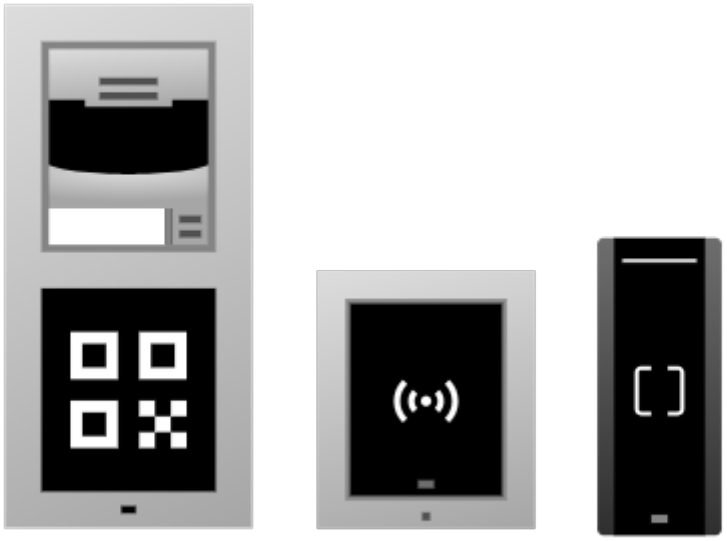
# Přístupové jednotky

## Konfigurační manuál



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

2N.com

# Obsah

# První přihlášení

## Nalezení zařízení v síti

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

### Doménové jméno

Pro přístup k webovému konfiguračnímu rozhraní je možné do prohlížeče místo IP adresy zadat doménové jméno ve formátu „hostname.local“. Hostname nového zařízení se skládá z produktového názvu a sériového čísla zařízení. Při zadávání hostname použijte pouze písmena a číslice; nepoužívejte mezery, tečky, pomlčky ani jiné speciální znaky.

**Výchozí doménové jméno zařízení :** 2NAccessUnit-{sériové číslo bez pomlček}.local (např.: „2NAccessUnit-0000000001.local“)

Formát názvu konkrétního zařízení je uveden v Instalačním manuálu daného produktu v kapitole Doménové jméno.

**TIP**
Hostname můžete později změnit ve webovém konfiguračním rozhraní a to v **Systém > Připojení k síti > karta Pokročilá konfigurace > Hostname**.

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

### IP adresa zařízení

V továrním nastavení používá zařízení dynamickou IP adresu přidělenou DHCP serverem.

Ke zjištění IP adresy zařízení 2N v lokální síti slouží aplikace 2N IP Utility. Aplikaci 2N IP Utility je možné stáhnout z webových stránek 2N.com. Pro instalaci je nutné mít nainstalovaný Microsoft .NET Framework 4.7.2.

S ohledem na možnosti daného zařízení je možné zjistit IP adresu také některým z následujících způsobů:

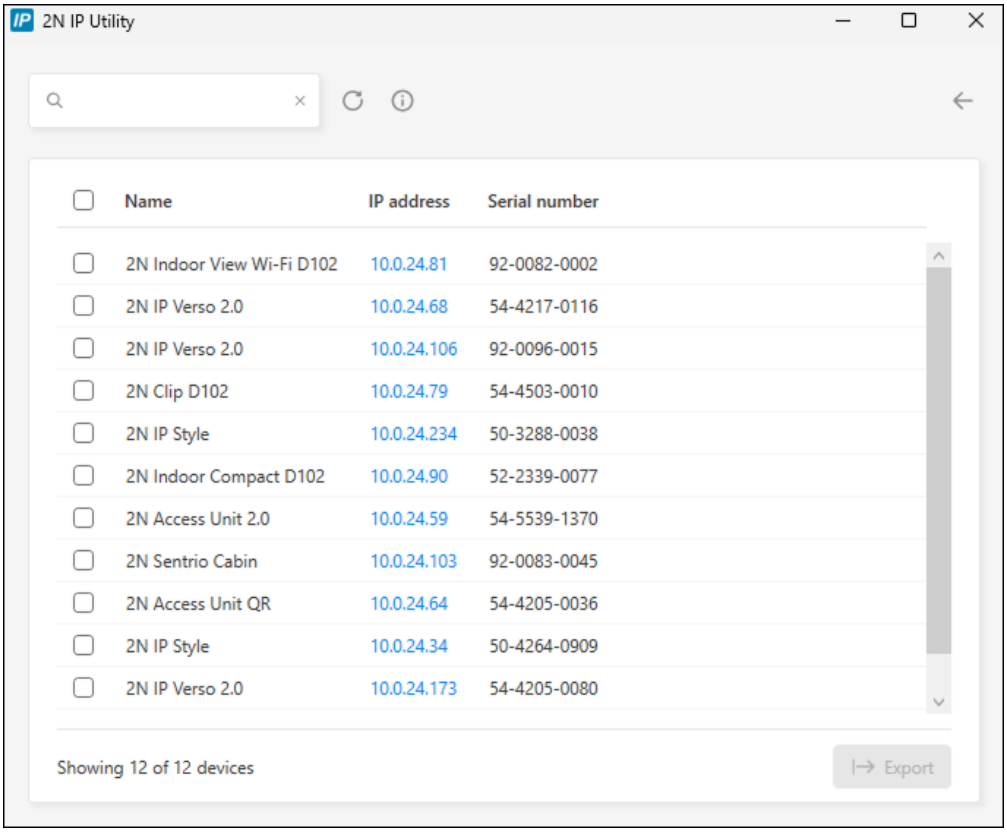
- tlačítkem RESET

### Zjištění IP adresy pomocí 2N IP Utility

Ke zjištění IP adresy zařízení 2N v lokální síti slouží aplikace 2N IP Utility. Aplikaci 2N IP Utility je možné stáhnout z webových stránek 2N.com. Pro instalaci je nutné mít nainstalovaný Microsoft .NET Framework 4.7.2.

1. Spusťte instalátor 2N IP Utility.
2. Instalací vás provede instalační Wizard.

3. Po nainstalování aplikace 2N IP Utility spusťte aplikaci z nabídky Start operačního systému Microsoft Windows.
   Po spuštění začne aplikace automaticky vyhledávat v lokální síti veškerá zařízení 2N a AXIS, která mají z DHCP přidělenou nebo staticky nastavenou IP adresu. Tato zařízení jsou následně zobrazena v tabulce.




4. Ze seznamu vyberte zařízení, které chcete konfigurovat, a klikněte na něj levým tlačítkem myši. Tím se otevře pravá část okna s webovým konfiguračním rozhraním.

**TIP**

- Přístup do webového konfiguračního rozhraní je také možný přes tlačítko **Open in external browser**, které umožňuje otevřít rozhraní v samostatném okně prohlížeče.
- Po kliknutí na zařízení v seznamu se zobrazí detailní informace. Kliknutím na tlačítko **IP settings** můžete změnit IP adresu následným zadáním požadované statické IP adresy nebo aktivací DHCP.
- Aplikace také umožňuje exportovat vybraná zařízení do souboru CSV. Nejprve vyberte zařízení zaškrtnutím políček u jednotlivých zařízení v seznamu, poté použijte tlačítko **Export**, které se zobrazuje v dolní části okna. Exportovaný soubor bude obsahovat jméno, IP adresu a sériové číslo vybraných zařízení.

Výchozí přihlašovací údaje jsou:
Uživatelské jméno: **Admin**
Heslo: **2n**
Po prvním přihlášení je třeba neprodleně změnit heslo.

**TIP**
Je doporučeno používat heslo, které je obtížné prolomit. Není doporučeno používat v hesle jména, názvy míst nebo věcí, obzvláště těch, které mají k uživateli přímou vazbu.

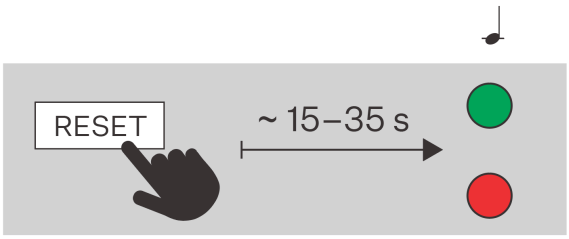
Pro vyšší bezpečnost hesla doporučujeme:

- využívat náhodný generátor hesel
- délku hesla minimálně 12 znaků
- kombinaci různých znaků z různých znakových sad (např. malá/velká písmena, číslice, speciální znaky, apod.)

