KONFIGURAČNÍ MANUÁL

Colias CSG-3xx

CSG-355 • CSG-365

CS-TECH

Konfigurační manuál vytváří CS-Tech s.r.o. v rámci svých možností a své kapacity. Vyhrazujeme si právo změnit obsah této příručky bez předchozího upozornění.

CS-Tech s.r.o. nenese odpovědnost za škody vzniklé nesprávným použitím nebo v kombinaci s necertifikovanými produkty. Podmínky použití jsou uvedené v Rychlé příručce, jež je součástí balení každého dodávaného zařízení.

Toto zařízení obsahuje software využívající komponenty šířené pod licencemi GNU GPL v2.0, GNU LGPL v2.1, Mozilla Public License 2.0, Apache License 2.0 a pod různými licencemi typu BSD. Seznam všech použitých open-source komponent spolu s úplnými texty licencí je dostupný v samotném zařízení. Najdete jej na stránce **Licenses** v sekci **Status** hlavního menu webového rozhraní.

V souladu s podmínkami licencí **GPL** a **LGPL** nabízíme každému uživateli tohoto zařízení možnost získat kompletní odpovídající zdrojové kódy těchto komponent, včetně všech změn provedených společností CS-Tech s.r.o. Zdrojové kódy jsou k dispozici zdarma (nejvýše za náklady na fyzickou distribuci) po dobu nejméně **tří let** od uvedení tohoto zařízení na trh.

V případě zájmu o zdrojové kódy nás kontaktujte na adrese:

obchod@cs-tech.cz

Obsah

Přílohy

ČÁST I

Úvodní informace

1. Před prvním přihlášením

DŮRAZNÉ VAROVÁNÍ

Než zařízení spustíte a začnete jej konfigurovat, ujistěte se, že je všechno správně zapojeno. Veškeré informace související s uvedením do provozu naleznete v uživatelském manuálu k danému zařízení.

1.1 Způsoby konfigurace zařízení

Zařízení nabízí dvě možnosti, které mohou být využity pro jeho konfiguraci:

- **Grafické rozhraní** dostupné prostřednictvím běžného webového prohlížeče. Jedná se o variantu, které je věnována tato příručka.
- **Příkazový řádek** dostupný přes SSH (Secure Shell, zabezpečený protokol pro vzdálenou správu). Podrobný popis všech příkazů, které lze pro konfiguraci zařízení použít, je uveden v samostatném dokumentu.

DOPORUČENÍ

Během konfigurace v grafickém rozhraní doporučujeme mít ve webovém prohlížeči povolený JavaScript. V opačném případě nebude dostupné ověřování správnosti dat vkládaných do určitých polí a některé další funkce.

1.2 Návrat k továrnímu nastavení

K tomuto účelu je na předním panelu zařízení k dispozici resetovací tlačítko (označené jako *RST*). Použít ho lze následujícími způsoby:

1. **Restart zařízení**
   - Stiskněte krátce tlačítko (**méně než čtyři sekundy**) a dojde k restartování zařízení. Veškerá uživatelská konfigurace zůstane zachována.
2. **Návrat k výchozímu továrnímu nastavení**
   - Podržte tlačítko stisknuté **déle než čtyři sekundy**. Zařízení se restartuje a vrátí konfiguraci do výchozího nastavení (včetně návratu k výchozímu heslu, které je uvedené na výrobním štítku).
   - Podržte tlačítko **stisknuté během zapnutí napájení**. Dojde ke kompletní obnově továrního nastavení zařízení (vymaže se kompletně vše včetně nainstalovaných softwarových modulů).
3. **Probuzení zařízení z režimu spánku**
   - Pokud se zařízení nachází v režimu spánku, dojde po krátkém stisknutí *RST* tlačítka k jeho probuzení.

Tabulka níže názorně ukazuje, co nastane při provedení jednotlivých typů resetů zařízení. Sloupce s označením A až C mají následující význam:

A Stisknuté RST tlačítko po dobu menší než čtyři sekundy.

B Stisknuté RST tlačítko po dobu delší než čtyři sekundy.

C Stisknuté RST tlačítko během zapnutí napájení.

Akce	A	B	C
Obnovení výchozí konfigurace firmwaru	✘	✔	✔
Obnovení výchozí konfigurace softwarových modulů	✘	✔	✔
Smazání všech softwarových modulů	✘	✘	✔
Smazání perzistentního logu (trvalých záznamů)	✘	✘	✔
Smazání shromážděných dat	✘	✘	✔
Restart zařízení	✔	✔	✘

Tabulka 1: Reakce na reset zařízení

2. První přihlášení

2.1 Výchozí tovární nastavení

Před zahájením konfigurace zařízení Colias CSG-3xx je třeba znát jeho výchozí nastavení uvedené v následující tabulce.

Položka	Hodnota
Uživatelské jméno	admin
Uživatelské heslo	*Uvedeno na produktovém štítku*
ETH0: IP adresa	192.168.1.1
ETH0: Síťová maska	255.255.255.0
ETH0: DHCP server	Enabled

Tabulka 2: Výchozí tovární nastavení

DŮLEŽITÁ INFORMACE

Ve výchozím nastavení jsou na zařízení povolena pouze rozhraní **Ethernet 0** a **Cellular**. Zároveň jsou standardně povoleny služby **HTTPS**, **DHCP** a **DNS**, které jsou dostupné z rozhraní Ethernet 0.

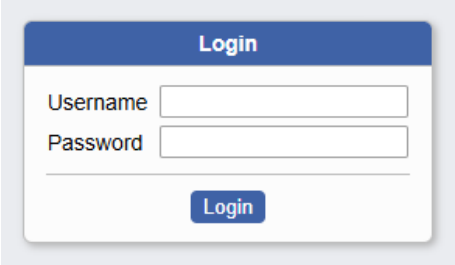
2.2 Přihlášení k webovému rozhraní

Chcete-li se přihlásit do webového rozhraní zařízení, postupujte podle následujících kroků.

1. Připojte počítač ethernetovým kabelem k portu **ETH0**.
2. Otevřete webový prohlížeč na svém počítači a do adresního řádku zadejte IP adresu ve tvaru **192.168.1.1**. Je možné využít také doménové jméno **device.home.arpa**.
3. Poté se k zařízení přihlaste pomocí výchozího uživatelského jména a hesla (viz výše).

POZNÁMKA

V síťovém nastavení počítače musí buď být aktivní DHCP nebo je nutné ručně nastavit IP adresu v rozsahu sítě **192.168.1.0/24**.



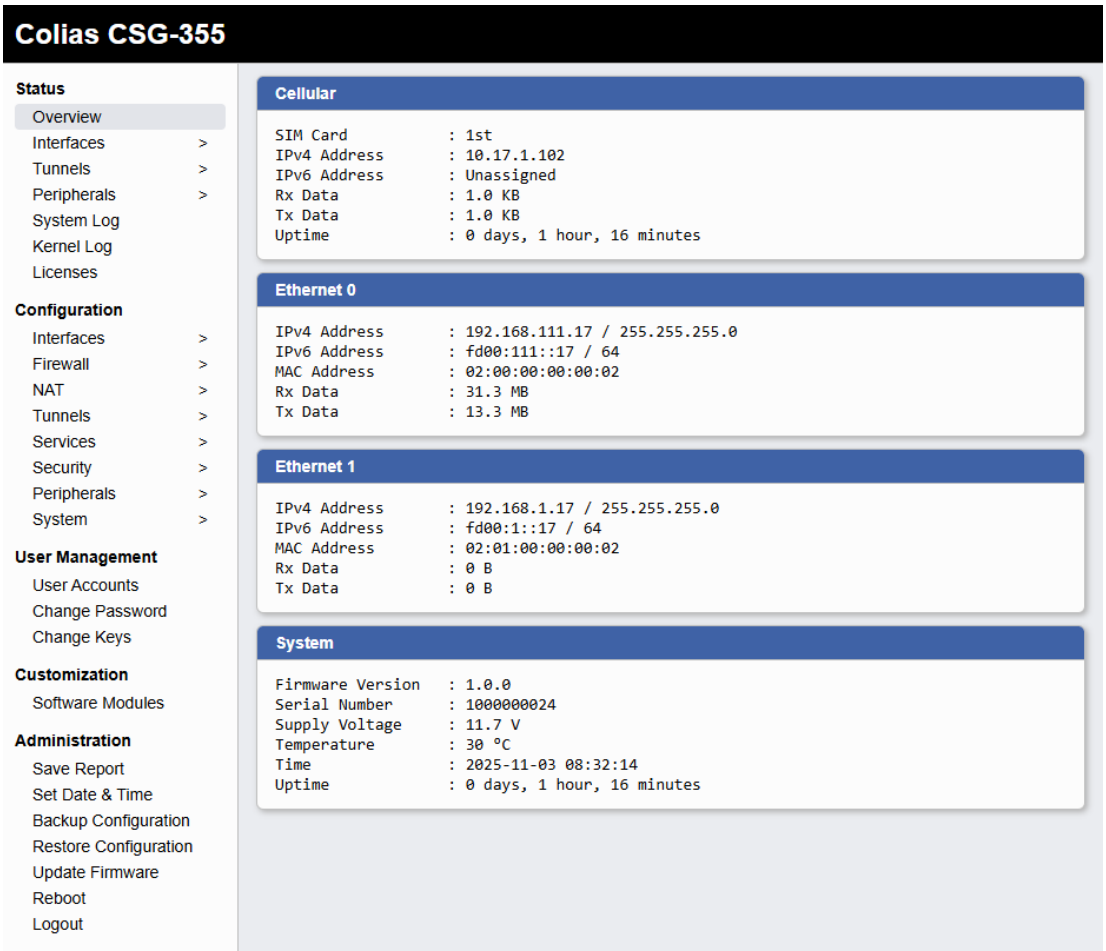
Obrázek 1: Přihlašovací stránka

DŮRAZNÉ VAROVÁNÍ

Důrazně doporučujeme po prvním přihlášení změnit své přihlašovací heslo (viz položka **User management** → **Change Password**).

2.3 Webové rozhraní

Webové rozhraní je rozděleno do tří částí. Horní část obsahuje pouze název zařízení. V levém panelu se nachází hlavní navigační menu. V pravém panelu se pak zobrazuje obsah pro každou položku zvolenou v menu. Na menších displejích je v levém horním rohu webového rozhraní také ikona se třemi vodorovnými čárkami, pomocí níž lze zobrazit či skrýt hlavní navigační menu.



Obrázek 2: Webové rozhraní

ČÁST II

Aktuální stav zařízení

3. Úvodní přehled

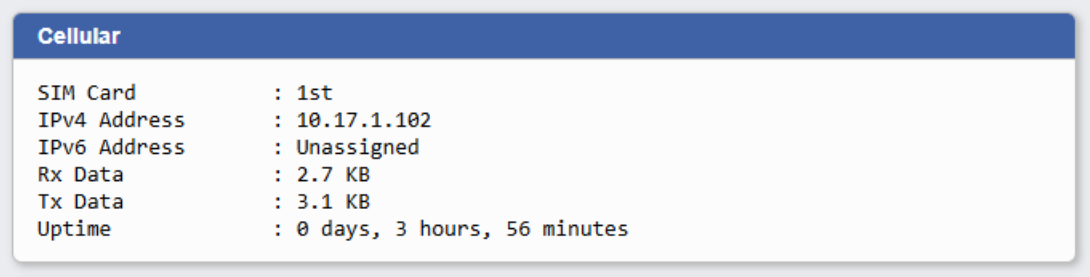
Cesta: Status → Overview

Úvodní stránka nabízí souhrn základních informací o zařízení a také o jeho aktivitách. Jedná se o výchozí stránku, která se zobrazí po každém přihlášení. Informace, které obsahuje, se automaticky aktualizují a jsou rozděleny do několika logických bloků.

3.1 Cellular

První blok obsahuje základní informace o mobilním připojení.

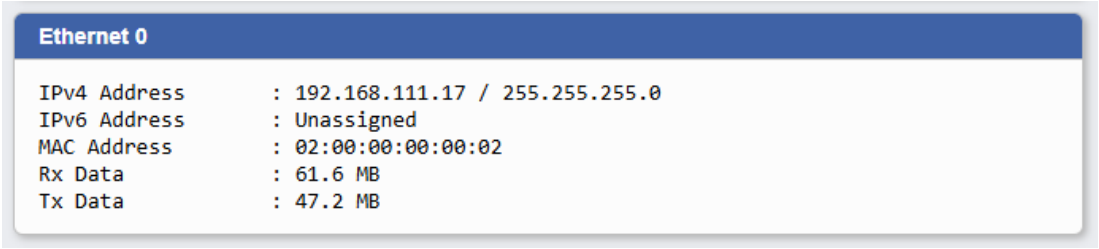
- **SIM Card**: Identifikace aktivní SIM karty (první či druhý slot).
- **IPv4 Address**: IPv4 adresa příslušného rozhraní.
- **IPv6 Address**: IPv6 adresa příslušného rozhraní.
- **Rx Data**: Celkový počet přijatých bajtů.
- **Tx Data**: Celkový počet odeslaných bajtů.
- **Uptime**: Čas, po který je navázáno datové připojení k mobilní síti.



Obrázek 3: Overview – Cellular

3.2 Ethernet

Pro každé ethernetové rozhraní je na stránce **Overview** zobrazen samostatný blok informací (**Ethernet 0** a **Ethernet 1**). Položky v této části mají stejný význam jako v bloku výše. Je zde navíc položka **MAC Address**, jež udává MAC adresu odpovídajícího rozhraní.



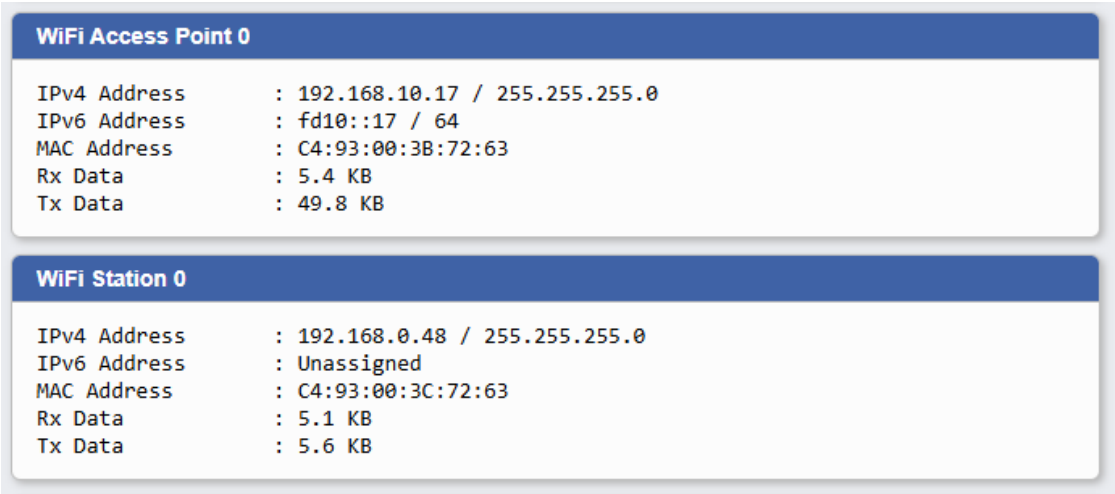
Obrázek 4: Overview – Ethernet

3.3 WiFi přístupový bod a stanice

DŮLEŽITÁ INFORMACE

Části **WiFi Access Point** a **WiFi Station** jsou zobrazeny pouze tehdy, jsou-li příslušná rozhraní povolena v konfiguraci.

Položky zobrazené v této části mají stejný význam jako položky v první části. Blok **WiFi Access Point** zobrazuje informace o WiFi rozhraní pracujícím v režimu přístupového bodu. Blok **WiFi Station** pak zobrazuje informace o WiFi rozhraní pracujícím v režimu stanice.

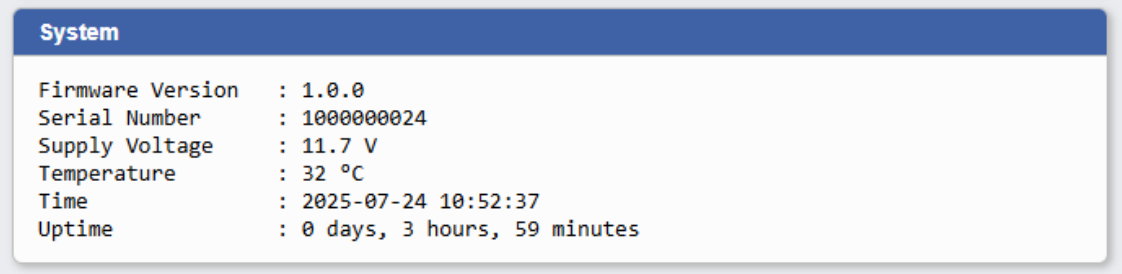


Obrázek 5: Overview – WiFi

3.4 System

Poslední část na stránce Overview (**System**) obsahuje základní informace o zařízení:

- **Firmware Version**: Verze nainstalovaného firmware.
- **Serial Number**: Sériové číslo zařízení.
- **Supply Voltage**: Informace o aktuálním napájecím napětí zařízení.
- **Temperature**: Teplota naměřená uvnitř zařízení.
- **Time**: Aktuální datum a čas, se kterým zařízení pracuje.
- **Uptime**: Doba, po kterou je zařízení v provozu.



Obrázek 6: Overview – System

4. Rozhraní

Výběrem možnosti **Interfaces** v hlavní nabídce webového rozhraní je možné získat detailní informace o vybraných rozhraních.

4.1 Cellular

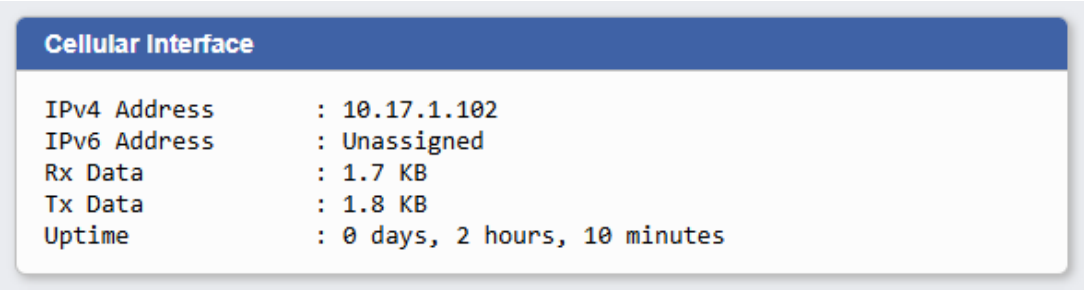
Cesta: Status → Interfaces → Cellular

Výběrem této položky se zobrazí podrobnosti o mobilním připojení, SIM kartě a použitém celulárním modulu.

4.1.1 Cellular Interface

První blok obsahuje základní informace o datovém připojení do mobilní sítě.

- **IPv4 Address**: IPv4 adresa příslušného rozhraní.
- **IPv6 Address**: IPv6 adresa příslušného rozhraní.
- **Rx Data**: Celkový počet přijatých bajtů v rámci mobilního připojení.
- **Tx Data**: Celkový počet odeslaných bajtů v rámci mobilního připojení.
- **Uptime**: Čas, po který je navázáno datové připojení k mobilní síti.



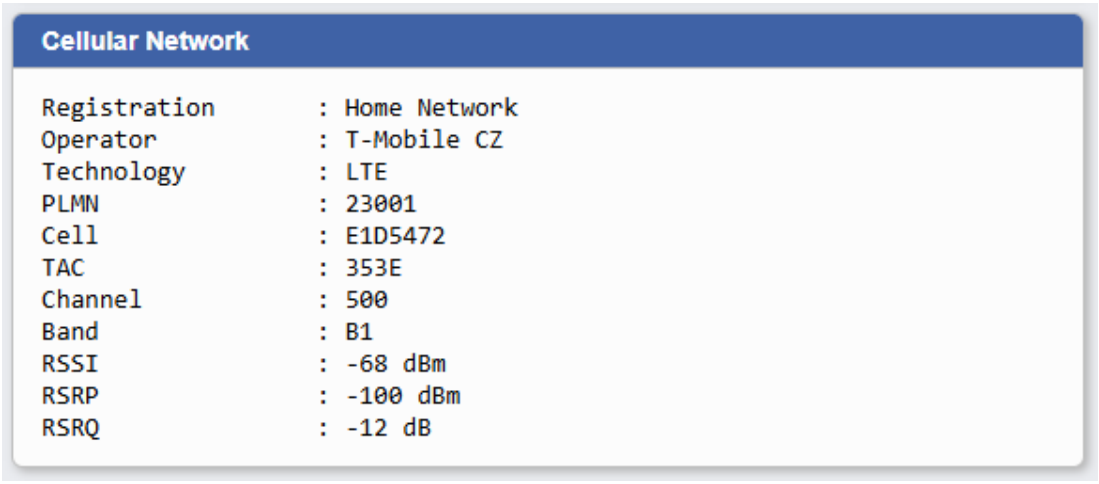
Obrázek 7: Informace o mobilním připojení

4.1.2 Cellular Network

Druhý blok (**Cellular Network**) zobrazuje podrobnosti týkající se přímo mobilní sítě.

- **Registration**: Stav registrace do mobilní sítě.
  - **Idle**: Zařízení není připojeno k žádné síti a aktivně se ani nepokouší o registraci.
  - **Searching**: Zařízení aktivně vyhledává dostupné mobilní sítě.
  - **Denied**: Pokus o registraci do sítě byl odmítnut.
  - **Home Network**: Zařízení je úspěšně registrováno v síti domácího operátora.
  - **Foreign Network**: Zařízení je registrováno v síti jiného operátora.
- **Operator**: Označení sítě operátora, v rámci níž zařízení komunikuje.
- **Technology**: Typ mobilní (přenosové) technologie.

- **PLMN**: Kód mobilní sítě.
- **Cell**: Buňka, ke které je zařízení připojeno (uváděno v hexadecimálním formátu).
- **TAC**: Kód oblasti přidělený operátorem (identifikátor pro určování polohy).
- **Channel**: Kanál, na kterém zařízení komunikuje.
- **Band**: Označení frekvenčního pásma.
- **RSSI**: Celková síla přijímaného signálu, která zahrnuje užitečný LTE signál, šum a také rušení z jiných buněk.
- **RSRP**: Referenční síla přijímaného signálu. Na rozdíl od RSSI ignoruje šum a rušení z okolí.
- **RSRQ**: Kvalita přijímaného referenčního signálu (poměr signál / rušení), která se vypočítává z RSRP a RSSI. Tato hodnota ukazuje, jak je signál „čistý“.



Obrázek 8: Informace o mobilní síti

POZNÁMKA

V případě, že bude sestaveno mobilní spojení prostřednictvím technologie UMTS nebo GPRS, budou se oproti výše uvedenému zobrazovat tyto položky:

- **LAC**: Jedinečný identifikátor oblasti v mobilní síti, která slouží k lokalizaci a správě připojení uživatele v rámci dané mobilní sítě.
- **RSCP**: Indikátor síly signálu konkrétního kódového kanálu v UMTS, který pomáhá zařízení i síti rozhodovat o kvalitě spojení a správě připojení.
- **Ec/Io**: Kvalita signálu, která je dána poměrem síly pilotního signálu (Ec) k šumu a interferencím v kanále (Io). Za výbornou kvalitu signálu lze považovat hodnoty vyšší než -9 dB a o špatné kvalitě signálu vypovídají hodnoty nižší než -15 dB.

Síla signálu	RSRP	RSCP	RSSI
Vynikající	> -90 dBm	> -75 dBm	> -70 dBm
Dobrá	-90 až -105 dBm	-76 až -85 dBm	-70 až -85 dBm
Dostatečná	-106 až -115 dBm	-86 až -95 dBm	-86 až -100 dBm
Slabá	< -115 dBm	< -95 dBm	< -100 dBm

Tabulka 3: Rozsahy hodnot síly signálu

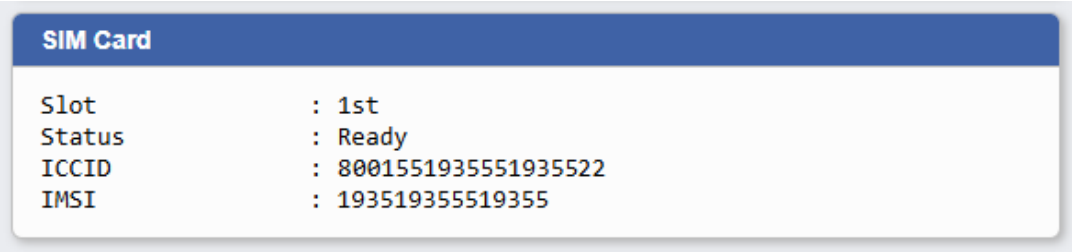
Kvalita signálu	RSRQ	Ec/Io
Vynikající	> -10 dBm	0 až -5 dBm
Dobrá	-10 až -15 dBm	-5 až -10 dBm
Dostatečná	-15 až -20 dBm	-10 až -15 dBm
Slabá	< -20 dBm	< -15 dBm

Tabulka 4: Rozsahy hodnot kvality signálu

4.1.3 SIM Card

V další části jsou k dispozici informace o aktivní SIM kartě. Aktivní SIM karta je ta, která se aktuálně využívá pro sestavení mobilního připojení.

- **Slot**: Identifikace aktivní SIM karty (první či druhý slot).
- **Status**: Aktuální stav SIM karty.
- **ICCID**: Unikátní sériové číslo SIM karty.
- **IMSI**: Jedinečný identifikátor přiřazený každé SIM kartě mobilním operátorem.

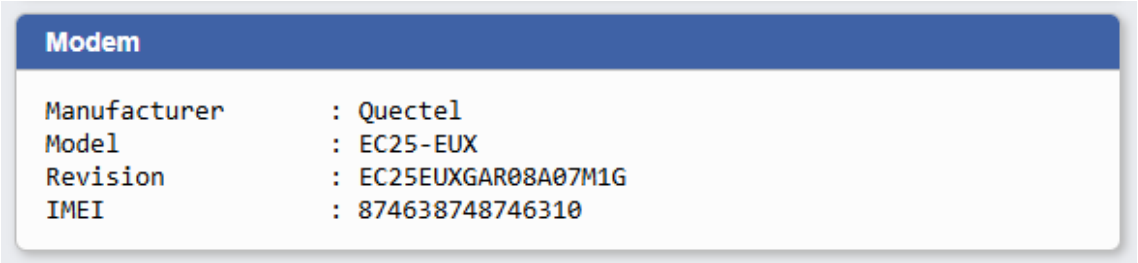


Obrázek 9: Informace o aktivní SIM kartě

4.1.4 Modem

V posledním bloku (**Modem**) se pak zobrazují detaily o celulárním modulu.

- **Manufacturer**: Výrobce celulárního modulu použitého v zařízení.
- **Model**: Označení modelu (typu) celulárního modulu.
- **Revision**: Revize použitého firmware v celulárním modulu.
- **IMEI**: Unikátní identifikační číslo přidělené každému celulárnímu modulu.



Obrázek 10: Informace o celulárním modulu

4.2 Ethernet

Cesta: Status → Interfaces → Ethernet 0 / 1

Na této stránce jsou zobrazeny podrobnosti týkající se rozhraní Ethernet. Informace jsou rozděleny do tří samostatných bloků.

4.2.1 Ethernet – Interface

První z nich (**Ethernet 0/1 Interface**) obsahuje základní informace týkající se příslušného rozhraní.

- **IPv4 Address**: IPv4 adresa příslušného rozhraní.
- **IPv6 Address**: IPv6 adresa příslušného rozhraní.
- **MAC Address**: MAC adresa příslušného ethernetového rozhraní.
- **Rx Data**: Celkový počet přijatých bajtů.
- **Tx Data**: Celkový počet odeslaných bajtů.

4.2.2 Ethernet – Neighbours

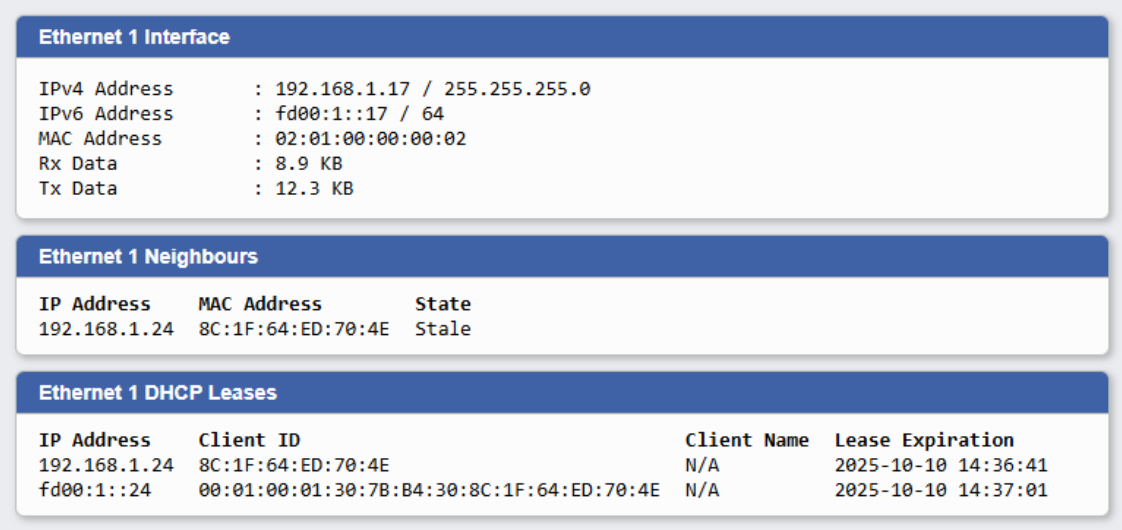
Druhá část (**Ethernet 0/1 Neighbours**) zobrazuje přehled sousedů, jehož součástí je mapování mezi IP adresami (**IP Address**) a MAC adresami (**MAC Address**) zařízení na lokálním síťovém segmentu. Ke každému záznamu je uveden jeden z následujících stavů:

- **Reachable**: Zařízení je dostupné, ARP/NDP záznam je platný a nedávno ověřený.
- **Stale**: Záznam existuje, ale nebyl delší dobu použit. Může být stále platný.
- **Delay**: Čeká se na potvrzení dostupnosti (probíhá zpoždění před testem).
- **Probe**: Posílá se ARP/NDP dotaz k ověření dostupnosti zařízení.
- **Incomplete**: Systém zatím nezná MAC adresu – čeká na ARP/NDP odpověď.
- **Failed**: Zjištění MAC adresy selhalo – zařízení je považováno za nedosažitelné.
- **Noarp**: Záznam bez ARP (staticky zadaný nebo pro speciální použití).
- **Permanent**: Trvalý záznam – nebude nikdy expirován (např. staticky zadaný).

