNS **10.0.100.5**

Záložka Licence

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

Licencované vlastnosti ▾

Automatické aktualizace	ANO
Rozšířené nastavení spínačů	ANO
HTTP API	ANO
Autentizace pomocí 802.1x	ANO
Automatizace	ANO
Podpora NFC	ANO
Podpora SNMP	ANO
TR069	ANO

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

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

ČAS	TYP UDÁLOSTI	POPIS
14 Dec 15:24:55	OutputChanged	port=led_secured, state=false
14 Dec 15:24:55	OutputChanged	port=led_secured, state=true
14 Dec 15:24:55	CardEntered	direction=any, reader=internal_cardreader, uid=4BCFDC13,
14 Dec 15:24:43	OutputChanged	port=relay1, state=false
14 Dec 15:24:43	SwitchStateChanged	switch=1, state=false
14 Dec 15:24:42	OutputChanged	port=relay1, state=true
14 Dec 15:24:42	SwitchStateChanged	switch=1, state=true
14 Dec 15:24:42	CardEntered	direction=any, reader=internal_cardreader, uid=04030201,
14 Dec 15:24:37	OutputChanged	port=led_secured, state=false
14 Dec 15:24:36	OutputChanged	port=led_secured, state=true
14 Dec 15:24:36	CardEntered	direction=any, reader=internal_cardreader, uid=4BCFDC13,
14 Dec 15:24:19	OutputChanged	port=led_secured, state=false
14 Dec 15:24:18	OutputChanged	port=led_secured, state=true
14 Dec 15:24:18	CardEntered	direction=any, reader=internal_cardreader, uid=1653200A,
14 Dec 15:24:05	OutputChanged	port=relay1, state=false
14 Dec 15:24:05	SwitchStateChanged	switch=1, state=false
14 Dec 15:24:04	OutputChanged	port=relay1, state=true
14 Dec 15:24:04	SwitchStateChanged	switch=1, state=true
14 Dec 15:24:04	CardEntered	direction=any, reader=internal_cardreader, uid=04030201,

5.2 Adresář

Zde je přehled toho, co v kapitole naleznete:

- 5.2.1 Uživatelé
- 5.2.2 Časové profily
- 5.2.3 Svátky
- 5.2.4 Přístupové karty

5.2.1 Uživatelé

2N Access Unit CZ | EN | DE | FR | IT | ES | RU Odhlásit

« < 1 2 3 4 5 6 7 8 9 10 > » Číslo → 🔍

Pozice povolena



Základní informace o uživateli ▾

Jméno	<input type="text"/>
E-Mail	<input type="text"/>
Režim autentizace	Jednoduchý ▾

Seznam uživatelů je jednou z nejdůležitějších částí konfigurace přístupového terminálu. Seznam uživatelů obsahuje důležité informace o uživateli, které zpřístupňují funkce přístupového terminálu, jako jsou, otvírání dveří pomocí RFID karet nebo spínání kódového zámku apod.

Seznam uživatelů je organizovaný jako tabulka obsahující až 1999 pozic – každému uživateli je přiřazena obvykle právě jedna pozice. Seznam uživatelů obsahuje jak informace o uživateli, kteří mají mít přístup do objektu pomocí RFID karty.

U Uživatelů, kteří mají mít přístup do objektu pomocí RFID karty nebo numerického kódu, ponechte telefonní číslo tohoto uživatele nevyplněné a vyplňte pouze ID RFID karty nebo numerický kód pro otvírání dveří. V takovém případě se tlačítko rychlé volby bude chovat jako nenaprogramované (pro volání).

Nastavení seznamu uživatelů nachází v menu **Adresář / Uživatelé**. Pomocí navigačního panelu lze jednoduše volit mezi pozicemi v seznamu. Šipky po stranách lze použít na stránkování. Můžete také zadat přímo číslo pozice a stiskem tlačítka  se přesunout rychle na zadanou pozici. Pokud znáte jméno uživatele, můžete jej v seznamu vyhledat stiskem tlačítka  .

Seznam parametrů

- **Pozice povolena** – Povoluje tuto pozici seznamu.

Pozice povolena


Základní informace o uživateli ▾

Jméno	<input type="text"/>
E-Mail	<input type="text"/>
Režim autentizace	Jednoduchý ▾

- **Jméno** – Jméno uživatele na dané pozici seznamu. Tento parametr je nepovinný a slouží pouze pro jednodušší orientaci a vyhledávání v seznamu.
- **E - mail** - e-mail uživatele, na který může být zaslána informace o zmeškaných nebo všech realizovaných hovorech
- **Režim autentizace** - Umožňuje nastavit režim dvojité autentizace uživatele pomocí karty a zároveň pomocí numerického kódu. Pro sepnutí spínače při zapnuté funkci dvojité aktivace, je potřeba nejprve přiložit platnou kartu uživatele a poté zadat jeden z platných kódů pro sepnutí spínače (do deseti sekund od přiložení karty)


Uživatelské kódy spínačů ▾

	KÓD	ČASOVÝ PROFIL
Spínač 1	<input type="text"/>	[nepoužito] ▾
Spínač 2	<input type="text"/>	[nepoužito] ▾

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

- **Kód** – Umožňuje nastavit soukromý kód uživatele pro sepnutí spínače. Kód může být až 16 znaků dlouhý a může obsahovat pouze číslice 0-9.
- **Časový profil** – Umožňuje přiřadit ke kódu pro sepnutí zámku časový profil a tak řídit jeho platnost. Pokud uvedený profil není aktivní, k sepnutí spínače při zadání kódu nedojde.

Uživatelské karty ▾


ID karty 

Časový profil ▾

Každý z uživatelů přístupového terminálu může mít přiřazenu jednu přístupovou RFID kartu. Více o přístupových kartách a dalších možnostech nastavení viz kapitola **Přístupové karty**.

- **ID karty** – Umožňuje nastavit ID přístupové karty uživatele. Každý uživatel může mít přiřazenu právě jednu přístupovou kartu. 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.
- **Časový profil** – Umožňuje přiřadit k přístupové kartě uživatele časový profil a tak řídit její platnost. Pokud profil není aktivní, přístupová karta uživatele je považována za neplatnou.

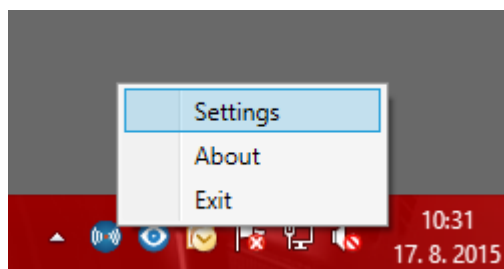
 **Tip**

- ID přístupové karty lze také zadat pomocí externí USB čtečky RFID karet (obj.č. 9137421E).
- Stiskněte tlačítko  a přiložte kartu k externí USB čtečce. Číslo karty se automaticky uloží do editačního pole **ID karty**.
- Ke správné funkci je potřeba nainstalovat ovladač USB čtečky karet, který lze stáhnout ze stránek www.2n.cz.