## Zjištění IP adresy pomocí tlačítka RESET

Pro zjištění aktuální IP adresy postupujte podle následujících bodů:

1. Stiskněte tlačítko RESET a držte jej stisknuté.
   a. Vyčkejte, než se současně rozsvítí červená a zelená LED na zařízení a zazní zvuková signalizace ♩ (cca 15–35 s).
2. Uvolněte tlačítko RESET.
3. Zařízení hlasově automaticky oznámí aktuální IP adresu.




**POZNÁMKA**
Časový interval od stisknutí tlačítka RESET do první světelné a zvukové signalizace je uveden v rozmezí 15–35 s, vždy záleží na konkrétním modelu zařízení.

## Přepnutí DHCP

V továrním nastavení používá zařízení dynamickou IP adresu přidělenou DHCP serverem.

## Dynamická IP Adresa

DHCP (Dynamic Host Configuration Protocol) je síťový protokol, který udržuje seznam dostupných IP adres a automaticky je přiděluje zařízením v lokální síti. Přidělená IP adresa je dynamická, zařízení tak může být po čase (po uplynutí lease time) přidělena nová IP adresa.

## Statická IP Adresa

Pokud má IP adresa zařízení zůstávat neměnná, je potřeba na zařízení vypnout přidělování IP adres DHCP serverem. Vypnutí DHCP serveru je možné provést ve webovém konfiguračním rozhraní nebo pomocí hardwaru zařízení.

**POZNÁMKA**
Konkrétní hodnoty pro statickou IP adresu je možné nastavit pouze ve webovém konfiguračním rozhraní zařízení.

## Nastavení síťových parametrů ve webovém konfiguračním rozhraní

1. Přejděte do webového konfiguračního rozhraní.
2. Přejděte do **Systém > Připojení k síti > karta Základní nastavení > Nastavení IP adresy**.
3. Nastavte požadované síťové parametry.
4. Uložte změny.

## Přepnutí DHCP na hardwaru zařízení

S ohledem na možnosti daného zařízení je možné přepnout IP adresu následovně:

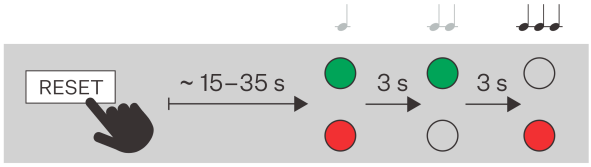
- tlačítkem RESET

**TIP**
Umístění tlačítka RESET najdete v Instalačním manuálu daného produktu.

### Nastavení dynamické IP adresy pomocí tlačítka RESET

Pro nastavení konfigurace sítě zařízení s dynamickou IP adresou (DCHP ON) postupujte podle následujících bodů:

1. Stiskněte tlačítko RESET a držte jej stisknuté.
   a. Vyčkejte, než se současně rozsvítí červená a zelená LED na zařízení a zazní zvuková signalizace ♩ (cca 15–35 s).
   b. Vyčkejte, než červená LED zhasne a zazní zvuková signalizace ♩♩ (cca další 3 s).
   c. Vyčkejte, než zelená LED zhasne a opět se rozsvítí červená LED a zazní zvuková signalizace ♩♩♩ (cca další 3 s).
2. Uvolněte tlačítko RESET.




### Nastavení statické IP adresy pomocí tlačítka RESET

Pro nastavení konfigurace sítě zařízení do režimu se statickou IP adresou (DHCP OFF) postupujte podle následujících bodů:

1. Stiskněte tlačítko RESET a držte jej stisknuté.
   a. Vyčkejte, než se současně rozsvítí červená a zelená LED na zařízení a zazní zvuková signalizace ♩ (cca 15–35 s).
   b. Vyčkejte, než červená LED zhasne a zazní zvuková signalizace ♫ (cca další 3 s).
2. Uvolněte tlačítko RESET.


**POZNÁMKA**
Po restartu bude mít zařízení nastaveny tyto síťové parametry:

- IP adresa: 192.168.1.100
- Maska sítě: 255.255.255.0
- Výchozí brána: 192.168.1.1

# Přístup do webové konfigurace zařízení

Konfiguraci zařízení se provádí prostřednictvím webového konfiguračního rozhraní, které je dostupné z webového prohlížeče.

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

Do webového konfiguračního rozhraní je také možné přejít z připojeného portálu My2N nebo z konfiguračního nástroje 2N Access Commander.

## Přihlášení do webového konfiguračního rozhraní

1. Spusťte internetový prohlížeč.
2. Zadejte IP adresu zařízení nebo doménové jméno zářízení (viz kapitola Nalezení zařízení v síti (str. 3)).
3. Pokud nemáte pro IP adresu vygenerovaný certifikát, může se zobrazit upozornění na neplatný bezpečnostní certifikát. V takovém případě je potřeba potvrdit, že chcete přejít na webové konfigurační rozhraní.
4. Zobrazí se přihlašovací obrazovka.
5. Zadejte přihlašovací údaje.
   Výchozí přihlašovací údaje jsou:
   - Uživatelské jméno: **Admin**
   - Heslo: **2n**
6. Po prvním přihlášení heslo změňte.

## Přístup z 2N Access Commanderu

1. Přihlaste se do rozhraní Access Commander.

2. Přejděte na stránku Zařízení.
3. U vybraného zařízení stiskněte .

## Změna hesla

Pro plný přístup k funkcím webového konfiguračního rozhraní je potřeba výchozí heslo změnit. Bez změny výchozího hesla není možné zařízení konfigurovat.

**TIP**
Je doporučeno používat heslo, které je obtížné prolomit. Není doporučeno používat v hesle jména, názvy míst nebo věcí, obzvláště těch, které mají k uživateli přímou vazbu.

Pro vyšší bezpečnost hesla doporučujeme:

- využívat náhodný generátor hesel
- délku hesla minimálně 12 znaků
- kombinaci různých znaků z různých znakových sad (např. malá/velká písmena, číslice, speciální znaky, apod.)

## Doporučené prohlížeče

Webové konfigurační rozhraní je optimalizováno pro webové prohlížeče založené na Chromiu (například Google Chrome, Microsoft Edge nebo Opera). Při použití jiných prohlížečů může dojít k drobným rozdílům ve funkčnosti nebo ve vzhledu rozhraní.

# Základní nastavení zařízení

## Aktualizace firmwaru

Nové verze firmwaru jsou dostupné na aktualizačním serveru. V případě, že není ve webovém konfiguračním rozhraní přístup k veřejnému internetu, je možné do zařízení nahrát soubor s firmwarem manuálně.

**POZNÁMKA**
Aktualizace firmwaru neprobíhá automaticky. Pro zajištění integrity systému a eliminaci neúmyslných poruch musí být všechny aktualizace uživatelem manuálně potvrzeny nebo iniciovány. Před provedením jakékoli aktualizace prosím zkontrolujte release notes nové verze a ověřte kompatibilitu se svou stávající infrastrukturou.

### Získání firmwaru z aktualizačního serveru

**VÝSTRAHA**
Ve verzi 3.0.0 je aktualizace firmwaru z aktualizačního serveru dostupná pouze ze starší verze webového rozhraní.

**a.** V záhlaví webového konfiguračního rozhraní klikněte na Přejít na staré rozhraní.

1. Přejděte do **Systém > Údržba > karta Firmware**.
2. Klikněte na tlačítko Zkontrolovat aktualizace.
3. Při dostupné aktualizaci se načtou její release notes. Aktualizaci spustíte kliknutím na Upgrade v záhlaví okna.
4. Po úspěšném nahrání firmwaru se zařízení automaticky restartuje. Po restartu je zařízení plně k dispozici s novým firmwarem. Aktualizace firmwaru neovlivňuje konfiguraci.