4.2.3 Ethernet – DHCP Leases

V poslední části je k dispozici seznam zařízení, kterým byla aktuálně přiřazena IP adresa prostřednictvím DHCP. Každý řádek představuje jeden DHCP lease záznam – tedy jedno zařízení, kterému byla přidělena IP adresa.

- **IP Address**: IP adresa, kterou DHCP server přidělil připojenému zařízení.
- **Client ID**: Identifikátor DHCP klienta, který se používá pro jednoznačnou identifikaci zařízení při přidělování IP adres. V případě klientů IPv4 je použita MAC adresa, u klientů IPv6 je využito DUID (DHCP Unique Identifier).
- **Client Name**: Hostname zařízení, který si sám klient pošle při žádosti o DHCP lease. Pokud dané zařízení hostname neposílá, je zobrazeno **N/A**.
- **Lease Expiration**: Čas, kdy vyprší DHCP lease, tedy doba, po kterou má zařízení zaručeno používání přidělené IP adresy.



Obrázek 11: Ethernet

4.3 Přístupový bod

Cesta: Status → Interfaces → WiFi Access Point 0 / 1

DŮLEŽITÁ INFORMACE

Část **WiFi Access Point** je dostupná pouze pro modely osazené WiFi modulem.

Na této stránce jsou zobrazeny podrobnosti týkající se WiFi rozhraní pracujících v režimu přístupového bodu. Informace jsou rozděleny do tří samostatných bloků – **Interface**, **Network** a **Connected Stations**.

4.3.1 Přístupový bod – Interface

První z bloků obsahuje základní informace týkající se příslušného rozhraní.

- **IPv4 Address**: IPv4 adresa příslušného rozhraní.
- **IPv6 Address**: IPv6 adresa příslušného rozhraní.
- **MAC Address**: Unikátní 48bitová adresa přiřazená WiFi rozhraní.
- **Rx Data**: Celkový počet přijatých bajtů.
- **Tx Data**: Celkový počet odeslaných bajtů.

4.3.2 Přístupový bod – Network

Položky v tomto bloku mají následující význam:

- **SSID**: Identifikátor WiFi sítě, který umožňuje od sebe jednotlivé sítě odlišit.
- **Country Code**: Kód země, v níž je zařízení nainstalováno. Používá se kód ve formátu ISO 3166-1 alpha-2.
- **Band**: Pásmo, ve kterém je WiFi síť provozována (2,4 GHz nebo 5 GHz).
- **Channel**: Kanál WiFi sítě, tj. konkrétní frekvenční rozsah využívaný pro přenos dat.

4.3.3 Přístupový bod – Seznam připojených zařízení

Druhý blok (**Connected Stations**) obsahuje seznam stanic připojených k přístupovému bodu. Pro každé připojené zařízení (stanici) jsou zobrazovány tyto informace:

- **Station**: MAC adresa připojené stanice.
- **Host**: Název připojené stanice.
- **IPv4 Address**: IPv4 adresa připojené stanice.
- **IPv6 Address**: IPv6 adresa připojené stanice.
- **Signal**: Síla WiFi signálu pro danou stanici. Optimální hodnota pro stabilní připojení se pohybuje kolem -40 dBm. Čím je hodnota dBm vyšší (blíže k nule), tím silnější je signál.

Vynikající	**Dobrý**	**Dostatečný**	**Slabý**
> -50 dBm	-51 až -60 dBm	-61 až -70 dBm	< -71 dBm

- **Rx Data**: Celkový počet přijatých bajtů připojenou stanicí.
- **Tx Data**: Celkový počet odeslaných bajtů připojenou stanicí.
- **Connection Time**: Celkový čas, po který je daná stanice připojena.
- **Flags**: Příznaky specifikující připojení daného klienta
  - [AUTH]: Stanice prošla základní 802.11 autentizací (jedná se o nízkoúrovňový proces *představení se*).
  - [ASSOC]: Stanice je úspěšně přidružena k přístupovému bodu. Proběhla výměna parametrů a přístupový bod o stanici ví.
  - [AUTHORIZED]: Stanice je plně autorizována k přenosu dat. To znamená, že úspěšně proběhl i *4-way handshake* (u WPA2/WPA3) a port je pro data otevřen.
  - [PENDING_POLL]: Přístupový bod čeká na odpověď stanice (tzv. polling), typicky při řízení spotřeby nebo testu dostupnosti.
  - [SHORT_PREAMBLE]: Stanice používá zkrácenou synchronizační hlavičku paketů. To vede ke zvýšení propustnosti sítě snížením režie (u starších 802.11b/g sítí).
  - [PREAUTH]: Stanice provedla předběžnou autentizaci (používá se pro rychlý roaming mezi přístupovými body v rámci jedné sítě).
  - [WMM]: Stanice podporuje QoS (Quality of Service). Umožňuje prioritizaci provozu (např. hlas nebo video před stahováním souborů).
  - [MFP]: Aktivní ochrana řídicích rámců (standard 802.11w). Brání útokům typu *deauthentication attack*, kdy se útočník snaží stanici odpojit.
  - [WPS]: Stanice podporuje Wi-Fi Protected Setup (párování pomocí tlačítka nebo PINu).
  - [MAYBE_WPS]: Přístupový bod detekoval indicii, že by stanice mohla WPS podporovat, ale zatím to není potvrzeno.
  - [WDS]: Stanice je připojena v režimu bridge (typicky pro propojení dvou přístupových bodů bezdrátově).
  - [NonERP]: Stanice nepodporuje ERP (Extended Rate PHY) – staré zařízení (standard 802.11b), což může zpomalovat ostatní.

– [WPS2]: Stanice podporuje Wi-Fi Protected Setup (párování pomocí tlačítka nebo PINu) v bezpečnější verzi 2.

– [GAS]: Protokol používaný pro dotazování na služby sítě ještě před připojením (často spojeno s Hotspot 2.0/Passpoint).

– [HT]: High Throughput, standard 802.11n (Wi-Fi 4).

– [VHT]: Very High Throughput, standard 802.11ac (Wi-Fi 5).

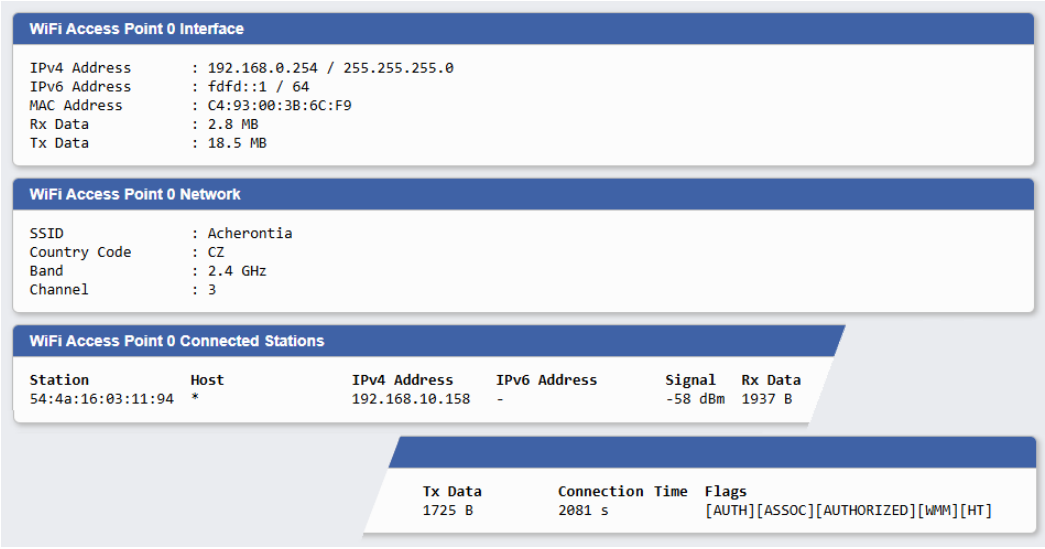
– [HE]: High Efficiency, standard 802.11ax (Wi-Fi 6).

– [EHT]: Extremely High Throughput, standard 802.11be (Wi-Fi 7).

– [6GHZ]: Stanice je připojena v pásmu 6 GHz (Wi-Fi 6E nebo 7).

– [VENDOR_VHT]: Proprietární rozšíření, které umožňuje technologie VHT ve frekvenčním pásmu 2.4 GHz.

– [WNM_SLEEP_MODE]: Stanice přešla do úsporného režimu v rámci Wireless Network Management. Zůstává připojena, ale vypíná rádiovou část na delší intervaly.



Obrázek 12: Podrobnosti o přístupovém bodu

4.4 WiFi stanice

Cesta: Status → Interfaces → WiFi Station 0 / 1

DŮLEŽITÁ INFORMACE

Část **WiFi Station** je dostupná pouze pro modely osazené WiFi modulem.

Na této stránce jsou zobrazeny informace týkající se WiFi připojení z pohledu stanice. Jsou rozděleny do dvou samostatných bloků (**Interface** a **Network**), přičemž první z nich obsahuje základní informace týkající se příslušného rozhraní.

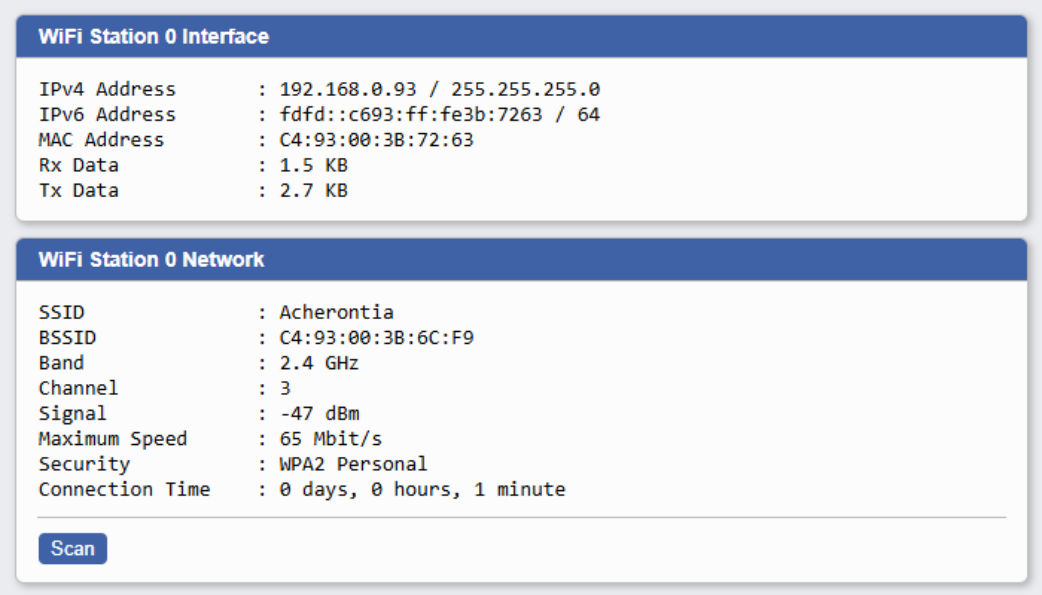
- **IPv4 Address**: IPv4 adresa pro rozhraní WiFi v režimu stanice.
- **IPv6 Address**: IPv6 adresa pro rozhraní WiFi v režimu stanice.
- **MAC Address**: Unikátní 48bitová adresa přiřazená příslušnému WiFi rozhraní.
- **Rx Data**: Celkový počet přijatých bajtů.
- **Tx Data**: Celkový počet odeslaných bajtů.

Ve druhé části jsou pak zobrazovány následující informace:

- **SSID**: Identifikátor WiFi sítě, do které se zařízení připojuje.
- **BSSID**: MAC adresa bezdrátového přístupového bodu (AP) ve WiFi síti.
- **Band**: Pásmo, ve kterém je daná WiFi síť provozována (2,4 GHz nebo 5 GHz).
- **Channel**: Kanál WiFi sítě, tj. konkrétní frekvenční rozsah využívaný pro přenos dat.
- **Signal**: Síla WiFi signálu. Optimální hodnota pro stabilní připojení se pohybuje kolem -40 dBm. Čím je hodnota dBm vyšší (blíže k nule), tím silnější je signál.

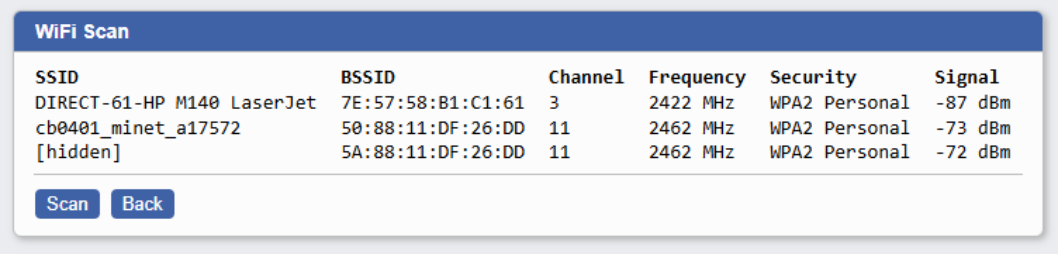
Vynikající	**Dobrý**	**Dostatečný**	**Slabý**
> -50 dBm	-51 až -60 dBm	-61 až -70 dBm	< -71 dBm

- **Maximum Speed**: Maximální přenosová rychlost mezi zařízením a přístupovým bodem.
- **Security**: Standard zabezpečení WiFi sítě, ke které je stanice připojena (WPA2 nebo WPA3 ve variantách s předsdíleným klíčem či s individuálními přihlašovacími údaji).
- **Connection Time**: Celková doba připojení k danému přístupovému bodu.



Obrázek 13: Podrobnosti o WiFi připojení z pohledu stanice

Kliknutím na tlačítko Scan v levém dolním rohu je možné získat přehled o dostupných WiFi sítích. Pro každou z nich jsou vypsány údaje **SSID**, **BSSID**, **Channel**, **Frequency**, **Security** a **Signal**. Významy všech těchto položek odpovídají popsaným položkám výše.



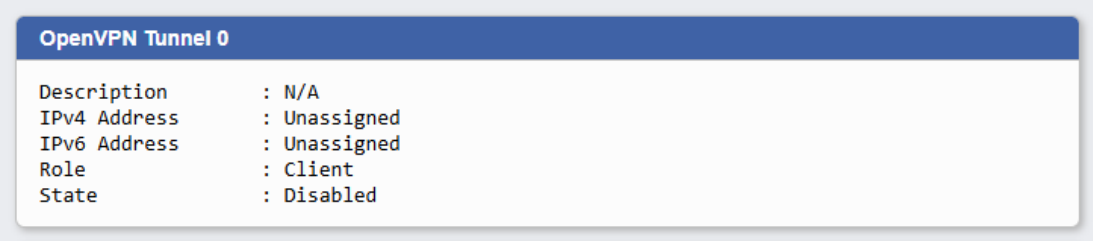
Obrázek 14: Přehled dostupných WiFi sítí

5. OpenVPN

Cesta: Status → Tunnels → OpenVPN

Na této stránce jsou zobrazeny základní informace o jednotlivých OpenVPN tunelech.

- **Description**: Textový popisek pro daný OpenVPN tunel.
- **IPv4 Address**: IPv4 adresa příslušného rozhraní.
- **IPv6 Address**: IPv6 adresa příslušného rozhraní.
- **Role**: Role, kterou zařízení plní v rámci daného tunelu.
  - **client**: Tento uzel navazuje spojení se serverem a používá jeho síťové zdroje.
  - **server**: Tento uzel poslouchá příchozí VPN připojení, ověřuje klienty a spravuje tunely.
- **State**: Aktuální stav daného OpenVPN tunelu.
  - **Connecting**: Klient zahajuje proces připojení k VPN serveru. Spouští se inicializace spojení a začíná komunikace se serverem.
  - **Wait**: Klient čeká na první odpověď od serveru. Pokud v tomto stavu OpenVPN visí dlouho, obvykle to znamená, že je server nedostupný nebo blokovaný firewallem.
  - **Auth**: Probíhá výměna certifikátů nebo ověřování uživatelského jména a hesla.
  - **Get config**: Klient si stahuje ze serveru instrukce (tzv. „push“ možnosti), jako je maska sítě, DNS servery nebo nastavení komprese.
  - **Assign IP**: Server přiděluje klientovi virtuální IP adresu pro VPN tunel. Tato IP adresa je používána pro komunikaci v rámci VPN sítě.
  - **Add routes**: Do směrovací tabulky systému se přidávají pravidla, která určují jaký provoz má jít přes VPN a jaký provoz má zůstat mimo VPN.
  - **Connected**: Spojení je úspěšně navázáno. VPN tunel je aktivní, šifrování funguje a data jsou bezpečně přenášena mezi klientem a serverem.
  - **Reconnecting**: Spojení bylo přerušeno. Klient se automaticky pokouší znovu navázat spojení.
  - **Exiting**: Proces ukončování spojení.
  - **Resolve**: Klient překládá doménové jméno serveru na číselnou IP adresu pomocí DNS.
  - **TCP connect**: Klient se pokouší navázat TCP spojení se serverem na definovaném portu (tento stav se zobrazuje při použití TCP protokolu).
  - **Auth pending**: Tento stav nastává, je-li vyžadována dvoufaktorová autentizace (server čeká na potvrzení v rámci ověřovacího procesu).
  - **Disabled**: Služba je vypnuta.



Obrázek 15: OpenVPN

6. Periferie

Stránka **Peripherals** nabízí souhrn základních informací o sériových linkách (**Serial Port 0** a **Serial Port 1**) a také o jednotlivých vstupech a výstupech (**Inputs & Outputs** a **Input Alarms**). Nedílnou součástí je rovněž podrobný přehled informací vyčtených dataloggerem.

> **POZNÁMKA**
>
> Tato část je zobrazena i v případě, že sériové linky, vstupy a výstupy nejsou využity.

6.1 Datalogger

Cesta: Status → Peripherals → Data Logger

Na této stránce jsou zobrazeny podrobnosti týkající se vyčtených dat (funkce dataloggeru). Informace jsou rozděleny do tří částí, přičemž v první z nich je k dispozici následující:

- **ID**: Unikátní identifikátor záznamu vyčtených dat.
- **Time**: Datum a čas, kdy byla data získána.
- **Temperature**: Naměřená teplota uvnitř zařízení.
- **Supply Voltage**: Naměřené napájecí napětí zařízení.

Druhá a třetí část pak obsahují podrobné informace o vstupech, výstupech a alarmech tak, jak byly v danou chvíli (**Time**) na zařízení zaznamenány.

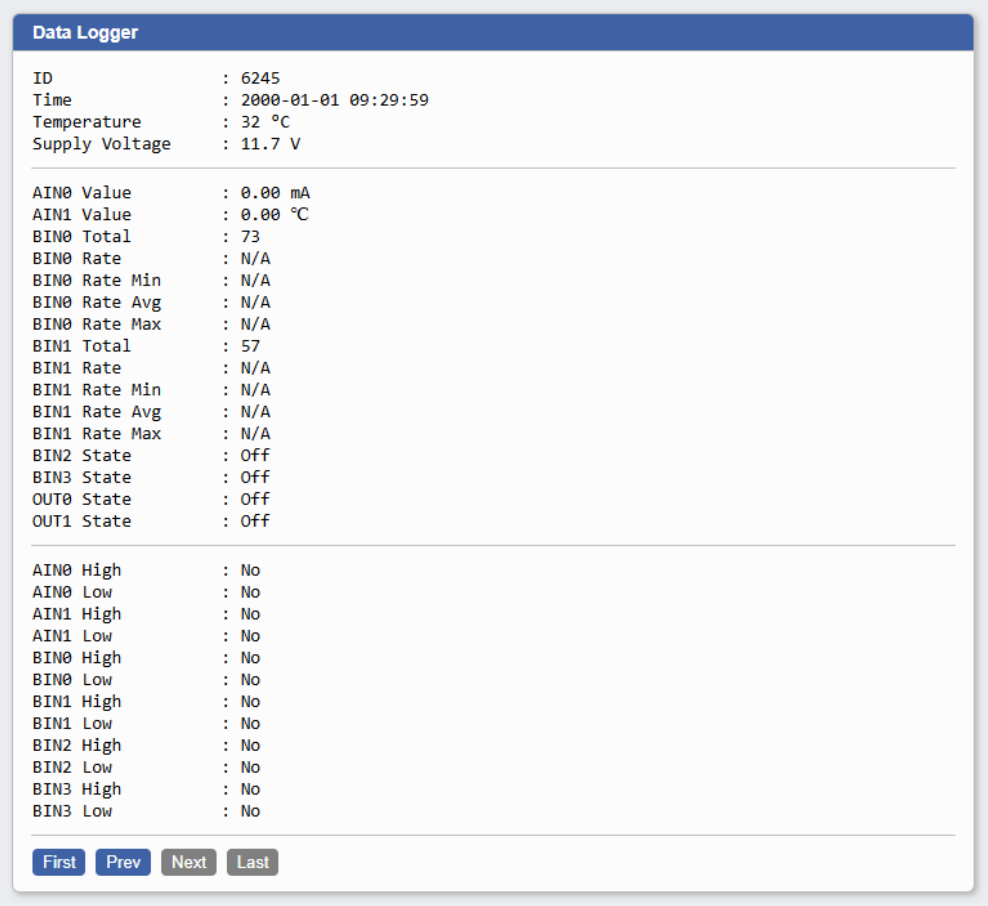
- **AIN*x* Value**: Okamžitá naměřená hodnota na analogovém vstupu.
- **BIN*x* State**: Logický stav binárního vstupu. Buď **On** (sepnuto), nebo **Off** (rozepnuto).
- **BIN*x* Total**: Celková hodnota naměřená na daném vstupu od posledního vynulování. V základním nastavení odpovídá počtu přijatých impulsů. Pokud je však nastaven přepočet (např. 1 impuls = 10 litrů), zobrazuje se již přepočtená hodnota – tedy celkové množství (např. počet impulsů × 10 = celkový objem v litrech).
- **BIN*x* Rate**: Okamžitá hodnota měřené veličiny. V základním nastavení se jedná o frekvenci impulsů. Při aktivním přepočtu (např. 1 impuls = 10 litrů) se zobrazuje přepočtená hodnota, tedy například průtok (např. litry za sekundu).
- **BIN*x* Rate Min**: Nejnižší zaznamenaná hodnota **BIN*x* Rate** v rámci sledovaného období.
- **BIN*x* Rate Avg**: Průměr hodnoty **BIN*x* Rate** v rámci sledovaného období.
- **BIN*x* Rate Max**: Nejvyšší zaznamenaná hodnota **BIN*x* Rate** v rámci sledovaného období.
- **OUT*x* State**: Logický stav binárního výstupu. Buď **On** (sepnuto), nebo **Off** (rozepnuto).
- **AIN*x* High**: Naměřená hodnota překročila horní alarmovou hranici.
- **AIN*x* Low**: Naměřená hodnota byla pod spodní alarmovou hranici.
- **BIN*x* High**: Naměřená hodnota překročila horní alarmovou hranici.
- **BIN*x* Low**: Naměřená hodnota byla pod spodní alarmovou hranici.

Ve spodní části této stránky (**Data Logger**) jsou umístěna tlačítka, která slouží k přepínání mezi jednotlivými záznamy.

- First : Zobrazí první záznam.
- Prev : Zobrazí předcházející záznam.
- Next : Zobrazí následující záznam.
- Last : Zobrazí poslední záznam.

POZNÁMKA

Je-li zobrazen poslední záznam, dochází k automatickému obnovování stránky.

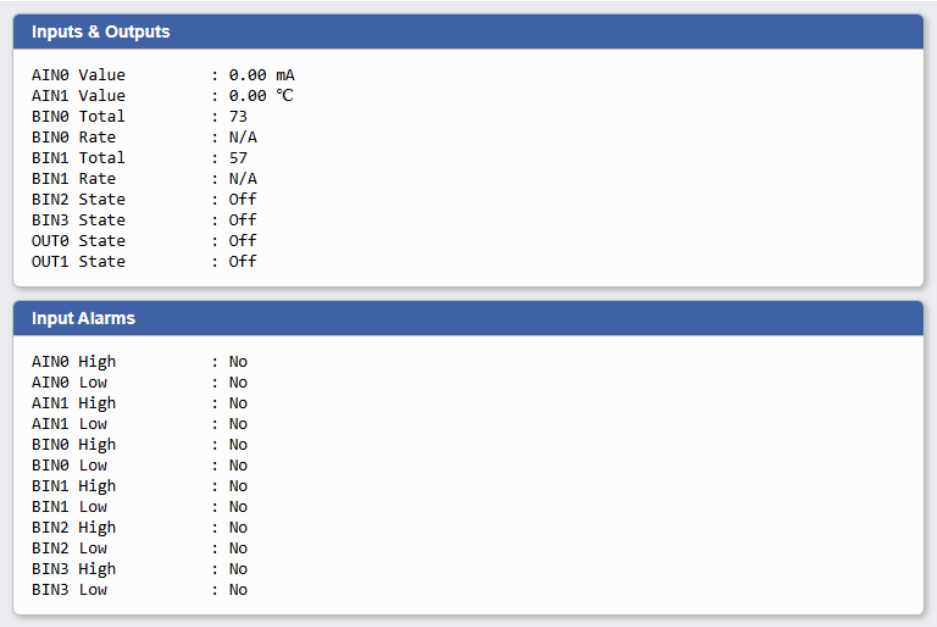


Obrázek 16: Datalogger

6.2 Vstupy a výstupy

Cesta: Status → Peripherals → Inputs & Outputs

Tato stránka obsahuje **aktuální** informace o jednotlivých vstupech a výstupech (**Inputs & Outputs** a **Input Alarms**). Význam jednotlivých položek odpovídá položkám popsaným v části **Datalogger**.



Obrázek 17: Vstupy a výstupy

6.3 Sériové linky

Cesta: Status → Peripherals → Serial Ports

Tato stránka zobrazuje základní informace o jednotlivých sériových linkách.

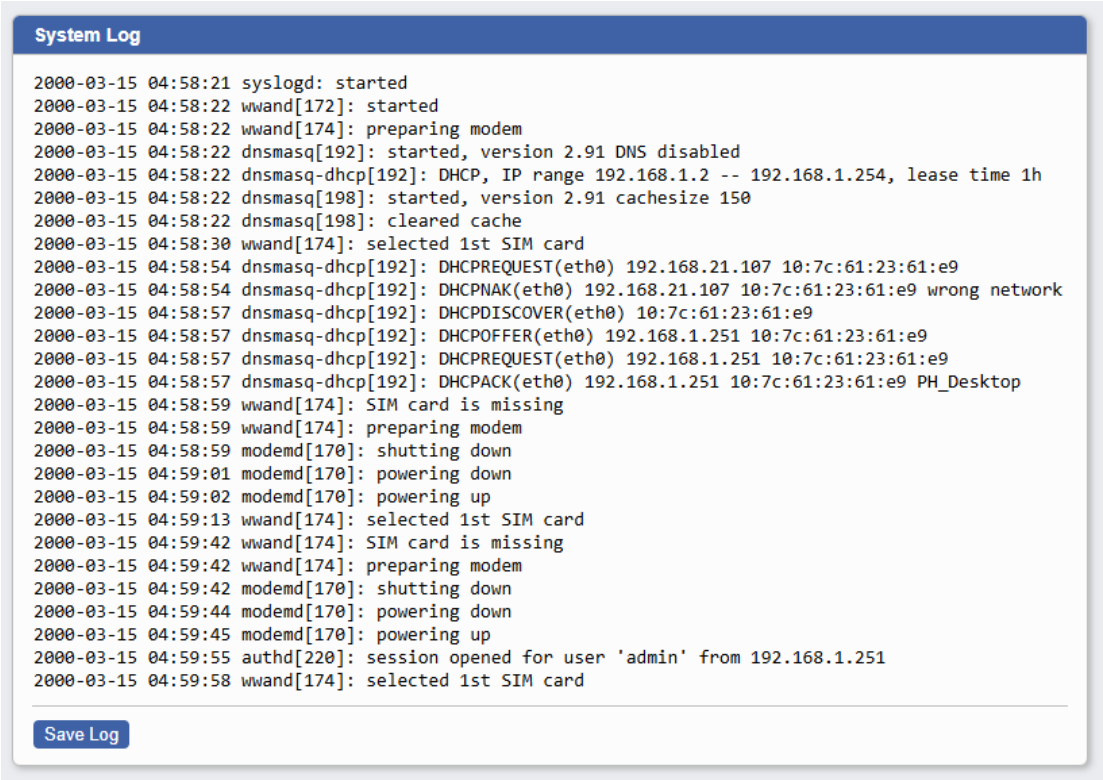
- **Port Type**: Typ sériové linky.
- **Rx Data**: Celkový počet bajtů, které zařízení přijalo z dané sériové linky.
- **Tx Data**: Celkový počet bajtů, které zařízení odeslalo přes danou sériovou linku.