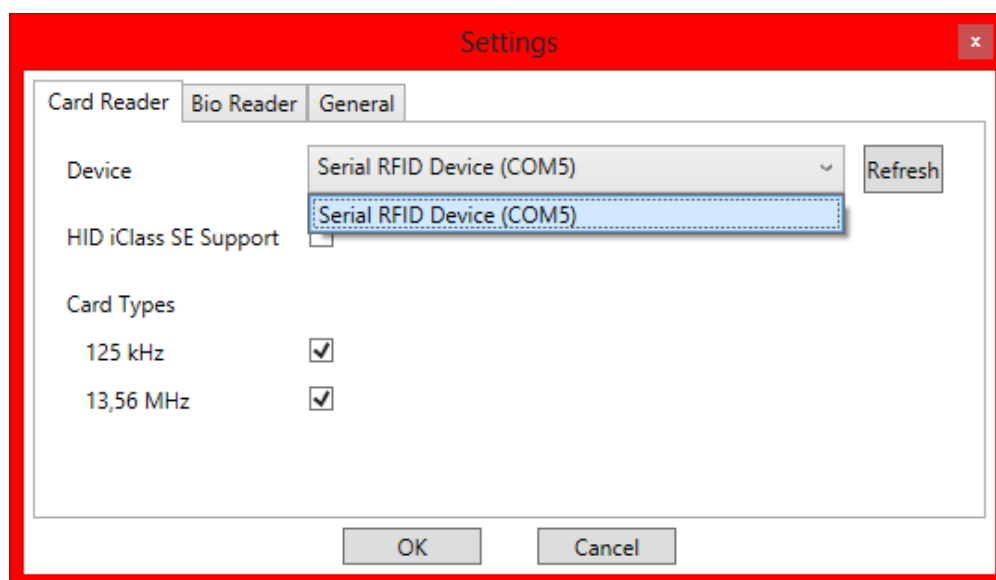
USB RFID čtečka karet

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

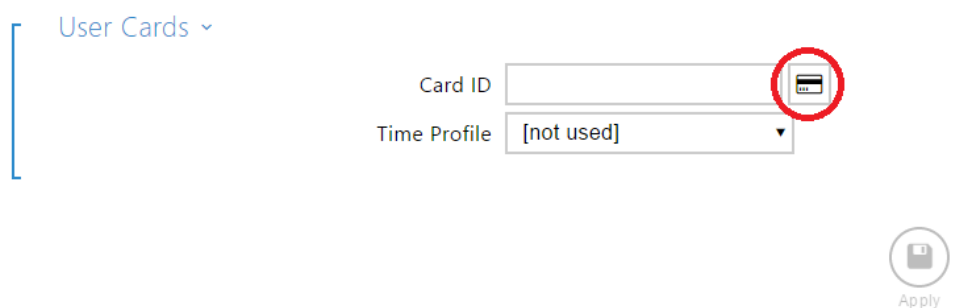
1. Jděte do nastavení 2N Helios IP USB Driver



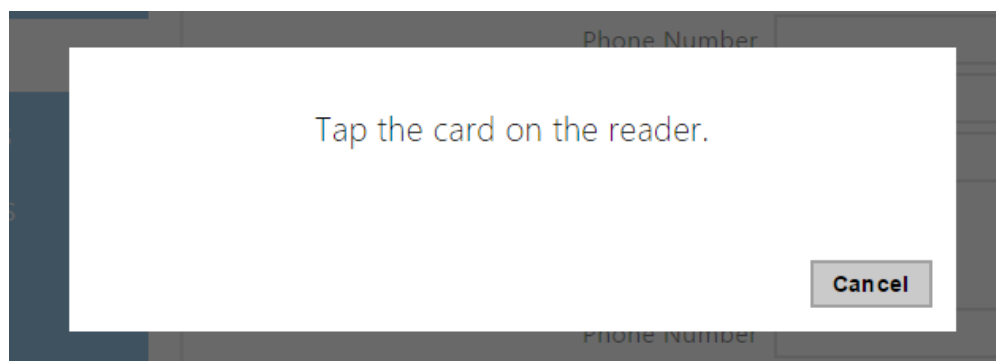
2. Nastavte COM port připojené čtečky



3. Na webu 2N Helios IP u uživatele zmáčkněte tlačítko načtení karty




4. Přiložte kartu na čtečku



5. Karta je načtená

User Cards ▾

Card ID	<input type="text" value="4BD9E903"/>	
Time Profile	<input type="text" value="[not used]"/>	▾

Nezapomeňte konfiguraci uložit.

5.2.2 Časové profily

The screenshot displays the configuration interface for time profiles. On the left, a blue sidebar menu contains icons and labels for 'Adresář', 'Uživatelé', 'Časové profily', 'Svátky', and 'Přístupové karty'. The main area is titled '2N Access Unit' and includes language options (CZ | EN | DE | FR | IT | ES | RU) and a 'Odhlásit' button. A breadcrumb trail shows '1' selected. Below, the 'Základní nastavení' section has a 'Název profilu' text input. The 'Časový plán profilu' section shows a 24-hour timeline for 'Neděle' with a blue bar from 08:00 to 16:00, and for 'Pondělí' with a blue bar from 07:00 to 17:00.

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

- zcela blokovat volání na vybraného uživatele mimo vyhrazený čas
- blokovat volání na vybraná telefonní čísla uživatele mimo vyhrazený čas
- blokovat přístup pomocí RFID karty uživatele mimo vyhrazený čas
- blokovat přístup pomocí vybraného numerického kódu mimo vyhrazený čas
- blokovat sepnutí spínače mimo vyhrazený čas

Každý časový profil definuje dostupnost funkce, se kterou je spojen pomocí týdenního kalendáře. Jednoduše lze nastavit čas od-do a příp. dny v týdnu, kdy má být funkce dostupná. **2N[®] Access Unit** umožňuje vytvořit až 20 různých časových profilů. Dané funkci můžete přiřadit libovolný vytvořený časový profil, viz nastavení Uživatelé, Přístupové karty, Spínače.

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

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

Seznam parametrů

Základní nastavení ▾

Název profilu

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

Časový plán profilu ▾

Neděle

06:00-16:00

Pondělí

07:00-17:00

Úterý

Středa

Čtvrtek

Pátek

Sobota

Svátek

Použit

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).

i 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

2N Helios IP Verso CZ | EN | DE | FR | IT | ES | RU Odhlásit

← Adresář

Uživatelé

Časové profily

Svátky >

Přístupové karty

Svátky ▾

■ Pravidelný svátek ■ Nepravidelný svátek

2016

Leden

Po	Út	St	Čt	Pá	So	Ne
			1	2	3	
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

2017

Únor

Po	Út	St	Čt	Pá	So	Ne
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29						

2018

Březen

Po	Út	St	Čt	Pá	So	Ne
1	2	3	4	5	6	
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

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 5 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 barvou. První kliknutí označí den jako pravidelný svátek, následující kliknutí označí den jako nepravidelný svátek a další kliknutí den ze seznamu svátků vyjme.

5.2.4 Přístupové karty

Každý uživatel přístupového terminálu může mít přiřazenu jednu nebo více přístupových RFID karet. ID přístupové karty se obvykle uvádí v seznamu uživatelů společně s dalšími údaji o uživateli, jako jsou telefonní čísla, e-mail apod. Alternativně je možné karty definovat v seznamu nazvaném Instalované karty. Tento seznam definuje omezený počet karet přiřazených nikoli konkrétnímu uživateli, ale např. návštěvám apod.

Seznam instalovaných karet lze spravovat ručně pomocí konfiguračního rozhraní přístupového terminálu – karty lze přidávat, odebírat, příp. upravovat. Hlavní výhodou tohoto seznamu je však možnost karty přidávat a odebírat bez nutnosti vstupu do konfiguračního rozhraní pouze pomocí tzv. servisní přidávací a odebírací karty. Na rozdíl od seznamu uživatelů, kde lze zadat až 1999 karet, je seznam instalovaných karet omezený pouze na 20 karet.

Pro přidání karty do seznamu přiložte ke čtečce nejprve přidávací kartu a poté kartu, kterou chcete do seznamu přidat. Karta bude do seznamu přidána vždy, pokud ještě není zcela plný a zároveň pokud karta v seznamu ještě není.

Pro odebrání karty ze seznamu přiložte ke čtečce nejprve odebírací kartu a poté kartu, kterou chcete ze seznamu odebrat. Záznam o přiložené kartě bude zrušen a přístup pomocí této karty bude blokován.

Servisní karty jsou dvě běžné karty, pouze vámi vyhrazené pro tento speciální účel. Jejich ID musíte uvést v položkách ID přidávací karty a ID odebírací karty v sekci **Servisní karty**.

ID přístupových karet je sekvence 6–32 znaků z množiny 0–9, A–F (tj. číslo v hexadecimálním tvaru o délce nejméně 24 bitů, nejvýše však 128 bitů). Počet znaků ID přístupové karty je dán typem karty a může se lišit. Platí však, že karty stejného typu mají ID vždy stejně dlouhé.

Jestliže používáte externí čtečku karet připojenou k přístupovému terminálu pomocí rozhraní wiegand, dochází při přenosu ID karty pomocí toho rozhraní ke zkrácení ID na 6 nebo 8 znaků (podle nastavení režimu přenosu). Pokud přiložíte stejnou kartu k

interní čtečce, obdržíte ID kompletní, které je obvykle delší – 8 znaků a více. Posledních 6 příp. 8 znaků ID je však shodných. Toho se využívá při porovnání ID karet s databází v interkomu – pokud porovnávaná ID mají různou délku, porovnávají se od konce a shoda musí být nalezena nejméně v 6 znacích. Pokud jsou ID stejně dlouhá, porovnávají se všechny znaky. Tímto mechanismem je dosaženo vzájemné kompatibility interní a externí čtečky.