### Nahrání nového firmwaru z úložiště

1. Přejděte do **Systém > Údržba > karta Firmware**.
2. Klikněte na tlačítko Nahrát firmware.
3. V otevřeném dialogovém okně vyberte soubor z vlastního úložiště.
4. Potvrďte nahrání souboru kliknutím na Nahrát.
   Zařízení kontroluje soubor firmwaru a neumožní nahrát nesprávný nebo poškozený soubor.
5. Po úspěšném nahrání firmwaru se zařízení automaticky restartuje. Po restartu je zařízení plně k dispozici s novým firmwarem. Aktualizace firmwaru neovlivňuje konfiguraci.

## Adresář

Sekce Adresář je klíčovou částí konfigurace zařízení. V adresáři vytvoříte uživatele a spravujete jejich přístupová práva.

### Manuální přidání uživatele do adresáře

1. Na stránce Adresář klikněte na Přidat uživatele.
2. Otevře se detail uživatele. V kartě Osobní údaje uživatele pojmenujte.
3. Možnosti přístupu nastavte podle Přístupy (str. 10).

### Hromadná správa uživatelů v Access Commanderu nebo v My2N

Pokud je zařízení spravováno prostřednictvím nástrojů hromadné konfigurace Access Commander nebo My2N, budou veškeré změny provedené ve webovém konfiguračním rozhraní přepsány nastavením v nástroji hromadné konfigurace. Uživatel vytvořený přímo ve webovém rozhraní bude smazán.

Sloupec **Držitel** v tabulce adresáře uvádí nástroj hromadné konfigurace, který uživatele vytvořil. Sloupec **Držitel** je ve výchozím nastavení skrytý.

## Přístupy

Jedna ze základních funkcí zařízení je správa přístupu a odemykání elektrického dveřního zámku. Zařízení přístupy spravuje na základě vyhodnocení požadavků na přístup podle předem definovaných přístupových pravidel. Pokud zařízení požadavek vyhodnotí jako oprávněný, zařízení sepne dveřní spínač, který ovládá elektrický zámek dveří. Tím dojde k odemknutí dveří.

Kromě běžného ověření uživatele (RFID kartou, biometrickými údaji, Bluetooth apod.) může být spínač sepnut také pomocí externích signálů a rozhraní, což zajišťuje flexibilní možnosti integrace a automatizace. Níže jsou popsány různé způsoby aktivace dveřního spínače:

### Ověření uživatele

Uživatel použije svou metodu autentizace a jestli jsou jeho uživatelská oprávnění v souladu s přístupovými pravidly, je mu povolen přístup. Povolený přístup sepne dveřní spínač.

Nastavení je popsáno v kapitole Nastavení přístupu uživatele (str. 11).

### Ve webovém konfiguračním rozhraní

1. Přejděte do **Integrace > Spínače**.
2. Najděte kartu spínače, který ovládá dveře.

> **POZNÁMKA**
> Funkci dveřního spínače v zařízení vykonává **Spínač 1**.

3. V části **Manuální ovládání spínače** klikněte na Podržet.
4. Spínač bude sepnut do doby, než opět zrušíte jeho podržení v manuálním ovládání.

### Nastavením časového profilu

Ve webovém konfiguračním rozhraní je možné nastavit, aby spínač podržel dveře odemknuté po předem určenou dobu, například přes čas oběda.

1. Přejděte do **Integrace > Spínače**.
2. Najděte kartu spínače, který ovládá dveře.

> **POZNÁMKA**
> Funkci dveřního spínače v zařízení vykonává **Spínač 1**.

3. Kliknutím na šipku → zvoleného spínače přejděte na jeho detail.
4. V **kartě Stav** povolte možnost **Časem řízené přidržení spínače**.

5. Vyberte časové profily, ve kterých má být spínač přidržen nebo zadejte vlastní časový úsek.

## Z hovoru (DTMF)

### Nastavení DTMF kódu

1. Přejděte do **Integrace > Spínače**.
2. Najděte kartu spínače, který ovládá dveře.

> **POZNÁMKA**
> Funkci dveřního spínače v zařízení vykonává **Spínač 1**.

3. Kliknutím na šipku → zvoleného spínače přejděte na jeho detail.
4. V **kartě Aktivační kódy** nastavíte kódy, které budete moct zadat přes DTMF v průběhu hovoru se zařízením.
   Platnost každého kódu je možné časově omezit.

> **POZNÁMKA**
> U prvního aktivačního kódu můžete nastavit jeho zpracování jako u starší formy kódu. V této formě nebude nutné daný kód potvrzovat hvězdičkou při zadávání na klávesnici telefonu.

### Použití DTMF kódu

1. Při spojeném hovoru se zařízením zadejte na klávesnici svého telefonu aktivační kód a potvrďte jej hvězdičkou.

> **POZNÁMKA**
> Příjem DTMF signálů je ve výchozím nastavení na zařízení povolen. Povolení si můžete ověřit na stránce služby volání (SIP / Lokální hovory) v záložce **Audio**, na kartě **Příjem DTMF**.

## Pomocí HTTP API

Kompletní používání včetně popisu potřebné autorizace HTTP API je popsáno v manuálu HTTP API manuálu pro zařízení 2N. Dveřní spínač je ovládán endpointem `api switch ctrl`. Pro sepnutí spínače 1 vypadá příkaz následovně: `https://ip_adresa/api/switch/ctrl?switch=1&action=on`.

## Nastavením Automatizace

Nastavování automatizací je popsáno v Automation manuálu. Sepnutí spínače vyvolává akce **ActivateSwitch**.

## Nastavení přístupu uživatele

Aby se uživatel mohl úspěšně autentizovat na přístupové jednotce a odemknout dveře, musí splňovat dvě podmínky: mít přidělená přístupová práva k danému zařízení a mít vytvořený alespoň jeden způsob autentizace. Dostupné metody autentizace závisí na konkrétním zařízení a mohou zahrnovat RFID karty, číselný PIN kód, QR kód ke skenování kamerou apod.

## Nastavení autentizace:

1. Přejděte na stránku **Adresář**.
2. Otevřete detail uživatele kliknutím na daný řádek nebo zvolte možnost Přidat uživatele pro založení nového uživatele.
3. V kartě **Autentizace** nastavte všechny metody, kterými se bude uživatel autentizovat, viz Metody autentizace (str. 12) .
4. V kartě **Nastavení přístupu** vyplňte, kdy má být uživateli udělen přístup pro vstup a pro výstup.
   - Kdykoli
   - Časový profil – nabízí nastavené **Časové profily**
   - Vlastní – tlačítkem Upravit můžete nastavit časové intervaly unikátní pro tohoto uživatele

   Nastavením termínu platnosti omezte přístup uživatele na konkrétní kalendářní období.
   Udělením **Výjimky** zajistíte uživateli trvalý přístup, který neomezí ani dočasné zamknutí zařízení udávané přístupovými pravidly (viz Přístupová pravidla (str. 14)).

## Metody autentizace

**VÝSTRAHA**
Dostupné metody autentizace závisí na konkrétním zařízení a připojených modulech.

### RFID karta

Jeden uživatel může mít přiřazeny až 2 RFID karty.

Identifikátor lze zadat ručně pomocí klávesnice nebo jej načíst přiložením karty na USB čtečku připojenou k počítači.

#### Požadavky na RFID kartu

- Identifikátor musí být hexadecimální číslo.
- Minimální délka identifikátoru je 6 znaků.
- Lze použít pouze karty podporované daným zařízením – typ karet musí být povolen v nastavení modulů (viz **Přístup > Moduly**).

**TIP**
Identifikátor existující karty můžete vyčíst z logu v **Systém > Protokol událostí**. Novou/nepřiřazenou kartu načtěte na zařízení a poté zkopírujte její identifikátor (UUID) z logu. Po vložení identifikátoru mezi RFID karty, může uživatel začít kartu používat k autentizaci.

### My2N

**My2N** – slouží k propojení s aplikací My2N aplikace umožňující autentizaci prostřednictvím Bluetooth.

### PIN kód / QR kód

PIN kód slouží jako osobní numerický přístupový kód, který uživatel zadává na klávesnici zařízení nebo jej může v podobě QR kódu nechat načíst kamerou zařízení.