Obrázek 18: Sériové linky

7. System Log

Cesta: Status → System Log

Tato stránka zobrazuje podrobné záznamy činnosti generované různými aplikacemi a službami spuštěnými na daném zařízení. Kliknutím na tlačítko Save Log je možné veškeré záznamy činnosti uložit do jednoho souboru ve formátu **.txt**.



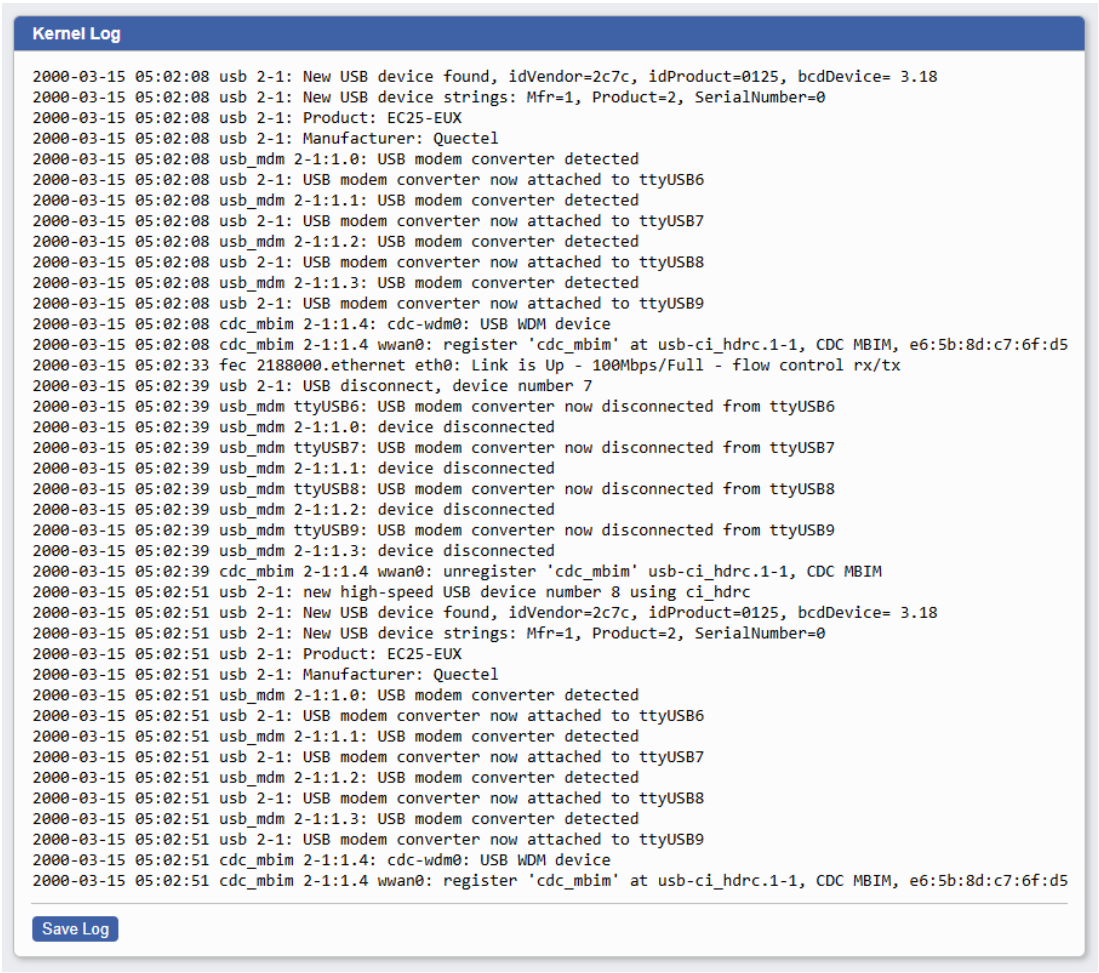
Obrázek 19: System Log

8. Kernel Log

Cesta: Status → Kernel Log

Kernel log obsahuje podrobné zprávy o průběhu bootování a další informace o událostech souvisejících s linuxovým jádrem. Jednotlivé záznamy se začínají zapisovat okamžitě se spuštěním systému a jsou velmi užitečné především pro řešení různých provozních potíží.

Kliknutím na tlačítko Save Log je možné veškeré záznamy uložit do jednoho souboru typu **.txt**.

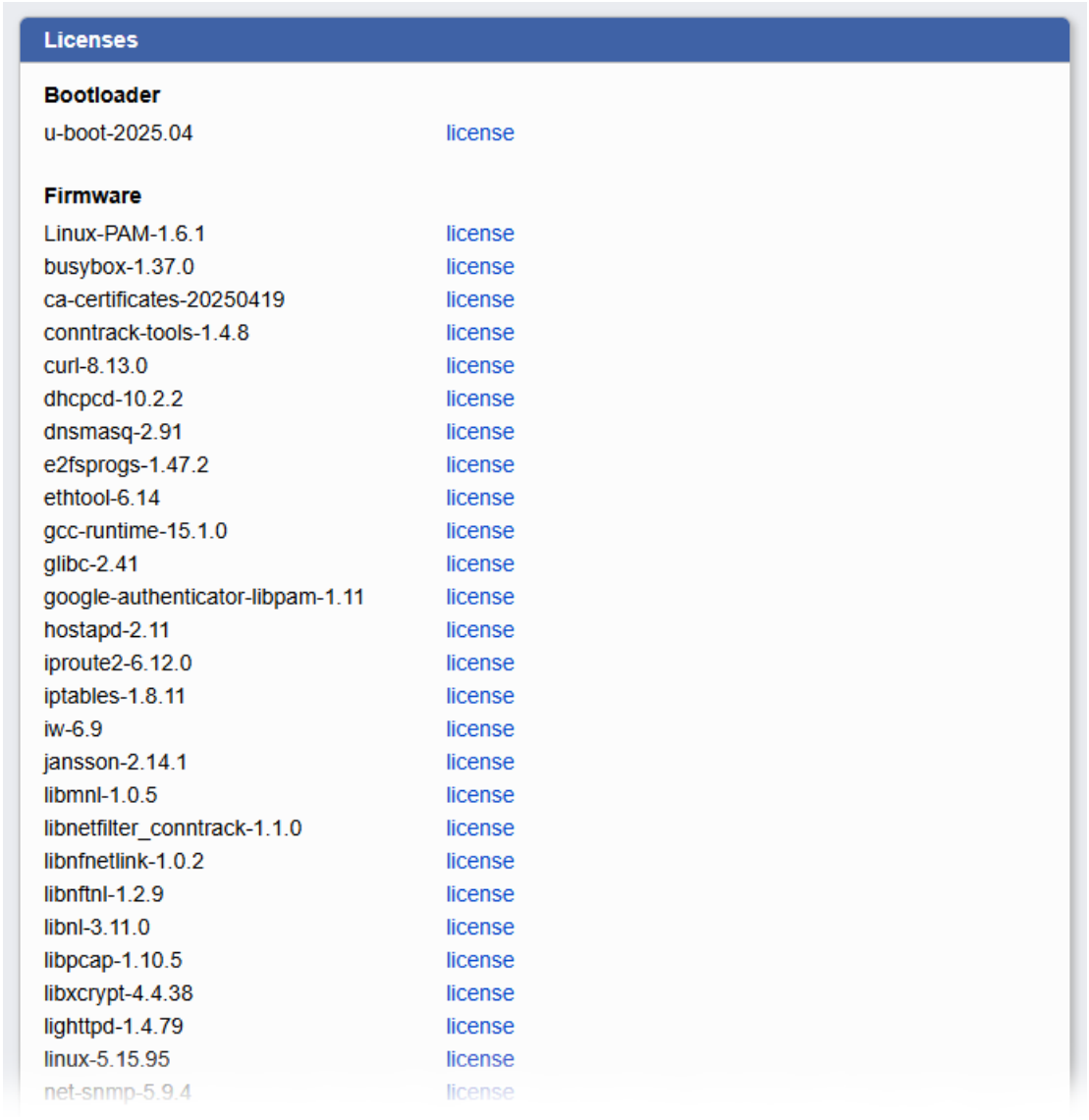


Obrázek 20: Kernel Log

9. Softwarové licence

Cesta: Status → Licenses

Tato stránka obsahuje seznam open source softwarových komponent firmwaru. Kliknutím na odkaz **license** získáte kompletní text licence.



Obrázek 21: Softwarové licence

ČÁST III

Konfigurace

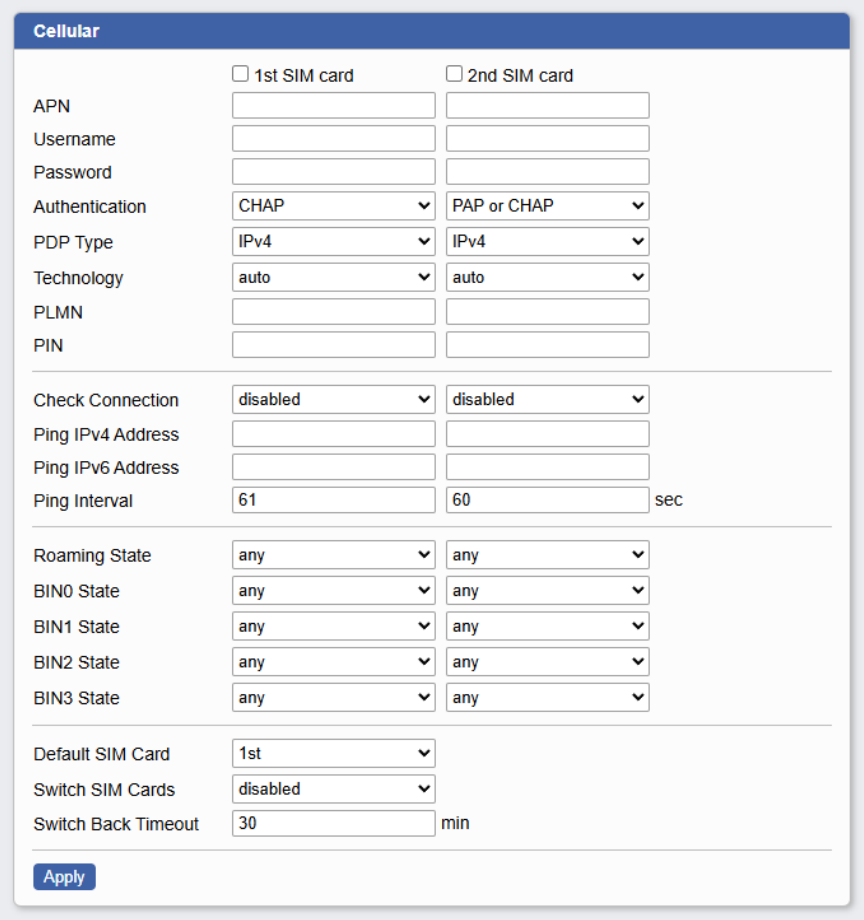
10. Rozhraní

Výběrem možnosti **Interfaces** v sekci **Configuration** je možné získat konfigurační formuláře vybraných rozhraní.

10.1 Připojení k mobilní síti

Cesta: Configuration → Interfaces → Cellular

Aby se zařízení mohlo bez problému připojit k mobilní síti, je nutné mít vloženu alespoň jednu SIM kartu a zaškrtnuté políčko ☐ **1st SIM card** (případně ☐ **2nd SIM card**), které povoluje používání příslušné SIM karty.



Obrázek 22: Připojení k mobilní síti

POZNÁMKA

Detailní informace o navázaném mobilním připojení jsou dostupné na stránce **Status → Interfaces → Cellular**.

Ke každé vložené SIM kartě lze nastavit následující parametry:

- **APN**: Název přístupového bodu.
- **Username**: Uživatelské jméno používané pro přihlášení do mobilní sítě.
- **Password**: Uživatelské heslo používané pro přihlášení do mobilní sítě.
- **Authentication**: Ověřovací protokol používaný v mobilní síti.
  - **PAP**: Jednoduchý, nešifrovaný ověřovací protokol sloužící k ověření uživatele posláním jeho uživatelského jména a hesla v čitelné podobě (plaintext).
  - **CHAP**: Autentizační protokol používaný k ověření identity uživatele prostřednictvím tříkrokového procesu (výzva, kontrola, ověření).
  - **PAP or CHAP**: Zařízení zvolí jeden z výše uvedených ověřovacích protokolů.
- **PDP Type**: Verze IP protokolu používaná v rámci mobilní sítě.
  - **IPv4**: Internetový protokol verze 4 s adresami dlouhými 32 bitů.
  - **IPv6**: Internetový protokol verze 6 s adresami dlouhými 128 bitů.
  - **IPv4/IPv6**: Nezávislý "dual stack" IPv4 a IPv6 umožňující odesílat a přijímat datové pakety pomocí kteréhokoli z těchto dvou protokolů.
- **Technology**: Použitá přenosová technologie. Je-li zvolena možnost **auto**, zařízení volí technologii automaticky podle dostupnosti, síly signálu a jeho kvality.
- **PLMN**: Unikátní identifikátor mobilní sítě (pěticiferné nebo šesticiferné číslo, které identifikuje zemi a operátora mobilní sítě v dané zemi). PLMN není typicky potřeba vyplňovat. Děje se tak pouze ve speciálních situacích, například při vynucení připojení k určitému operátorovi, nebo naopak, pokud se zařízení připojuje k nežádoucímu operátorovi.
- **PIN**: PIN kód k odemčení SIM karty (pouze pokud jej SIM karta vyžaduje). **Bude-li opakovaně použit chybný PIN kód, může dojít k zablokování SIM karty.**

Ve druhé části tohoto formuláře je možné konfigurovat kontrolu mobilního připojení (pro každou SIM kartu separátně). Je-li položka **Check Connection** nastavena na **enabled** nebo **enabled if idle**, dochází k pravidelnému posílání výzev (tzv. pingů) na předem definovanou cílovou adresu (**Ping IPv4 Address** nebo **Ping IPv6 Address**). Četnost posílání kontrolních ICMP pingů lze nastavit v kolonce **Ping Interval**. Je-li **Check Connection** nastaveno na **enabled if idle**, připojení se kontroluje pouze v době nečinnosti.

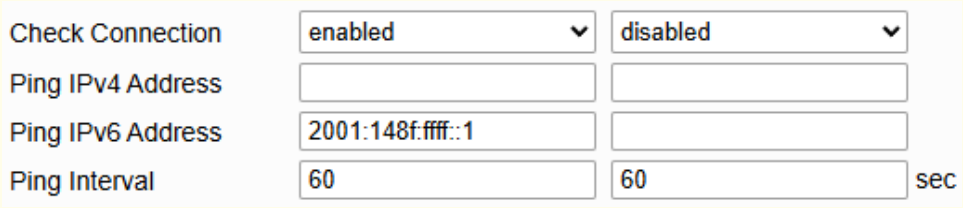
V případě neúspěšného pingu bude v rámci pravidelného intervalu odeslán nový ping. Pokud je tato výzva třikrát za sebou neúspěšná, dojde k ukončení mobilního připojení a zahájí se proces sestavení nového spojení.

DŮLEŽITÁ INFORMACE

Je-li vyplněna IPv4 i IPv6 adresa, probíhají dvě kontroly připojení. Je-li jedna z těchto kontrol třikrát za sebou neúspěšná, dojde k ukončení spojení a navázání nového.

PŘÍKLAD

Na obrázku níže je znázorněna situace, ve které je na první SIM kartě povolena kontrola mobilního připojení. Pokud je tato SIM karta aktivní, je každých **60 sekund** odesílán kontrolní ping na adresu **2001:148f:ffff::1**. Na druhé SIM kartě kontrola připojení povolena není a nebude se tedy posílat žádný kontrolní ping.



Ve třetí části konfiguračního formuláře **Cellular** je pro obě SIM karty možné nastavit tyto parametry:

- **Roaming State**: Definuje použití dané SIM karty na základě roamingu.
  - **any**: SIM kartu lze použít kdekoliv (v jakékoliv síti).
  - **home network only**: SIM kartu lze použít pouze v případě, že není detekován roaming.
- **BIN0 State**: Definuje použití dané SIM karty na základě stavu binárního vstupu.
  - **any**: SIM kartu lze použít bez ohledu na stav daného binárního vstupu.
  - **off**: SIM kartu lze použít pouze v případě, že vstup není aktivní (příslušný pin není připojen ke GND).
  - **on**: SIM kartu lze použít pouze v případě, že vstup je aktivní (příslušný pin je připojen ke GND).

POZNÁMKA

Závislost použití SIM karty na binárních vstupech BIN1, BIN2 a BIN3 je možné konfigurovat stejným způsobem, který je popsán pro BIN0.

Poslední část tohoto formuláře je věnována konfiguraci přepínání SIM karet.

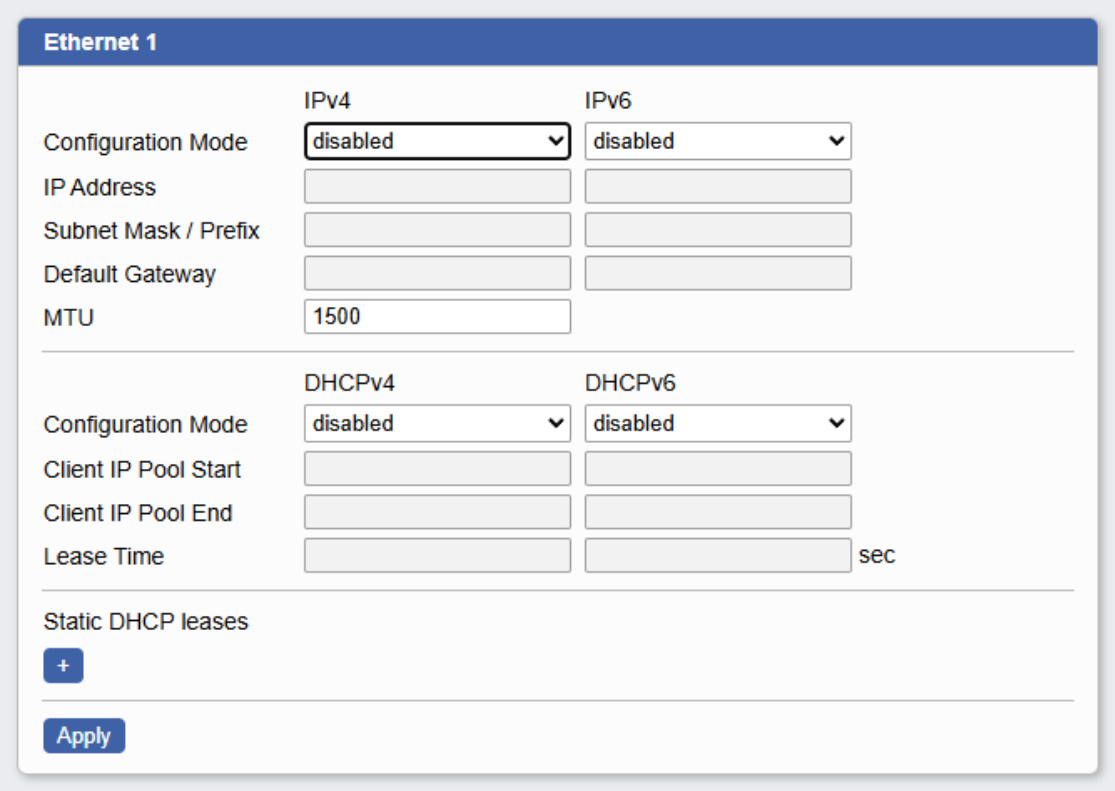
- **Default SIM Card**: Určuje výchozí SIM kartu, která je primární pro navázání spojení. Volit lze z možností **1st**, **2nd** či **none** (žádná).
- **Switch SIM Cards**: Povoluje (resp. zakazuje) přepínání mezi SIM kartami.
  - **disabled**: Automatické přepínání SIM karet je zakázáno.
  - **if connection fails**: Pokud selže připojení, dochází k přepnutí SIM karty.
- **Switch Back Timeout**: Doba, po kterou zařízení čeká před prvním pokusem o přepnutí zpět na výchozí SIM kartu (**Default SIM Card**).

10.2 Připojení k Ethernetu

Cesta: Configuration → Interfaces → Ethernet 0 / 1

Pro konfiguraci připojení k Ethernetu jsou určeny konfigurační formuláře s označením **Ethernet 0** a **Ethernet 1**. Výchozí IP adresa rozhraní ETH0 je 192.168.1.1. Změnit ji můžete pomocí kolonky **IP Address**. Zařízení podporuje IPv4 / IPv6 dual stack, což znamená, že umožňuje nezávisle odesílat a přijímat datové pakety pomocí protokolů IPv4 a IPv6. Konfigurační formulář je proto rozdělen do dvou sloupců, které odpovídají nastavení pro dané protokoly.

- **Configuration Mode**: Způsob přidělení IP adresy a dalších souvisejících parametrů.
  - **manual**: Uživatel vyplní potřebné údaje pomocí položek níže.
  - **disabled**: Ethernetové rozhraní je na zařízení vypnuto.
- **IP Address**: Pevná IP adresa odpovídajícího ethernetového rozhraní (IPv6 adresu lze zadat ve zkrácené notaci).
- **Subnet Mask / Prefix**: Maska sítě pro IP adresu verze 4 (určuje, které bity označují síť, či podsíť, a které bity označují zařízení). V případě použití IPv6 adresy je třeba zadat prefix, tedy číslo v rozsahu 8 až 128.
- **Default Gateway**: IP adresa výchozí brány (tj. zařízení, které slouží jako výstupní bod pro komunikaci mimo lokální síť).
- **MTU**: Maximální velikost datového paketu. Výchozí hodnotou je 1500 bajtů.



Obrázek 23: LAN konfigurace

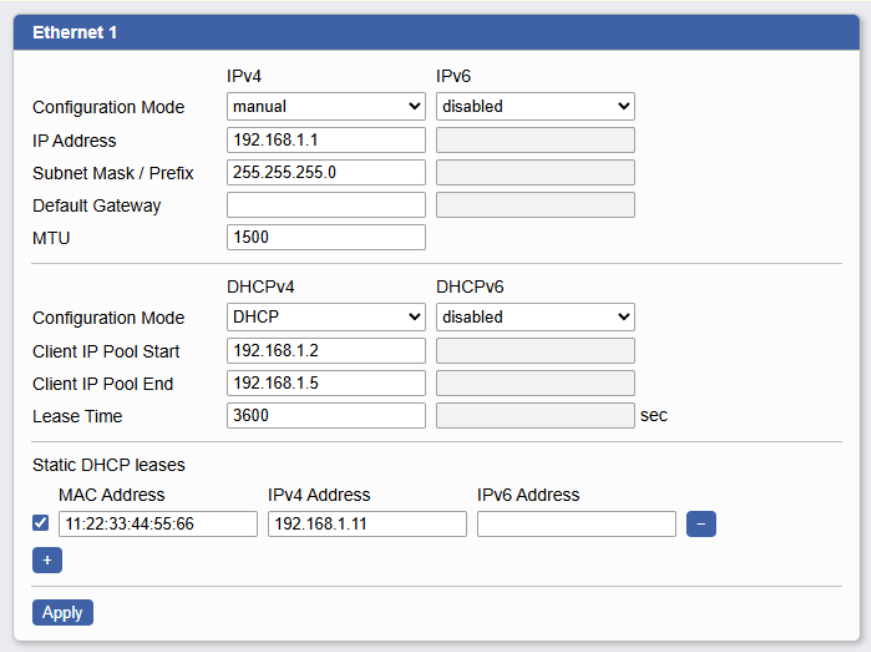
10.2.1 DHCP Server

DHCP server přiřazuje připojeným klientům IP adresu, IP adresu výchozí brány a zároveň IP adresu DNS serveru. Podporováno je statické (**Static DHCP leases**) a také dynamické přiřazování IP adres. Dynamické přiřazování adres přiděluje klientům IP adresy z definovaného adresního prostoru (viz položky **Client IP Pool Start** a **Client IP Pool End**). Statické přiřazování adres přiděluje IP adresy, které odpovídají MAC adresám připojených klientů (přidat je lze tlačítkem +).

- **Configuration Mode**: Povoluje dynamické přiřazování IP adres. V případě používání IPv6 adresy je třeba zvolit metodu přidělování adres.
  - **DHCP**: Stavová autokonfigurace – zařízení oznámí typ autokonfigurace a vše ostatní zajišťuje DHCPv6 server. Varianta výhodná především v situacích, kdy se v síti mohou vyskytovat zařízení, kterým dostatečně nedůvěřujeme, anebo je potřeba mít o všech zařízeních v síti přehled.
  - **SLAAC**: Bezstavová autokonfigurace, která ke konfiguraci klienta využívá pouze informace poskytované zařízením. Jedná se o výhodné řešení především pro malé sítě s několika jednotkami zařízení nebo rozsáhlé sítě s mnoha malými podsítěmi, kde každá podsíť má definovaný vlastní prefix.
  - **DHCP + SLAAC**: Hybridní režim přidělování síťových adres a parametrů. SLAAC zajišťuje konektivitu a DHCP dodává specifické parametry sítě. Hlavní výhodou je maximální kompatibilita (některá zařízení preferují adresu z DHCP, zatímco jiná se spoléhají výhradně na SLAAC, v tomto režimu funguje obojí).
- **Client IP Pool Start**: Počáteční IP adresa rozsahu pro dynamické přidělení.
- **Client IP Pool End**: Koncová IP adresa rozsahu pro dynamické přidělení.
- **Lease Time**: Doba platnosti IP adresy před jejím uvolněním a opětovným přidělením. Zadaná hodnota odpovídá času v sekundách.

PŘÍKLAD

Tento příklad znázorňuje situaci, ve které jsou přiřazovány IP adresy staticky i dynamicky. Síť je tvořena zařízením s MAC adresou **11:22:33:44:55:66** a staticky přidělenou IP adresou **192.168.1.11**. Zároveň je tu prostor pro připojení dalších čtyř zařízení, kterým bude přidělena adresa dynamicky z rozsahu **192.168.1.2** až **192.168.1.5** (na **1 hodinu**).



10.3 WiFi připojení

DŮLEŽITÁ INFORMACE

Konfigurační formuláře **WiFi Access Point** a **WiFi Station** jsou dostupné pouze pro modely osazené WiFi modulem.

Zařízení podporuje tzv. **multi-role režim**, což znamená, že zařízení může fungovat současně jako přístupový bod (AP) a stanice (STA).

10.3.1 Přístupový bod

Cesta: Configuration → Interfaces → WiFi Access Point 0 / 1

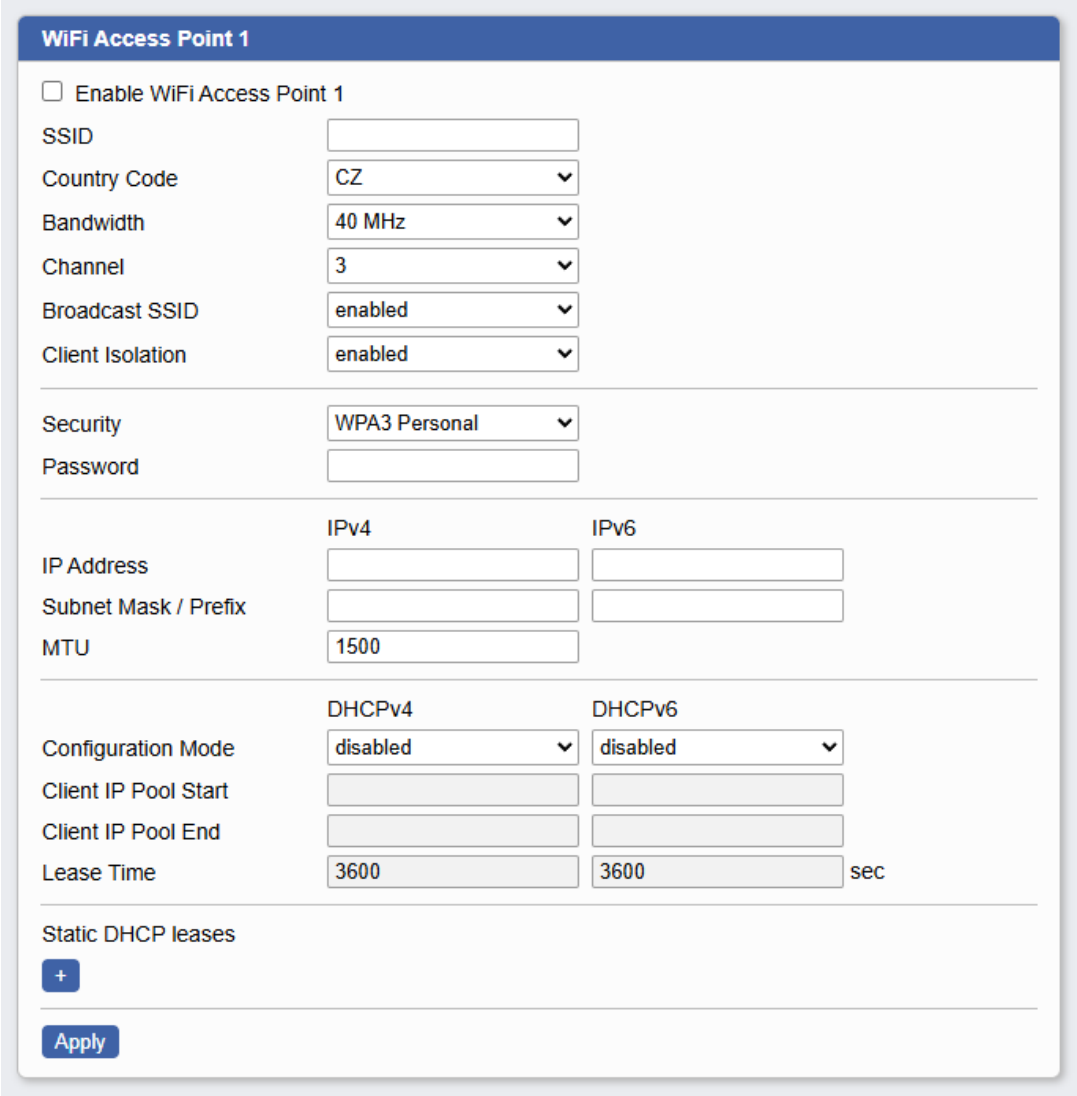
Přístupový bod v bezdrátové WiFi síti je zařízení, ke kterému se připojují jednotlivé stanice. Ty spolu nekomunikují přímo, ale právě prostřednictvím přístupového bodu, takže mohou být jednodušší a nemusejí být ve vzájemném rádiovém spojení. Zařízení podporuje konfiguraci dvou samostatných sítí WLAN (**WiFi Access Point 0** a **WiFi Access Point 1**).