Všechny karty přiložené k interní čtečce nebo přijaté pomocí rozhraní wiegand jsou zaznamenávány a posledních 10 přiložených karet si můžete zobrazit v menu **Stav / Historie přístupů**. V seznamu můžete kromě ID karet nalézt také jejich typ, čas přiložení a příp. další informace. V případě malého systému můžete využít pro zadávání ID karet jednoduchý trik – přiložte kartu ke čtečce interkomu a vyhledejte ji v záložce **Historie přístupů**. ID karty označte pomocí myši, 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 přístupového terminálu.


Po přiložení karty k RFID čtečce je ID karty porovnáno s databází karet v přístupovém terminálu. 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** u modulu čtečky karet.


Nastavení přístupových karet se nachází v menu **Adresář / Přístupové karty**..

Seznam parametrů

Záložka Karty


Servisní karty ▾

ID přidávací karty 

ID odebírací karty 

- **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 odebrání ze seznamu instalovaných karet. ID karty je sekvence 6-32 znaků z množiny 0-9, A-F.

Instalované karty ▾

	ID KARTY		ČASOVÝ PROFIL	POPIS
Karta 1	<input type="text"/>		[nepoužito] ▾	<input type="text"/>

- **ID karty** - ID přístupové karty. ID přístupové karty je sekvence 6-32 znaků z množiny 0-9, A-F.
- **Časový profil** - Umožňuje přiřadit k přístupové kartě uživatele časový profil a tak řídit její platnost. Pokud profil není aktivní, přístupová karta uživatele je považována za neplatnou.
- **Popis** - Do tohoto pole můžete uložit libovolnou informaci, jako je např. jméno vlastníka karty apod. Popis se zobrazí při přiložení karty v záložce Záznamy. Popis slouží pouze pro lepší přehled v seznamu karet a na funkci přístupového terminálu nemá vliv.

5.3 Hardware

Zde je přehled toho, co v kapitole naleznete:

- 5.3.1 Spínače
- 5.3.2 Audio
- 5.3.3 Čtečka karet
- 5.3.4 Digitální vstupy
- 5.3.5 Rozšiřující moduly

5.3.1 Spínače

2N Access Unit CZ | EN | DE | FR | IT | ES | RU Odhlásit

← Hardware

- Spínače >
- Audio
- Čtečka karet
- Digitální vstupy
- Rozšiřující moduly

Spínač 1
Spínač 2

Spínač povolen

Základní nastavení ▾

Režim spínače	Monostabilní ▾
Doba sepnutí	1 [s]
Časový profil	[nepoužito] ▾

Rozlišovat kódy pro sepnutí a vypnutí

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

Spínač může být aktivován:

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

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

Pokud je spínač aktivní, lze nastavit:

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

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

Spínač může signalizovat svůj stav pomocí:

- konfigurovatelného pípnutí
- signalizační LED diodou

Seznam parametrů

Spínač povolen

- **Spínač povolen** – Globálně povoluje nebo zakazuje řízení spínače. Pokud spínač není povolen, nelze jej sepnout žádným ze zadaných kódů (včetně uživatelských kódů spínačů), nelze jej aktivovat tlačítkem rychlé volby.

Základní nastavení ▾

Režim spínače	Monostabilní ▾
Doba sepnutí	5 [s]
Časový profil	[nepoužito] ▾
Rozlišovat kódy pro sepnutí a vypnutí	<input type="checkbox"/>

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.
- **Časový profil** – Umožňuje přiřadit spínači časový profil, který povoluje sepnutí spínače. Pokud přiřazený časový profil není aktivní, nelze spínač sepnout pomocí kódu, nelze jej aktivovat hovorem ani tlačítkem rychlé volby.
- **Rozlišovat kódy pro sepnutí a vypnutí** - Umožňuje nastavit režim kódů spínačů, kdy liché kódy (1., 3., atd.) jsou určeny pro sepnutí a sudé kódy (2., 4., atd) jsou pro vypnutí spínače. Tento režim lze použít pouze, pokud je spínač nastaven do bistabilního režimu.

Nastavení výstupu ▾

Řízený výstup	Relay 1 ▾
Typ výstupu	Normální ▾

- **Řízený výstup** – Umožňuje přiřadit spínači elektrický výstup. Lze vybrat mezi všemi dostupnými výstupy příslušného modelu přístupového terminálu – relé, výkonové výstupy, výstupy na rozšiřujících modulech apod. Pokud zvolíte volbu **žádný**, spínač nebude ovládat žádný elektrický výstup, můžete jej stále však použít pro řízení externího zařízení pomocí HTTP příkazů.

- **Typ výstupu** – Pokud používáte 2N[®] Helios IP Bezpečnostní relé, nastavte typ výstupu na hodnotu **security**. V režimu **security** výstup pracuje v inverzním režimu, tj. je stále sepnutý, a modul 2N[®] Helios IP Bezpečnostní relé ovládá pomocí specifické sekvence pulzů. Pokud používáte reverzní zámek dveří (tj. dveře jsou při přivedení napětí na zámek uzamčeny), nastavte typ výstupu na hodnotu **inverzní**.

Kódy pro sepnutí ▾

	KÓD	ČASOVÝ PROFIL
1	<input type="text" value="00"/>	<input type="text" value="[nepoužito]"/>
2	<input type="text" value="1234"/>	<input type="text" value="[nepoužito]"/>
3	<input type="text"/>	<input type="text" value="[nepoužito]"/>

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

- **Kód** – Umožňuje zadat číselný kód spínače. Kód musí obsahovat alespoň dva znaky. Pokud má být kód dostupný z numerické klávesnice přístupového terminálu, doporučujeme použít alespoň čtyři znaky. Kódy 00 a 11 nelze zadávat z numerické klávesnice. Kód se potvrzuje znakem *. Kód může být až 16 znaků dlouhý.
- **Časový profil** – Umožňuje přiřadit ke kódu spínače časový profil a tak řídit jeho platnost

Signalizace stavu ▾

Zvuková signalizace

- **Zvuková signalizace** – Umožňuje nastavit typ zvukové signalizace při sepnutí spínače. Je možné vybrat mezi Krátkým tónem a Dlouhým tónem (po celou dobu sepnutí).

Synchronizace ▾

Synchronizovat [nepoužito] ▾

Zpoždění synchronizace 0 [s]

- **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**.

HTTP Příkazy ▾

Příkaz odeslaný při sepnutí http://192.168.23.66/rele=o

Příkaz odeslaný při vypnutí

- **Příkaz odeslaný při sepnutí** - Umožňuje nastavit příkaz odesílaný externímu zařízení (např. WEB relé) při sepnutí spínače. Příkaz se odesílá pomocí protokolu HTTP (GET request). Příkaz musí být ve tvaru **http://ip_adresa/cesta**. Např. **http://192.168.1.50/relay1=on**.
- **Příkaz odeslaný při vypnutí** - Umožňuje nastavit příkaz odesílaný externímu zařízení (např. WEB relé) při vypnutí spínače. Příkaz se odesílá pomocí protokolu HTTP (GET request). Příkaz musí být ve tvaru **http://ip_adresa/cesta**. Např. **http://192.168.1.50/relay1=off**

 **Tip**

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

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

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

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

5.3.2 Audio

2N Access Unit CZ | EN | DE | FR | IT | ES | RU Odhlásit

Hlasitost signalizace ▾

Hlasitost pípnutí při stisku klávesy	0 dB ▾
Hlasitost varovných tónů	0 dB ▾
Hlasitost signalizace sepnutí spínače	0 dB ▾

Hardware

- Spínače
- Audio >
- Klávesnice
- Čtečka karet
- Digitální vstupy
- Rozšiřující moduly

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

5.3.3 Čtečka karet

2N Access Unit CZ | EN | DE | FR | IT | ES | RU Odhlásit

← Hardware

Spínače

Audio

Čtečka karet >

Digitální vstupy

Rozšiřující moduly

Základní nastavení ▾

Asociovaný spínač

Signalizace čtení karty

Směr

Rozhraní RFID ▾

Povolené typy karet

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

Seznam parametrů

Základní nastavení ▾

Asociovaný spínač

Signalizace čtení karty

Směr

- **Asociovaný spínač** - Umožňuje vybrat spínač aktivovaný po přiložení platné karty. Nastavená hodnota se neuplatní v případě přiložení platné karty uživatele při zároveň nastavené funkci dvojité autentizace tohoto uživatele. V takovém případě se po přiložení platné karty očekává zadání numerického kódu pro sepnutí spínače a tento numerický kód identifikuje následně sepnutý spínač.
- **Signalizace čtení karty** - Nastavuje způsob signalizace přiložené karty. **Úplná** - zvuková signalizace rozlišuje mezi platnou a neplatnou kartou, **Jedno pípnutí** - platná i neplatná karta je signalizovaná jedním pípnutím, **Žádná** - karta není zvukově signalizována.
- **Směr** - Umožňuje nastavit směr pro zaznamenání do systému: **Nespecifikováno** /**Příchod**/**Odchod**. Parametr směr je využíván docházkovým systémem.