**VÝSTRAHA**
QR kódy lze načítat pouze na interní kameře zařízení.

**Požadavky na PIN kód**

- Minimální délka je 2 číslice.
- Kód může obsahovat pouze číslice (0–9).
- QR kódy lze použít pouze pro PIN kódy dlouhé 4 až 15 číslic.
- Pokud používáte funkci **Tichý alarm**, doporučujeme vytvářet sudé PIN kódy.

**POZNÁMKA**
Při použití hexadecimálního QR kódu je nutné hodnotu před zadáním převést do decimálního formátu.

Akceptovaný hexadecimální rozsah: 1000 až FFFFFFFF.

## Otisk prstu

Každému uživateli je možné nahrát až 2 otisky prstů. Pro jejich nahrání použijte externí čtečku otisků prstů. Zkontrolujte, zda máte nainstalovaný ovladač 2N USB Driver. Ovladač je ke stažení zde.

Nahraný otisk prstu uživatele lze použít k následujícím akcím:

- Otevřít dveře;
- Spustit tichý alarm – lze nastavit pouze v případě aktivní funkce Otevření dveří;
- Automatizace F1 a F2 – generuje událost FingerEntered v Automation. F1 a F2 slouží k rozlišení přiloženého prstu v Automation.

## Poznávací značka

Některá zařízení podporují rozpoznávání poznávací značky vozidel pomocí externích kamer AXIS vybavených doplňkovou aplikací **VaxALPR**. Rozpoznané poznávací značky jsou odesílány v HTTP požadavku na endpoint `api/lpr/licenseplate` (více HTTP API manuál pro IP interkomy).

**TIP**
Postup přidání externí kamery je popsán v Nastavení kamery a videa (str. 21).

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

**Požadavky na poznávací značku:**

- Maximální délka jedné poznávací značky je 10 znaků.
- Jednomu uživateli je možné přiřadit až 20 poznávacích značek.
- Každá poznávací značka by měla být přiřazena pouze jednomu uživateli – při vícenásobném přiřazení se použije první nalezený záznam.
- Poznávací značky jsou využity ve funkci rozpoznávání z obrazu externí kamery (viz Interoperability manuál).

### Virtuální karta

Virtuální karta slouží k identifikaci uživatele v zařízeních připojených přes rozhraní Wiegand. Po úspěšné autentizaci uživatele přes aplikaci My2N nebo na biometrické čtečce se ID virtuální karty odesílá na rozhraní Wiegand (pokud je v konfiguraci zapnuto odesílání identifikátorů, viz **Přístup > Přístupová pravidla > karta Příchod/Odchod > Pokročilé**).

**Požadavky na virtuální kartu:**

- ID musí být hexadecimální číslo (znaky 0–9, A–F).
- Délka ID je 6 až 32 znaků.
- Jeden uživatel může mít přiřazenou právě jednu virtuální kartu.

### Kód Spínače

**Kód spínače** – umožňuje nastavení až 4 kódů pro aktivací spínačů (např. dveřního zámku). Kód spínače slouží k otevření zámku pomocí klávesnice na zařízení i jako DTMF kód.

## Přístupová pravidla

Na stránce **Přístup > Přístupová pravidla** se nastavují parametry a logika odemykání dveří, které spravuje dveřní spínač zařízení. Tato konfigurace určuje způsob vyhodnocování žádostí o přístup (autentizací), podmínky nutné pro úspěšnou autorizaci uživatele a pravidla správy jednotlivých přístupů.

Zatímco v nastavení uživatelů definujete individuální oprávnění, prostřednictvím přístupových pravidel určíte kdy, za jakých podmínek a jak lze tato oprávnění použít. Můžete například nastavit, zda je průchod dveří povolen pouze v jednom směru, zda autentizace může spustit tichý alarm nebo zda se může uživatel autentizovat pouze jednou za definovaný časový interval.

### Stav dveří a zámku

**Karta Stav** zobrazuje, zda je dveřní spínač aktivní a zda jsou dveře otevřené.

**Dveře**

- „Otevřené“ – byl udělen přístup, dveřní spínač je sepnut a dveře lze otevřít.
- „Zavřené“ – dveře jsou zamčené a nelze je otevřít.

**Zámek**

- „Odemknuto“ – spínač je aktivní, lze jej ovládat.
- „Zamknuto“ – spínač je deaktivován a nemůže být ovládán přístupovými pravidly.

**TIP**
K zamknutí nebo odemknutí spínače z webového rozhraní slouží tlačítko se symbolem zámku na této kartě.

### Detekce dveří

V kartě **Dveře** je možné zapnout, aby neoprávněné otevření dveří nebo jejich dlouhé otevření vyvolalo událost. Na tuto událost je pak možné navázat následující akce prostřednictvím automatizací. Události se také propíší do logu zařízení.

### Příchod a Odchod

Jedno zařízení lze využívat pro správu průchodů ve dvou směrech. K zařízení můžete některé moduly umístit na opačnou stranu dveří a tyto dvě strany pak nastavovat separátně. Můžete tak omezit, v jakou denní dobu bude umožněn průchod ve směru **Příchod** a v jakou denní dobu bude umožněn průchod ve směru **Odchod**, případně jaké způsoby autentizace budou v daném směru akceptovány apod.

## Rozřazení modulů pro příchod nebo odchod

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

**TIP**

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

### Přístupová pravidla

Přístupová pravidla určují, jaké metody autentizace budou akceptovány pro udělení přístupu. Je možné nastavit více přístupových pravidel pro různé časové profily. Pomocí přístupových pravidel lze také určit, kdy má být jakýkoliv přístup zamezen.

Pomocí přístupových pravidel můžete omezit akceptované metody autentizace, tím lze uživatele např. donutit, aby od 8:00 do 9:00 byli uživatelé nuceni použít RFID kartu.

**TIP**

Omezení autentizace se hodí použít na zařízení, které spravuje klíče k **2N IP Fortis**. Uživatelé tak budou nuceni si pravidelně aktualizovat klíče k **2N IP Fortis** na své RFID kartě.

Při nastavování pravidel můžete zvolit, jestli bude možné k otevírání dveří používat zónový kód. **Zónový kód** se uplatňuje, když je zařízení zařazené do zóny v hromadné správě zařízení (např. v Access Commanderu). **Zónový kód** je možné také manuálně nastavit v části **Pokročilé**. Funguje podobně jako **Aktivační kód Spínače**; jeho zadání na klávesnici modulu sepne dveřní spínač.

### Tichý alarm

Tichý alarm je speciální režim otevření zámku, který umožňuje nenápadně spustit bezpečnostní akci. Tichý alarm nachází své uplatnění zejména v prostorách a objektech, které jsou vyhledávány lupiči – v kasínech, finančních centrech, bankách apod. Po zadání PIN kódu se dveře otevřou, ale zároveň se aktivuje poplach, aniž by si toho útočník všiml.

Aktivace tichého alarmu vyvolá událost **SilentAlarm**. Na tuto událost lze navázat automatizace, například:

- Odeslání HTTP požadavku na zabezpečovací systém.
- Pořízení snímků z kamery zařízení.
- Sestavení volání na přednastavenou destinaci.

## Aktivace tichého alarmu

1. Uživatel zadá kód o jedničku vyšší než jeho běžný PIN kód.
   Příklad: Uživatel má nastaven PIN kód „1926“. Pro otevření dveří zadá kód „1927“. Dveře se otevřou a současně se spustí událost SilentAlarm.

**VÝSTRAHA**
Pro možnost otevírání dveří PIN kódem (a to i při současném spuštění Tichého alarmu) je potřeba povolit níže v kartě **Vstup/Výstup**.

### Blokování přístupu po neúspěšných pokusech

Po pěti po sobě následujících neúspěšných pokusech o přístup bude přístup zablokován na 30 sekund. Po tuto dobu nebude umožněn přístup ani v případě platné autentizace uživatele.

Tato funkce blokuje pouze přístup autorizací uživatele. Dveřní spínač je dále možné sepnout jinými metodami jako DTMF, HTTP příkazem atd.

### Čtení QR kódů

Uživateli přidělený přístupový PIN kód případně aktivační kód spínačů je možné načítat kamerou ve formě QR kódu.