Pokud chcete povolit režim přístupového bodu, zaškrtněte políčko ☐ **Enable WiFi Access Point** v horní části konfiguračního formuláře. Níže jsou uvedeny dostupné možnosti konfigurace.

- **SSID**: Identifikátor WiFi sítě, který AP periodicky vysílá v řídícím rámci (není-li SSID skryto).
- **Country Code**: Kód země, v níž je zařízení nainstalováno. Používá se **kód ve formátu ISO 3166-1 alpha-2**. Volba kódu země ovlivňuje hodnoty dalších parametrů.
- **Bandwidth**: Šířka kanálu pro přenos dat. Širší kanály (**40 MHz** a **80 MHz**) nabízejí vyšší rychlost, ale jsou náchylnější k rušení, zatímco užší kanály (**20 MHz**) jsou spolehlivější, ale pomalejší.
- **Channel**: Kanál WiFi sítě, tj. konkrétní frekvenční rozsah využívaný pro přenos dat.
- **Broadcast SSID**: Periodický přenos názvu WiFi sítě (**SSID**), díky kterému je síť viditelná v seznamu dostupných sítí, ke kterým se mohou připojit zařízení v okolí.
- **Client Isolation**: Funkce síťového zabezpečení, jež brání bezdrátovým zařízením ve stejné síti v přímé komunikaci mezi sebou a zároveň jim umožňuje přístup k Internetu a dalším externím zdrojům. Pokud je tato funkce zakázána (**disabled**), přístupový bod funguje jako přepínač, který umožňuje klientům ve stejné místní síti vidět se a komunikovat mezi sebou.
- **Security**: Způsob zabezpečení WiFi sítě.
  - **WPA2 Personal**: Metoda zabezpečení, která používá předem sdílený klíč (tzv. pre-shared key) k šifrování a ověřování dat mezi přístupovým bodem a jednotlivými stanicemi. Prakticky to znamená, že pro připojení k WiFi síti (k AP) je nutné zadat heslo nastavené v konfiguraci (položka **Password**).
  - **WPA2 Enterprise**: Vysoce bezpečná metoda vyžadující jedinečnou autentizaci pro každého uživatele. Využívá se protokol 802.1X s centrálním RADIUS serverem pro ověřování požadavků na připojení. Zvolíte-li tuto možnost, zpřístupní se tyto konfigurační položky:
    - **RADIUS Auth Server**: IPv4 nebo IPv6 adresa ověřovacího serveru RADIUS.
    - **RADIUS Auth Password**: Přístupové heslo pro ověřovací server RADIUS.
    - **RADIUS Auth Port**: Číslo portu ověřovacího serveru RADIUS.
    - **RADIUS NAS Identifier**: Identifikátor NAS (Network Access Server) používaný při komunikaci s RADIUS serverem.
  - **WPA3 Personal**: Nejnovější standard zabezpečení WiFi sítě, který používá metodu Simultaneous Authentication of Equals (SAE) zajišťující robustnější a bezpečnější ověřování pomocí hesel ve srovnání s **WPA2 Personal**.

  - **WPA3 Enterprise**: Nejnovější generace zabezpečení WiFi s pokročilými kryptografickými nástroji. V porovnání s předchozími standardy nabízí silnější šifrování (až 192bitové) a povinnou ochranu řídicích rámců (PMF) pro odolnost proti útokům. Zvolíte-li toto zabezpečení, zobrazí se stejné konfigurační položky jako v případě zabezpečení **WPA2 Enterprise**.

- **IP Address**: Pevná IP adresa WiFi rozhraní (IPv6 adresu lze zadat ve zkrácené notaci).
- **Subnet Mask / Prefix**: Maska sítě pro IP adresu verze 4 (určuje, které bity označují síť, či podsíť, a které bity označují zařízení). V případě použití IPv6 adresy je třeba zadat prefix, tedy číslo v rozsahu 8 až 128.
- **MTU**: Maximální velikost datového paketu.



Obrázek 24: Konfigurace přístupového bodu

DHCP Server

DHCP server přiřazuje připojeným klientům IP adresu, IP adresu výchozí brány a zároveň IP adresu DNS serveru. Podporováno je statické (**Static DHCP leases**) a také dynamické přiřazování IP adres. Dynamické přiřazování adres přiděluje klientům IP adresy z definovaného adresního prostoru (viz položky **Client IP Pool Start** a **Client IP Pool End**). Statické přiřazování adres přiděluje IP adresy, které odpovídají MAC adresám připojených klientů (přidat je lze tlačítkem +).

- **Configuration Mode**: Povoluje dynamické přiřazování IP adres. V případě používání IPv6 adresy je třeba zvolit metodu přidělování adres.
  - **DHCP**: Stavová autokonfigurace – zařízení oznámí typ autokonfigurace a vše ostatní zajišťuje DHCPv6 server. Varianta výhodná především v situacích, kdy se v síti mohou vyskytovat zařízení, kterým dostatečně nedůvěřujeme, anebo je potřeba mít o všech zařízeních v síti přehled.
  - **SLAAC**: Bezstavová autokonfigurace, která ke konfiguraci klienta využívá pouze informace poskytované zařízením. Jedná se o výhodné řešení především pro malé sítě s několika jednotkami zařízení nebo rozsáhlé sítě s mnoha malými podsítěmi, kde každá podsíť má definovaný vlastní prefix.
  - **DHCP + SLAAC**: Hybridní režim přidělování síťových adres a parametrů. SLAAC zajišťuje konektivitu a DHCP dodává specifické parametry sítě. Hlavní výhodou je maximální kompatibilita (některá zařízení preferují adresu z DHCP, zatímco jiná se spoléhají výhradně na SLAAC, v tomto režimu funguje obojí).
- **Client IP Pool Start**: Počáteční IP adresa rozsahu pro dynamické přidělení.
- **Client IP Pool End**: Koncová IP adresa rozsahu pro dynamické přidělení.
- **Lease Time**: Doba platnosti IP adresy před jejím uvolněním a opětovným přidělením. Zadaná hodnota odpovídá času v sekundách.

10.3.2 Stanice

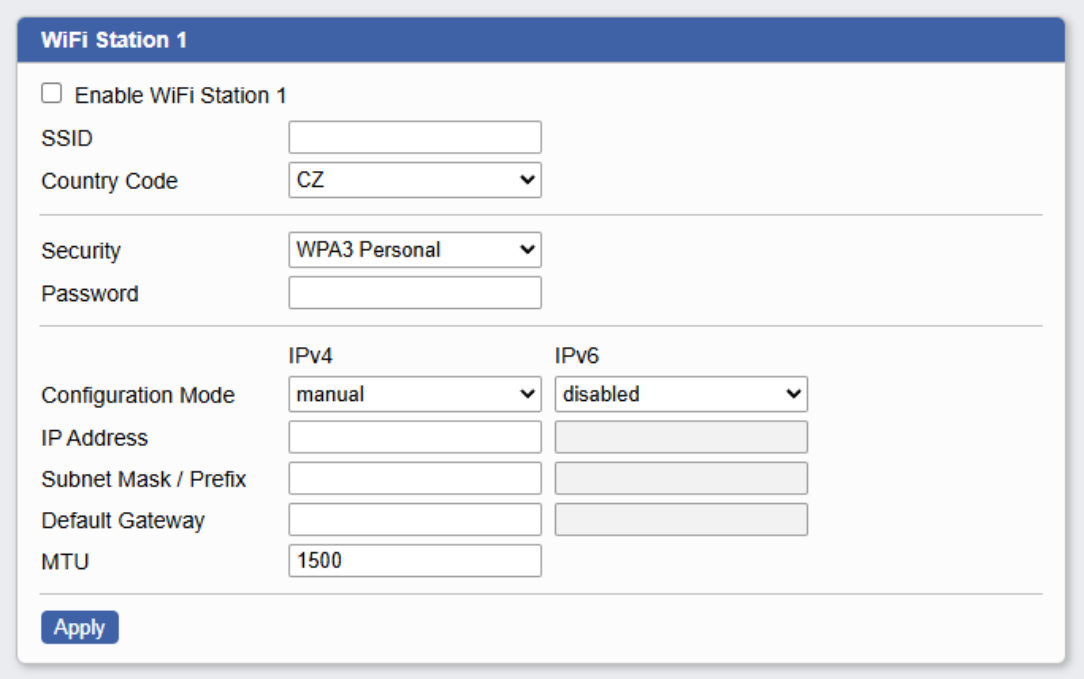
Cesta: Configuration → Interfaces → WiFi Station 0 / 1

Na této stránce je možné konfigurovat WiFi připojení, ve kterém bude zařízení fungovat jako stanice. To znamená, že se bude připojovat k definovanému přístupovému bodu (AP) ve svém okolí. Pro aktivaci tohoto režimu zaškrtněte políčko ☐ **Enable WiFi Station** v horní části konfiguračního formuláře. Níže jsou uvedeny dostupné možnosti konfigurace.

- **SSID**: Identifikátor WiFi sítě (přístupového bodu), do které se zařízení připojuje.
- **Country Code**: Kód země, v níž je zařízení nainstalováno. Používá se kód ve formátu ISO 3166-1 alpha-2.
- **Security**: Způsob zabezpečení dané WiFi sítě.
  - **WPA2 Personal**: Metoda zabezpečení, která používá předem sdílené heslo (tzv. pre-shared key) k šifrování a ověřování dat mezi přístupovým bodem a jednotlivými stanicemi. Prakticky to znamená, že pro připojení k WiFi síti (k AP) je nutné zadat heslo nastavené v konfiguraci (položka **Password**).
  - **WPA2 Enterprise**: Vysoce bezpečná metoda vyžadující jedinečnou autentizaci pro každého uživatele. Využívá se protokol 802.1X s centrálním RADIUS serverem pro ověřování požadavků na připojení. Jestliže tuto možnost zvolíte, zpřístupní se volba **Authentication**, což je metoda zabezpečení autentizačního procesu. Zvolit lze pouze možnost **PEAP/MSCHAPv2**, díky níž dojde k vytvoření šifrovaného tunelu pro ochranu přihlašovacích údajů uživatele (uživatelské jméno a heslo – **Identity** a **Password**), jež se používají k autentizaci proti RADIUS serveru.
  - **WPA3 Personal**: Nejnovější standard zabezpečení WiFi sítě, který používá metodu Simultaneous Authentication of Equals (SAE) zajišťující robustnější a bezpečnější ověřování pomocí hesel ve srovnání s **WPA2 Personal**.

  - **WPA3 Enterprise**: Nejnovější generace zabezpečení WiFi s pokročilými kryptografickými nástroji. V porovnání s předchozími standardy nabízí silnější šifrování (až 192bitové) či povinnou ochranu řídicích rámců (PMF) pro odolnost proti útokům. Zvolíte-li toto zabezpečení, zobrazí se stejné konfigurační položky jako v případě zabezpečení **WPA2 Enterprise**.

- **Configuration Mode**: Způsob přidělení IP adresy a dalších souvisejících parametrů.
  - **DHCP**: Přiřazení potřebných údajů řeší DHCP server.
  - **manual**: Uživatel vyplní potřebné údaje pomocí položek níže.
  - **disabled**: WiFi rozhraní nemá přidělenu fixní IP adresu.
- **IP Address**: Pevná IP adresa WiFi rozhraní stanice (IPv6 adresu je možné vyplnit ve zkrácené notaci).
- **Subnet Mask / Prefix**: Maska sítě pro IP adresu verze 4 (určuje, které bity označují síť, či podsíť, a které bity označují zařízení). V případě použití IPv6 adresy je třeba zadat prefix, tedy číslo v rozsahu 8 až 128.
- **Default Gateway**: IP adresa výchozí brány (tj. zařízení, které slouží jako výstupní bod pro komunikaci mimo lokální síť).
- **MTU**: Maximální velikost datového paketu.



Obrázek 25: Konfigurace WiFi stanice

10.4 Provoz více WiFi rozhraní současně

Zařízení umožňuje nakonfigurovat a aktivně využívat dva přístupové body (AP) a také dvě stanice (STA), tedy až čtyři WiFi rozhraní současně. Zároveň však platí, že oba přístupové body budou fungovat na stejném kanále apod. Přehled možných kombinací a jejich omezení je podrobně popsán v následující tabulce.

Počet	Kombinace	Popis
2	2× AP	Dvě rozhraní fungující na stejném kanálu.
	AP + STA	Dvě rozhraní na dvou různých kanálech.
	2× STA	Dvě rozhraní na dvou různých kanálech.
3	2× AP + STA	Všechny tři rozhraní fungují na jednom kanále.
	AP + 2× STA	Použití této kombinace je limitováno na dva kanály. Na společném kanálu budou buď AP+STA nebo 2× STA.
4	2× AP + 2× STA	Varianta, která není příliš vhodná k praktickému použití. Všechny čtyři rozhraní fungují na jednom kanále.

Tabulka 5: Provoz více WiFi rozhraní současně

11. Firewall

Každé zařízení připojené k síti je vystaveno celé řadě bezpečnostních hrozeb – od pokusů o neoprávněný přístup až po útoky škodlivého softwaru či narušení soukromí. Základním prvkem obrany proti těmto rizikům je firewall, který slouží k řízení a ochraně datového provozu mezi různými sítěmi.

Zařízení s integrovaným firewallem navíc také aktivně filtruje provoz podle definovaných pravidel. Díky tomu může blokovat nežádoucí příchozí spojení z veřejné sítě, omezovat přístup ke konkrétním službám nebo chránit jednotlivá zařízení před útoky zvenčí. Firewall tak představuje první linii obrany celé sítě – a jeho správné nastavení je klíčové pro zajištění kybernetické bezpečnosti.

11.1 Základní informace

DŮLEŽITÁ INFORMACE

Firewall chrání veškerý příchozí provoz a také veškeré přeposílání paketů na správné rozhraní v rámci zařízení (tzv. forwarding). Pouze výstup z procesů spuštěných na zařízení není firewallem jakkoliv kontrolován.

Firewall na tomto zařízení se skládá z několika vrstev. Nejnižší vrstvou je základní politika, jež je definována na stránce **General Rules**. V mnoha situacích bude zcela dostačující provést konfiguraci právě na této stránce. O úroveň výše je přístup k jednotlivým službám, které na zařízení běží (konfigurovat jej lze na stránce **Service Access**). Nejvyšší vrstvou s nejvyšší prioritou jsou pak pravidla, která určují, jaký provoz může vstoupit přímo do samotného zařízení (formulář **Input Rules**), a pravidla, která řídí přeposílání (forwarding) provozu skrz zařízení – tedy mezi různými sítěmi (formulář **Forward Rules**).

11.2 Obecná konfigurace (General Rules)

Cesta: Configuration → Firewall → General Rules

Na této stránce je možné konfigurovat základní politiku na nejnižší úrovni firewallu, ve které každé rozhraní spadá do nějaké zóny a síťový provoz mezi jednotlivými zónami je tímto formulářem povolen (**allow**) či zakázán (**deny**).

Ve horní části formuláře je k dispozici seznam dostupných rozhraní. Pro každé z nich lze nastavit tyto parametry:

- **Zone**: Položka, která definuje, do jaké zóny uvedené rozhraní spadá.
- **Masquerade**: Dynamický překlad síťových adres, který přepisuje zdrojovou IP adresu v odchozím provozu.

Ve spodní části formuláře je názorná matice, která slouží pro konfiguraci síťového provozu mezi jednotlivými zónami. Řádky představují zóny, ze kterých provoz přichází, a sloupce zóny, do kterých provoz směřuje. Síťový provoz lze pro jednotlivé možnosti povolit (**allow**) či zakázat (**deny**) a nadefinovat tak základní bezpečnostní politiku na nejnižší úrovni firewallu.

- **LAN**: Lokální síťová zóna, která pokrývá malé geografické území.
- **DMZ**: Částečně izolovaná (zpravidla lokální) síťová zóna, která umožňuje přístup na určité servery.
- **WAN**: Zóna primárně určená pro širokopásmovou (veřejnou) síť.
- **Tunnel**: Zóna primárně určená pro síťová rozhraní patřící do tunelových (VPN) spojení.
- **Other**: Síťová zóna pro nezařazený nebo neklasifikovaný provoz.
- **Service**: Zóna jednotlivých služeb, které na zařízení běží.
- **SW Module**: Zóna softwarových modulů a aplikací.

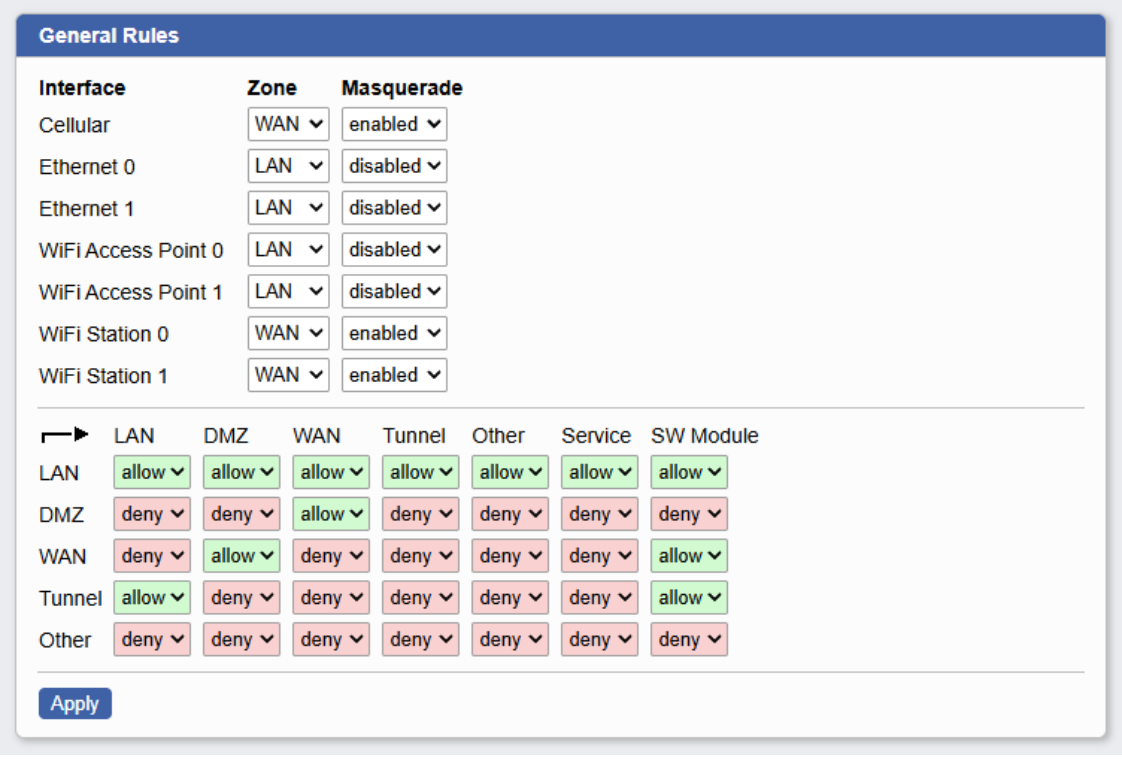
PŘÍKLAD

Nastavení znázorněné na obrázku níže říká, že např. provoz přicházející z demilitarizované zóny (**DMZ**) má přístup k rozhraním v zóně **WAN**. Z DMZ se však není možné dostat k vnitřním službám zařízení (zóna **Service**) ani k rozhraním přiřazeným do zóny **LAN**.

V rámci stejného nastavení (obrázek níže) naopak provoz přicházající z lokální sítě (zóna **LAN**) není nijak blokován (v rámci této základní politiky) a je možné tak přistoupit do všech ostatních zón.

DŮLEŽITÁ INFORMACE

V případě služeb **DNS**, **DHCP** a **NTP** platí na této rozhodovací úrovni, že provoz směřující k těmto službám je v zónách **LAN a DMZ vždy povolen** a v zónách **WAN a Other vždy zakázán** nezávisle na nastavení přístupu k vnitřním službám zařízení (zóna **Service**).



Obrázek 26: Firewall – Obecná konfigurace

11.3 Přístup ke službám

Cesta: Configuration → Firewall → Service Access

Konfigurační formulář **Service Access** umožňuje nastavit přístupová pravidla firewallu k interním službám zařízení.

Aktivovat tuto vrstvu firewallu lze volbou ☐ **Enable service access**. Jednotlivá pravidla se přidávají pomocí tlačítka + (tlačítkem − se odebírají). Pro každé pravidlo je pak možné nastavit tyto parametry:

- **Service**: Služba, ke které je tvořeno přístupové pravidlo (**HTTPS**, **SSH**, **SNMP**).
- **Input Interface**: Rozhraní, přes které přichází síťový provoz k dané službě.
- **Family**: Typ IP adres, který se má použít v daném pravidle – **IPv4**, **IPv6** nebo oba.
- **Source IP Address**: Zdrojová IP adresa, ze které přichází požadavek na zařízení. Pravidlo se uplatní jen na provoz, který přichází právě z této konkrétní IP adresy.
- **Prefix**: Určuje rozsah IP adres, které jsou zahrnuty v definovaném pravidle. Uvádí se ve zkráceném zápise, tzv. CIDR notaci (např. 32 v případě jediné adresy).
- **Public Port**: Číslo portu, přes který je přístupná zvolená služba zařízení (**Service**).
- **Policy**: Zvolená politika – přístup je povolen (**allow**) nebo zakázán (**deny**).

Obrázek 27: Přístup ke službám

11.4 Pravidla pro příchozí provoz (Input Rules)

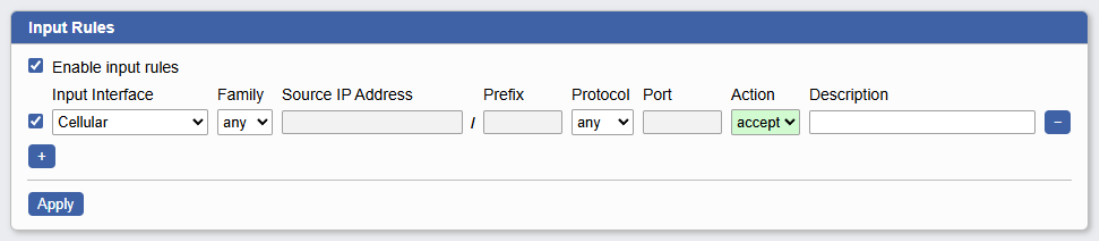
Cesta: Configuration → Firewall → Input Rules

Input Rules jsou bezpečnostní pravidla, která určují, jaký provoz je povolen nebo zakázán přímo na samotné zařízení – tedy když je zařízení cílovým bodem komunikace. Tvoří nejvyšší vrstvu firewallu a mají nejvyšší prioritu.

Povolit nebo zakázat celý blok pravidel lze volbou ☐ **Enable input rules**. Jednotlivá pravidla se přidávají pomocí tlačítka + (a tlačítkem − se odebírají). Pro každé z nich je pak možné nastavit tyto parametry:

- **Input Interface**: Rozhraní, přes které přichází síťový provoz. Umožňuje aplikovat pravidlo pouze na vybrané rozhraní.
- **Family**: Typ IP adres, který se bude brát v potaz v daném pravidle – **IPv4**, **IPv6** nebo oba tyto typy (**any**).
- **Source IP Address**: Zdrojová IP adresa, ze které přichází požadavek na zařízení. Pravidlo se uplatní jen na provoz, který přichází právě z této konkrétní IP adresy.

- **Prefix**: Určuje rozsah IP adres, které jsou zahrnuty v definovaném pravidle. Uvádí se ve zkráceném zápise, tzv. CIDR notaci (např. 32 v případě jediné adresy).
- **Protocol**: Druh síťové komunikace (protokol), na který se pravidlo firewallu vztahuje (**TCP**, **UDP**, **ICMP** nebo jakýkoliv).
- **Port**: Číslo cílového portu, na který směřuje síťová komunikace.
- **Action**: Určuje, co má firewall udělat s provozem, který odpovídá pravidlu (jsou splněny podmínky).
  - **drop**: Provoz je zahozen a odesílatel nedostane žádnou odpověď.
  - **accept**: Provoz je povolen a dorazí k cíli.
  - **reject**: Provoz je odmítnut a odesílatel dostane odpověď, že byl zablokován.
- **Description**: Uživatelem definovaný popis daného pravidla.



Obrázek 28: Pravidla pro příchozí provoz

DŮLEŽITÁ INFORMACE

Přidané pravidlo se stane aktivním až po stisknutí tlačítka Apply. Pokud přidání pravidla tímto tlačítkem nepotvrdíte, nebudou změny uloženy.

11.5 Pravidla pro přeposílaný provoz (Forward Rules)

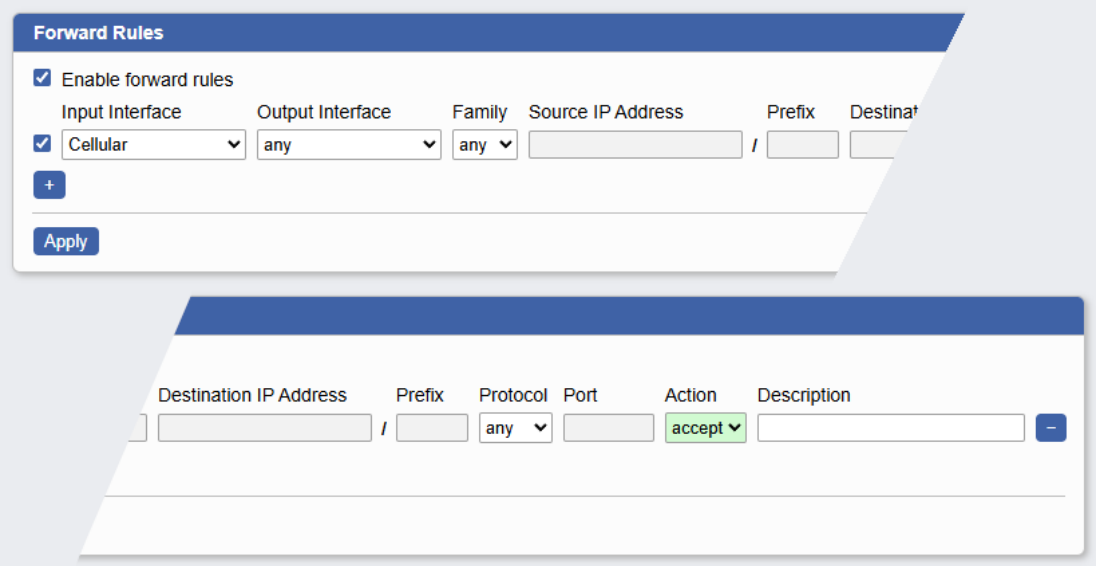
Cesta: Configuration → Firewall → Forward Rules

Forward Rules jsou bezpečnostní pravidla určující, jaký provoz může procházet přes firewall mezi různými sítěmi – tedy když pakety směřují z jednoho rozhraní do druhého. Jsou nejvyšší vrstvou firewallu a mají nejvyšší prioritu.

