

The background of the page features a cityscape at dusk or dawn, with various skyscrapers and buildings illuminated. Overlaid on this are large, semi-transparent red geometric shapes, including a large triangle pointing downwards and several overlapping lines and polygons in shades of red and orange.

NODER EE12/EWE4

Síťový přístupový systém

Pokyny pro spuštění a konfiguraci

Obsah

Obsah.....	2
1. Před zahájením konfigurace.....	3
2. Popis zařízení.....	3
3. Konfigurace Noder modulu	4
3.1 Instalace systému	4
3.2 Noder Server	4
3.3 Objekt Noder.....	6
3.4 Kontrolér Noder.....	7
3.4.1 Záložka Akce.....	8
3.4.2 Záložka Komunikace	10
3.4.3 Záložka Nastavení	12
3.4.4 Záložka formát karet.....	13
3.4.5 Záložka OSDP.....	14
3.4.6 Záložka Další.....	15
3.5 Čtečky	16
3.5.1 Záložka Základní nastavení.....	18
3.5.2 Záložka Alarmy a logy.....	20
3.5.3 Záložka Ostatní	23
3.5.4 Záložka Online režim a AntiPassBack.....	24
3.6 Vstupy	24
3.6.1 Konfigurace vstupů	26
3.6.2 Diagramy zapojení vstupů v přístupovém systému	28
3.6.3 Diagramy zapojení vstupu v zabezpečovacím systému	29
3.7 Výstupy.....	31
3.8 Výtahové moduly.....	33
3.8.1 Konfigurace výtahového modulu	33
3.8.2 Konfigurace podlaží.....	34
3.9 Noder IAS Zóna	36
4. Správa uživatelů.....	38

1. Před zahájením konfigurace

Před konfigurací Noderu musí být síťový kontrolér EE12 / EWE4 správně nainstalován, připojen a spuštěn v souladu s Technickou dokumentací.

2. Popis zařízení

Síťový kontrolér přístupového a zabezpečovacího systému je pokročilé mikroprocesorové I/O zařízení pro automatickou identifikaci uživatele. Může být použit pro bezpečnostní systémy budov, řízení přístupu, docházku, hotely a rekreační zařízení. Systémem pro řízení a správu je platforma **Axxon Intellect**.

Detaily o spuštění, konfiguraci síťového nastavení a připojení zařízení ke kontroléru naleznete v technické dokumentaci kontrolérů.

3. Konfigurace Noder modulu

Tato kapitola představí spuštění a konfiguraci modulu Noder.

3.1 Instalace systému

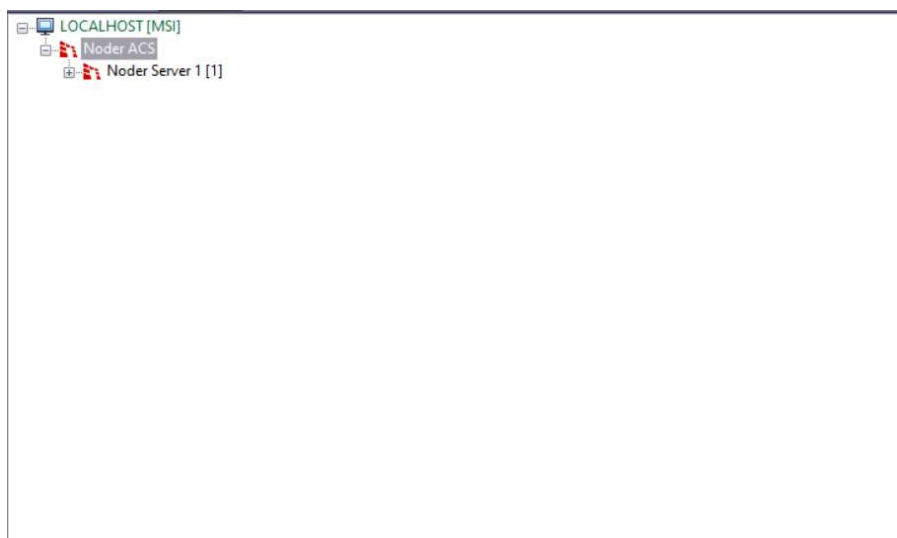
Přístupový a zabezpečovací systém Noder funguje pod platformou Axxon Intellect Enterprise. Dedikovaný modul "NoderEe12.run" má na starost komunikaci s kontroléry. Pro správné fungování ACS Noder, následující komponenty musí být nainstalovány na serveru:

- Axxon Intellect Enterprise Základní verze (verze 4.10.4 nebo vyšší)
- Modul ACFA (verze 6.7 nebo vyšší):
 - Noder EE12/EWE4 ze Systémů řízení přístupu
 - Správce Přístupu z Aplikačního software

Funkce zabezpečovacího systému je k dispozici pouze pro kontroléry s MB revizí alespoň 1,06 pro EWE4 a 1,08 pro EE12. Verze modulu alespoň 2.1.1.204, verze firmwaru alespoň RC38 2021-06-02 (aktualizace 517).