Pro správně načítání je potřeba nastavit **Režim čtení QR kódů**. V zařízení se kódy ukládají vždy v decimálním formátu. Při čtení v decimálním režimu musí načítané QR kódy přesně odpovídat PIN kódům (o délce 4 až 15 číslic) uloženým v zařízení. V hexadecimálním režimu jsou QR kódy po přečtení převedeny na decimální formát čísla a až tak jsou porovnány s uloženými decimálními kódy. Předřazené nuly jsou při hexadecimálním čtení ignorovány.

**POZNÁMKA**
Akceptovaný hexadecimální rozsah: 1000 až FFFFFFFF.

U čtení QR kódů můžete také nastavit, aby jejich načtení místo ovládání dveřního spínače pouze vyvolalo událost **CodeEntered**. Na tuto událost je pak možné navázat další akce prostřednictvím Automatizací.

Načtený QR kód lze přeposílat dál do externího přístupového systému, který komunikuje pomocí Wiegand rozhraní (viz ???).

### Anti-passback

Anti-passback je rozšíření systému kontroly přístupů, které zabraňuje opakovanému vstupu během nastaveného časového intervalu. Zařízení v tomto režimu umožní uživateli vstoupit pouze jednou za daný čas. Po úspěšném vstupu uživatele systém zaznamená tuto událost a další přístup může tento uživatel provést až po uplynutí stanovené doby. Tato doba se nastavuje při povolení Anti-passbacku.

**Režimy funkce Anti-passback:**

- „Hard“ – Uživatel nemůže projít zařízením v žádném směru po nastavenou dobu. Přístup je uživateli odepřen, dokud interval neuplyne nebo není přístup obnoven správcem zařízení.
- „Soft“ – Porušení pravidla se pouze zaznamená do logu a může upozornit správce, ale samotný přístup je uživateli umožněn.

### Přeposílání dat pro Wiegand

**VÝSTRAHA**
Pro přeposílání Wiegand dat musí být k zařízení správně připojen rozšiřující modul Wiegand. Rozšiřující Wiegand modul zpravidla není součástí balení produktu.

Funkce přeposílání na Wiegand umožňuje zařízení odeslat identifikační data autentizovaného uživatele dál do externího přístupového systému, který komunikuje pomocí Wiegand rozhraní. To zajišťuje integraci zařízení 2N s tradičními přístupovými systémy. Nastavení umožňuje vybrat odpovídající skupinu pro směrování dat.

Přeposílání dat pro Wiegand se nastavuje v **Přístup > Přístupová pravidla > Příchod/Odchod > Pokročilé**. Odesílání autorizací uživatelů, kteří načetli svůj QR kód se nastavuje v kartě **Příchod/Odchod** u povolování čtení QR kódů.

## Nastavení přístupu přes Bluetooth

Autentizace uživatele prostřednictvím Bluetooth se provádí prostřednictvím My2N aplikace, kterou musí mít uživatel staženou ve svém mobilním telefonu.

GET IT ON Google Play

Download on the App Store

**VÝSTRAHA**
Nastavení párovacího kódu je aktuálně nutné provést ve starém konfiguračním rozhraní.

### Vytvoření párovacího kódu na zařízení

1. Přejděte na **Adresář** a otevřete detail uživatele, pro kterého chcete párovací kód vytvořit.
2. V záhlaví webového konfiguračního rozhraní klikněte na Přejít na staré rozhraní.
   Otevře se detail uživatele ve staré podobě konfiguračního rozhraní.
3. V bloku **WaveKey** klikněte na .
   V otevřeném dialogovém okně se vygeneruje párovací kód, který je nutné zadat do aplikace My2N ve vašem zařízení.
4. Otevřete aplikaci My2N a zadejte párovací PIN.

   **POZNÁMKA**
   Pokud již máte aplikaci spojenou s jiným zařízením, párovací PIN vložíte přes ikonu pro přidání v horní části obrazovky.
5. Postupujte podle instrukcí na mobilním telefonu – přibližte se k zařízení v párovacím režimu a klikněte na Zahájit párování.

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

### **Párování v mobilní aplikaci** Mobile Key

1. Stáhněte si aplikaci Mobile Key do svého mobilního telefonu. Aplikace je dostupná na App Store a Google Play.
2. Otevřete aplikaci a povolte aplikaci Mobile Key přístup k Bluetooth.
3. Podle typu mobilního klíče se přibližte s mobilním telefonem k USB čtečce nebo k párovacímu zařízení.
4. V aplikaci Mobile Key klikněte na nabízené zařízení pro párování.
5. Aplikace vás vyzve k zadání PIN kódu. Zadejte párovací kód a jeho zadání potvrďte.

## Způsoby autentizace Bluetooth

Ve webovém konfiguračním rozhraní lze nastavit různé způsoby Bluetooth autentizace.

- **Přímo v mobilní aplikaci** – uživatel přímo v mobilní aplikaci My2N vybere dveře, které chce otevřít. Pokud je jeho mobilní zařízení v dosahu zařízení 2N, se zařízením se spojí, a pokud jsou přístupová pravidla splněna, dveře se odemknou.
- **Přiblížením mobilního telefonu k zařízení a dotekem zařízení** – uživatel s mobilním zařízením a zapnutým Bluetooth přistoupí k zařízení 2N a dotkne se na zařízení 2N místa určeného k Bluetooth autentizaci, které je obvykle označeno ikonou Bluetooth . Po navázání spojení a ověření přístupových práv se dveře odemknou.
- **Detekcí pohybu** – zařízení 2N s kamerou rozpozná pohyb v okolí, automaticky aktivuje Bluetooth. Pokud zařízení 2N v dosahu zaznamená mobilní zařízení uživatele s platným přístupem, dveře se odemknou.

### Nastavení akceptovaných způsobů autentizace Bluetooth

1. Přejděte na stránku **Přístup > Moduly**.
2. V **kartě pro Bluetooth modul** vyberte možné způsoby v poli **Spustit autentizaci**.
3. Pokud jste vybrali „detekce pohybu“, zvolte profil, podle kterého se má pohyb detekovat.

**POZNÁMKA**
Profily detekce pohybu se nastavují v **Přizpůsobení > Kamera > Interní kamera**.

## Řízení výtahu

Pomocí připojení reléového modulu AXIS A9188 k interkomu 2N nebo k přístupové jednotce 2N lze řídit přístup na jednotlivá patra výtahu v budově. K jednomu interkomu 2N či přístupové jednotce 2N je možné připojit max. 8 těchto reléových modulů, přičemž každý z modulů může ovládat 8 pater, dohromady tedy max. 64 pater. Pro využití této funkce je nutné mít aktivní licenci: pro IP interkomy (obj. č. 9137916) nebo pro přístupové jednotky (obj. č. 9160401).

## Připojení výtahu

1. Připojte vstupy kontrolerů výtahu k relé AXIS A9188 a relé zapojte do IP sítě. Poznamenejte si IP adresu relé.
   Postupujte podle dokumentace k AXIS A9188 I/O Relay Module, která je dostupná na adrese http://www.axis.com.
2. Otevřete webové konfigurační rozhraní zařízení 2N, které má přístupy do výtahu spravovat.
3. Přejděte do **Integrace > Řízení přístupu > záložka Výtah**.
4. Na kartě **Reléové moduly (AXIS A9188)** povolte jeden z modulů.
5. Klikněte na ikonu tužky a v otevřeném poli zadejte IP adresu reléového modulu.
6. Pokud je přístup k relé podmíněn autentizací, zadejte uživatelské jméno a heslo v kartě **Obecné**.
7. Po povolení reléového modulu se objeví patra, která tento modul spravuje v kartě **Výtahová patra**. Jednotlivá patra můžete pojmenovat.

## Nastavení veřejného přístupu na patro

1. V kartě **Výtahová patra** vyberte patra, která mají být přístupná veřejnosti (není přístup k nim podmíněn autorizací).
2. Klikněte na ikonu tužky u vybraného patra.
3. V otevřeném nastavení povolte **Veřejný přístup.**
4. Volitelně omezte dobu veřejného přístupu výběrem časového profilu nebo nastavením vlastní doby přístupnosti.