Povolit nebo zakázat celý blok pravidel lze volbou ☐ **Enable forward rules**. Jednotlivá pravidla se přidávají pomocí tlačítka + (a tlačítkem − se odebírají). Pro každé z nich je pak možné nastavit tyto parametry:

- **Input Interface**: Rozhraní, přes které přichází síťový provoz. Umožňuje zacílit pravidlo jen na určitý síťový vstup.
- **Output Interface**: Rozhraní, přes které odchází síťový provoz po průchodu zařízením.
- **Family**: Typ IP adres, který se bude brát v potaz v daném pravidle – **IPv4**, **IPv6** nebo oba tyto typy (**any**).
- **Source IP Address**: Zdrojová IP adresa, ze které přichází požadavek směrem na zařízení. Pravidlo se uplatní jen na provoz, který přichází právě z této konkrétní IP adresy.
  - **Prefix**: Určuje rozsah zdrojových IP adres, které jsou zahrnuty v pravidle. Uvádí se ve zkráceném zápise, tzv. CIDR notaci (např. 32 v případě jediné adresy).

- **Destination IP Address**: IP adresa zařízení, kam provoz směřuje (kam se paket přeposílá skrz firewall).
  - **Prefix**: Určuje rozsah IP adres cílových zařízení, které jsou zahrnuty v pravidle. Uvádí se ve zkráceném zápise – CIDR notaci (např. 32 v případě jediné adresy).
- **Protocol**: Druh síťové komunikace (protokol), na který se pravidlo firewallu vztahuje (**TCP**, **UDP**, **ICMP** nebo jakýkoliv).
- **Port**: Číslo cílového portu, na který směřuje síťová komunikace.
- **Action**: Určuje, co má firewall udělat s provozem, který odpovídá pravidlu (jsou splněny podmínky).
  - **drop**: Provoz je zahozen a odesílatel nedostane žádnou odpověď.
  - **accept**: Provoz je povolen a dorazí k cíli.
  - **reject**: Provoz je odmítnut a odesílatel dostane odpověď, že byl zablokován.
- **Description**: Uživatelem definovaný popis daného pravidla.



Obrázek 29: Pravidla pro přeposílaný provoz

DŮLEŽITÁ INFORMACE

Přidané pravidlo se stane aktivním až po stisknutí tlačítka Apply. Pokud přidání pravidla tímto tlačítkem nepotvrdíte, nebudou změny uloženy.

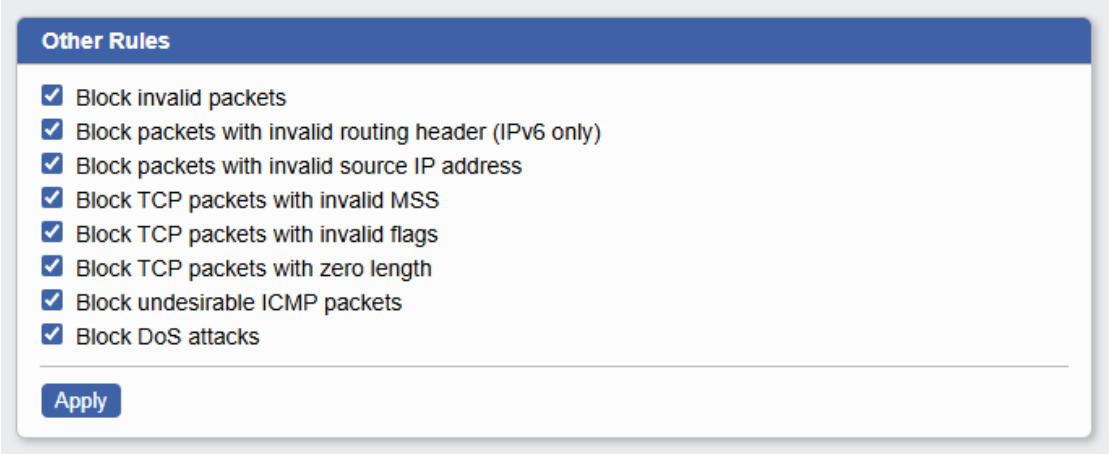
11.6 Další pravidla firewallu

Cesta: Configuration → Firewall → Other Rules

Na této stránce je možné povolit či zakázat všechna ostatní pravidla, která firewall ještě nabízí.

- ☐ **Block invalid packets**: Automatické blokování síťových paketů, které neodpovídají platnému stavu spojení nebo porušují protokolová pravidla. Jde o bezpečnostní opatření, které chrání síť před podvrženým, poškozeným nebo podezřelým (nečekaným) síťovým provozem.
- ☐ **Block packets with invalid routing header (IPv6 only)**: Zablokování IPv6 paketů, které obsahují neplatnou nebo podezřelou směrovací hlavičku – tedy takovou, která nesplňuje standardy nebo může být zneužita k útoku (např. pro obcházení filtrů nebo sledování trasy).

- ☐ **Block packets with invalid source IP address**: Zablokování síťových paketů, které mají neplatnou nebo podezřelou zdrojovou IP adresu (jako je např. 0.0.0.0, 127.0.0.1 nebo třeba také 169.254.x.x). Jedná se o velmi účinnou ochranu proti spoofingu, skenování a dalším síťovým útokům.
- ☐ **Block TCP packets with invalid MSS**: Automatické blokování TCP paketů obsahujících neplatnou nebo podezřelou hodnotu MSS (Maximum Segment Size), což je největší množství dat, které může být přeneseno v jednom TCP segmentu (bez hlaviček). Tato funkce pomáhá chránit síť před síťovými útoky (např. fragmentačními útoky) nebo třeba také před chybami v připojení kvůli špatné velikosti paketů.
- ☐ **Block TCP packets with invalid flags**: Zablokování TCP paketů, jež obsahují neplatné nebo podezřelé kombinace TCP příznaků (flags). Jde o bezpečnostní opatření, které chrání síť před různými typy síťových útoků a skenů, které zneužívají nestandardní TCP flagy k obcházení firewallů nebo detekci aktivních služeb.
- ☐ **Block TCP packets with zero length**: Zablokuje TCP pakety, které neobsahují žádná data – tedy jejich datová část (payload) má délku 0 bajtů. Jedná se o ochranu před **Stealth Scan** útoky, **TCP Flood** útoky či síťovým průzkumem.
- ☐ **Block undesirable ICMP packets**: Blokování nežádoucích nebo potenciálně zneužitelných ICMP paketů, které by mohly být použity k útokům, průzkumu sítě, zahlcení nebo obcházení bezpečnostních pravidel. Tato ochrana pomáhá zabránit síťovému průzkumu (např. pomocí programu nmap).
- ☐ **Block DoS attacks**: Detekce a blokování podezřelého síťového provozu, jenž může být součástí DoS (Denial of Service) útoku – tedy pokusu o zahlcení zařízení, sítě nebo služby. Pomáhá chránit před útoky typu **SYN Flood** či **Ping Flood**.



Obrázek 30: Další pravidla firewallu

DOPORUČENÍ

Z bezpečnostních důvodů doporučujeme ponechat všechna výše uvedená pravidla povolená. Dočasné vypnutí je vhodné pouze při řízeném testování nebo analýze konfigurace firewallu.

12. NAT

Položka **NAT**, jež je umístěná v sekci **Configuration** hlavního menu webového rozhraní, sdružuje konfigurační formuláře určené pro nastavení překladu síťových adres (NAT, Network Address Translation). Jedná se o způsob úpravy síťového provozu přepisem zdrojové nebo cílové IP adresy, případně i hlaviček protokolů vyšších vrstev.

V rámci hierarchie vyhodnocování je nejvýše **Port Forwarding**, následuje **NAT 1:1**. Na nejnižší úrovni vyhodnocování je **Default Server**.

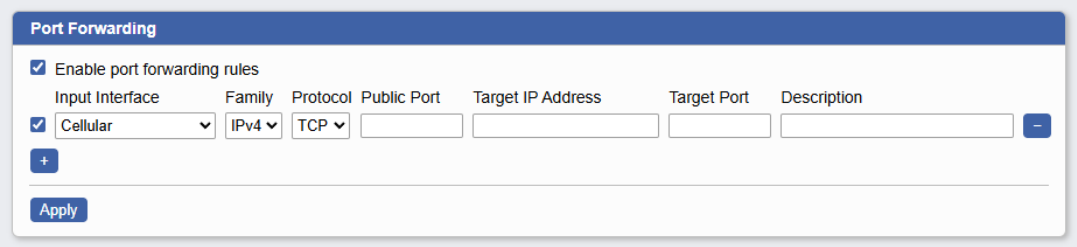
12.1 Port Forwarding

Cesta: Configuration → NAT → Port Forwarding

Port Forwarding je metoda směrování portů z jednoho síťového uzlu na druhý. Typickým použitím je umožnění vnějšímu uživateli připojit se na port na soukromé adrese v lokální síti.

Tuto funkcionalitu aktivujete zaškrtnutím volby ☐ **Enable port forwarding rules**. Jednotlivá pravidla se přidávají pomocí tlačítka + (a tlačítkem − se odebírají). Pro každé pravidlo je pak možné nastavit tyto parametry:

- **Input Interface**: Rozhraní, přes které přichází síťový provoz v rámci něhož se budou přesměrovávat porty.
- **Family**: Typ IP adres, který se má použít v daném pravidle – **IPv4** nebo **IPv6**.
- **Protocol**: Tato položka určuje, jaký typ protokolu se má přesměrovat (**TCP** nebo **UDP**).
- **Public Port**: Číslo portu, na kterém zařízení naslouchá příchozím požadavkům a následně je přesměrovává dál do vnitřní sítě.
- **Target IP Address**: IP adresa, na kterou bude zařízení posílat síťový provoz, který přijde na výše určený port (**Public Port**).
- **Target Port**: Číslo portu, na kterém cílové zařízení přijímá přesměrovávaný provoz.
- **Description**: Uživatelem definovaný popis daného pravidla.



Obrázek 31: Port Forwarding

DŮLEŽITÁ INFORMACE

Přidané pravidlo se stane aktivním až po stisknutí tlačítka Apply. Pokud přidání pravidla tímto tlačítkem nepotvrdíte, nebudou změny uloženy.

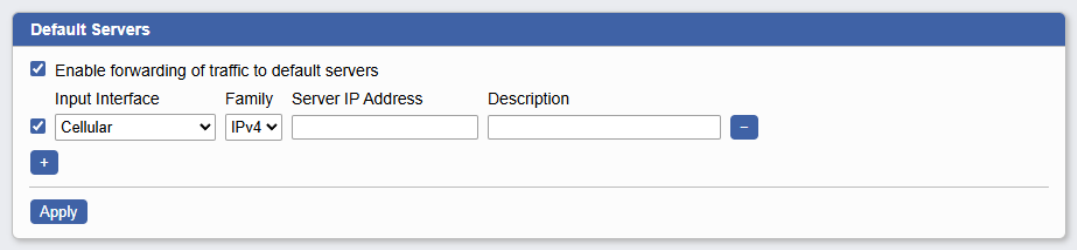
12.2 Default Servers

Cesta: Configuration → NAT → Default Servers

Default Server je místo v síti, na které bude zařízení přesměrovávat veškerý neidentifikovaný příchozí provoz (tj. nemá vlastní pravidlo port forwardingu).

Aktivovat tuto funkci lze volbou ☐ **Enable forwarding of traffic to default servers**. Jednotlivá pravidla se pak přidávají pomocí tlačítka + (tlačítkem − se odebírají). Pro každé pravidlo je pak možné nastavit tyto parametry:

- **Input Interface**: Rozhraní, v rámci něhož se bude přesměrovávat veškerý neidentifikovaný příchozí provoz.
- **Family**: Typ IP adres, který se má brát v potaz v daném pravidle – IPv4 nebo IPv6.
- **Server IP Address**: IP adresa zařízení, na které bude přesměrováván veškerý příchozí provoz, který nemá vlastní pravidlo port forwardingu.
- **Description**: Uživatelem definovaný popis daného pravidla.



Obrázek 32: Default Servers

DŮLEŽITÁ INFORMACE

Přidané pravidlo se stane aktivním až po stisknutí tlačítka Apply. Pokud přidání pravidla tímto tlačítkem nepotvrdíte, nebudou změny uloženy.

12.3 NAT 1:1

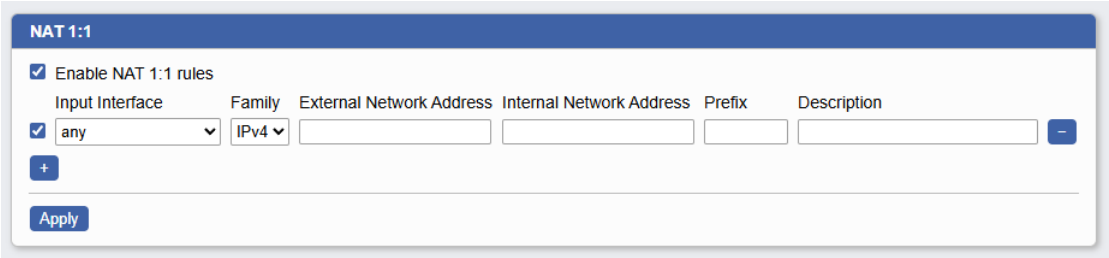
Cesta: Configuration → NAT → NAT 1:1

Jedná se o typ překladu síťových adres, při kterém zařízení přiřadí jednu veřejnou IP adresu jednomu konkrétnímu zařízení ve vnitřní síti. Překlad je trvalý a statický, takže určité zařízení ve vnitřní síti vždy komunikuje s vnější sítí přes stejnou veřejnou IP adresu.

Aktivovat tuto funkcionalitu lze volbou ☐ **Enable NAT 1:1 rules**. Jednotlivá pravidla se přidávají pomocí tlačítka + (a tlačítkem − se odebírají). Pro každé pravidlo je pak možné nastavit tyto parametry:

- **Input Interface**: Síťové rozhraní, přes které probíhá komunikace.
- **Family**: Typ IP adres, který se má brát v potaz v daném pravidle – IPv4 nebo IPv6.
- **External Network Address**: Externí IP adresa, která bude překládána na konkrétní interní (soukromou) IP adresu.
- **Internal Network Address**: Soukromá IP adresa zařízení ve vnitřní síti, na kterou se překládá provoz přicházející z externí IP adresy.

- **Prefix**: Síťová maska, která určuje, kolik adres je zahrnuto v nadefinovaném překladu. Používá se v případě, kdy je potřeba mapovat více IP adres najednou.
- **Description**: Uživatelem definovaný popis daného pravidla.



Obrázek 33: NAT 1:1

DŮLEŽITÁ INFORMACE

Přidané pravidlo se stane aktivním až po stisknutí tlačítka Apply. Pokud přidání pravidla tímto tlačítkem nepotvrdíte, nebudou změny uloženy.

PŘÍKLAD

V případě potřeby překladu rozsahu **8 IP adres**, může situace vypadat takto:

- **Interface**: any
- **Family**: IPv4
- **External Network Address**: 203.0.113.0
- **Internal Network Address**: 192.168.1.0
- **Mask**: 29

Výsledkem bude, že na všech rozhraních budou IPv4 adresy překládány způsobem:

- **203.0.113.1** $\longleftrightarrow$ **192.168.1.1**,
- **203.0.113.2** $\longleftrightarrow$ **192.168.1.2**,
- **203.0.113.3** $\longleftrightarrow$ **192.168.1.3**,
- ...

13. Tunely

13.1 OpenVPN

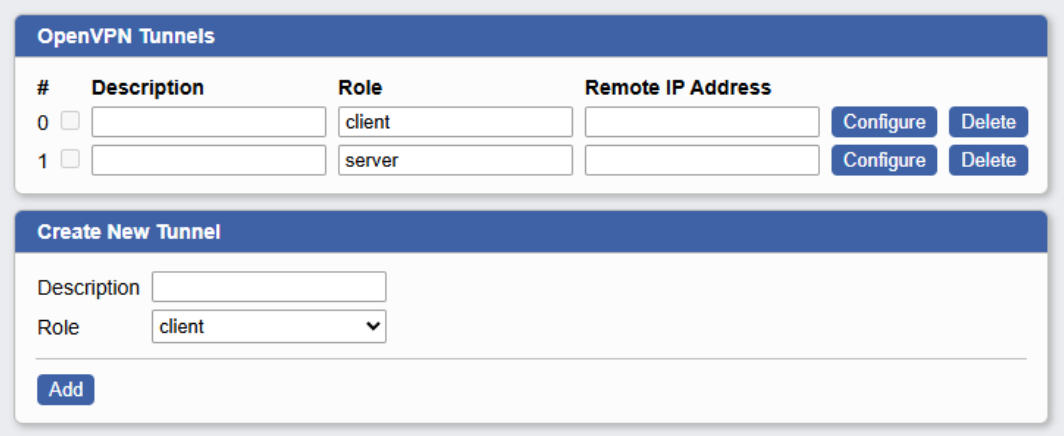
Cesta: Configuration → Tunnels → OpenVPN

OpenVPN umožňuje vytvořit šifrované (VPN) spojení mezi dvěma nebo více zařízeními (či LAN sítěmi) přes Internet nebo jinou nedůvěryhodnou síť.

Kliknutím na tlačítko Add, které je umístěné ve spodní části formuláře, je možné přidávat jednotlivé OpenVPN tunely. Pro každý z nich je třeba zadat informaci o tom, zda zařízení bude plnit roli klienta či serveru (položka **Role**). Zároveň je možné vždy vyplnit popis daného tunelu (**Description**).

V horní části formuláře je k dispozici přehled již vytvořených tunelů. Součástí přehledu jsou také následující tlačítka:

- Configure: Otevření stránky s podrobnou konfigurací daného tunelu.
- Delete: Smazání daného VPN tunelu.



Obrázek 34: OpenVPN – Vytvoření tunelu

13.1.1 Konfigurace OpenVPN tunelu

Podrobná konfigurace OpenVPN tunelu je rozdělena do několika bloků. V prvním z nich je možné daný tunel aktivovat zaškrtnutím boxu ☐ **Enable OpenVPN tunnel** a nastavit základní parametry.

- **Description**: Textový popisek pro daný OpenVPN tunel.
- **Role**: Role, kterou bude zařízení plnit v rámci daného tunelu.
  - **client**: Tento uzel navazuje spojení se serverem a používá jeho síťové zdroje.
  - **server**: Tento uzel poslouchá příchozí VPN připojení, ověřuje klienty a spravuje tunely.
- **Topology**: Určuje způsob adresování a směrování v rámci virtuální sítě VPN. Nastavuje se pouze tehdy, je-li role zařízení v daném OpenVPN tunelu nastavena na **Server**.
  - **peer-to-peer**: Přímé propojení mezi dvěma koncovými body, které jsou rovnocenné.
  - **star**: Server funguje jako centrální uzel a všichni klienti jsou připojeni přímo k serveru.

- **Interface Type**: Určuje, na které vrstvě síťového modelu OSI bude OpenVPN tunel pracovat. Tato volba ovlivňuje způsob, jakým probíhá komunikace v rámci VPN tunelu.
  - **TUN (layer 3)**: Vytváří oddělenou virtuální podsíť pro OpenVPN klienty, která je směrována do lokální sítě. Mezi hlavní výhody patří **nižší režie** (přenáší se pouze IP pakety, ne celé ethernetové rámce) a **vyšší rychlost** (nepřenáší se zbytečný broadcast provoz).
  - **TAP (layer 2)**: Tunel přenáší celé Ethernetové rámce, včetně MAC adres. Klienti se tak stávají součástí té samé lokální podsítě jako ostatní zařízení. Hlavní výhodou je tedy **transparentnost**.
- **Family**: Typ IP adres, který bude použit v rámci sestavování tunelu – **IPv4** nebo **IPv6**.
- **Protocol**: Typ protokolu, který bude použit v rámci sestavování tunelu – **TCP** nebo **UDP**.
- **Remote IP Address**: IP adresa protější strany, k níž se má klient připojit nebo odkud server očekává spojení. Položku není nutné vyplňovat (u role server a zvolené topologii hvězda je dokonce nežádoucí, aby položka byla vyplněna).
- **Port**: Číslo portu, na kterém OpenVPN naslouchá (server) nebo se připojuje (klient).

Následuje část konfigurace, která je zaměřená na autentizaci a bezpečnost.

- **Authentication**: Metoda, kterou server a klient ověřují pravost druhé strany během navazování OpenVPN tunelu.
  - **certificates (TLS)**: Standardní a doporučený způsob, kdy se identita serveru a klienta ověřuje na základě kryptografických certifikátů.
  - **username / password**: Pro navázání spojení je nutné se prokázat klasickými přihlašovacími údaji (uživatelské jméno a heslo).
  - **static key**: Jednoduchý, ale méně bezpečný způsob, ve kterém obě strany sdílí jeden předem vytvořený klíč.
- **Username**: Uživatelské jméno určené pro přihlášení k VPN serveru.
- **Password**: Uživatelské heslo určené pro přihlášení k VPN serveru.
- **CA Certificate**: Jedná se o veřejný certifikát certifikační autority (CA), která vydala a podepsala certifikáty pro OpenVPN server a klienty. Tento soubor musí mít server i všichni klienti (nemusí být stejný). Umožňuje serveru i klientům ověřit, že certifikát druhé strany je platný a pochází z důvěryhodného zdroje.
- **Local Certificate**: Certifikát, který obsahuje veřejný klíč uzlu a informace o jeho identitě. Během navazování TLS/SSL spojení jej odesílá daný uzel (klient serveru, server klientovi) k ověření. Druhá strana ho ověří proti **CA Certificate**, aby se ujistila, že je pravý a důvěryhodný.
- **Local Private Key**: Ke každému lokálnímu certifikátu (**Local Certificate**) existuje odpovídající **Local Private Key** (Soukromý klíč), který musí zůstat utajen. Zatímco certifikát se posílá přes síť, soukromý klíč se používá lokálně k dešifrování dat a k digitálnímu podepisování v průběhu TLS handshake.
- **DH Parameters**: Předem vygenerované kryptografické konstanty potřebné pro algoritmus Diffie-Hellman (DH) pro výměnu klíčů. Nastavuje se pouze tehdy, je-li role zařízení v daném OpenVPN tunelu nastavena na **Server**.
- **Minimum TLS Security**: Nastavuje minimální sílu šifry (v bitech), kterou TLS musí mít. Volit lze mezi **112 bits**, **128 bits**, **192 bits** a **256 bits**.

- **Additional TLS Verification**: Pokud je tato položka nastavena na **enabled**, je striktně vyžadováno, aby certifikát předložený serverem obsahoval specifické pole pro ověření, že se jedná skutečně o certifikát pro server. Nastavuje se pouze tehdy, je-li role zařízení v daném OpenVPN tunelu nastavena na **Client**.
- **Additional TLS Security**: Dodatečná bezpečnostní opatření, jež se provádí na úrovni TLS handshaku mezi klientem a serverem.
  - **TLS-Auth**: Přidává HMAC podpis (jednoduché ověření integrity a autenticity) ke každému TLS paketu. Klient i server použijí klíč specifikovaný v položce **Static Key**. Server odmítne jakýkoliv paket bez správného podpisu – útočníci se tedy ani nedostanou do TLS handshake.
  - **TLS-Crypt**: Dělá totéž co **TLS-Auth**, ale navíc šifruje celý TLS handshake. Ten pak vypadá jako náhodný šum, což znamená, že firewall nebo útočník vůbec nepozná, že jde o OpenVPN.
- **Static Key**: Symetrický klíč, který má v konfiguraci OpenVPN tunelu dva účely. Prvním z nich je použití v případě, že je položka **Authentication** nastavena na **static key**. Druhé využití je v případě, je-li v položce **Additional TLS Security** vybráno **TLS-Auth** nebo **TLS-Crypt**.
- **Encryption**: Šifrovací algoritmus, který bude OpenVPN používat pro přenos dat (po navázání TLS spojení). Jde o datovou šifru, kterou se šifruje veškerý provoz uvnitř VPN tunelu. Na výběr jsou možnosti **AES-128-CBC**, **AES-192-CBC**, **AES-256-CBC**, **AES-128-GCM**, **AES-192-GCM**, **AES-256-GCM** a **CHACHA20-POLY1305**. **Použití kryptografického režimu CBC se v nových instalacích nedoporučuje.** Tento režim je podporován pouze pro účely zpětné kompatibility se staršími zařízeními a protokoly.

DŮLEŽITÁ INFORMACE

Veškerý kryptografický materiál lze spravovat prostřednictvím formuláře **Configuration** → **Security** → **Keys & Certificates**.

Ve třetí části formuláře je možné nastavovat položky, které mají zásadní vliv na stabilitu a diagnostiku připojení.

- **Ping Interval**: Určuje, jak často OpenVPN posílá kontrolní ping pakety, aby udržel spojení aktivní a detekoval výpadky.
- **Ping Timeout**: Udává, po kolika sekundách bez odpovědi se spojení považuje za mrtvé (a OpenVPN se pokusí připojit znovu).
- **Log Verbosity**: Určuje, kolik detailů souvisejících s OpenVPN se zapisuje do logu. Volit lze mezi možnostmi **low**, **middle**, **high** a **very high**. Pro běžné účely doporučujeme ponechat nastavení na hodnotě **low**.

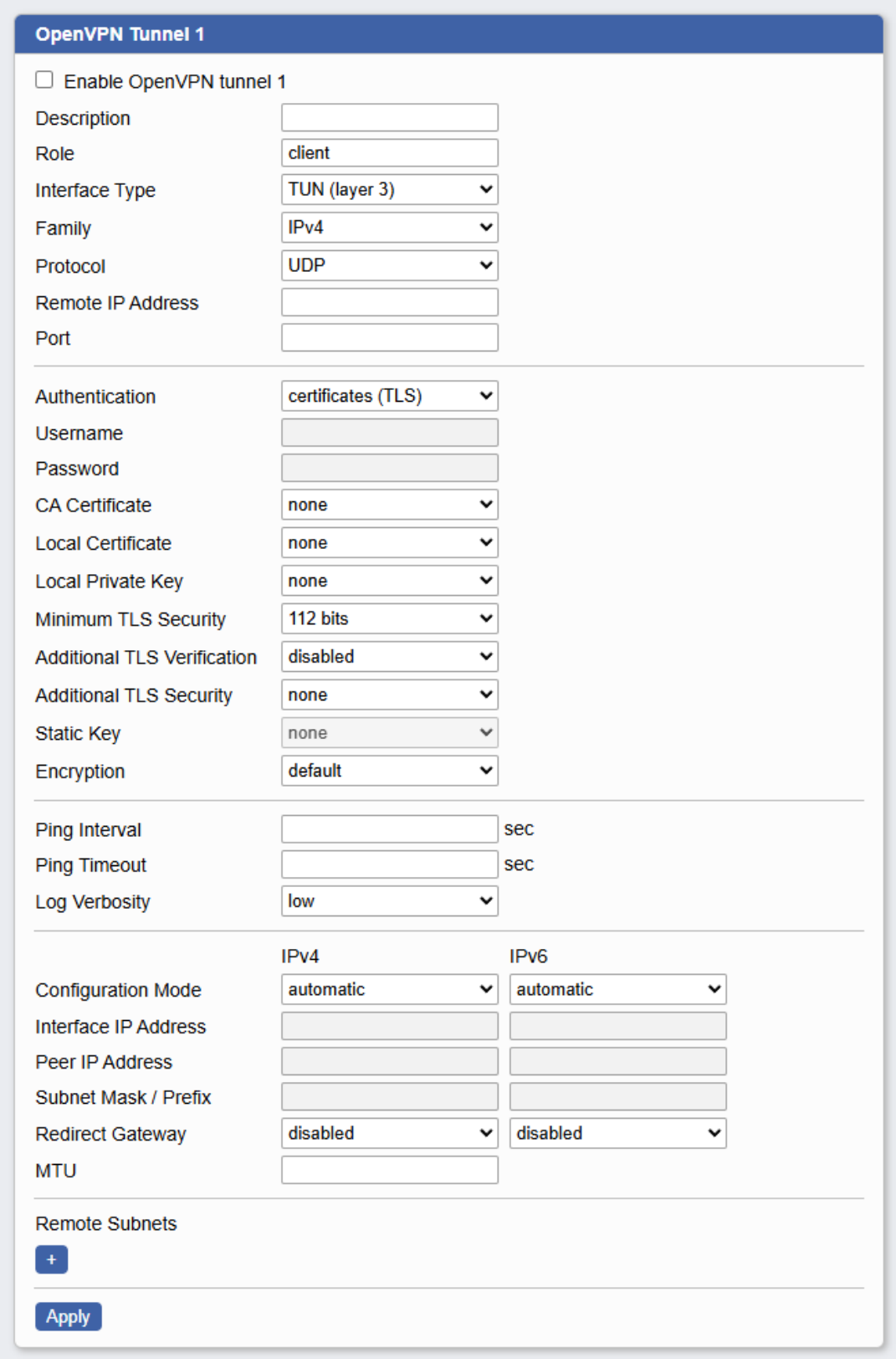
V další části konfiguračního formuláře jsou k dispozici položky, které se vztahují k síťové části konfigurace OpenVPN. Tedy k tomu, jak se přiřazují IP adresy v rámci VPN tunelu a jak je paketový provoz přenášen.

- **Configuration Mode**: Způsob přidělení IP adresy a dalších souvisejících parametrů. Nastavuje se pouze tehdy, je-li role zařízení v daném OpenVPN tunelu nastavena na **Client**.
  - **manual**: Uživatel vyplní potřebné údaje pomocí položek níže.
  - **automatic**: Potřebné údaje jsou získávány automaticky.
- **IP Address**: IP adresa, kterou má daná strana (server nebo klient) uvnitř VPN tunelu (virtuální tunelová adresa).