3.2 Noder Server

Konfigurace prvků systému Noder se provádí z administračního panelu serveru Intellect. V **Hardware** záložce na serveru, kde má modul fungovat, přidáme nový objekt s názvem **Noder Server** skrze **Vytvořit objekt**. Vytvoří se nový objekt ve složce s názvem **Noder ACS**.



Noder Server je modul odpovědný za komunikaci s kontroléry. Noder Server obsahuje objekty Noder Objekt.



Debug – Možnost pro programátory umožňující určit nastavení souborů obsahujících logy z komunikace s kontroléry.

Úroveň – možnost dovoluje specifikovat úroveň logů, které budou uloženy.

Kontrolér – možnost dovoluje specifikovat konkrétní kontrolér, pro který budou ukládány logy.

Nastavení aktualizace uživatelů:

Dynamická aktualizace uživatelů – tahle funkce umožňuje automatické posílání uživatelů a přístupových úrovní do kontroléru s každou změnou.

Neodesílat do kontrolérů – tahle funkce umožňuje provádění jakýchkoliv změn uživatelských oprávnění a jejich přístupových úrovní bez toho, aby se tyto změny automaticky projeví na kontrolérech. Pokud je tahle možnost vybrána, uživatelská oprávnění a přístupové úrovně budou muset být poslány do kontroléru manuálně.

SSH nastavení:

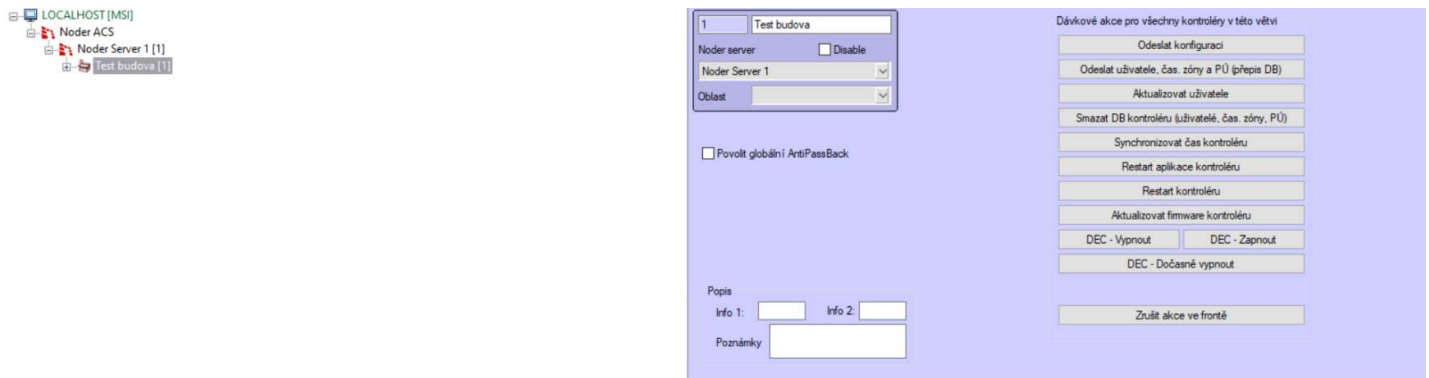
Rozsah portů SSH – rozsah portů pro SSH tuneling.

Verze modulu – pole zobrazuje aktuální verzi Noder modulu.

Dávkové akce pro všechny kontroléry v této větvi – umožňuje provést vybranou akci na všech kontrolérech ve stromu s nastaveným časovým zpožděním. Pokud je v systému více než 50 kontrolérů, budou příkazy pro další kontroléry odesílány postupně. Jednotlivé možnosti jsou popsány na kartě Akce.

3.3 Objekt Noder

Element, který dovoluje rozdělit systém do logických částí (patra, budovy, oddělení) a spravovat je.