## Nastavení dveřního spínače

Dveřní spínač je logická funkce zařízení, která ovládá elektrický zámek dveří. Spínač lze aktivovat různými způsoby (např. HTTP příkazem, RFID kartou nebo DTMF signálem).

Funkci dveřního spínače v zařízení vykonává **Spínač 1**.

Na stránce **Přístup > Moduly** pak lze přiřadit konkrétnímu přístupovému modulu ovládání jiného spínače.

## Nastavení dveřního spínače

1. Připojte kontakty elektrického zámku dveří (např. magnetický kontakt) k určenému vstupu na interkomu.
2. Ve webovém konfiguračním rozhraní přejděte do **Integrace > Spínače**.
3. Otevřete nastavení Spínače 1 kliknutím na šipku v záhlaví karty.

4. V kartě **Konfigurace** spínače nastavte parametry hardwarového výstupu, který má dveřní spínač ovládat.
   - **Řízený výstup** – určuje výstup, který spíná elektrický zámek dveří.
   - **Režim** – Monostabilní / Bistabilní.
   - **Doba zapnutí** – nastavuje dobu sepnutí spínače v monostabilním režimu. V bistabilním režimu spínače se nastavená doba sepnutí neuplatní.
   - **Typ výstupu** – v režimu „Security“ pracuje výstup v inverzním režimu, což znamená, že je trvale sepnutý a ovládá Bezpečnostní relé pomocí specifické pulzní sekvence. Pokud používáte reverzní zámek dveří (tzn. při napájení je zámek uzamčen), nastavte typ výstupu na hodnotu „Inverzní“.

     **TIP**
     Pokud používáte Bezpečnostní relé, nastavte typ výstupu na „Security“.

     Pokud je na jeden výstup napojeno více spínačů s odlišně nastaveným typem výstupu, řídí se podle následující priority:

     1. Security
     2. Inverzní
     3. Normální
5. V kartách **Aktivace** a **Aktivační kódy** můžete nastavit další způsoby sepnutí spínače. Pokud žádné další způsoby nenastavíte, spínač bude aktivován pouze povolením přístupu uživateli.
6. Změny uložte.

## Moduly

Stránka **Přístup > Moduly** poskytuje centrální správu všech přístupových hardwarových technologií zařízení. Každý modul má na stránce vlastní kartu, která umožňuje jeho správu. Spravují se zde jak moduly přímo integrované v hlavní jednotce zařízení, tak i ty, které jsou připojené přes VBUS.

Každý modul lze pojmenovat a přiřadit mu konkrétní spínač, který bude ovládat. Ostatní parametry závisí na typu modulu.

V továrním nastavení všechny moduly ovládají dveřní spínač.

# Rozšířené nastavení

## Nastavení kamery a videa

Kamera zařízení **2N Access Unit QR** detekuje pohyb v okolí zařízení a čte QR kódy.

### Nastavení interní kamery

1. Přejděte do **Přizpůsobení > Kamera**.
2. Na kartě **Interní kamera** klikněte na →.
3. V kartě **Nastavení** můžete upravovat základní parametry obrazu kamery.
4. Po uložení se změny se projeví v náhledu kamery.

### Režim

Režim kamery umožňuje nastavit optimální kombinaci expozičního režimu a frekvence napájení pro dosažení stabilního a kvalitního obrazu. Tento režim slouží ke snížení nežádoucího blikání, které může vznikat při použití umělého osvětlení nebo při rozdílné frekvenci elektrické sítě. Při instalaci kamer v interiéru lze zvolit vhodný způsob potlačení blikání způsobeného světelnými zdroji, zatímco při venkovním umístění je možné aktivovat režim potlačení přímého slunečního záření, který zajišťuje optimální přizpůsobení obrazu aktuálním světelným podmínkám.

### IR LED

Funkce přisvícení IR LED slouží k zajištění kvalitního obrazu i při nízké úrovni okolního osvětlení. Tento režim se spouští při poklesu světelných podmínek pod nastavenou úroveň. Limitní úroveň světelných podmínek se nastavuje až po povolení IR LED přísvitu.

**POZNÁMKA**
Pokud by mohlo dojít k překročení povoleného odběru napájení – například při současném provozu více rozšiřujících modulů napájených přes PoE – je úroveň IR přisvitu automaticky optimalizována tak, aby byla zachována stabilita funkce zařízení.

### Pokročilé nastavení

**Denní/noční režim** – umožňuje přepínat mezi barevným a černobílým obrazem podle světelných podmínek. Nastavte **Vždy den**, pokud chcete, aby kamera používala filtr potlačující infračervené záření a IR přisvícení bylo vypnuté. Nastavení „Vždy noc“ naopak vypne filtr a zapne IR přisvícení, což přepne obraz do černobílého režimu, vhodného pro noční vidění. Automatický režim kameru přepíná mezi těmito dvěma stavy podle úrovně okolního světla.

**Lokální kontrast** – zvýrazňuje detaily a textury tím, že zvyšuje rozdíly jasu mezi sousedními oblastmi obrazu (hranami).

**Mapování tónů** – zvyšuje jas a viditelnost obrazu, může však způsobit mírné zkreslení barev.

**Maximální doba expozice** – určuje maximální čas, po který je snímek exponován. Když je k dispozici více světla, nemusí být závěrka otevřena po celou dobu a kamera si automaticky nastaví kratší aktuální dobu expozice.

## Detekce pohybu

Detekce pohybu na zařízeních 2N je funkce, která automaticky rozpozná pohyb v zorném poli interní kamery a umožňuje spustit různé akce, například aktivace Bluetooth nebo nebo odeslání notifikace.

Pro optimální fungování je možné kalibrovat detekci podle prostředí a podmínek, například změnou parametrů citlivosti a oblasti, kterou má kamera sledovat.

## Nastavení detekce pohybu

1. Přejděte do **Přizpůsobení > Kamera**.
2. Na kartě **Interní kamera** klikněte na →.
3. V kartě **Náhled kamery** klikněte na ikonu tužky u parametru **Detekce pohybu**.
4. Otevře se okno s nastavením profilů detekce pohybu.
5. Rozbalte kartu profilu, který chcete nastavit.
6. Úpravou čtverce v náhledu kamery určité oblasti, ve které má kamera pohyb zaznamenávat.

> **VÝSTRAHA**
> Oblast obrazu je vztažená k aktuálnímu výřezu obrazu. Pokud změníte výřez obrazu kamery, stávající oblasti zůstanou stejné, ale budou fakticky pokrývat jinou část prostoru. Po úpravě výřezu je proto vždy doporučeno tyto oblasti zkontrolovat a upravit.

7. Vyberte režim zaznamenávání pohybu v daném profilu, viz Režimy profilu (str. 22)
8. Podle režimu nastavte případně další parametry.
9. Nezapomeňte profil vždy povolit!
10. Pro uložení změn klikněte na tlačítko **Uložit** nebo **Uložit a zavřít** v horní části stránky.

### Režimy profilu

#### Spouštění událostí

V tomto režimu kamera zachycuje okamžité, jednorázové pohyby. Příkladem použití je pořizování snímku, když někdo vstoupí do místnosti nebo když poblíž zařízení projede vozidlo.

Aktivaci vyvolané události lze oddálit pomocí nastavené prodlevy.

Pomocí filtru definujete typy pohybů, které má kamera ignorovat – například malé objekty (drobné ptactvo) nebo opakované pohyby (stromy ve větru).

#### Nahrávání

Tento profil při detekci pohybu zahájí událost v trvání 30 sekund. Dojde-li v této době k dalšímu pohybu, profil vše spojí do jedné události. Tento režim je vhodný pro nepřetržité sledování a zabraňuje vytváření velkého množství krátkých záznamů.

Pomocí filtru definujete typy pohybů, které má kamera ignorovat – například malé objekty (drobné ptactvo) nebo opakované pohyby (stromy ve větru).

#### Detekce přítomnosti obličejů

Profil rozpoznává pohyb tehdy, pokud se v monitorované oblasti objeví obličej. Událost může vzniknout i v případě, kdy se v záběru objeví statický obraz obličeje (např. fotografie).

#### Detekce příchozích osob

Profil rozpoznává výhradně pohybující se osoby a ignoruje statické obrázky tváří.