Rozhraní RFID ▾

Povolené typy karet MIFARE Mini, MIFARE C ▾

- **Rozhraní RFID** - Umožňuje vybrat povolené typy karet (označením /odznačením).

Rozhraní RFID ▾

Povolené typy karet

MIFARE Mini, MIFARE C ▾	
MIFARE Mini	✓
MIFARE Classic 1k	✓
MIFARE Classic 4k	✓
MIFARE Plus S	✓
MIFARE Plus X	✓
MIFARE Ultralight C	✓
MIFARE DESFire	✓
HID iClass CSN	
Cepas 2.0	✓
Sony Felica	✓
NFC/HCE	✓

5.3.4 Digitální vstupy

2N Access Unit CZ | EN | DE | FR | IT | ES | RU Odhlásit

← Hardware

Spínače

Audio

Čtečka karet

Digitální vstupy >

Rozšiřující moduly

Řízení stavu zabezpečeno ▾

Přiřazený vstup

Režim vstupu

Řízení vstupu REX ▾

Přiřazený vstup

Režim vstupu

Asociovaný spínač

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

Seznam parametrů

Řízení stavu zabezpečeno ▾

Přiřazený vstup

Režim vstupu

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

Řízení vstupu REX ▾

Přiřazený vstup

Režim vstupu

Asociovaný spínač

- **Přiřazený vstup** - Umožňuje určit jeden z logických vstupů (příp. žádný vstup) pro funkci odchodového tlačítka. Aktivace vstupu odchodového tlačítka dojde k sepnutí spínače zvoleného spínače. Doba a způsob sepnutí jsou dány aktuálním nastavením zvoleného spínače.
- **Režim vstupu** - Umožňuje nastavit aktivní úroveň (polaritu) vstupu.
- **Asociovaný spínač** - Umožňuje nastavit jeden ze spínačů aktivovaný zvoleným logickým vstupem.

Ochranný spínač ▾

Přiřazený vstup

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[®] Helios IP HTTP API**).

- **Přiřazený vstup** - Umožňuje vybrat logický vstup, ke kterému je připojen ochranný spínač. Při aktivaci ochranného spínače je signalizována událost **TamperSwitchActivated**.

Stav dveří ▾

Přiřazený vstup

Režim vstupu

Detekce neautorizovaného otevření dveří

Detekce dlouho otevřených dveří

Maximální čas otevření dveří [s]

Modely vybavené alespoň jedním digitálním vstupem umožňují připojit snímač otevřených dveří a signalizovat neautorizované otevření dveří, příp. nezavření dveří do nastavené doby po otevření. Události jsou zapisovány do logu, který lze vyčítat pomocí HTTP API (viz manuál **2N[®] Helios IP HTTP API**).

- **Přiřazený vstup** - Umožňuje přiřadit jeden z logických vstupů snímači otevřených dveří.
- **Režim vstupu** - Umožňuje nastavit aktivní úroveň (polaritu) vstupu.
- **Detekce neautorizovaného otevření dveří** - Povoluje signalizaci události **UnauthorizedDoorOpen**. Tato událost je signalizována v případě, že dveře byly otevřeny v době, kdy nebyl aktivován elektrický zámek.
- **Detekce dlouho otevřených dveří** - Povoluje signalizaci události **DoorOpenTooLong**. Tato událost je signalizována v případě, že dveře jsou blokovány v otevřeném stavu po delší než nastavenou dobu.
- **Maximální čas otevření dveří** - Nastavuje maximální dobu otevření dveří, po které je detekován stav dlouho otevřených dveří.

i Poznámka

Menu Digitální vstupy je dostupné na modelech:

- *2N[®] Helios IP Verso*
- *2N[®] Helios IP Vario* a *2N[®] Helios IP Force* pokud jsou vybaveny interní čtečkou karet
- *2N[®] Access Unit*

5.3.5 Rozšiřující moduly

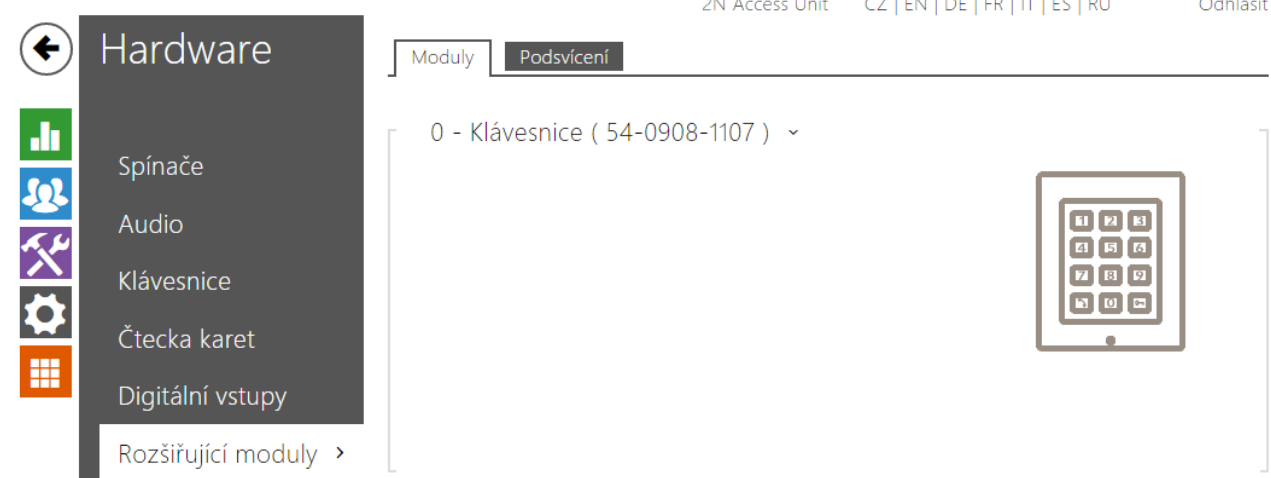
W

2N Access Unit CZ | EN | DE | FR | IT | ES | RU Odhlásit

Hardware

Moduly Podsvícení

0 - Klávesnice (54-0908-1107) ▾



The screenshot shows a web-based configuration interface. On the left, a dark grey sidebar contains a 'Hardware' menu with several icons and labels: a bar chart, 'Spínače', 'Audio', 'Klávesnice', 'Čtečka karet', 'Digitální vstupy', and 'Rozšiřující moduly >'. The main content area has a breadcrumb trail 'Moduly Podsvícení' and a dropdown menu '0 - Klávesnice (54-0908-1107) ▾'. To the right of the dropdown is a small image of a keypad device.

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

- modul s pěti tlačítky
- modul klávesnice
- modul infopanelu
- modul čtečky karet
- modul vstupů a výstupů
- modul rozhraní Wiegand

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.

i 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.*

Podsvícení

Na této záložce lze nastavit nezávisle úroveň podsvícení jmenovek, tlačítek apod. a úroveň svitu signalizačních LED.

Moduly Podsvícení

Řízení jasu podsvícení ▾

Jas ve dne 100% ▾

Řízení jasu signalizačních LED ▾

Jas ve dne 100% ▾

i Poznámka

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


Konfigurace modulu tlačítek

3 - Tlačítka (54-0769-0005) ▾

Funkce tlačítek

Tlačítka rychlé volby 2 - 6 ▾

Vlastní konfigurace




- Funkce tlačítek – Umožňuje přiřadit tlačítkům pozice v seznamu uživatelů.

Konfigurace modulu klávesnice

2 - Klávesnice (54-0770-0014) ▾


Vlastní konfigurace



- Žádné parametry tohoto modulu nejsou v současné době zveřejněny.