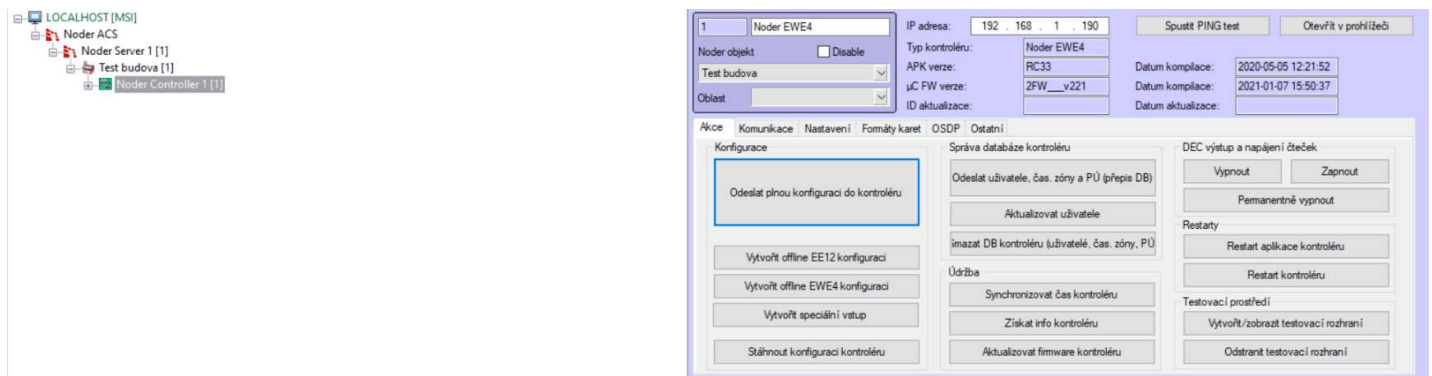
Povolit globální AntiPassBack – možnost povolí funkci AntiPassBack na daném objektu

Popis – pole pro informace o daném objektu. Funkce **neovlivňuje logiku kontroléru**.

Dávkové akce pro všechny kontroléry v této větvi – sekce umožňuje provést vybranou akci na všech kontrolérech v objektu. Jednotlivé možnosti jsou popsány na kartě Akce.

3.4 Kontrolér Noder

Objekt umožňující připojení s kontrolérem a jeho konfiguraci.

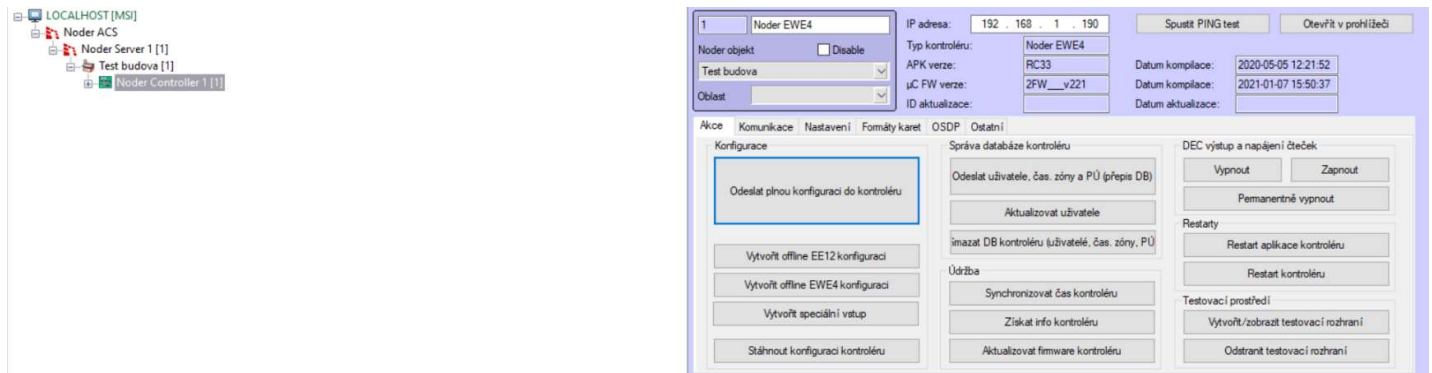


Po přidání objektu Kontroléru se zobrazí rozhraní pro konfiguraci. V poli **IP adresa** zadejte nastavenou IP adresu kontroléru. **Spustit PING test** spustí cmd.exe a monitoruje zařízení pomocí ICMP protokolu. **Otevřít v prohlížeči** otevře výchozí webový prohlížeč systému a automaticky se přihlásí na webovou stránku kontroléru.

Po úspěšném připojení kontroléru, se řádky **APK verze**, **uC FW verze** s **Datum kompilace** a **ID aktualizace** s **Datum aktualizace** automaticky vyplní informacemi stáhnutými z kontroléru.

3.4.1 Záložka Akce

Karta Akce umožňuje vytváření, kontrolu a odesílání konfigurace kontrolérů a odesílání uživatelů. Karta umožňuje vzdálené ovládání, restart zařízení a vytvoření testovacího rozhraní.