## Ochrana soukromí

Funkce ochrana soukromí zamaskuje část obrazu tak, aby nebyla ve videu viditelná ani nebyla zaznamenávána. Tato možnost je ideální například pro situace, kdy chcete chránit citlivé oblasti obrazu. Například

pokud je zařízení umístěno u recepce a kamera snímá i chodbu, po které se pohybují cizí osoby, můžete oblast chodby skrýt.

**VÝSTRAHA**
Ochrana soukromí může omezovat činnost čtení QR kódů nebo detekci pohybu. Nedoporučujeme používat ochranu soukromí s uvedenými funkcemi zároveň.

### Nastavení detekce pohybu

1. Přejděte do **Přizpůsobení > Kamera**.
2. Na kartě **Interní kamera** klikněte na .
3. V kartě **Náhled kamery** klikněte na ikonu tužky u parametru **Ochrana soukromí**.
4. V náhledu kamery upravte čtverec tak, aby pokrýval oblast, kterou chcete zamaskovat.

   **VÝSTRAHA**
   Oblast obrazu je vztažená k aktuálnímu výřezu obrazu. Pokud změníte výřez obrazu kamery, stávající oblasti zůstanou stejné, ale budou fakticky pokrývat jinou část prostoru. Po úpravě výřezu je proto vždy doporučeno tyto oblasti zkontrolovat a upravit.
5. Zvolte mód zamaskování:
   - **Barva** – vybraná oblast bude překryta barvou dle výběru
   - **Mozaika** – vybraná oblast bude rozpixelována. Velikost mozaiky nastavte podle míry potřebné anonymizace dat.
6. Nezapomeňte ochranu soukromí povolit v záhlaví nastavení parametrů!
7. Pro uložení změn klikněte na tlačítko **Uložit** nebo **Uložit a zavřít** v horní části stránky.

## Externí kamera

Externí kamera se k zařízení 2N přidává jako video stream (RTSP). Připojení externí kamery umožňuje během hovoru přepínat mezi pohledy. Funkce externí kamery je tedy čistě zobrazovací.

**VÝSTRAHA**
QR kódy lze načítat pouze na interní kameře zařízení.

### Přidání externí kamery

1. Přejděte do **Přizpůsobení > Kamera**.
2. V kartě **Externí kamera** zvolte možnost Přidat kameru.
3. V otevřeném dialogovém okně kameru povolte.
4. Zadejte adresu zdroje streamu externí IP kamery ve formátu `rtsp://ip_adresa_kamery/parametry`.
5. Pokud je stream externí kamery podmíněn autentizací, vyplňte **přihlašovací údaje ke streamu**.
6. Změny uložte kliknutím na Přidat kameru.
7. Má-li mít externí kamera funkci hlavní kamery zařízení, pak po uložení na kartě **Externí kamera** klikněte na Nastavit jako výchozí zdroj.
   Při hovoru se zařízením se jako první zobrazí obraz z kamery nastavené jako výchozí zdroj.

## Vytvoření video streamu z kamery zařízení

Funkce streamování videa slouží k přenosu živého videozáznamu z kamery zařízení přes síť do přijímacího zařízení jako může být aplikace v mobilu, sledovací software nebo na počítači v přehrávači videí. Tento proces zajišťuje, že uživatelé mohou sledovat video v reálném čase z různých zařízení.

## Vytvoření video streamu

1. Přejděte na **Integrace > Video**.
2. Povolte službu **RTSP server**.
3. Nastavte parametry streamu, viz Parametry video streamu (str. 24).
4. V kartě **Omezení připojení** můžete vyplnit IP adresy, ze kterých bude stream dostupný. Pokud nejsou vyplněny žádné IP adresy, je možné se připojit z libovolné IP adresy.
5. V kartě **Předkonfigurované streamy** určete, zda má být stream přístupný:
   - anonymně
   - s ověřením – nastavte údaje k ověření v kartě **Autentizace**.
6. V karta **Předkonfigurované streamy** naleznete IP adresy nastavených streamů podle vybraného videokodeku.

## Parametry video streamu

### Obecná nastavení streamů

**Kompenzace jitteru** – nastavuje délku vyrovnávací paměti pro kompenzaci nerovnoměrnosti intervalů mezi příchody audio paketů. Delší paměť znamená vyšší odolnost proti výpadkům, ale větší zpoždění zvuku.

**Hodnota QoS DSCP** – nastavuje prioritu audio a video RTP paketů v síti. Nastavená hodnota se odesílá v poli TOS (Type of Service) v záhlaví IP paketu.

**Povolení režimu UDP unicast** – povoluje režim odesílání dat audio a video streamu pomocí RTP/UDP protokolu. Pokud je tento režim vypnut, data audio a video streamu se přenáší vždy pouze pomocí RTP/RTSP protokolu.

**Počáteční RTP port** – nastavuje počáteční lokální RTP port v rozsahu o délce 60 portů používaných při přenosu audia a videa. Výchozí hodnota je 4800 (tj. používaný rozsah je 4800–4859).

**Zipstream** – vybírá výchozí úroveň komprese Zipstream (pro H.264). AXIS Zipstream zachovává všechny důležité forenzní detaily, které potřebujete, a zároveň snižuje požadavky na datový přenos a úložiště v průměru o 50 %.

### Nastavení streamů vlastního formátu

1. V kartě **Streamy vlastního formátu** klikněte na Generovat stream URL. Otevře se dialogové okno.
2. V dialogovém okně nastavte:
   - **Kodek** – vybírá z dostupných kodeků
   - **Povolení zvuku** – určuje, zda se má přenášet pouze video, nebo video se zvukem
   - **Rozlišení** – nastavuje rozlišení obrazu
   - **Framerate** – nastavuje snímkovou frekvenci zaznamenávaného videa
   - **Datový tok** – nastavuje bitrate
   - **Zipstream** – vybírá výchozí úroveň komprese Zipstream (pro H.264). AXIS Zipstream zachovává všechny důležité forenzní detaily, které potřebujete, a zároveň snižuje požadavky na datový přenos a úložiště v průměru o 50 %.
3. Ve spodní části dialogového okna se automaticky načte adresa streamu s parametry.
4. Zkopírujte si adresu streamu a změny uložte.

# Nastavení zvuku

## Nastavení hlasitosti zařízení

Hlasitost zařízení nastavíte v **Přízpůsobení > Audio**.

### Uživatelské zvuky

Zařízení vykonává několik akcí, které jsou doprovázeny zvukem (vyzvánění, sepnutí spínače apod.). Přehrávané zvuky můžete změnit v **Přizpůsobení > Uživatelské zvuky**.

Do zařízení lze také možné nahrát až 10 vlastních uživatelských zvuků.

### Další audio funkce zařízení

### Detekce šumu

Zařízení může sledovat zvuk přijímaný mikrofonem a jakmile úroveň signálu mikrofonu překročí nastavený práh, může zařízení vyvolat událost `Event.NoiseDetected`. Na tuto událost je možné v automatizaci navázat další akce (viz Automatizace (str. 31)).

### Aktivace detekce hluku

1. Přejděte do **Integrace > Audio**.
2. V záhlaví karty **Detekce šumu** funkci povolte.
3. V parametru **Prahová úroveň hluku** určete hodnotu [dB], po jejímž překročení se spustí událost **Event.NoiseDetected**.
4. V parametru **Zpoždění začátku alarmu** můžete nastavit dobu, po kterou musí být hluk nad prahovou úrovní, aby se událost aktivovala.
5. V parametru **Zpoždění konce alarmu** naopak můžete určit dobu, po kterou musí být signál pod prahovou hodnotou, aby se událost ukončila.

### Audio test

Výsledek posledního testu najdete v **Integrace > Audio > záložka Obecné > karta Audio test**.

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

**POZNÁMKA**
Pokud v čase spuštění audio testu probíhá hovor, je audio test odložen dokud není hovor ukončen. Audio test proběhne ihned po ukončení hovoru.

## Časové profily

Některé funkce, které zařízení vykonává, jsou podmíněny časem. Sekce **Časové profily** vám umožní přednastavit časové intervaly, ze kterých pak můžete u těchto funkcí vybírat. Díky tomu nemusíte při každém nastavení zadávat čas ručně. Časový profil si můžete pro lepší přehlednost pojmenovat.