Konfigurace modulu infopanelu

0 - Infopanel (54-0771-0147) ▾



- Žádné parametry tohoto modulu nejsou v současné době zveřejněny.

Konfigurace modulu čtečky karet

1 - Čtečka karet 125 kHz (54-0968-0001) ▾


Jméno modulu

Formát HID karet
 ▾

Asociovaný spínač
 ▾

Signalizace čtení karty
 ▾

Přeposílat na wiegand výstup
 ▾



- **Jméno modulu** - Nastavuje název modulu. Název modulu se používá při logování událostí čtečky karet.
- **Formát HID karet** - Umožňuje nastavit typ HID Prox karty, který bude čtečkou akceptován. Čtečka podporuje v jednom okamžiku pouze jeden typ karty. Pokud nepoužíváte HID Prox karty, nastavení se neuplatní. (Parametr je dostupný pouze u čtečky 125kHz karet).
- **Asociovaný spínač** - Nastavuje číslo spínače aktivovaného po přiložení platné RFID karty. Nastavená hodnota se neuplatní v případě přiložení platné karty uživatele při zároveň nastavené funkci dvojité autentizace tohoto uživatele. V takovém případě se po přiložení platné karty očekává zadání numerického kódu pro sepnutí spínače a tento numerický kód identifikuje následně sepnutý spínač.
- **Signalizace čtení karty** - Nastavuje způsob signalizace přiložené karty. **Úplná** - zvuková signalizace rozlišuje mezi platnou a neplatnou kartou, **Jedno pípnutí** - platná i neplatná karta je signalizovaná jedním pípnutím, **Žádná** - karta není zvukově signalizována.
- **Přeposílat na wiegand výstup** - Nastavuje skupinu wiegand výstupů, na kterou budou přeposílány všechny přijaté ID RFID karet.

Konfigurace modulu vstupů a výstupů

4 - Modul I/O (54-0761-0006) ▾

Jméno modulu



Vlastní konfigurace


- **Jméno modulu** - Nastavuje název modulu. Název modulu se používá při specifikaci vstupu nebo výstupu v objektech SetOutput, GetInput a InputChanged v nastavení 2N[®] Helios IP 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 přístupový terminál 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[®] Helios IP Automation.

2 - Modul Wiegand (54-0983-0013) ▾

Jméno modulu



Asociovaný spínač

Spínač 1 ▾

Formát přijímaných kódů

Wiegand 26 bit ▾

Signalizace čtení karty

Úplná ▾

Přeposílat na wiegand výstup

Skupina 1 ▾

Formát vysílaných kódů

Wiegand 26 bit ▾

Facility kód

Skupina wiegand výstupu

Skupina 1 ▾

- **Jméno modulu** - Nastavuje název modulu. Název modulu se používá při specifikaci vstupu nebo výstupu v objektech SetOutput, GetInput a InputChanged v nastavení 2N[®] Helios IP Automation.
- **Asociovaný spínač** - Nastavuje číslo spínače aktivovaného po přijetí platného kódu.
- **Formát přijímaných kódů** - Nastavuje formát přijímaných kódů (Wiegand 26, 32, 37 a RAW).

- **Signalizace čtení karty** - Nastavuje způsob signalizace přijatého kódu. **Úplná** - zvuková signalizace rozlišuje mezi platným a neplatným kódem, **Jedno pípnutí** - platný i neplatný kód je signalizován jedním pípnutím, **Žádná** - přijatý kód není zvukově signalizován.
- **Přeposílat na wiegand výstupu** - Nastavuje skupinu wiegand výstupů, na kterou budou přeposílány všechny přijaté kódy.
- **Formát vysílaných kódů** - Nastavuje formát vysílaných 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.

5.4 Služby

Zde je přehled toho, co v kapitole naleznete:

- 5.4.1 E-Mail
- 5.4.2 Automatizace
- 5.4.3 HTTP API
- 5.4.4 Web server
- 5.4.5 SNMP

5.4.1 E-Mail

2N Access Unit CZ | EN | DE | FR | IT | ES | RU Odhlásit

Služby

SMTP E-Mail - karta

Povolení služby SMTP

Nastavení SMTP serveru ▾

Adresa serveru

Port serveru

Přihlášení k SMTP serveru ▾

E-Mail >

Automatizace

HTTP API

Web Server

SNMP

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

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

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

Poznámka

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

Seznam parametrů

Záložka SMTP

Povolení služby SMTP

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

Nastavení SMTP serveru ▾

Adresa serveru

Port serveru

- **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.

Přihlášení k SMTP serveru ▾

Jméno uživatele

Heslo

Osobní certifikát ▾

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

Obecné nastavení emailů ▾

Adresa odesilatele

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

Rozšířené nastavení ▾

Doručit do ▾

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

Diagnostika odesílání e-mailů ▾

Adresa testovacího e-mailu:

Uložit a otestovat

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

Záložka E-Mail - karta

Na této záložce lze nastavit odesílání e-mailů v okamžiku přiložení RFID karty ke čtečce karet.

Nastavení odesílání e-mailů ▾

Posílat e-mail při

Posílat e-mail při – Umožňuje nastavit odesílání e-mailu po přiložení RFID karty. Lze volit mezi následujícími možnostmi:

- Neplatné přístupy – e-mail bude odeslán po přiložení neplatné karty
- Všechny přístupy – e-mail bude odeslán po přiložení libovolné karty
- Neodesílat email – e-maily nebudou odesílány

Šablona zprávy ▾

Výchozí příjemce

Předmět

Obsah zprávy

```
<h1> Hello, $User$ </h1> <br>
<h2> You had a card reader event at:
$DateTime$ </h2>
<p>
<h2> The Authorisation ID is
$AuthId$</h2>
<p>
<b> This mail is generated
automatically by the $HeliosId$ device.
Do not reply to this please.
</b>
```

- **Výchozí příjemce** – Interkom odesílá zprávy na e-mailovou adresu uvedenou u příslušného uživatele (v případě přiložení platné karty uživatele). V případě neplatné karty, příp. pokud u uživatele není uveden e-mail, zpráva je odeslána na e-mail uvedený v tomto poli. Pokud příjemce není uveden ani v telefonním seznamu, ani v tomto poli, e-mail nebude odeslán. V případě potřeby lze zadat více e-mailových adres oddělených čárkou.
- **Předmět** – Nastavuje předmět odesílané e-mailové zprávy.
- **Obsah zprávy** – Umožňuje upravit obsah odesílané zprávy. V textu lze používat formátovací značky jazyka HTML. Do textu lze vkládat speciální zástupné symboly pro jméno uživatele, datum a čas, identifikaci zařízení příp. identifikátor přiložené karty. Tyto zástupné symboly budou před odesláním zprávy nahrazeny aktuální hodnotou. Viz následující tabulka zástupných symbolů:

1. \$User\$ Jméno volaného uživatele
2. \$DateTime\$ Aktuální datum a čas
3. \$AuthId\$ Identifikátor přiložené karty
4. \$HeliosId\$ Identifikace interkomu

Přílohy zprávy ▾

Přiložit snímek

Rozlišení snímku

- **Přiložit snímek** – Povoluje odeslání přílohy s jedním snímkem z kamery sejmutých v okamžiku přiložení karty.
- **Rozlišení snímků** – Nastavuje rozlišení odesílaného snímku.

5.4.2 Automatizace

2N Access Unit CZ | EN | DE | FR | IT | ES | RU Odhlásit

← Služby

Automatizace >

HTTP API

Web Server

SNMP

Funkce 1 Funkce 2 Funkce 3 Funkce 4 Funkce 5

Funkce povolena

Stav funkce ▾

Funkce povolena **Spuštěno**

Definice funkce ▾

ID	TYP OBJEKTU	PARAMETRY
1	None ▾	

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

Detailní popis funkce a konfigurace **2N[®] Helios IP Automation** je k dispozici v manuálu Konfigurace **2N[®] Helios IP Automation**.

5.4.3 HTTP API

Služby

Účet 1

Účet 2

Účet 3

Účet 4

Účet 5

Služby HTTP API ▾

SLUŽBA	POVOLENÍ	TYP PŘIPOJENÍ	AUTENTIZACE
System API	<input checked="" type="checkbox"/>	Zabezpečené (TLS) ▾	Digest ▾
Switch API	<input checked="" type="checkbox"/>	Zabezpečené (TLS) ▾	Digest ▾
I/O API	<input checked="" type="checkbox"/>	Zabezpečené (TLS) ▾	Digest ▾
Audio API	<input checked="" type="checkbox"/>	Zabezpečené (TLS) ▾	Digest ▾
Logging API	<input checked="" type="checkbox"/>	Zabezpečené (TLS) ▾	Digest ▾

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

2N[®] Helios IP HTTP API je podle funkce rozděleno do následujících služeb:

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

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

Detailní popis funkce a nastavení HTTP API je k dispozici v manuálu 2N[®] Helios IP HTTP API.