Konfigurace:

Odeslat plnou konfiguraci do kontrolérů – pošle aktuální nastavení v modulu Noder ACS. Konfigurace je posílána dynamicky, to znamená že všechny konfigurované změny jsou průběžně posílány do kontroléru.

Vytvořit offline EE12 konfiguraci, Vytvořit offline EWE4 konfiguraci – funkce vytvoření konfigurace v situaci, kde nemáme spojení s kontrolérem a chceme systém nakonfigurovat předem v offline režimu.

Vytvořit speciální vstupy – funkce vytvoření speciálních vstupů (21-BAT, 22-AC, 23-TMP, 24-DR) a nastavení jejich výchozích hodnot pro účel popsany v kapitole 3.5.5.

Stáhnout konfiguraci kontroléru – získá nastavení kontroléru. Nový kontrolér má vždy spouštěcí konfiguraci, musí být stažen při prvním spuštění.

Správa databáze kontroléru:

Odeslat uživatele, čas. zóny a PÚ (přepis DB) – smaže všechny uživatele, přístupové úrovně a časové zóny v kontroléru, a uloží celou databázi znovu.

Aktualizovat uživatele – pošle všechny změny v uživateli z vyrovnávací paměti modulu Noder ACS.

Smazat DB kontroléru – smaže všechny uživatele, přístupové úrovně a časové zóny v kontroléru.

Údržba:

Synchronizovat čas kontroléru – synchronizuje čas a datum kontroléru se serverem. Tahle funkce se spouští automaticky každé 4 hodiny, když je kontrolér připojen.

Získat info kontroléru – stáhne informace o verzi firmware kontroléru a čteček.

Aktualizovat firmware kontroléru – nahraje firmware z vybrané složky.

DEC výstup a napájení čteček:

Vypnout – možnost používaná k deaktivaci zařízení napájených z portů řadiče a výstupu DEC.

Zapnout – možnost používaná k povolení zařízení napájených z portů řadiče a výstupu DEC.

Dočasně vypnout – možnost používaná k dočasnému vypnutí zařízení napájených z portů řadiče a výstupu DEC. Čas lze konfigurovat na kartě Nastavení. Tuto funkci lze použít např. pro restartování čteček.

Restarty:

Restart aplikace kontroléru – restartuje aplikaci (APK) zodpovědnou za logiku kontroléru.

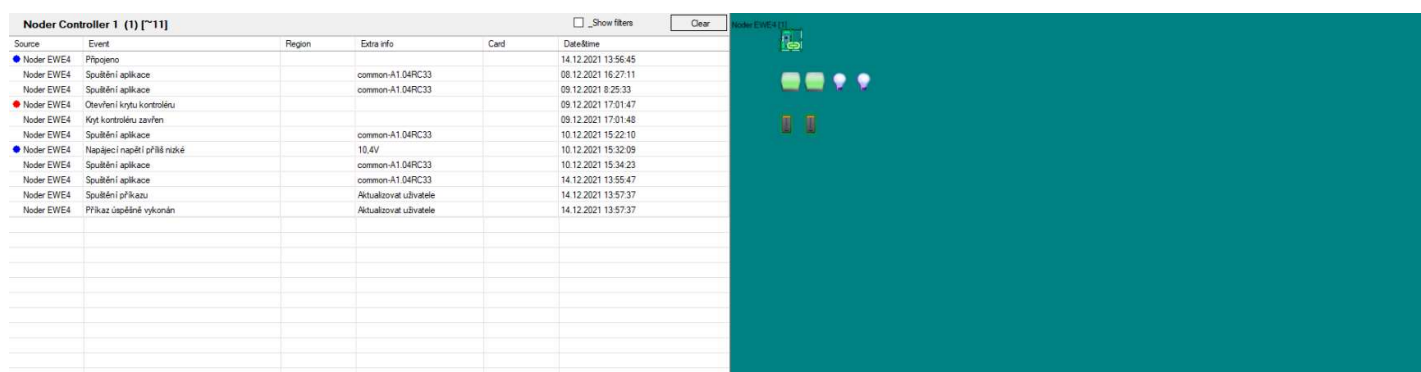
Restart kontroléru – úplné restartování kontroléru.

Testovací prostředí:

Vytvořit/zobrazit testovací rozhraní – vytvoří rozhraní kontroléru skládající se z prohlížeče událostí souvisejících s daným kontrolérem a mapy s ikonami všech čteček a vstupů daného kontroléru. Pokud bylo takové testovací rozhraní vytvořeno dříve, vyvolání této funkce obnoví mapu podle aktuální konfigurace a rozhraní zobrazí.