### Vytvoření časového profilu

1. Přejděte do **Přizpůsobení > Časové profily**.
2. Klikněte na prázdný pro vytvoření nového profilu.
3. Zadejte název profilu.
4. Klikněte na Uložit. Otevře se detail profilu.

5. Nastavte intervaly, kdy má být časový profil aktivní.
   1. Klikněte na požadovaný interval.
   2. V otevřené nabídce můžete upřesnit začátek a konec.

> **POZNÁMKA**
> Řádek **Svátky** slouží k nastavení odlišných časových intervalů během vybraných dnů, viz Svátky (str. 26).

6. Změny uložte.

## Svátky

V konfiguraci zařízení můžete několik definovat dny, které budou označovány jako svátky. Pro tyto dny se pak nastavují v časových profilech speciální intervaly. Typicky se jedná o dny jako státní, svátky, firemní volno a další mimořádné dny.

U každého svátku určíte, zda platí jen pro konkrétní rok, nebo se opakuje každý rok ve stejný den. Svátky je možné naplánovat na několik let dopředu.

## Nastavení svátků:

1. Přejděte do **Přizpůsobení > Časové profily > karta Svátky**.
2. Vyberte rok, pro který chcete svátek nastavit.
3. Klikněte na den v kalendáři:
   - První kliknutí označí svátek, který se bude opakovat každý rok v daný den a měsíc.
   - Druhé kliknutí změní svátek na jednorázový pro vybraný rok.
4. Změny uložte.

# Systém

## Nastavení data a času

**VÝSTRAHA**
Pokud je zařízení spravováno nástrojem pro hromadnou správu (2N Access Commander / 2N My2N) může být čas zařízení řízen tímto nástrojem. Manuální změna ve webovém rozhraní zařízení pak nemá na nastavení času vliv.

### Synchronizace s NTP

Pokud je zařízení připojeno k internetu, může se čas a datum synchronizovat pomocí NTP.

1. Přejděte do **Systém > Datum a čas**.
2. Na kartě **Nastavení synchronizace času** aktivujte možnost **Automatický čas z NTP nebo internetu**.
3. Zadejte adresu vámi zvoleného NTP serveru.

### Aktualizace času při jeho výpadku

1. Přejděte do **Systém > Datum a čas**.
2. Na kartě **Nastavení synchronizace času** klikněte na Synchronizace s prohlížečem.
   Tím se synchronizuje čas zařízení s časem ve vašem počítači.

**POZNÁMKA**
Zařízení 2N jsou vybaveny zálohovanými hodinami reálného času, které umožňují překonat výpadek napájení po dobu až několika dnů.

## Nastavení sítě

V továrním nastavení používá zařízení dynamickou IP adresu přidělenou DHCP serverem.

Správné nastavení IP adresy je klíčové pro zajištění stabilního a spolehlivého připojení zařízení k vaší síti.

1. Nastavení síťových parametrů zařízení provedete v **Systém > Připojení k síti**.

2. V kartě Základní nastavení > Nastavení IP adresy můžete povolit nebo zakázat server DHCP.

### Nastavení statické IP adresy:

a. Zakažte možnost **server DHCP**.
b. Zadejte požadovanou IP adresu, masku podsítě, výchozí bránu a DNS servery.
c. Uložte změny. Zařízení se restartujte.

### Nastavení DHCP

a. Povolte možnost **server DHCP**.
b. Zadejte požadovanou IP adresu, síťovou masku, výchozí bránu a DNS servery.
c. Uložte změny. Zařízení se restartujte.

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

## Licence

Některé funkce jsou dostupné pouze na základě příslušné licence. Přehled licencí a zda jsou aktivní, naleznete v **Systém > Licence > záložka Obecné informace.** V záložce **Licencované funkce** pak naleznete přehled dostupných funkcí, které jsou podmíněné licencí.

**POZNÁMKA**
Po výběru vhodné licence kontaktujte prodejce 2N. Jste-li partnerem společnosti 2N, můžete se obrátit na naše oddělení péče o zákazníky na adrese customercare@2n.com. V žádosti uveďte sériové číslo zařízení.

### Aktualizace licenčního klíče

Aktuální licenční klíč je dostupný na aktualizačním serveru. V případě, že není ve webovém konfiguračním rozhraní přístup k veřejnému internetu, je možné do zařízení nahrát soubor s klíčem manuálně.

Po každém restartu zařízení se znovu načte poslední dostupný licenční klíč.

### Zkušební licence

Zkušební licence umožňuje dočasně využívat všechny funkce licence Gold a Microsoft Teams licence, a to po dobu maximálně 800 hodin od její aktivace. Aktivovanou zkušební licenci nelze pozastavit.

Aktivace zkušební licence se prování v **Systém > Licence > karta Zkušební licence**.

**VÝSTRAHA**
Při každém restartu zařízení se odebere jedna hodina zkušební licence.

# Použité porty

| Služba | Port | Protokol | Směr | Standardně zapnuté | Nastavitelné | Nastavení |
|---|---|---|---|---|---|---|
| 802.1x | – | – | In/Out | × | × | – |
| DHCP | 68 | UDP | In/Out | ✓ | × | – |
| DNS | 53 | TCP/UDP | In/Out | ✓ | × | – |
| Echo (device discovery)* | 8002 | UDP | In/Out | ✓ | × | – |
| FTP | 21 | TCP | Out | × | × | – |
| 2N IP Eye | 8003 | UDP | Out | × | × | – |
| HTTP | 80 | TCP | In/Out | ✓ | ✓ | **Systém > Připojení k síti > záložka WEB SERVER** |
| HTTPS | 443 | TCP | In/Out | ✓ | ✓ | **Systém > Připojení k síti > záložka WEB SERVER** |
| NTP klient | 123 | UDP | In/Out | ✓ | × | – |
| SLP | 427 | UDP | In/Out | ✓ | × | – |
| SMTP | 25 | TCP | Out | × | ✓ | **Integrace > E-mailové oznámení** |
| Syslog | 514 | UDP | Out | × | × | – |
| TFTP | 69 | UDP | Out | × | × | – |

| Služba | Port | Protokol | Směr | Standardně zapnuté | Nastavitelné | Nastavení |
|---|---|---|---|---|---|---|
| My2N Knocker | 443 | TCP | Out | ✓ | × | – |
| My2N Tribble Tunnel | 443 | TCP | Out | ✓ | × | – |
| SNMP Agent | 161 | UDP | In/Out | ✓ | × | – |
| SNMP Trap | 162 | UDP | Out | ✓ | × | – |
| Multicast receiver (Automation) | 4433 | UDP | In | × | × | – |
| Multicast DNS | 5353 | UDP | In/Out | ✓ | × | – |

# Automatizace

Standardní konfigurace zařízení 2N pokrývá většinu běžných scénářů. Pro pokročilé případy jako je potřeba zařízení přizpůsobit specifickým požadavkům nebo jej integrovat se systémy třetích stran, lze využít funkci Automatizace. Automatizace umožňují definovat vlastní logiku chování zařízení, která reaguje na různé události, signály nebo kombinace podmínek. Lze například spouštět specifické akce při stisku tlačítka konkrétního rychlé volby, aktivací Tichého alarmu, detekcí otevřených dveří, sepnutím vstupu nebo detekcí pohybu poblíž zařízení.

## Nastavení automatizace:

1. Ve webovém rozhraní zařízení přejděte na stránku **Integrace > Automatizace**.
2. V přehledu funkcí povolte počet funkcí podle potřeby.
3. Kliknutím na  otevřete konfigurační rozhraní automatizací.
4. V záhlaví rozhraní automatizací zadejte název funkce, pod kterým bude funkce uložena.
5. Vytvořte tok automatizace.
   Detailní popis funkce a konfigurace Automatizace je k dispozici v Automation manuálu.
6. Po dokončení funkce klikněte na SAVE a opusťte rozhraní automatizací.


Přístupové jednotky – Konfigurační manuál

© 2N Telekomunikace a. s., 2026

**2N.com**