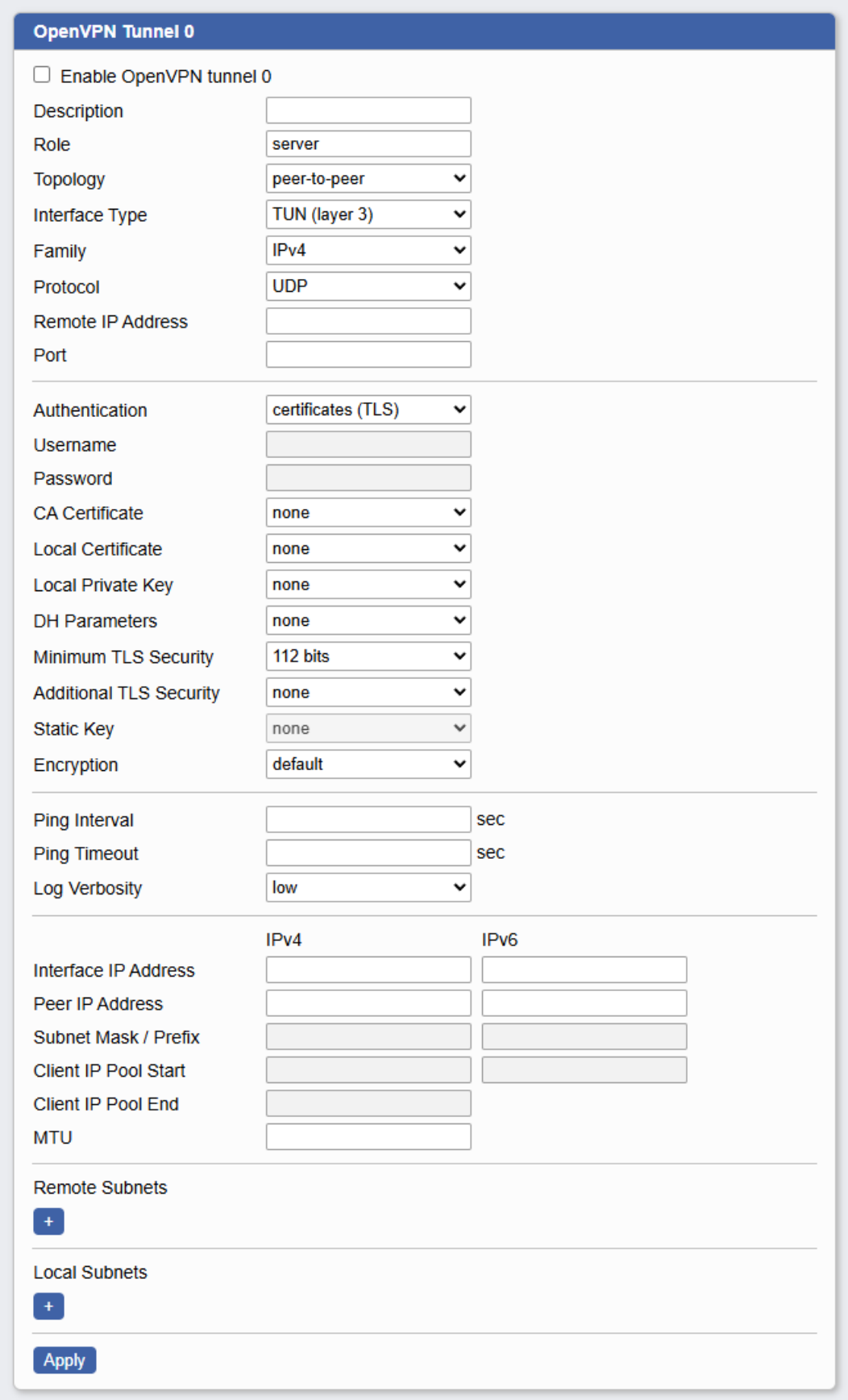
- **Peer IP Address**: Tunelová IP adresa protější strany (na serveru je to adresa klienta, na klientovi je to adresa serveru). Používá se v případě, že je **Interface Type** nastaven na **TUN (layer 3)**.
- **Subnet Mask / Prefix**: Rozsah sítě (subnet), který OpenVPN používá pro přidělování IP adres klientům v tunelu. Používá se v případě, že je **Interface Type** nastaven na **TAP (layer 2)** nebo v situaci, kdy je použita topologie hvězda (**star** v položce **Topology**).
- **Redirect Gateway**: Je-li nastaveno na **enabled**, veškerý internetový provoz klienta (tj. defaultní síťová brána) se přesměruje přes VPN tunel. Nastavuje se pouze tehdy, je-li role zařízení v daném OpenVPN tunelu nastavena na **Client**.
- **Client IP Pool Start**: Začátek rozsahu IP adres, které OpenVPN může přidělit klientům (v rámci výše definované sítě) v topologii **star**. Nastavuje se pouze tehdy, je-li role zařízení v daném OpenVPN tunelu nastavena na **Server**.
- **Client IP Pool End**: Koncová adresa rozsahu pro přidělování klientských IP adres v topologii **star**. Nastavuje se pouze tehdy, je-li role zařízení v daném OpenVPN tunelu nastavena na **Server**.
- **MTU**: Určuje maximální velikost IP paketu (v bajtech), který lze poslat skrz VPN tunel, aniž by se musel fragmentovat.

Ve spodní části této stránky je možné pomocí tlačítka + přidávat (a pomocí tlačítka − odebírat) jednotlivé podsítě, jejichž význam je následující:

- **Remote Subnets**: Síť, která leží za vzdáleným koncem tunelu (za serverem či klientem) a bude dostupná pro konfigurované zařízení. Dochází k doplnění lokální routovací tabulky.
- **Local Subnets**: Síť, která leží za OpenVPN serverem a která bude zpřístupněna připojeným klientům. Odesílá se požadavek na doplnění routovací tabulky vzdálené strany tunelu.



Obrázek 35: OpenVPN – Klient



Obrázek 36: OpenVPN – Server

14. Služby

14.1 HTTPS

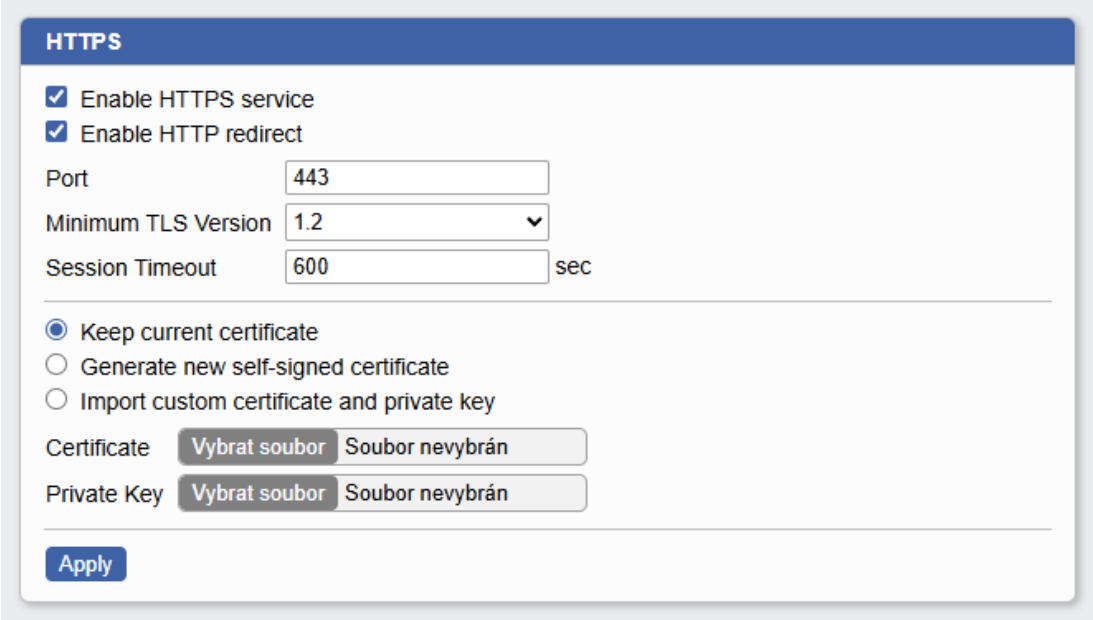
Cesta: Configuration → Services → HTTPS

HTTPS je šifrovaná verze internetového protokolu HTTP, která umožňuje uživateli přistupovat k webovému serveru a dané zařízení konfigurovat. Zabezpečuje komunikaci mezi webovým prohlížečem a serverem pomocí TLS/SSL šifrování, čímž chrání přenášená data před zneužitím a odposlechem.

- ☐ **Enable HTTPS service**: Zapnutí (aktivace) HTTPS protokolu na daném zařízení.
- ☐ **Enable HTTP redirect**: Automaticky přesměrovává nezabezpečené HTTP připojení na zabezpečené HTTPS.
- **Port**: Port, na kterém bude server naslouchat příchozím HTTPS připojením. Nejčastěji se používá **443**.
- **Minimum TLS Version**: Nejnižší povolená verze protokolu TLS (Transport Layer Security), kterou musí klient (webový prohlížeč) použít, aby se mohl bezpečně připojit k serveru. Zvolit lze bezpečnou a běžně používanou verzi 1.2 nebo nejnovější verzi 1.3, jež je ještě bezpečnější a také rychlejší.
- **Session Timeout**: Doba neaktivity (v sekundách), po které bude uživatelská relace automaticky ukončena.

Ve spodní části formuláře je možné spravovat certifikát a privátní klíč:

- **Keep current certificate**: Ponechání aktuálně používaného certifikátu (to znamená, že nedojde k žádné změně).
- **Generate new self-signed certificate**: Vygenerování nového self-signed certifikátu podepsaného samotným serverem, neověřený certifikační autoritou.
- **Import custom certificate and private key**: Možnost nahrání PEM certifikátu z externího zdroje (může být ověřen certifikační autoritou).
  - **Certificate**: Pomocí tlačítka Vybrat soubor zvolte soubor s PEM certifikátem.
  - **Private Key**: Pomocí tlačítka Vybrat soubor zvolte soubor se soukromým klíčem k certifikátu.



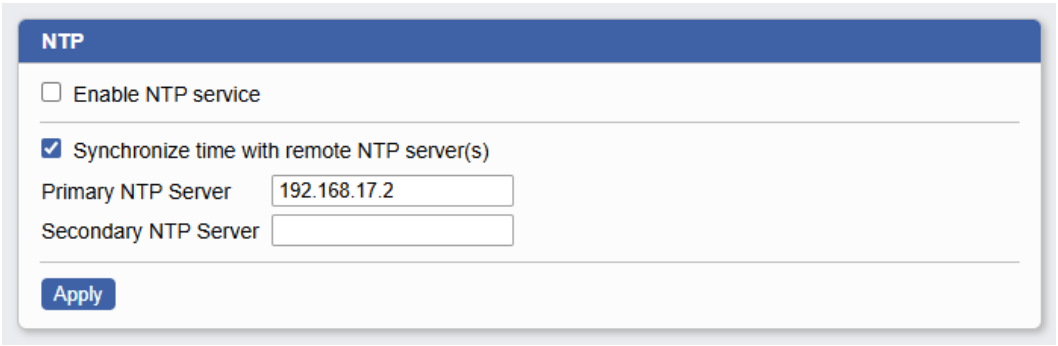
Obrázek 37: HTTPS

14.2 NTP

Cesta: Configuration → Services → NTP

Na této stránce je možné konfigurovat synchronizaci času mezi zařízeními v síti. Colias může pracovat jak v režimu NTP serveru, tak i v režimu NTP klienta.

- ☐ **Enable NTP service**: Pokud je políčko zaškrtnuto, funguje zařízení jako NTP server, což umožňuje ostatním zařízením v místní síti synchronizovat s ním svůj čas.
- ☐ **Synchronize time with remote NTP server(s)**: Je-li políčko zaškrtnuto, je čas zařízení automaticky synchronizován se vzdáleným serverem.
- **Primary NTP Server**: IP adresa nebo doménové jméno primárního vzdáleného NTP serveru.
- **Secondary NTP Server**: IP adresa nebo doménové jméno sekundárního vzdáleného NTP serveru. Tento server je dotazován, pokud je primární NTP server nedostupný.



Obrázek 38: NTP

14.3 SNMP

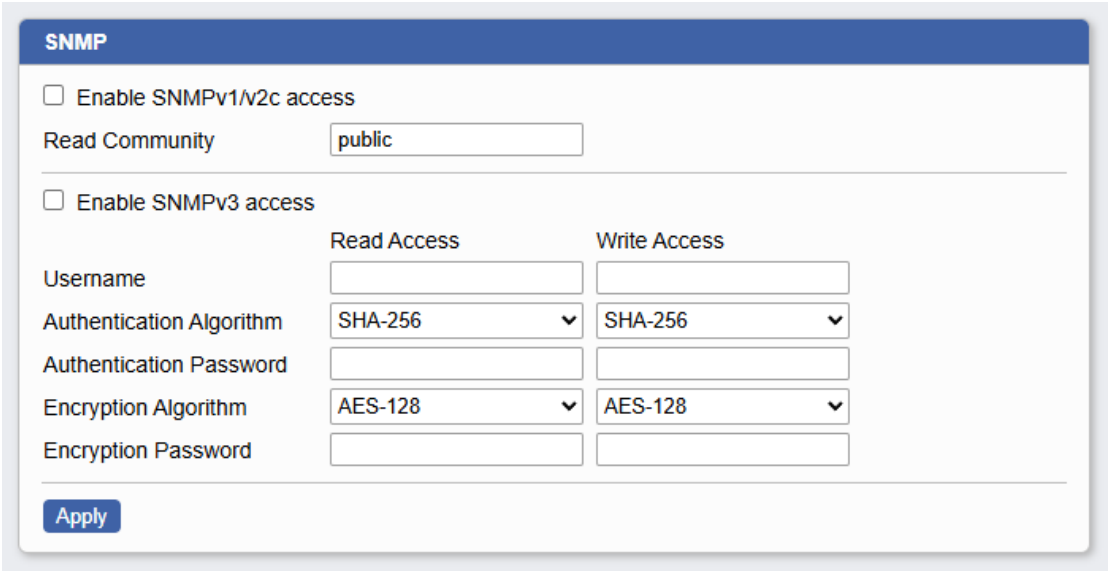
Cesta: Configuration → Services → SNMP

Prostřednictvím tohoto konfiguračního formuláře lze spravovat SNMP agenta, který přenáší informace o stavu zařízení do řídicí stanice (tzv. SNMP manažera, který slouží ke správě a monitorování zařízení pomocí protokolu SNMP). Ve verzi SNMP v3 je komunikace zabezpečena šifrováním.

Jestliže chcete povolit SNMPv1/v2c, zaškrtněte políčko ☐ **Enable SNMPv1/v2c access** a zadejte do položky **Read Community** heslo, které umožňuje SNMP manažeru číst data z agenta (bez možnosti cokoliv měnit).

Ve druhé části formuláře lze povolit agenta SNMP v3 pomocí položky ☐ **Enable SNMPv3 access** a nastavit parametry popsané níže. SNMP v3 umožňuje konfigurovat až dva uživatele. Jednoho s přístupem pouze pro čtení (sloupec **Read Access**) a druhého s přístupem pro čtení a zápis (sloupec **Write Access**).

- **Username**: Uživatelský účet, který se používá k autentizaci přístupu k SNMP agentovi.
- **Authentication Algorithm**: Hašovací funkce použitá k ověření identity uživatele přistupujícího k SNMP agentovi. Zvolit lze mezi **SHA-1**, **SHA-256**, **SHA-384** nebo **SHA-512**. **Použití hašovací funkce SHA-1 se v nových instalacích nedoporučuje.** Tato hašovací funkce je podporována pouze pro účely zpětné kompatibility se staršími zařízeními a protokoly.
- **Authentication Password**: Heslo, které se použije k vygenerování ověřovacího klíče.
- **Privacy Algorithm**: Šifrování obsahu SNMP komunikace mezi manažerem a agentem, aby data nebyla čitelná třetí stranou. Zvolit lze **AES-128**, **AES-192**, **AES-256** nebo šifrování nepoužívat (**none**).
- **Privacy Password**: Heslo, které se použije k šifrování a dešifrování SNMP dat, pokud je nastaveno šifrování v položce **Privacy Algorithm**.



Obrázek 39: SNMP

14.4 SSH

Cesta: Configuration → Services → SSH

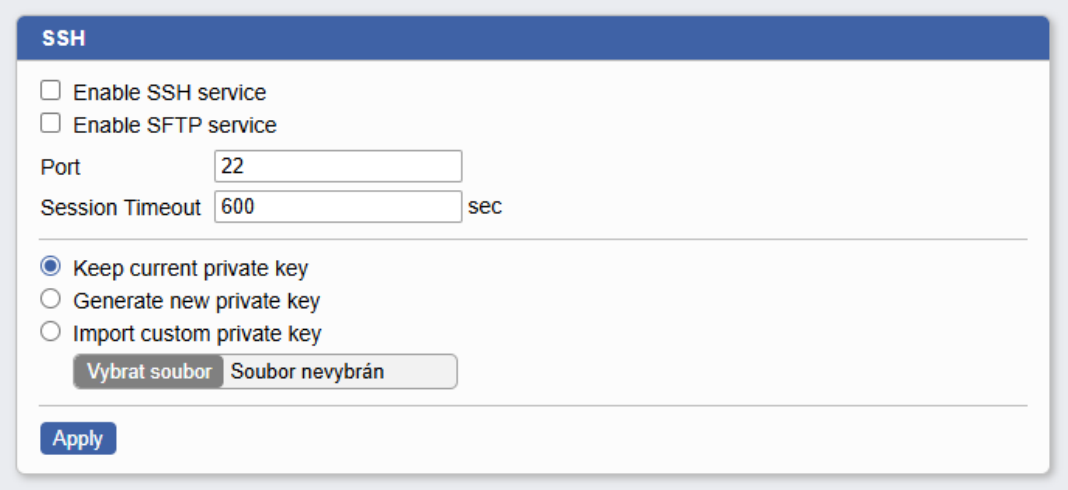
SSH (Secure Shell) je bezpečnostní síťový protokol používaný pro šifrovanou komunikaci a vzdálenou správu. Nahrazuje starší nezabezpečené protokoly, jako je Telnet, a poskytuje tak bezpečné připojení přes nedůvěryhodné sítě.

Volba ☐ **Enable SSH service** aktivuje SSH server na zařízení, který umožní vzdálený přístup přes zabezpečený terminál (SSH). Pro povolení bezpečného přenosu souborů přes SFTP (SSH File Transfer Protocol, běží nad protokolem SSH), použijte volbu ☐ **Enable SFTP service**. V rámci konfigurace pak lze nastavit ještě tyto parametry:

- **Port**: Port, na kterém SSH server naslouchá a přijímá připojení. Nejčastěji se používá **22**.
- **Session Timeout**: Doba neaktivity (v sekundách), po které bude uživatelská relace automaticky ukončena.

Ve spodní části formuláře je možné spravovat privátní klíč:

- **Keep current private key**: Ponechání aktuálně používaného SSH klíče (nedochází k žádné změně).
- **Generate new private key**: Vytvoří se nový SSH klíč.
- **Import custom private key**: Nahrání SSH klíče z externího zdroje.



Obrázek 40: SSH

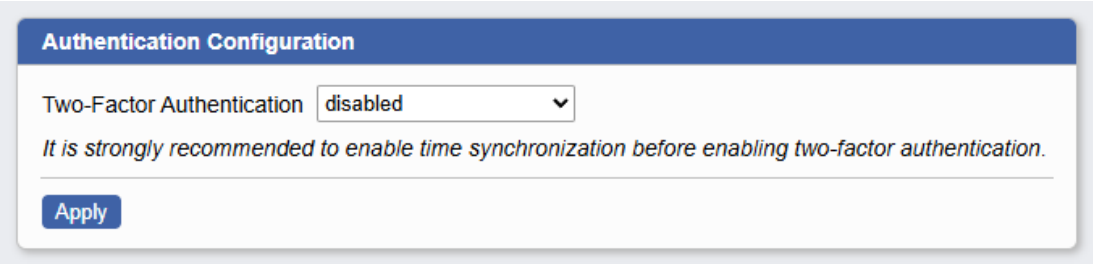
15. Bezpečnost

15.1 Dvoufaktorové ověření

Cesta: Configuration → Security → Authentication

Dvoufaktorové ověření (2FA) je metoda zabezpečení přístupu k zařízení, která vyžaduje dva různé důkazy pro potvrzení identity uživatele. Ve výchozím stavu je tato metoda deaktivována (**disabled**). Změnu lze provést na této stránce pomocí položky **Two-Factor Authentication**, kde je možné zvolit variantu **Google Authenticator**. Jedná se pouze o první (globální) polovinu konfigurace dvoufaktorového ověření.

Je-li dvoufaktorové ověření aktivní, aplikuje se na přístup přes webové rozhraní i přes SSH. V obou případech bude postup takový, že příchozí uživatel bude vyzván k zadání přihlašovacího jména a hesla a ve druhém kroku pak k zadání ověřovacího kódu. Tento kód uživatel získá z aplikace Google Authenticator (čas pro použití kódu je omezený).



Obrázek 41: Dvoufaktorové ověření

DŮRAZNÉ VAROVÁNÍ

Pro úspěšné přihlášení pomocí dvoufaktorového ověřování musí být nastaven správný systémový čas, proto důrazně doporučujeme povolit možnost synchronizace času se vzdáleným NTP serverem (viz položka **Synchronize clock with remote NTP server(s)** na stránce **Configuration → Services → NTP**).

Pokud se konfigurace dvoufaktorového ověřování nezdaří nebo se neukončí správně, nebude možné se k zařízení přihlásit pomocí daného uživatelského účtu a bude nutné se přihlásit jiným existujícím účtem, který nemá 2FA povolenu. Pokud to není možné, zbývá návrat k výchozímu (továrnímu) nastavení pomocí tlačítka RST (**pozor, dojde ke ztrátě konfigurace!**).

POZNÁMKA

Aplikaci Google Authenticator pro dvoufaktorové ověřování si do svého mobilního telefonu můžete stáhnout prostřednictvím **Google Play**[1] nebo **App Store**[2].

[1] https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
[2] https://apps.apple.com/us/app/google-authenticator/id388497605

15.2 Automatická aktualizace

Cesta: Configuration → Security → Automatic Update

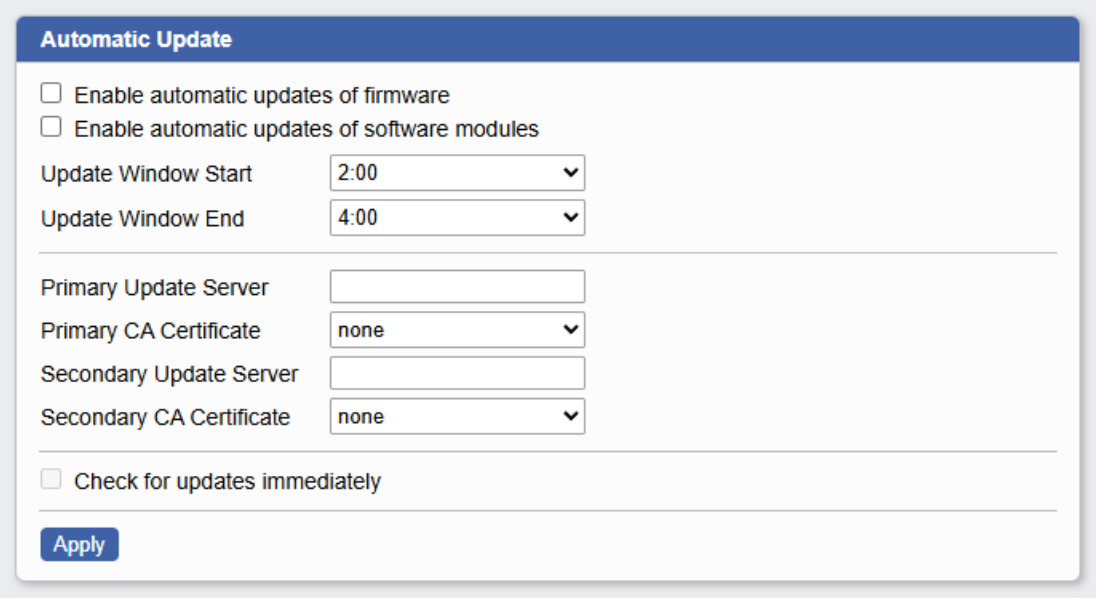
Tento konfigurační formulář umožňuje samostatně povolit automatickou aktualizaci firmware zařízení (☐ **Enable automatic updates of firmware**) a také automatickou aktualizaci softwarových modulů (☐ **Enable automatic updates of software modules**).

- **Update Window Start**: Začátek časového okna, ve kterém se zařízení připojí k serveru a zkontroluje dostupnost aktualizací. Bude-li k dispozici novější verze firmware (nebo softwarového modulu), dojde k automatické aktualizaci.
- **Update Window End**: Konec časového okna pro automatickou aktualizaci.
- **Primary Update Server**: Doménové jméno či IP adresa vzdáleného serveru, ze kterého budou čerpána data pro automatickou aktualizaci. Nová verze firmware bude očekávána v adresáři **firmware** a nové softwarové moduly v adresáři **module**.
- **Primary CA Certificate**: CA certifikát sloužící k ověření důvěryhodnosti spojení mezi zařízením a serverem. Není-li zadán, použije se předinstalovaný balík kořenových certifikátů udržovaný společností Mozilla.
- **Secondary Update Server**: Doménové jméno či IP adresa vzdáleného serveru, který bude sloužit jako záložní pro automatickou aktualizaci. Na tento server se bude zařízení připojovat pouze tehdy, pokud nebude dostupné připojení k primárnímu serveru.
- **Secondary CA Certificate**: CA certifikát sloužící k ověření důvěryhodnosti spojení mezi zařízením a záložním serverem.

DŮLEŽITÁ INFORMACE

Veškerý kryptografický materiál lze spravovat prostřednictvím formuláře **Configuration → Security → Keys & Certificates**.

Ve spodní části formuláře je k dispozici zaškrtávací box ☐ **Check for updates immediately**, který umožňuje provést kontrolu aktualizací okamžitě. Bude-li na serveru dostupná novější verze firmware (nebo softwarového modulu), dojde ihned k aktualizaci.



Obrázek 42: Automatická aktualizace

15.3 Správa kryptografického materiálu

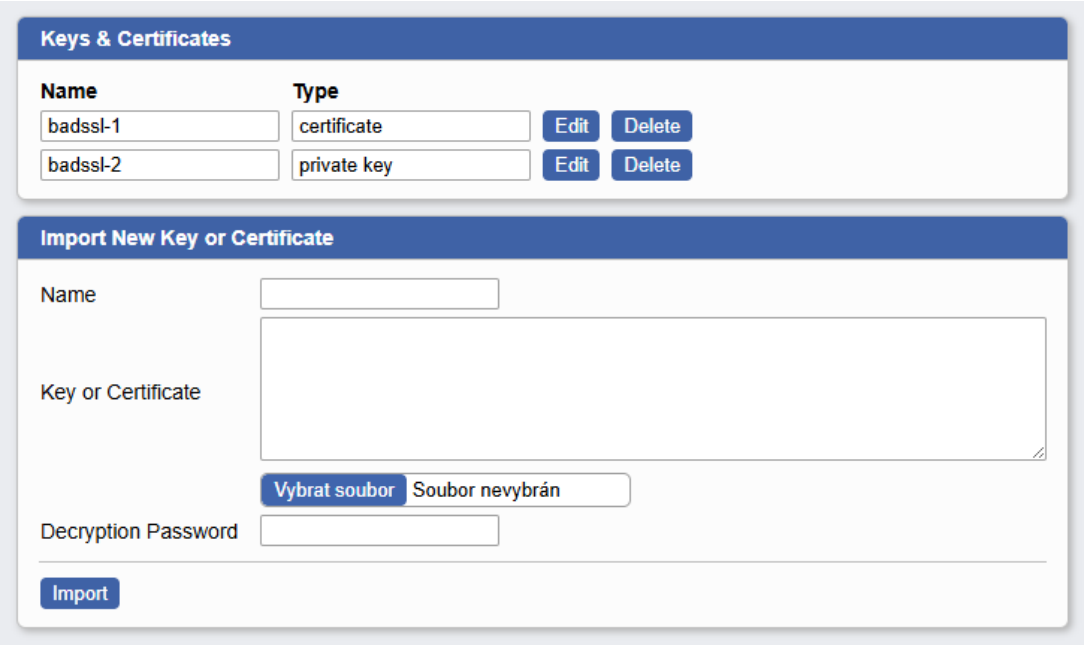
Cesta: Configuration → Security → Keys & Certificates

DŮLEŽITÁ INFORMACE

Tato část menu webového rozhraní je dostupná pouze uživatelům s rolí **administrator**.

Chcete-li do zařízení vložit nový kryptografický materiál (klíč či certifikát), použijte formulář na této stránce. Vyberte jej pomocí tlačítka Vybrat soubor nebo jej vložte do pole **Key or Certificate** a vyplňte pole pro název (**Name**). Pokud je zvolený materiál chráněný heslem, zadejte ho kvůli dešifrování do pole **Decryption Password**. Následně nahrání potvrďte tlačítkem Import.