Odstranit testovací rozhraní – odstraní testovací rozhraní.

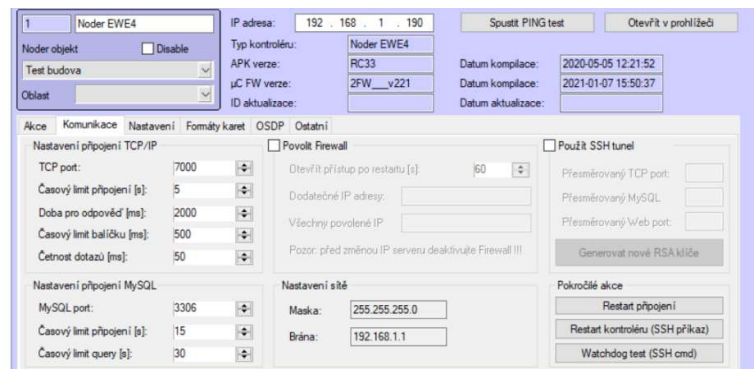
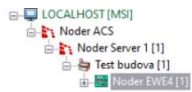
Ukázka testovacího rozhraní:



Source	Event	Region	Extra info	Card	Date/Time
Noder EWE4	Připojeno				14.12.2021 13:56:45
Noder EWE4	Spuštění aplikace		common-A1 04RC33		08.12.2021 16:27:11
Noder EWE4	Spuštění aplikace		common-A1 04RC33		09.12.2021 8:25:33
Noder EWE4	Otevření krytu kontroléru				09.12.2021 17:01:47
Noder EWE4	Kytí kontroléru zavřeno				09.12.2021 17:01:48
Noder EWE4	Spuštění aplikace		common-A1 04RC33		10.12.2021 15:22:10
Noder EWE4	Napájecí napětí příliš nízké		10,4V		10.12.2021 15:32:09
Noder EWE4	Spuštění aplikace		common-A1 04RC33		10.12.2021 15:34:23
Noder EWE4	Spuštění aplikace		common-A1 04RC33		14.12.2021 13:55:47
Noder EWE4	Spuštění příkazu		Aktualizovat uživatelé		14.12.2021 13:57:37
Noder EWE4	Příkaz úspěšně vykonán		Aktualizovat uživatelé		14.12.2021 13:57:37

3.4.2 Záložka Komunikace

V záložce jsou dostupné možnosti konfigurace TCP/IP spojení, firewall a SSH tunelingu.



Nastavení připojení TCP/IP:

TCP port – port 7000 používaný pro připojení TCP s kontrolérem.

Časový limit připojení [s] – maximální doba čekání odezvy kontroléru během připojení. Pro rychlé opětovné připojení tuto dobu snižte.

Doba pro odpověď [ms] – maximální doba čekání na odpověď kontroléru během komunikace. Pro rychlé opětovné připojení tuto dobu snižte.

Časový limit balíčku [ms] – maximální doba čtení odpovědi z kontroléru. Pro rychlé opětovné připojení tuto dobu snižte.

Četnost dotazů [ms] – čas mezi předchozí a další kontrolou událostí a stavů.

Nastavení připojení MySQL:

MySQL port – port 3306 pro přímé připojení k databázi kontroléru. Toto připojení se používá hlavně pro rychlou aktualizaci uživatelů (až 1 000 za sekundu).

Časový limit připojení [s] – maximální doba čekání na odezvu databáze řadiče během připojení.

Časový limit query [s] – maximální doba čekání na provedení SQL dotazu.

Firewall:

Otevřít přístup po restartu [s] – když je firewall zapnutý, zařízení s nepovolenými adresami se nemohou připojit. Díky této možnosti se uživatel může připojit ke kontroléru po nastavenou dobu od spuštění APK ovladače, i když je mimo povolené IP adresy.

Dodatečné IP adresy – správce má možnost přidat další IP adresy, které budou patřit k povoleným IP adresám. Jako oddělovač použijte čárku. Příklad: 10.10.1.50,192.168.1.10,192.168.1.22

Všechny povolené IP – souhrn se seznamem povolených IP adres. Kromě vlastních budou všechny IP adresy počítače, kam patří server Noder.

Nastavení sítě – maska a brána kontroléru nakonfigurovaná v prohlížeči.

SSH tunel – funkce pro vytvoření šifrovaného kanálu mezi serverem a kontrolérem, než přesměrování celé komunikace přes tento kanál:

Přesměrovaný TCP port – informace s použitým lokálním portem pro TCP spojení přes SSH tunel.

Přesměrovaný MySQL – informace s použitým lokálním portem pro připojení k databázi přes SSH tunel.