Služby

Účet 1

Účet 2

Účet 3

Účet 4

Účet 5

 Účet povolen

Nastavení uživatele ▾

Jméno uživatele

admin

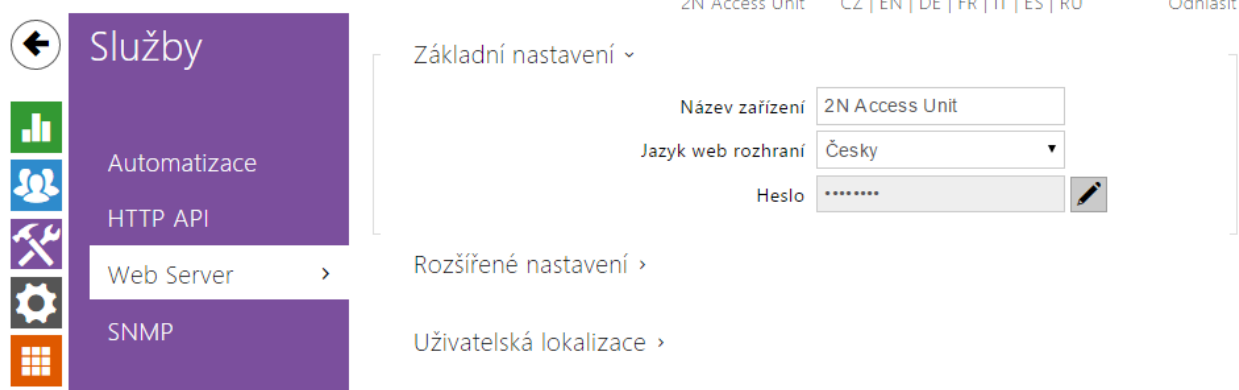
Heslo

••

Uživatelská práva ▾

POPIS	SLEDOVÁNÍ	ŘÍZENÍ
Přístup k systému	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Přístup k V/V	<input type="checkbox"/>	<input type="checkbox"/>
Přístup ke spínačům		<input type="checkbox"/>
Přístup k audio		<input checked="" type="checkbox"/>
Přístup k UID (karty a wiegand)	<input type="checkbox"/>	
Přístup ke klávesnici	<input type="checkbox"/>	

5.4.4 Web server



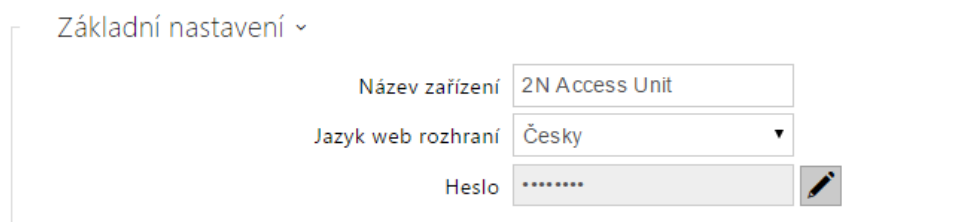
Přístupové terminály **2N[®] Access Unit** lze konfigurovat pomocí běžného prohlížeče, který přistupuje k web serveru integrovanému v přístupovém terminálu. Pro komunikaci mezi prohlížečem a přístupovým terminálem se používá zabezpečený protokol HTTPS. Pro přihlášení k přístupovému terminálu je nutné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

Služba web server je využívána i dalšími funkcemi interkomu:


1. a. HTTP příkazy pro ovládání spínačů, viz kapitola Spínače
- b. Událost Event.HttpTrigger ve **2N[®] Helios IP 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 Helios IP Manager, 2N Helios IP Network Scanner apod.)
- **Jazyk web rozhraní** – Nastavuje výchozí jazyk po přihlášení k administračnímu web serveru. Jazyk webového rozhraní můžete kdykoli dočasně změnit pomocí tlačítek v horní liště stránky.





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

Rozšířené nastavení ▾

HTTP Port	<input type="text" value="80"/>
HTTPS Port	<input type="text" value="443"/>
HTTPS osobní certifikát	<input type="text" value="Self Signed"/> ▾
Povolit vzdálený přístup	<input checked="" type="checkbox"/>

- **HTTP port** – Nastavuje komunikační port web serveru pro komunikaci pomocí nezabezpečeného protokolu HTTP. Změna portu se projeví až po restartu přístupového terminálu.
- **HTTPS port** – Nastavuje komunikační port web serveru pro komunikaci pomocí zabezpečeného protokolu HTTPS. Změna portu se projeví až po restartu přístupového terminálu.
- **Osobní certifikát** – Nastavuje uživatelský certifikát a privátní klíč, pomocí kterých se provádí šifrování komunikace mezi HTTP serverem přístupového terminálu a webovým prohlížečem na straně uživatele. Lze zvolit jednu ze tří sad uživatelských certifikátů a privátních klíčů, viz kapitola Certifikáty, nebo ponechat nastavení **Self Signed**, kdy se použije automaticky vygenerovaný certifikát vytvořený při prvním spuštění zařízení.
- **Povolit vzdálený přístup** – Umožňuje povolit vzdálený přístup k web serveru přístupového terminálu z IP adres mimo lokální síť.

Uživatelská lokalizace ▾

SOUBOR	VELIKOST	
Originální jazyk	130 kB	
Uživatelský jazyk	N/A	  

- **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.