Seznam vložených klíčů a certifikátů je k dispozici v úvodní části této stránky. Je zde uvedeno vždy jméno (**Name**) zadané při vložení kryptografického materiálu a typ tohoto materiálu (**Type**). Tlačítko Delete slouží ke smazání daného materiálu a Edit je určeno k okamžité úpravě daného kryptografického materiálu. Po kliknutí na toto tlačítko se obsah otevře ve spodní části. **Pozor, po dokončení editace dojde k restartu služeb, které daný kryptografický materiál využívají.**



Obrázek 43: Správa kryptografického materiálu

DŮRAZNÉ VAROVÁNÍ

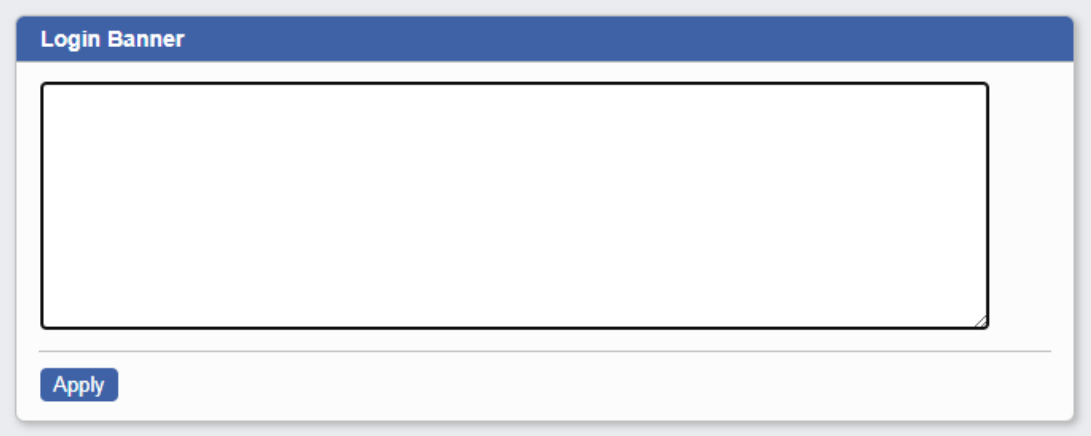
Pokud komunikujete se zařízením pomocí služby OpenVPN, u které se chystáte změnit kryptografický materiál, **může dojít k trvalé ztrátě připojení k zařízení**. Součástí procesu změny kryptografického materiálu u zvolené služby je také restartování této služby, což znamená, že se spojení přeruší. Aby bylo znovu řádně navázáno, postupujte dle kroků uvedených níže.

1. Vložte kompletní nový kryptografický materiál.
2. Nahraďte všechny odpovídající klíče a certifikáty v konfiguraci služby. **Po kliknutí na tlačítko Apply bude daná služba restartována** a dojde k požadované změně.
3. Smažte původní kryptografický materiál (není-li využíván u jiné služby).

15.4 Login Banner

Cesta: Configuration → Security → Login Banner

Na této stránce je možné konfigurovat text, který se zobrazí na přihlašovací stránce v barevném poli nad kolonkami pro zadání přihlašovacích údajů. Tento text se také zobrazí během přihlašování přes SSH.



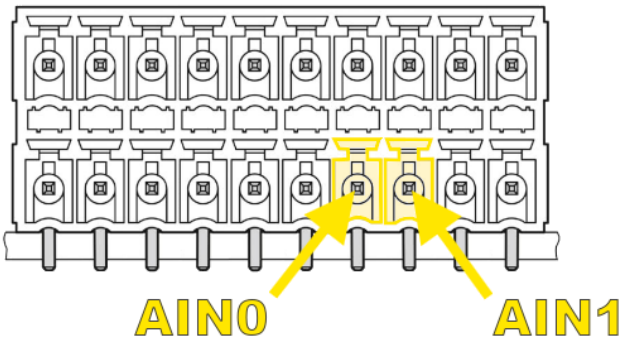
Obrázek 44: Login Banner

16. Periferie

16.1 Analogové vstupy

Cesta: Configuration → Peripherals → Analog Inputs

Tento konfigurační formulář umožňuje spravovat veškeré parametry, které se týkají analogových vstupů. Stránka je rozdělena do dvou sloupců (**AIN0** a **AIN1**) podle analogových vstupů, kterými toto zařízení disponuje.



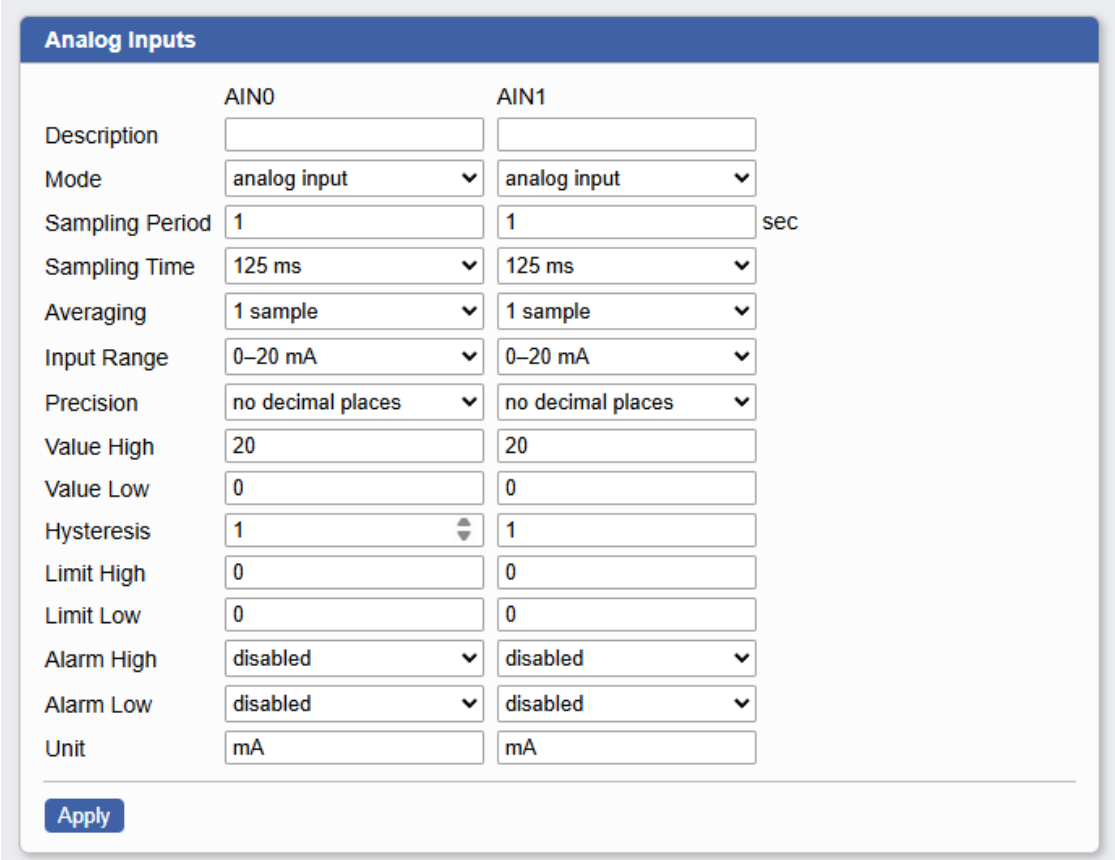
Obrázek 45: Analogové vstupy – konektor

- **Description**: Textový popisek pro daný analogový vstup.
- **Mode**: Tato volba umožňuje přepnout režim analogového vstupu (**analog input**) na binární vstup (**binary input**).
- **Sampling Period**: Časový interval mezi dvěma po sobě jdoucími vzorky (měřeními) analogového signálu. Zadává se hodnota v sekundách.
- **Sampling Time**: Doba vzorkování, což je čas, po který je proudová smyčka uzavřena. K dispozici jsou možnosti **62.5 ms**, **125 ms**, **250 ms** a **500 ms**.
- **Averaging**: Počet vzorků analogového signálu, které se zpracovávají a následně zprůměrovávají za účelem zlepšení kvality měření. Zvolit lze **1**, **2**, **4**, **8** a **16** vzorků.
- **Input Range**: Rozsah proudů (**0–20 mA** nebo **4–20 mA**), které může analogový vstup přijmout a převést na digitální hodnotu.
- **Precision**: Počet desetinných míst výsledné hodnoty – žádné (**no decimal places**) až tři (**3 decimal places**).
- **Value High**: Nejvyšší (maximální) hodnota veličiny, která odpovídá nejvyšší možné hodnotě signálu na analogovém vstupu.
- **Value Low**: Nejnižší hodnota veličiny, která odpovídá nejnižší možné hodnotě signálu na analogovém vstupu.
- **Hysteresis**: Údaj určující, o kolik se musí změnit vstupní analogová hodnota (vypočítaná veličina!) směrem dolů pod **Limit High** nebo směrem nahoru nad **Limit Low**, aby došlo k deaktivaci alarmu. Hystereze přináší větší stabilitu systému (bez hystereze by se alarm mohl neustále spouštět a deaktivovat, pokud by hodnota kolísala kolem limitní hranice).

- **Limit High**: Horní mez pro spuštění alarmu (v intervalu **Value Low** – **Value High**).
- **Limit Low**: Spodní mez pro spuštění alarmu (v intervalu **Value Low** – **Value High**).
- **Alarm High**: Aktivace alarmu (**enabled**), který se spouští ve chvíli, kdy hodnota překročí definovanou horní mez (**Limit High**).
- **Alarm Low**: Aktivace alarmu (**enabled**), který se spouští ve chvíli, kdy hodnota klesne pod definovanou spodní mez (**Limit Low**).
- **Unit**: Označení jednotky používané veličiny.

POZNÁMKA

Je-li zvolen režim binární vstup (**binary input**), je konfigurace omezena na textový popisek daného binárního vstupu (**Description**) a na aktivaci (či deaktivaci) alarmů, tedy položky **Alarm High** (vstup je aktivní, pin AINx je připojen ke GND) a **Alarm Low** (vstup není aktivní, pin AINx není připojen ke GND).

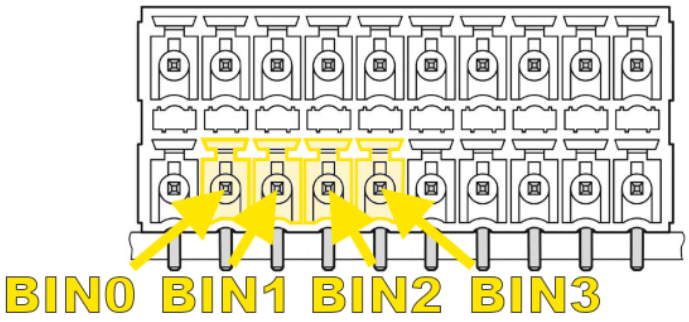


Obrázek 46: Analogové vstupy – webové rozhraní

16.2 Binární vstupy

Cesta: Configuration → Peripherals → Binary Inputs

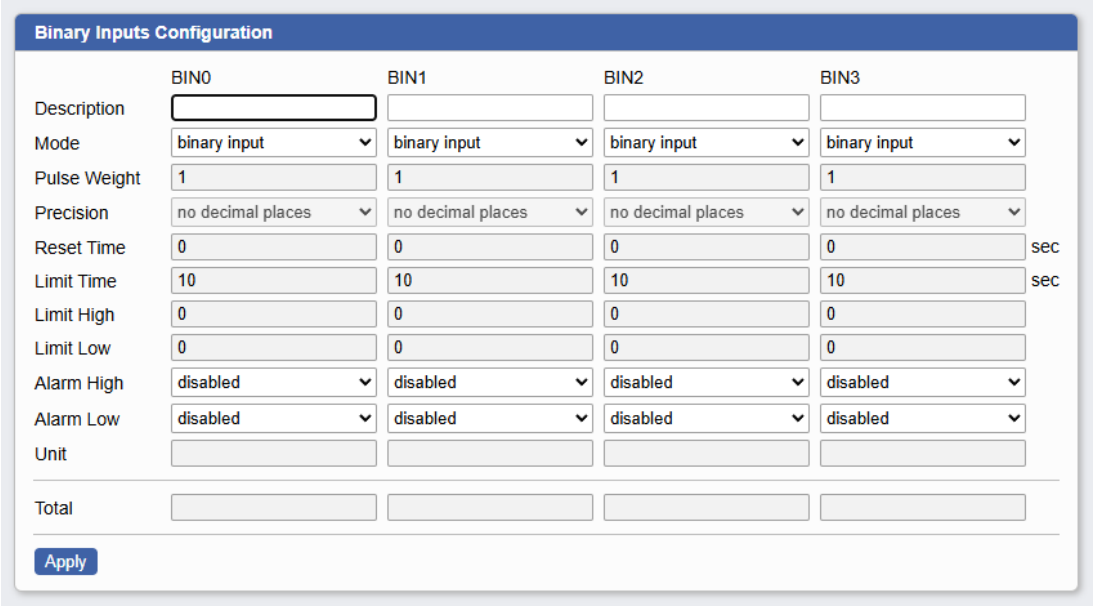
Tato stránka je rozdělena do čtyř sloupců (**BIN0**, **BIN1**, **BIN2** a **BIN3**) podle binárních vstupů, kterými zařízení disponuje.



Obrázek 47: Binární vstupy – konektor

- **Description**: Textový popisek pro daný binární vstup.
- **Mode**: Tato volba umožňuje přepnout režim binárního vstupu (**binary input**) na režim čítačového vstupu (**counter input**).
- **Pulse Weight**: Počet jednotek veličiny představující jeden pulz na čítačovém vstupu.
- **Precision**: Počet desetinných míst frekvence – žádné (**no decimal places**) až tři (**3 decimal places**).
- **Reset Time**: Časová prodleva, po které je frekvence nastavena na nulovou hodnotu, jestliže nepřijde nový impuls.
- **Limit Time**: Čas udávaný v sekundách, během kterého musí být limit překročen, aby se aktivoval alarm.
- **Limit High**: Horní mez frekvence pro spuštění alarmu (Alarm High = Rate >= Limit High).
- **Limit Low**: Spodní mez frekvence pro spuštění alarmu (Alarm Low = Rate <= Limit Low).
- **Alarm High**: Aktivace alarmu (**enabled**), který se spouští ve chvíli, kdy frekvence překročí definovanou horní mez (**Limit High**).
- **Alarm Low**: Aktivace alarmu (**enabled**), který se spouští ve chvíli, kdy frekvence klesne pod definovanou spodní mez (**Limit Low**).
- **Unit**: Označení jednotky používané veličiny.
- **Total**: Umožňuje upravit aktuální hodnotu daného čítače.

> **POZNÁMKA**
>
> Je-li zvolen režim binární vstup (**binary input**), je konfigurace omezena na textový popisek daného binárního vstupu (**Description**) a na aktivaci (či deaktivaci) alarmů, tedy položky **Alarm High** (vstup je aktivní, pin BINx je připojen ke GND) a **Alarm Low** (vstup není aktivní, pin BINx není připojen ke GND).



Obrázek 48: Binární vstupy – webové rozhraní

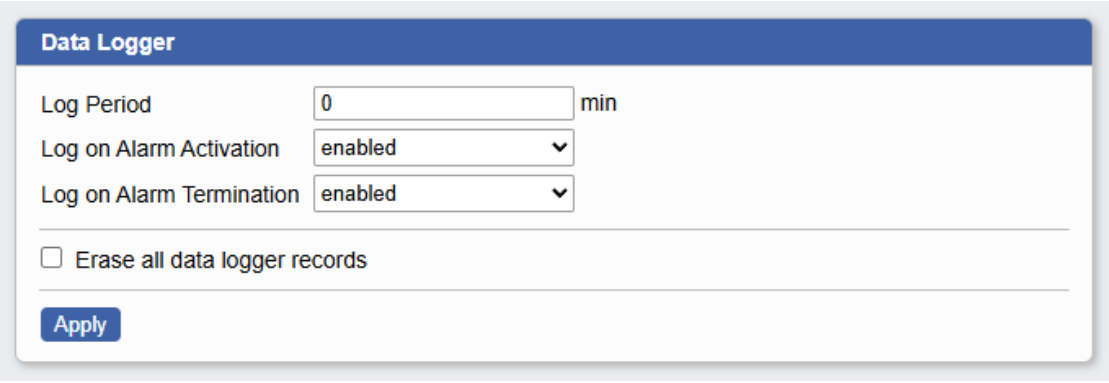
16.3 Data Logger

Cesta: Configuration → Peripherals → Data Logger

Tato stránka slouží ke konfiguraci dataloggerových funkcí. Nastavit lze tyto parametry:

- **Log Period**: Interval, ve kterém zařízení ukládá naměřené hodnoty do své paměti (zadává se v minutách).
- **Log on Alarm Activation**: Zalogování vždy při spuštění alarmu.
- **Log on Alarm Termination**: Zalogování vždy s ukončením alarmu.

Zaškrtnutím položky ☐ **Erase all data logger data** dojde k odstranění všech naměřených dat.

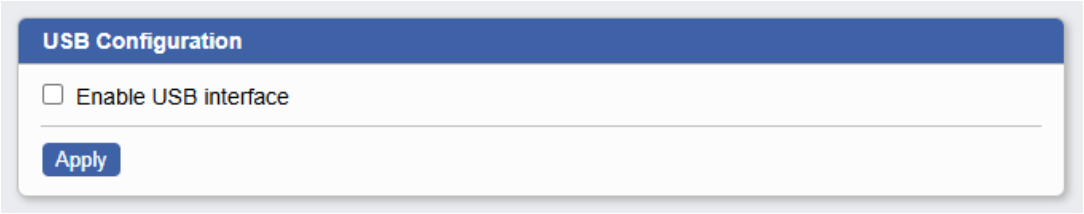


Obrázek 49: Datalogger

16.4 USB port

Cesta: Configuration → Peripherals → USB port

Tato stránka slouží k aktivaci a deaktivaci externího USB rozhraní. Pro aktivaci je třeba zaškrtnout políčko ☐ **Enable USB interface** a potvrdit.



Obrázek 50: USB port

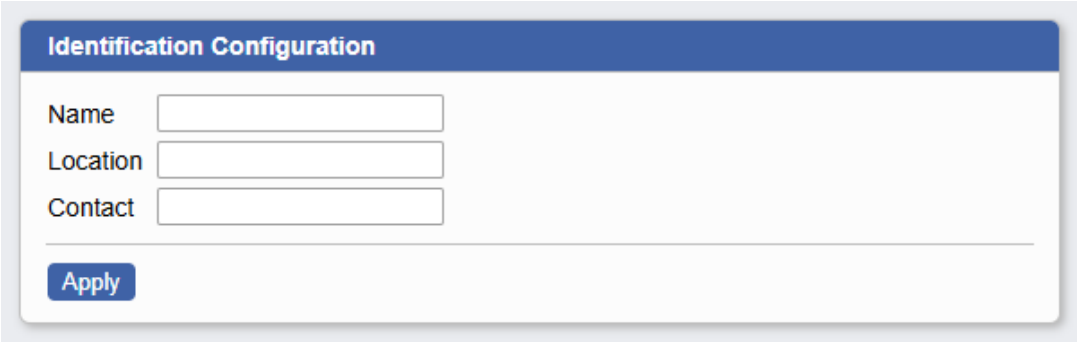
17. Konfigurace systému

Položka **System** v sekci **Configuration** hlavního menu webového rozhraní sdružuje konfigurační formuláře určené pro různá nastavení systému.

17.1 Identifikace zařízení

Cesta: Configuration → System → Identification

Stránka **Identification** umožňuje vložit údaje, které mohou pomoci zařízení identifikovat. Pro tento účel jsou připraveny položky **Name** (jméno zařízení), **Location** (popis místa, kde se zařízení nachází) a **Contact** (informace o kontaktní osobě). Tyto hodnoty využívá SNMP.



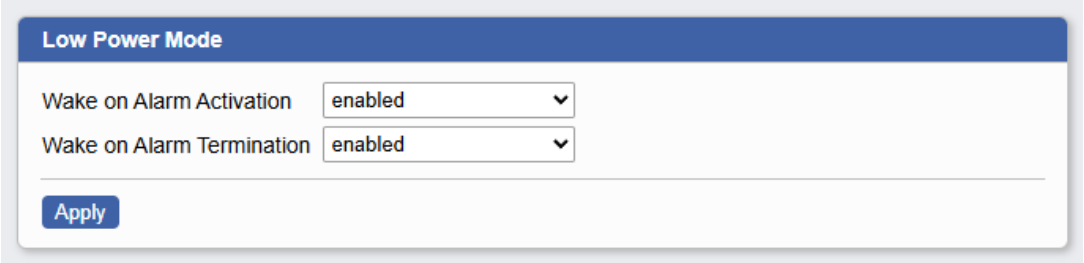
Obrázek 51: Identifikace zařízení

17.2 Režim snížené spotřeby

Cesta: Configuration → System → Low Power Mode

Konfigurační formulář **Low Power Mode** definuje, jakým způsobem bude zařízení reagovat na alarmy v režimu snížené spotřeby (alarmy pro jednotlivé binární i analogové vstupy lze konfigurovat v části Configuration → Peripherals). K dispozici jsou tyto možnosti:

- **Wake on Alarm Activation**: Probuzení zařízení při spuštění alarmu.
- **Wake on Alarm Termination** Probuzení zařízení s ukončením alarmu.



Obrázek 52: Režim snížené spotřeby

17.3 Startup skript

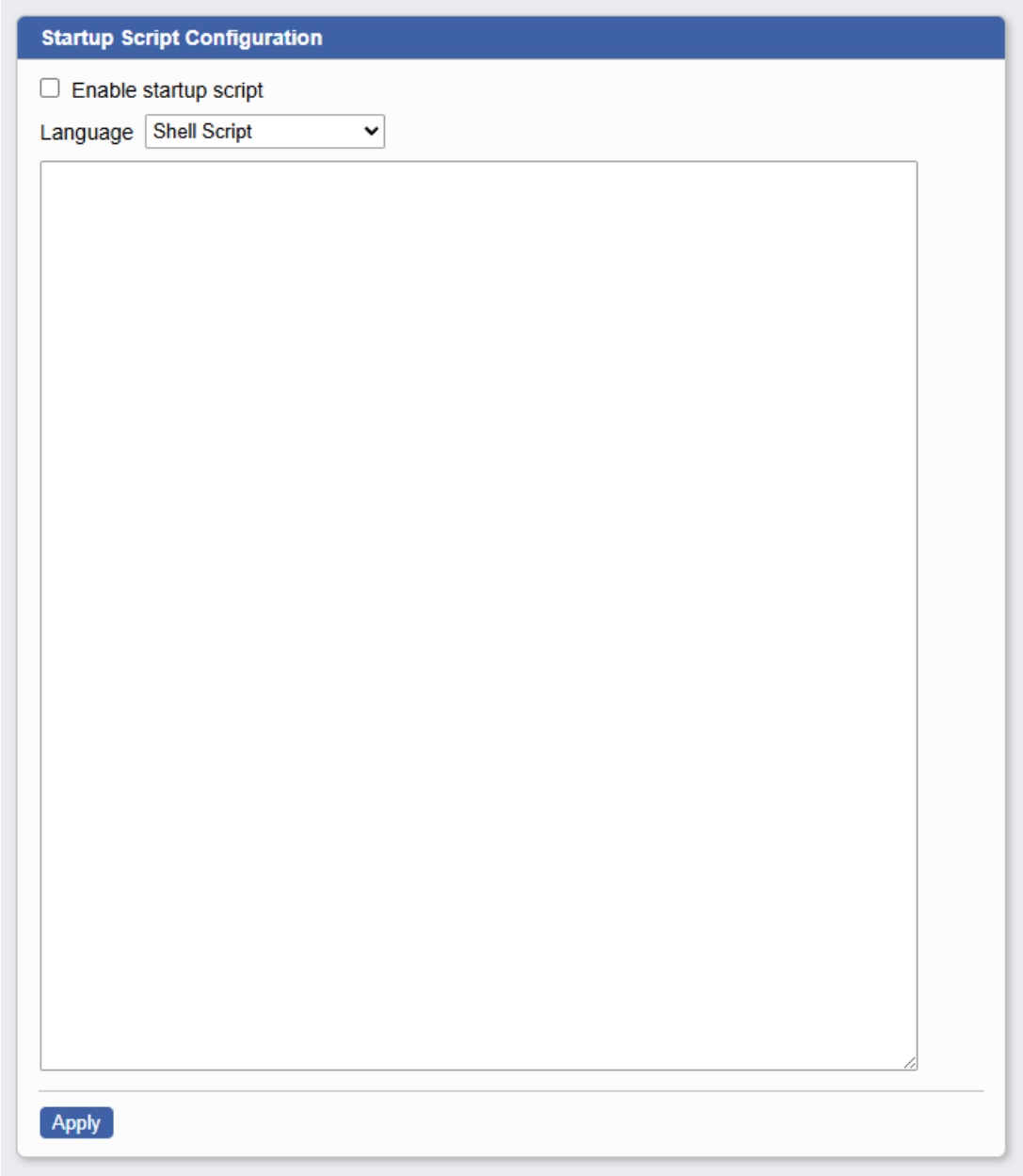
Cesta: Configuration → System → Startup Script

Stránka **Startup Script** umožňuje vložit skript, který se provádí vždy při zapnutí zařízení nebo po jeho restartu.

Zadaný skript se stane aktivním po zaškrtnutí políčka ☐ **Enable startup script** a následným stisknutím tlačítka Apply . Kolonka **Language** slouží ke specifikaci použitého programovacího jazyka – **Shell Script** nebo **Python**.

DŮLEŽITÁ INFORMACE

Pro používání skriptů psaných v jazyce **Python** je potřeba mít nainstalovaný softwarový modul Python.



Obrázek 53: Startup skript

17.4 Nastavení systémového logu

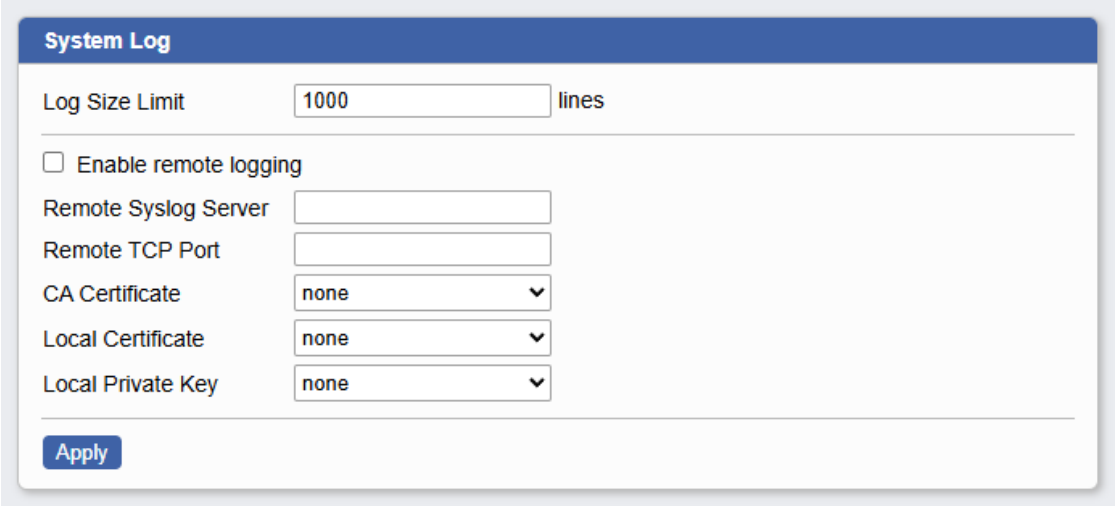
Cesta: Configuration → System → System Log

Prostřednictvím tohoto formuláře lze konfigurovat systémový log, který je zobrazen na stránce **Status → System Log**.

- **Local Log Size Limit**: Maximální velikost systémového logu, jež je udávaná v řádcích.
- **Remote Syslog Server**: Doménové jméno nebo IP adresa vzdáleného serveru, na který bude v reálném čase odesílána kopie systémového logu.
- **Remote TCP Port**: TCP port vzdáleného serveru specifikovaného v **Remote Server**.
- **CA Certificate**: Jedná se o certifikát certifikační autority, která vydala certifikát vzdálenému serveru. Zařízení jej používá k ověření identity vzdáleného serveru, aby se připojilo jen k důvěryhodnému serveru a ne k podvrženému zařízení.
- **Local Certificate**: Certifikát samotného zařízení, který může být vzdálenému serveru předložen pro vzájemnou autentizaci. Server tak ví, že se připojuje oprávněné zařízení.
- **Local Private Key**: Soukromý klíč odpovídající **Local Certificate**, který zařízení používá k šifrování a digitálnímu podepisování komunikace.

DŮLEŽITÁ INFORMACE

Veškerý kryptografický materiál lze spravovat prostřednictvím formuláře **Configuration → Security → Keys & Certificates**.



Obrázek 54: Konfigurace systémového logu

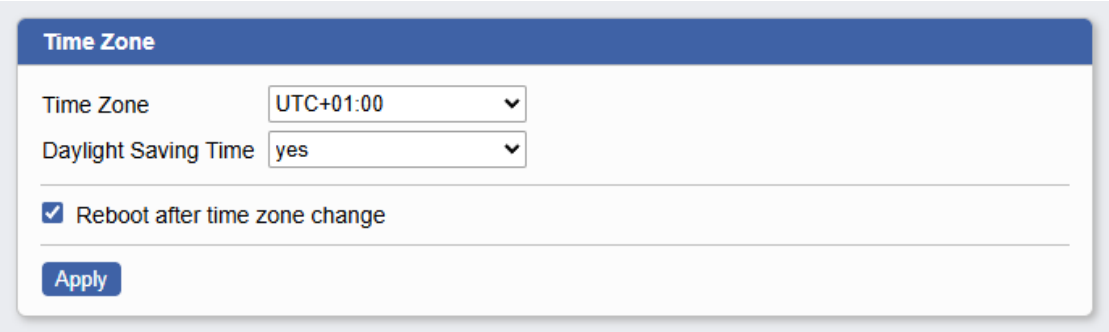
17.5 Nastavení časového pásma

Cesta: Configuration → System → Time Zone

Pokud chcete manuálně upravit časové pásmo, ve kterém se zařízení nachází, použijte formulář na této stránce. Položka **Time Zone** slouží k nastavení požadovaného časového pásma. Pomocí **Daylight Saving Time** pak lze specifikovat, zda má být použit letní čas (**yes**) či nikoliv (**no**).