Přesměrovaný web port – informace s použitým lokálním portem pro připojení k webovým stránkám kontroléru přes SSH tunel.

Generovat nové RSA klíče – tlačítko pro vygenerování párů RSA klíčů (veřejného a soukromého) pro připojení SSH a příkazy SSH.

SSH připojení je na 22 portu. Při použití tunelu SSH je ve výchozím nastavení povolen také firewall a porty 3306 a 80 jsou uzavřeny. TCP port 7000 se používá pouze pro získání verze kontroléru, poté je zřízen SSH tunel. Tato funkce je v ovladačích od verze APK >= RC37.

Pokročilé akce:

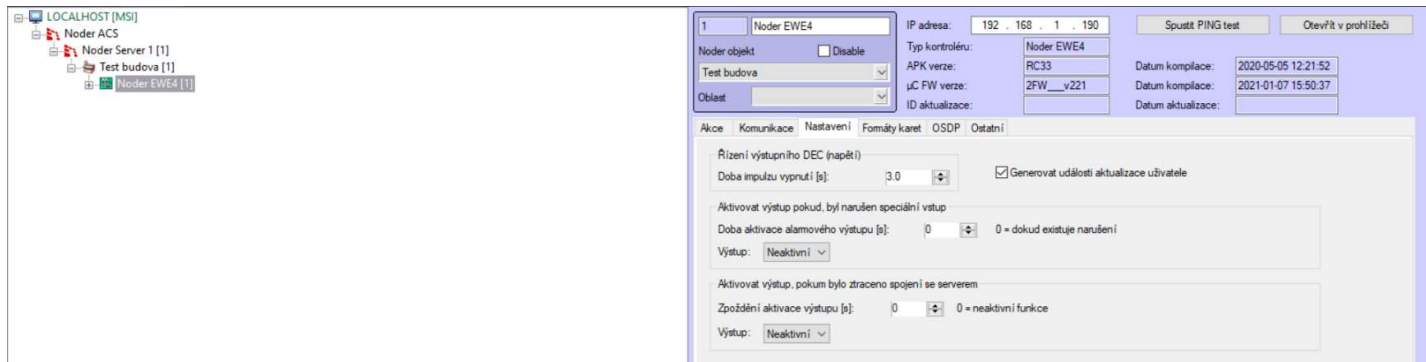
Restart připojení – tlačítko pro odpojení kontroléru a opětovné připojení.

Restart kontroléru (SSH příkaz) – zabezpečený příkaz na 22 portu pro restartování kontroléru (funguje, i když je kontrolér odpojen od Intellectu).

Watchdog test (SSH příkaz) – příkaz zastaví srdeční zprávu z operačního systému kontroléru do mikrokontroléru základní desky, kterou by měl hlídací pes detekovat až do 2 minut. To způsobí restart kontroléru krátkým brzděním napájení. Tento příkaz nespouštějte, pokud máte starou základní desku bez nainstalovaného externího hlídacího psa. Po příkazu se spojení ztratí za cca. 2 minuty. Toto je zabezpečený příkaz na 22 portu fungující, i když je kontrolér odpojen od Intellectu.

3.4.3 Záložka Nastavení

Záložka Nastavení umožňuje konfigurovat výstup DEC. Záložka navíc umožňuje konfigurovat výstupy v případě ztráty a narušení spojení



Řízení výstupního DEC (napětí):

Doba impulsu vypnutí [s] – volba umožňuje nastavení doby dočasného vypnutí výstupu DEC.

Generovat události aktualizace uživatele – po výběru vygeneruje každá aktualizace uživatele událost v systému.

Aktivovat výstup, pokud byl narušen speciální vstup:

Doba aktivace alarmového výstupu [s] – doba, po kterou má být výstup aktivován po narušení speciálního vstupu (21-24). Když je hodnota 0, výstup je aktivní, dokud nedojde k narušení.