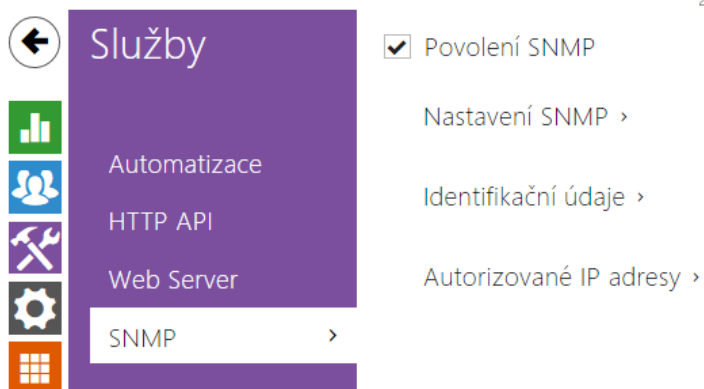
```
<?xml version="1.0" encoding="UTF-8"?>
<strings language="English" languageshort="EN">
  <!-- Global enums-->
  <s id="enum/error/1">Invalid value!</s>
  <s id="enum/bool_yesno/0">NO</s>
  <s id="enum/bool_yesno/1">YES</s>
  <s id="enum/bool_user_state/0">ACTIVE</s>
  <s id="enum/bool_user_state/1">INACTIVE</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 nepravujte hodnoty atributů **id**. Jméno jazyka dané atributem **language** elementu **<strings>** bude uvedeno ve volbách parametru Jazyk web rozhraní. Zkratka jména jazyka daná atributem **languageshort** elementu **<strings>** bude uvedena v seznamu jazyku v horním pravém rohu okna a bude sloužit k rychlému přepínání mezi jazyky.

5.4.5 SNMP

2N Access Unit CZ | EN | DE | FR | IT | ES | RU

Odhlásit



Služby

- Automatizace
- HTTP API
- Web Server
- SNMP >

Povolení SNMP

Nastavení SNMP >

Identifikační údaje >

Autorizované IP adresy >

Přístupové terminály 2N[®] Access Unit integrují funkcionalitu umožňující vzdálený dohled přístupových terminálu v síti pomocí protokolu SNMP. Interkomy podporují SNMP protokol verze 2c.

Seznam parametrů

Povolení SNMP

- **Povolení SNMP** - Umožňuje zapnutí této funkce

Nastavení SNMP >

Identifikátor komunity

IP adresa pro trapy

Stáhnout soubor MIB

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

Identifikační údaje ▾

Kontakt	<input type="text"/>
Název	<input type="text"/>
Umístění	<input type="text"/>

- **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).

Autorizované IP adresy ▾

IP adresa 1	<input type="text"/>
-------------	----------------------

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

5.5 Systém

Zde je přehled toho, co v kapitole naleznete:

- 5.5.1 Síť
- 5.5.2 Datum a čas
- 5.5.3 Licence
- 5.5.4 Certifikáty
- 5.5.5 Aktualizace
- 5.5.6 Syslog
- 5.5.7 Údržba

5.5.1 Síť

2N Access Unit CZ | EN | DE | FR | IT | ES | RU Odhlásit

← Systém

Síť >

Datum a čas

Licence

Certifikáty

Aktualizace

Syslog

Údržba

Základní **802.1x** Trace

Použít DHCP server

Manuální nastavení ▾

Statická IP adresa

Síťová maska

Výchozí brána

Primární DNS

Sekundární DNS

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

Tip

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

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

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

Seznam parametrů

Použít DHCP server

- **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.

Manuální nastavení ▾

Statická IP adresa	192.168.33.79
Síťová maska	255.255.255.0
Výchozí brána	192.168.1.1
Primární DNS	192.168.23.5
Sekundární DNS	

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

Záložka 802.1x

Identita interkomu ▾

Identita zařízení

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

MD5 autentizace ▾

MD5 autentizace povolena

Heslo

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

TLS autentizace ▾




TLS autentizace povolena

Certifikát certifikační autority

Osobní certifikát

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

Záložka Trace

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




Stav zachytávání paketů ▾

Aktuální stav **SPUŠTĚNO**

Velikost bufferu **4096 kB**

Využití bufferu **4096 kB**

Počet zachycených paketů **30666**

Řízení zachytávání paketů   

5.5.2 Datum a čas

2N Access Unit CZ | EN | DE | FR | IT | ES | RU Odhlásit

← **Systém**

Síť

Datum a čas >

Licence

Certifikáty

Aktualizace

Syslog

Údržba

Aktuální čas ▾

Aktuální čas zařízení **15/12/2015 07:48:26**

Synchronizovat s prohlížečem

Časová zóna ▾

Časová zóna (UTC+01:00) Europe/Paris ▾

Pravidlo časové zóny

NTP server ▾

Použít NTP server

Adresa NTP serveru time.nist.gov

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

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

i Poznámka

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

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

Seznam parametrů

Aktuální čas ▾

Aktuální čas zařízení **15/12/2015 07:48:43**

Synchronizovat s prohlížečem

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

Časová zóna ▾

Časová zóna (UTC+01:00) Europe/Paris ▾

Pravidlo časové zóny

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

NTP server ▾

Použít NTP server

Adresa NTP serveru time.nist.gov

Stav času z NTP **Není seřízen**

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

5.5.3 Licence

The screenshot shows the 'Licence' menu on the left with options: Síť, Datum a čas, Licence, Certifikáty, Aktualizace, Syslog, and Údržba. The 'Licence' option is selected. The main content area shows the 'Nastavení licence' configuration page with the following details:

- Sériové číslo: **54-0984-0032**
- Licenční klíč:
- Platný licenční klíč: **NE**

Navigation links include 'Stav licence >' and 'Trial licence >'.

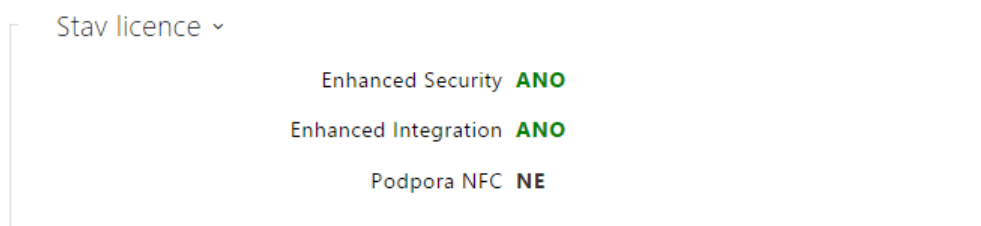
Některé funkce 2N[®] Access Unit jsou dostupné pouze po zadání platného licenčního klíče. Seznam možností licencování přístupových terminálů naleznete v kapitole Licencované funkce.

Seznam parametrů

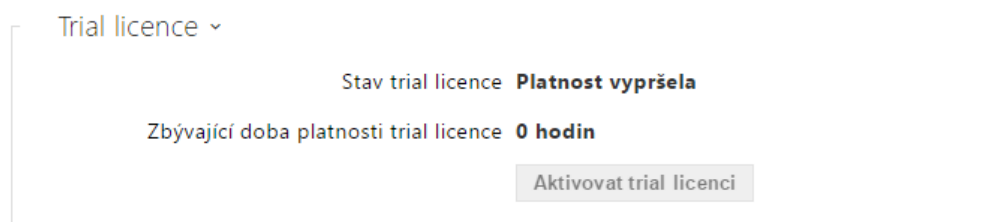
The detailed view of the 'Nastavení licence' configuration page shows the following parameters:

- Sériové číslo: **54-0984-0032**
- Licenční klíč:
- Platný licenční klíč: **NE**

- **Licenční klíč** – Umožňuje vložit platný licenční klíč.
- **Platný licenční klíč** – Zobrazuje, zda vložený licenční klíč je platný.



- **Enhanced Security** – Zobrazuje, zda jsou k dispozici funkce aktivované licencí Enhanced Security.
- **Enhanced Intergration** – Zobrazuje, zda jsou k dispozici funkce aktivované licencí Enhanced Integration.
- **Podpora NFC** – Zobrazuje, zda je k dispozici funkce NFC.



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

5.5.4 Certifikáty

2N Access Unit CZ | EN | DE | FR | IT | ES | RU Odhlásit

← **Systém**

Sít

Datum a čas

Licence

Certifikáty >

Aktualizace

Syslog

Údržba

Certifikáty certifikačních autorit ▾

IDENTITA CA	VYDAVATELE	PLATNOST DO	
(1)			x
(2)			x
(3)			x

Osobní certifikáty >

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

Služby přístupového terminálu, které využívají protokol TLS:

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

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

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

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

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

i Poznámka

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



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

Certifikáty certifikačních autorit ▾

	IDENTITA CA	VYDAVATELE	PLATNOST DO		
(1)				x	📁
(2)				x	📁
(3)				x	📁

Osobní certifikáty ▾

	IDENTITA CA	VYDAVATEL	PLATNOST DO		
(1)				x	📁
(2)				x	📁
(3)				x	📁

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

5.5.5 Aktualizace

The screenshot displays the web interface for configuring a 2N Access Unit. On the left is a navigation menu under the heading "Systém" (System), with "Aktualizace" (Updates) selected. The main content area shows the "Konfigurace" (Configuration) section for "TR069". A checkbox "Automaticky aktualizovat firmware" (Automatically update firmware) is checked. Below this is a "Nastavení serveru" (Server settings) section with the following fields:

- Způsob získání adresy (Address acquisition method): Manuální nastavení (Manual setting)
- Adresa serveru (Server address): tftp://10.0.27.238
- DHCP (Option 66/150) adresa (DHCP address): <none>
- Cesta k souboru (File path): /
- Použít autentizaci (Use authentication): checked
- Uživatelské jméno (Username):
- Heslo (Password):

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

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

Záložka Firmware

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

2N[®] Access Unit očekává na serverech soubory s názvy:

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

MODEL v názvu souboru specifikuje model interkomu:

1. au - 2N[®] Access Unit

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

Příklad:

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

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

Záložka Konfigurace

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

Seznam parametrů

Automaticky aktualizovat firmware

- **Automaticky aktualizovat firmware/konfiguraci** - Povoluje automatické stahování firmware/konfigurace z TFTP/HTTP serveru.

Automaticky aktualizovat firmware

Nastavení serveru ▾