DOPORUČENÍ

Doporučujeme ponechat zaškrtnuté políčko ☐ **Reboot after time zone change** pro následný restart zařízení, který je nutný pro změnu časového pásma.



Obrázek 55: Nastavení časového pásma

ČÁST IV

Správa uživatelských účtů

18. Správa uživatelských účtů

18.1 Uživatelské účty

Cesta: User Management → User Accounts

> **DŮLEŽITÁ INFORMACE**
>
> Tato část menu webového rozhraní je dostupná pouze uživatelům s rolí **administrator**.

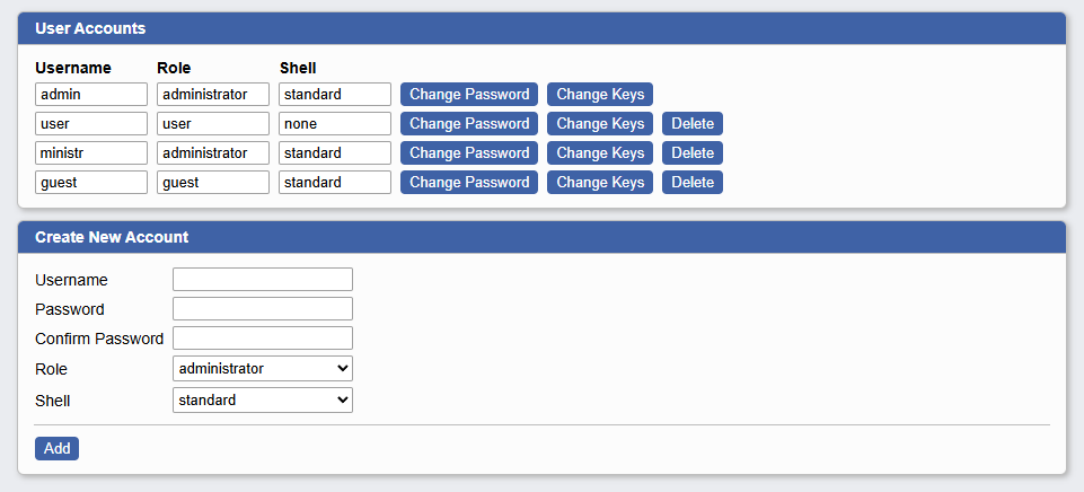
První část tohoto konfiguračního formuláře obsahuje seznam všech existujících uživatelů. Pro každý z nich jsou dostupné tyto základní operace:

- Change Password : Změna hesla pro daný uživatelský účet.
- Change Keys : Změna SSH a TFA klíče pro daný uživatelský účet.
- Delete : Smazání daného uživatelského účtu.

Druhá část konfiguračního formuláře umožňuje přidání nového uživatele. Pro vytvoření uživatelského účtu je třeba vyplnit všechny položky a následně potvrdit tlačítkem Add .

- **Username**: Jméno daného uživatelského účtu.
- **Password**: Přihlašovací heslo vytvářeného uživatele.
- **Confirm Password**: Potvrzení hesla (ověření správnosti předchozího zadání).
- **Role**: Úroveň uživatelského oprávnění.
  - Guest: Uživatelský účet na nejnižší úrovni, na které je přístup omezen pouze na některé status stránky.
  - User: Přístup pro čtení k většině konfiguračních formulářů. Uživatel může aktivně měnit pouze své heslo a SSH + TFA klíče. Zároveň může restartovat zařízení.
  - Administrator: Plný přístup ke všem stránkám a položkám ve webovém rozhraní.
- **Shell**: Definuje přístup pro nového uživatele prostřednictvím textového shellu. K dispozici je standardní přístup (standard), nebo žádný (none). Uživatel typu **guest** tento přístup automaticky nemá a není možné zvolit jinak.

> **DOPORUČENÍ**
>
> Minimální požadovaná délka hesla je **osm znaků**. Z důvodu většího zabezpečení však doporučujeme zadávat delší hesla.

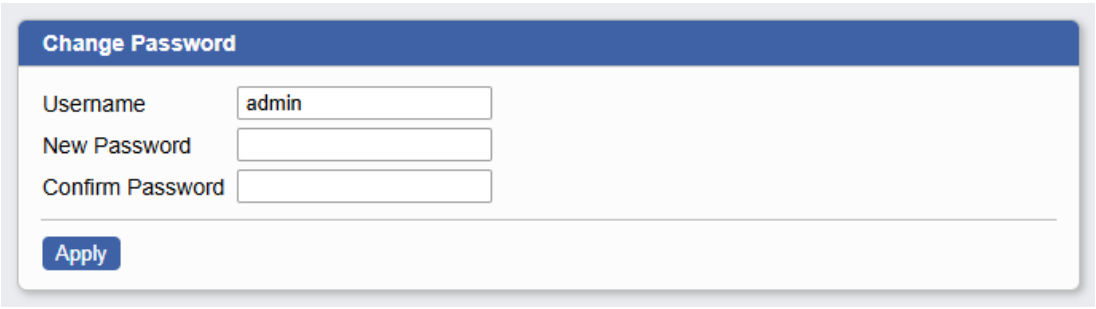


Obrázek 56: Správa uživatelských účtů

18.2 Změna uživatelského hesla

Cesta: User Management → Change Password

Kliknutím na položku **Change Password** v hlavním menu webového rozhraní zobrazíte formulář, pomocí něhož můžete změnit heslo ke svému uživatelskému účtu. Do pole **Password** zadejte své nové heslo a do kolonky níže (**Confirm Password**) jej zopakujte. Poté změnu potvrďte kliknutím na tlačítko Apply. Stejný formulář získáte také kliknutím na tlačítko Change Password u svého účtu na stránce **User Accounts**.



Obrázek 57: Změna uživatelského hesla

DOPORUČENÍ

Z bezpečnostních důvodů doporučujeme zvolit co možná nejsilnější heslo. Ihned po prvním přihlášení proveďte změnu hesla!

18.3 Změna SSH a TFA klíčů

Cesta: User Management → Change Keys

Tato stránka umožňuje spravovat SSH a TFA klíče.

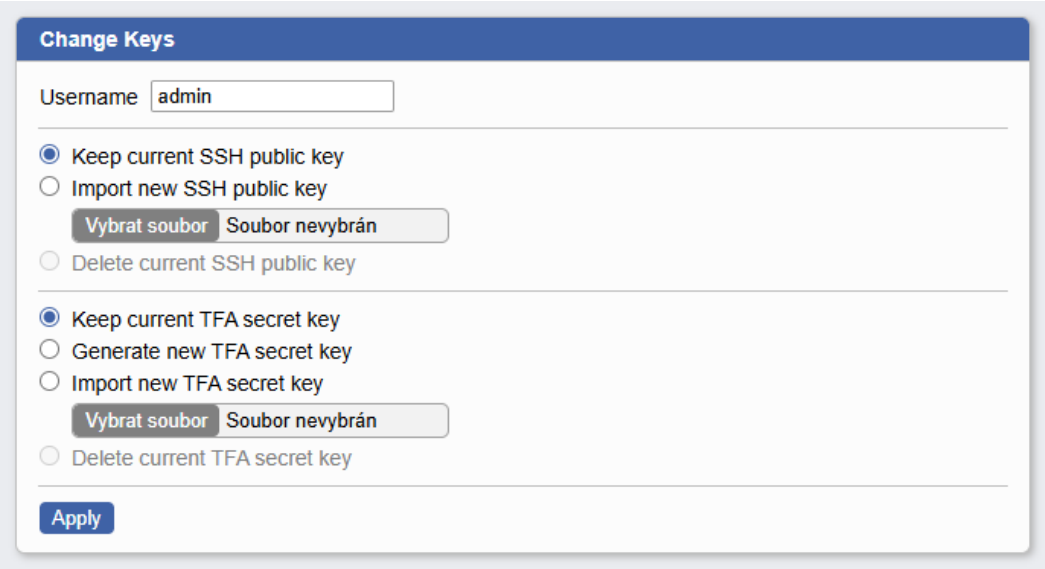
- **SSH klíč**: Veřejný klíč umožňující zabezpečenou autentizaci při připojení přes protokol SSH. Hlavní výhody použití:
  - Vyšší bezpečnost než v případě použití hesla (soukromý klíč se neposílá přes síť a tedy není sdílen).
  - Umožňuje automatizovat proces připojení bez nutnosti pokaždé zadávat heslo.
  - SSH klíče jsou odolnější vůči útokům hrubou silou (ve srovnání s hesly).
- **TFA klíč**: Jedná se o klíč určený ke dvoufaktorové autentizaci. Hlavní výhodou dvoufaktorové autentizace je přidání další vrstvy ochrany nad klasické heslo. Je-li heslo prozrazeno, útočník potřebuje ještě druhý faktor.

Správa SSH a TFA klíčů zahrnuje následující operace:

- **Keep current SSH public key** / **Keep current TFA secret key**: Ponechání aktuálně používaného klíče (nedojde k žádné změně).
- **Generate new TFA secret key**: Vygenerování nového TFA klíče.
- **Import new SSH public key** / **Import new TFA secret key**: Nahrání nového SSH či TFA klíče ze souboru.
- **Delete current SSH public key** / **Delete current TFA secret key**: Smazání aktuálně používaného klíče.

POZNÁMKA

SSH klíče lze vygenerovat například pomocí volně dostupného nástroje PuTTY. Postup, jak to provést, naleznete v příloze **Vygenerování SSH klíče pomocí PuTTY**.



Obrázek 58: Správa SSH a TFA klíčů

ČÁST V

Customizace

19. Softwarové moduly

Cesta: Customization → Software Modules

Softwarové moduly rozšiřují softwarovou funkcionalitu zařízení. Je možné využít některou z aplikací připravených společností CS-Tech s.r.o. nebo si napsat svou vlastní.

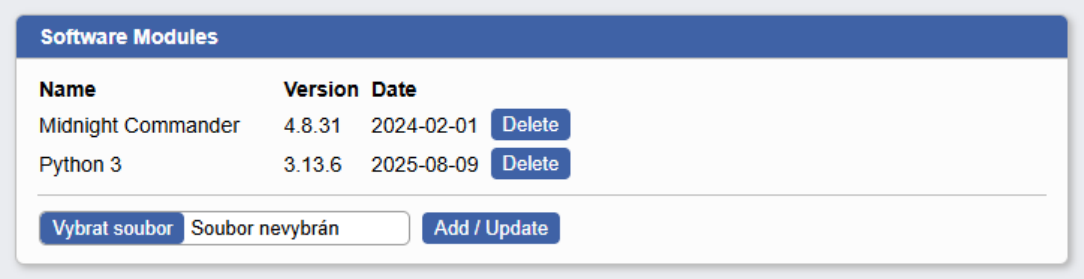
POZNÁMKA

Softwarové moduly jsou "softwarové balíčky" s příponou **.tgz**.

Stránka **Software Modules** zobrazuje základní informace o nainstalovaných aplikacích:

- **Name**: Jméno nainstalovaného softwarového modulu.
- **Version**: Verze nainstalovaného softwarového modulu.
- **Date**: Datum vydání dané verze softwarového modulu.

Pomocí tlačítka Delete je možné nainstalovaný softwarový modul smazat. Pokud chcete do zařízení nahrát novou aplikaci, vyberte ji pomocí tlačítka Vybrat soubor a následně její nahrání potvrďte tlačítkem Add / Update. V případě aktualizace na novější verzi modulu postupujte stejným způsobem jako byste chtěli nahrát novou aplikaci.



Obrázek 59: Softwarové moduly

DŮLEŽITÁ INFORMACE

Každý softwarový modul může mít své vlastní konfigurační stránky, které lze zobrazit kliknutím na název modulu. Podrobné informace o konfiguraci lze nalézt v dokumentaci k danému modulu.

ČÁST VI

Administrace

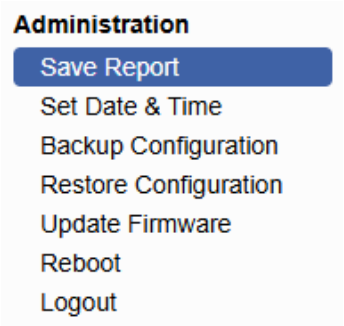
20. Správa systému

V poslední části navigačního menu (**Administration**) jsou k dispozici položky pro správu samotného systému.

20.1 Uložení reportu

Cesta: Administration → Save Report

Kliknutím na **Save Report** vygenerujete komplexní diagnostickou zprávu, která se uloží jako textový soubor s příponou **.txt** (**neobsahuje citlivé údaje jako jsou hesla a soukromé klíče**). Tento soubor je velmi užitečný pro řešení různých provozních potíží. Při komunikaci s technickou podporou tento soubor vždy vygenerujte a přiložte ke svému dotazu.

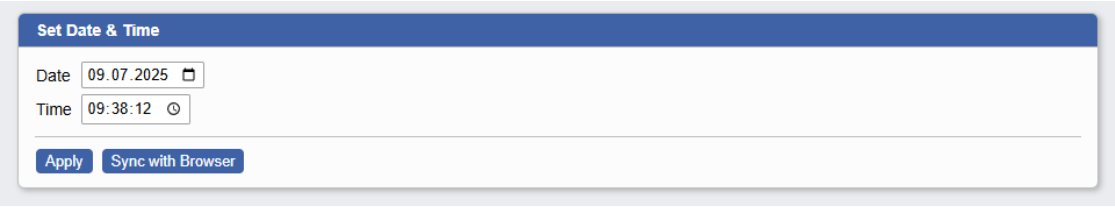


Obrázek 60: Uložení reportu

20.2 Datum a čas

Cesta: Administration → Set Date & Time

Chcete-li manuálně nastavit datum a čas zařízení, použijte formulář na této stránce. Ve spodní části tohoto formuláře je také možnost synchronizace s datumem a časem, který aktuálně používáte ve svém webovém prohlížeči (tlačítko Sync with Browser).



Obrázek 61: Datum a čas

DŮRAZNÉ VAROVÁNÍ

Nastavení správného času v zařízení je velmi důležité pro správné fungování a ověřování jednotlivých certifikátů, pro zaznamenávání událostí do logu a také pro dataloggerové funkce zařízení.

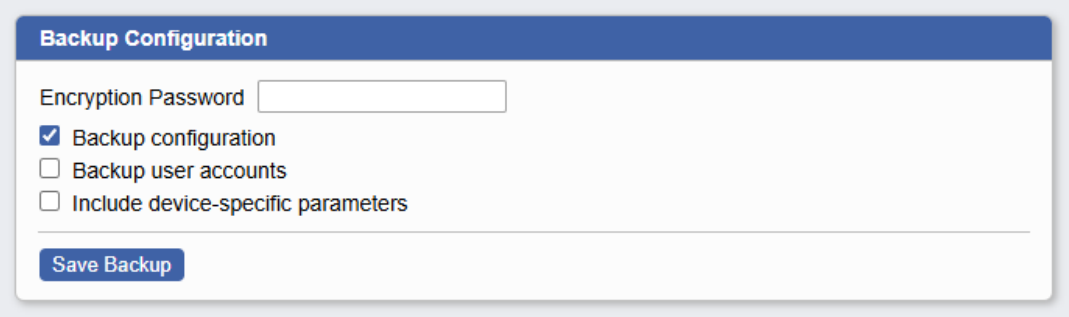
20.3 Záloha konfigurace

Cesta: Administration → Backup Configuration

Aktuální konfiguraci zařízení je možné uložit pomocí položky **Backup Configuration**. Zálohovat lze následující:

- Konfigurace zařízení (☐ **Backup configuration**)
- Konfigurace všech uživatelských účtů (☐ **Backup user accounts**)
- Unikátní parametry (☐ **Include device-specific parameters**)

Po stisknutí tlačítka Save Backup se do počítače uloží konfigurační soubor s příponou **.conf**.



Obrázek 62: Záloha konfigurace

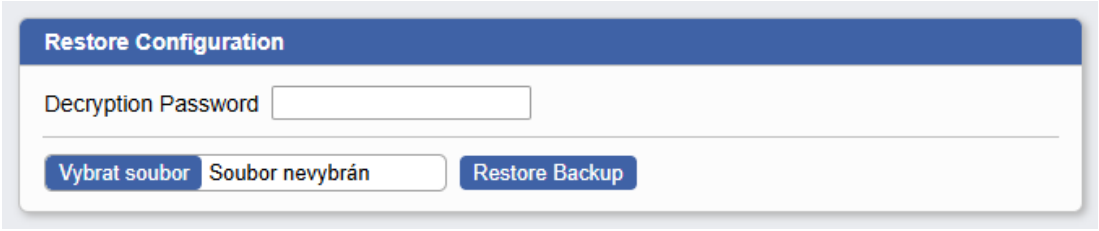
DŮRAZNÉ VAROVÁNÍ

Při vytváření zálohy využijte možnost zašifrování konfiguračních souborů (vyplňte heslo do kolonky **Encryption Password**).

20.4 Obnovení konfigurace

Cesta: Administration → Restore Configuration

Konfiguraci uloženou v souboru můžete obnovit na stránce **Restore Configuration**. Zde klikněte na tlačítko Vybrat soubor a přejděte do adresáře s požadovaným konfiguračním souborem. Pokud je tento soubor zašifrován, zadejte do kolonky **Decryption Password** dešifrovací heslo. Poté klikněte na tlačítko Restore Backup pro zahájení procesu obnovy.



Obrázek 63: Obnovení konfigurace

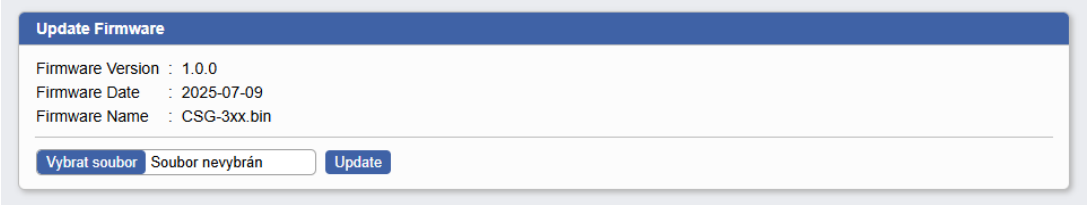
20.5 Aktualizace firmware

Cesta: Administration → Update Firmware

Tato stránka zobrazuje informace o

- aktuální verzi firmwaru (**Firmware Version**),
- datu uvolnění (**Firmware Date**),
- názvu firmwaru (**Firmware Name**).

Tato stránka rovněž umožňuje aktualizovat firmware. Klikněte na tlačítko Vybrat soubor, najděte a zvolte požadovaný soubor s novou verzí firmwaru a následně zahajte proces aktualizace kliknutím na tlačítko Update. Po dokončení aktualizace firmwaru se zařízení restartuje a uživatel bude automaticky přesměrován na přihlašovací stránku.



Obrázek 64: Aktualizace firmware

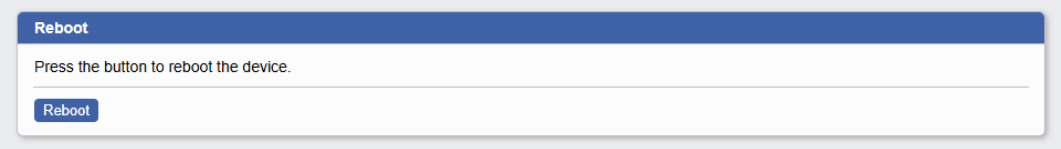
DŮRAZNÉ VAROVÁNÍ

Z důvodu maximální bezpečnosti pravidelně aktualizujte firmware na nejnovější verzi. Ze stejného důvodu důrazně nedoporučujeme provádět downgrade firmwaru.

20.6 Restart

Cesta: Administration → Reboot

Pro restartování zařízení vyberte položku **Reboot** a poté stiskněte tlačítko Reboot.

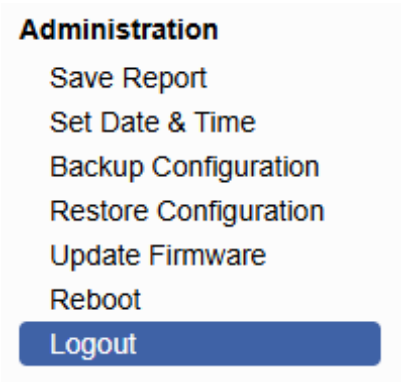


Obrázek 65: Restartování zařízení

20.7 Odhlášení

Cesta: Administration → Logout

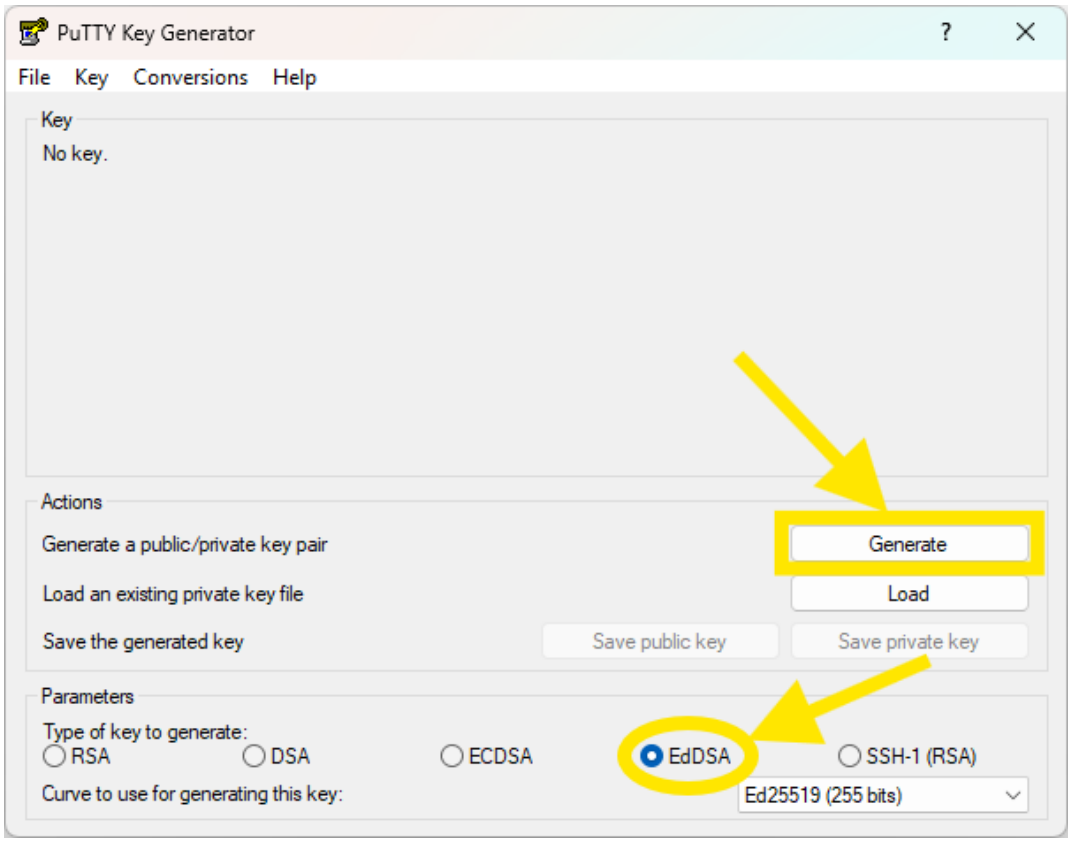
Kliknutím na položku **Logout** se odhlásíte z webového rozhraní.



Obrázek 66: Odhlášení

A. Vygenerování SSH klíče pomocí PuTTY

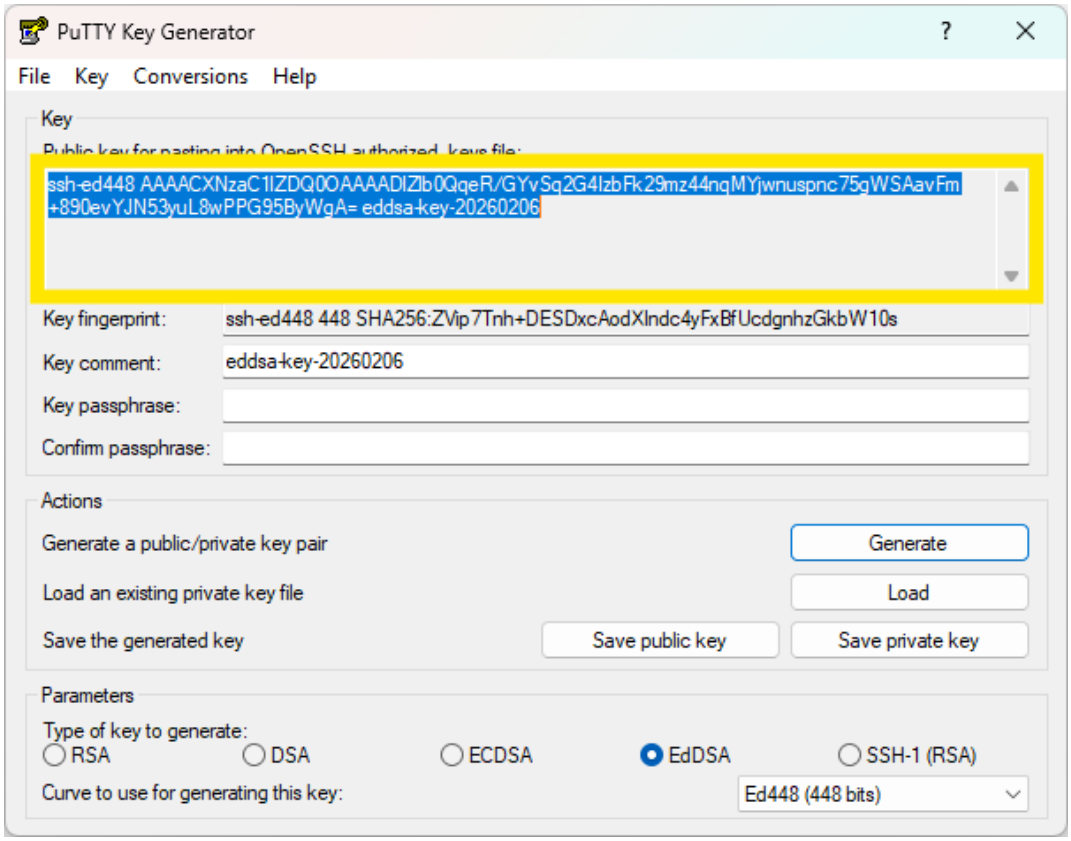
Na **této adrese*** vyhledejte sekci s názvem **Alternative binary files** a stáhněte si aplikaci pojmenovanou **puttygen.exe**. Spusťte ji a ujistěte se, že je ve spodní části označené jako **Parameters** zvolen typ klíče **EdDSA** (viz obrázek níže). Poté klikněte na tlačítko **Generate** a náhodným pohybem myši v okně klíč vygenerujte.



Obrázek 67: Nastavení aplikace puttygen

*https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

Jakmile je proces generování ukončen, zkopírujte kompletní obsah pole s veřejným klíčem (vyznačeno na obrázku níže) a uložte jej do textového souboru. Důležité je, aby klíč začínal řetězcem **ssh-ed25519** (resp. **ssh-ed448**). Jinak nebude po vložení do zařízení správně rozpoznán a přihlášení přes SSH selže. Poté uložte také odpovídající privátní klíč, což můžete udělat kliknutím na **Save private key**.



Obrázek 68: Kopírování veřejného klíče

A.1 Připojení pomocí vygenerovaného klíče

Přihlaste se k webovému rozhraní zařízení a na stránce **User Management** → **Change Keys** vložte soubor s nově vygenerovaným veřejným klíčem. Nahrání klíče se provede po stisknutí tlačítka Apply.

Poté otevřete aplikaci PuTTY.exe a v menu zvolte položku **Connection** → **Data**. Do kolonky **Auto-login username** zadejte název uživatelského účtu, kterému byl veřejný klíč uložen na zařízení Colias. Na stránce **Connection** → **SSH** → **Auth** → **Credentials** klikněte na tlačítko **Browse** u kolonky **Private key file for authentication** a vložte svůj privátní klíč.

Na závěr se vraťte na výchozí stránku **Session** a nakonfigurujte připojení dle pokynů níže. Nakonec stiskněte tlačítko **Save**, abyste konfiguraci uložili.

- **Host Name (or IP Address)**: IP adresa zařízení.
- **Port**: Ponechte výchozí hodnotu 22.
- **Connection Type**: Rovněž ponechte výchozí hodnotu (SSH).
- **Saved Session**: Zvolte jméno, které budete pro tuto relaci využívat.

CS-Tech s.r.o.

Adresa: Lázeňská 354, 562 01 Ústí nad Orlicí
Telefon: +420 731 602 099 (obchodní oddělení)
E-mail: obchod@cs-tech.cz