Výstup – reléový výstup pro aktivaci

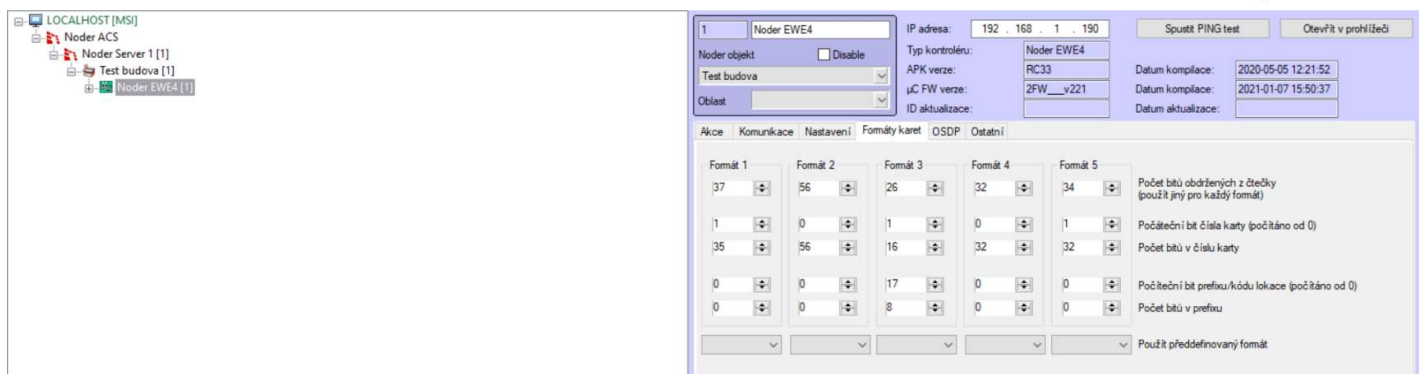
Aktivovat výstup, pokud bylo ztraceno spojení se serverem:

Zpoždění aktivace výstupu [s] – po uplynutí nastavené doby od ztráty spojení s výstupem serveru se aktivuje. Když je hodnota 0, funkce je neaktivní.

Výstup – reléový výstup pro aktivaci

3.4.4 Záložka formát karet

Nastavení různých formátů karet dává možnost připojení čteček s různými parametry čtených karet k jednomu kontroléru.



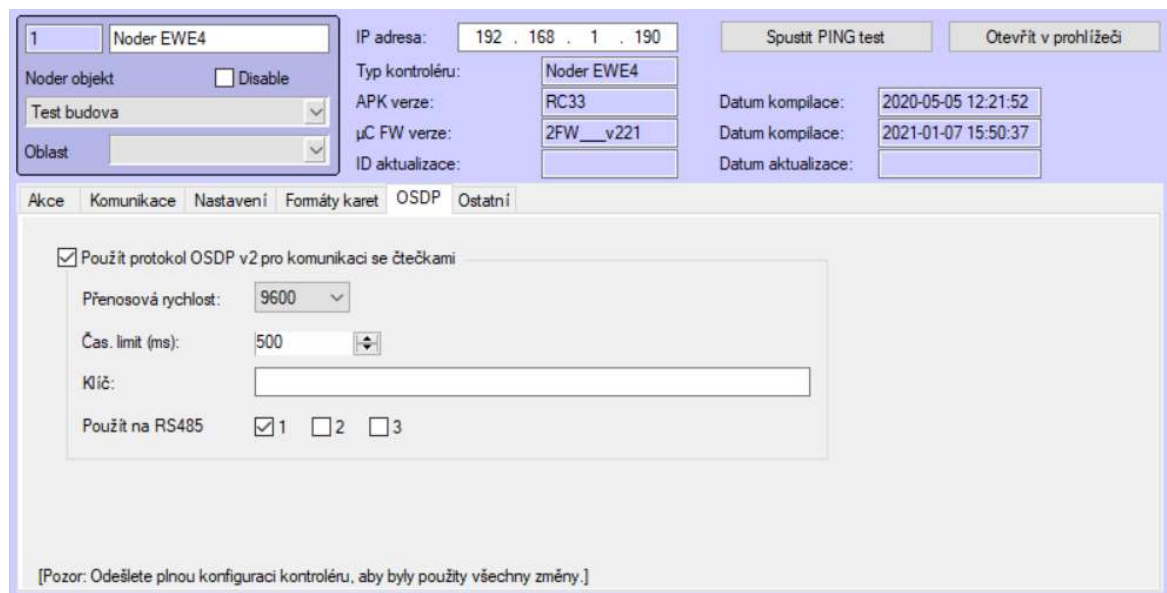
Kontrolér zvládne 5 formátů karet podle počtu přijatých bitů. Intellect dává na výběr předdefinované formáty karet nebo jejich manuální konfiguraci.

Použití karty s nedefinovaným počtem bitů ve formátech karet vygeneruje v systému událost „Neplatný počet bitů“ s informací o tom, kolik bitů bylo přečteno.

Source	Event	Region	Add. info
Noder Reader 1	Invalid number of bits read		37

3.4.5 Záložka OSDP

Kontroléry umožňují komunikaci se čtečkou protokolem OSDP v2.