Způsob získání adresy

Adresa serveru

DHCP (Option 66/150) adresa

Cesta k souboru

Použít autentizaci

Uživatelské jméno

Heslo

- **Způsob získání adresy** - Umožňuje zvolit, zda adresa TFTP/HTTP serveru bude zadána manuálně nebo se použije adresa získaná automaticky z DHCP serveru pomocí parametru Option 66.
- **Adresa serveru** - Umožňuje manuálně zadat adresu serveru TFTP (`tftp://ip_adresa`), HTTP (`http://ip_adresa`) nebo HTTPS (`https://ip_adresa`).
- **DHCP (Option 66) adresa** - Zobrazuje adresu serveru získanou pomocí DHCP Option 66 nebo 150.
- **Cesta k souboru** - Nastavuje adresář příp. předponu názvu souboru s firmware nebo konfigurací na serveru. Přístupový terminál očekává soubory s názvy `au_firmware.bin`, `au-common.xml` a `au-MACADDR.xml`.
- **Použít Autentizaci** - Umožňuje zadat uživatelské jméno a heslo pro přístup k serveru.

Plán aktualizací ▾

Při startu zařízení ▾

Perioda aktualizace ▾

Čas aktualizace

Čas příští aktualizace **16/12/2015 01:00:00**

- **Při startu zařízení** - Povoluje kontrolu anebo provedení aktualizace po každém startu přístupového terminálu.
- **Perioda aktualizace** - Nastavuje periodu provádění aktualizace. Lze nastavit provádění jednou za hodinu, den, týden a měsíc.
- **Čas aktualizace** - Umožňuje nastavit čas ve formátu HH:MM, kdy se má aktualizace pravidelně provádět. Takto lze nastavit provádění aktualizace v době, kdy je přístupový terminál nejméně využíván. Parametr se neuplatní, pokud perioda aktualizace je nastavena na dobu kratší než jeden den.
- **Čas příští aktualizace** - Zobrazuje čas naplánovaného provedení další aktualizace.

Stav aktualizací ▾

Čas poslední aktualizace **15/12/2015 01:00:00**

Výsledek aktualizace **Server není dostupný**

- **Čas poslední aktualizace** - Zobrazuje čas naposledy provedené aktualizace.
- **Výsledek aktualizace** - Zobrazuje výsledek naposledy provedené aktualizace. Možné hodnoty jsou následující:

Výsledek	Popis
Probíhá...	Aktualizace právě probíhá
Aktualizováno	Konfigurace/firmware byl bezchybně aktualizován. V případě stažení firmware dojde během několika sekund k restartu zařízení.
Firmware je aktuální	Byl proveden pokus o stažení nového firmware a bylo zjištěno, že firmware zařízení je aktuální.

Výsledek	Popis
Server není dostupný	Nepodařilo se načíst adresu serveru pomocí DHCP Option 66 nebo 150.
Neplatné doménové jméno	Doménové jméno serveru není platné, příp. DNS server je špatně nakonfigurován nebo není dostupný.
Server není dostupný	Dotazovaný HTTP/TFTP server neodpovídá.
Stahování selhalo	Při stahování souboru nastala dále nespecifikovaná chyba.
Soubor nenalezen	Soubor na serveru nebyl nalezen.
Soubor není platný	Stahovaný soubor je poškozen nebo není správného typu.

Záložka My2N / TR069

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

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

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

My2N / TR069 povoleno

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

Obečné nastavení ▾

Aktivní profil

Další synchronizace za **0h 1m 30s**

Stav připojení **Připraveno**

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

Nastavení My2N ▾

My2N ID

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

Nastavení vlastního serveru ▾

Adresa ACS serveru	<input type="text"/>	i
Uživatelské jméno	<input type="text"/>	i
Heslo	<input type="password"/>	i
Certifikát certifikační autority	<input type="text" value="Nepoužito"/>	▾
Osobní certifikát	<input type="text" value="Self Signed"/>	▾
Povolení periodického přihlašování	<input checked="" type="checkbox"/>	i
Interval pro periodické přihlašování	<input type="text"/>	i

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

5.5.6 Syslog

2N Access Unit CZ | EN | DE | FR | IT | ES | RU Odhlásit

← **Systém**

Sít

Datum a čas

Licence

Certifikáty

Aktualizace

Syslog >

Údržba

Odesílat Syslog zprávy

Nastavení Syslog ▾

Adresa serveru

Úroveň odesílaných zpráv

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

Seznam parametrů

Odesílat Syslog zprávy

- **Odesílat Syslog zprávy** – Povoluje odesílání systémových zpráv Syslog serveru. Pro správnou funkci musí být nastavena platná adresa serveru.

Nastavení Syslog ▾

Adresa serveru

Úroveň odesílaných zpráv

- **Adresa serveru** – IP/MAC adresa serveru, na kterém běží aplikace pro záznam systémových hlášení.
- **Úroveň odesílaných zpráv** – Nastavuje úroveň podrobnosti odesílaných zpráv.

5.5.7 Údržba

2N Access Unit CZ | EN | DE | FR | IT | ES | RU Odhlásit

←

Systém

Sít

Datum a čas

Licence

Certifikáty

Aktualizace

Syslog

Údržba >

Konfigurace ▾

Nahrát konfigurační soubor do zařízení Obnovit konfiguraci

Stáhnout konfigurační soubor ze zařízení Zálohovat konfiguraci

Obnovit tovární nastavení zařízení Výchozí nastavení

System ▾

Verze firmware **2.12.0.21.1**

Verze bootloaderu **2.10.0.19.3**

Typ sestavení software **alpha_58f19f9bc93239...**

Datum a čas sestavení softwaru **3/19/2015 16:19:07**

Aktualizovat firmware zařízení Aktualizovat firmware

Restartovat zařízení Restartovat

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

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

Upozornění

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

- **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 přístupového terminálu můžete zvolit, zda se z konfiguračního souboru má uplatnit nastavení síťových parametrů a nastavení připojení k SIP ústředně.
- **Výchozí nastavení** - slouží k nastavení všech parametrů přístupového terminálu do výchozího stavu s výjimkou parametrů nastavení sítě. Pokud chcete přístupový terminál uvést do úplného výchozího stavu, použijte příslušnou propojku nebo tlačítko reset, viz instalační manuál k přístupovému terminálu.

 **Upozornění**

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

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

6. Doplnkové informace

Zde je přehled toho, co v kapitole naleznete:

- 6.1 Řešení problémů
- 6.2 Směrnice, zákony a nařízení
- 6.3 Obecné pokyny a upozornění

6.1 Řešení problémů



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

6.2 Směrnice, zákony a nařízení

2N[®] Access Unit splňuje všechny požadavky následujících směrnic, zákonů a nařízení.

Zákon č. 22/1997 Sb. ze dne 24. ledna 1997 o technických požadavcích na výrobky a o změně a doplnění některých zákonů.

Nařízení vlády č. 426/2000 Sb., kterým se stanoví technické požadavky na rádiová a na koncová telekomunikační zařízení.

Nařízení vlády č. 17/2003 Sb., kterým se stanoví technické požadavky na elektrická zařízení nízkého napětí.

Nařízení vlády č. 616/2006 Sb., kterým se stanoví technické požadavky na výrobky z hlediska jejich elektromagnetické kompatibility.

Směrnice Evropského parlamentu a Rady 1999/5/ES rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody.

Směrnice Rady 2004/108/ES ze dne 15. prosince 2004 o sblížování právních předpisů členských států týkajících se elektromagnetické kompatibility.

Směrnice Rady 2006/95/ES ze dne 12. prosince 2006 o harmonizaci právních předpisů členských států týkajících se elektrických zařízení určených pro užívání v určených mezích napětí.

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

Nařízení Evropského parlamentu a Rady (ES) č. 1907/2006 ze dne 18. prosince 2006 o registraci, hodnocení, povolování a omezování chemických látek, o zřízení Evropské agentury pro chemické látky, o změně směrnice 1999/45/ES a o zrušení nařízení Rady (EHS) č. 793/93, nařízení Komise (ES) č. 1488/94, směrnice Rady 76/769/EHS a směrnic Komise 91/155/EHS, 93/67/EHS, 93/105/ES a 2000/21/ES.

Směrnice Evropského parlamentu a Rady 2012/19/ES ze dne 4. července 2012 o odpadních elektrických a elektronických zařízeních (OEEZ).

Nařízení Komise (ES) č. 1275/2008, ze dne 17. prosince 2008, kterým se provádí směrnice Evropského parlamentu a Rady 2005/32/ES, pokud jde o požadavky na ekodesign z hlediska spotřeby elektrické energie elektrických a elektronických zařízení určených pro domácnosti a kanceláře v pohotovostním režimu a ve vypnutém stavu.

6.3 Obecné pokyny a upozornění

Před použitím tohoto výrobku si prosím pečlivě přečtete 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, instalací, 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 výrobcí, 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.



2N TELEKOMUNIKACE a.s.

Modřanská 621, 143 01 Prague 4, Czech Republic

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

E-mail: sales@2n.cz

Web: www.2n.cz

v2.16