The screenshot shows the configuration interface for a Noder EWE4 controller. The 'OSDP' tab is selected. The 'Použít protokol OSDP v2 pro komunikaci se čtečkami' checkbox is checked. Below it, the 'Přenosová rychlost' is set to 9600, 'Čas. limit (ms)' is 500, and 'Klíč' is empty. The 'Použít na RS485' section has checkboxes for ports 1, 2, and 3, with port 1 selected. A warning message at the bottom states: '[Pozor: Odešlete plnou konfiguraci kontroléru, aby byly použity všechny změny.]'

Použit OSDP v2 pro komunikaci se čtečkami – výběr této funkce umožňuje používat OSDPv2. Jinak bude komunikace se čtečkami probíhat podle protokolu **RS485**. OSDP v2 možnosti:

Přenosová rychlost – dostupné v rozevíracím seznamu jsou následující přenosové rychlosti: 9600, 19200, 38400, 57600, 115200.

Čas. limit (ms) – časový limit odezvy čtečky v komunikaci s kontrolérem.

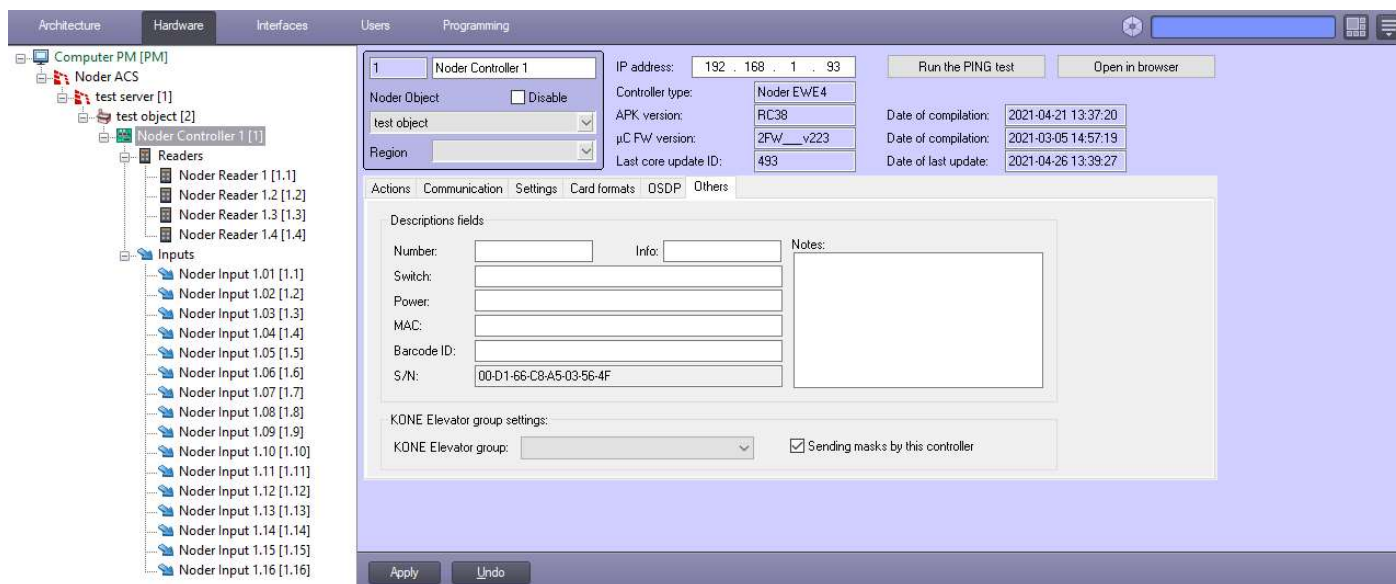
Klíč – 128bitový klíč v hexadecimální podobě (32 znaků) např. výchozí klíč pro čtečky HID v režimu instalace: 303132333435363738393A3B3C3D3E3F.

Použit na RS485 – výběr portů RS485 pro použití OSDP v2. EE12 umožňuje současné použití protokolu OSDP v2 a nativního protokolu (např. port 1 – OSDP v2, port 2 – nativní, port 3 – nativní).

OSDPv2 implementovaný v kontroléru je kompatibilní s podporovaným protokolem OSDP implementovaným ve čtečkách HID, Elatec a ISBC ESMART. Čtečky by měly nastavit adresu v rozsahu od 1 do 4. Čtečka musí nastavit volbu **Compliance** na 0x02 (řadič **nepodporuje OSDPv1**).

3.4.6 Záložka Další

Karta se používá ke konfiguraci dalších nastavení kontroléru.



Popis – zde mohou být uloženy informace o síti a elektrické infrastruktuře. Můžete zaznamenat číslo vypínače a zásuvky, elektrický rozvaděč a pojistku, adresu MAC kontroléru a další. Uložené informace **neovlivňují logiku** kontroléru.

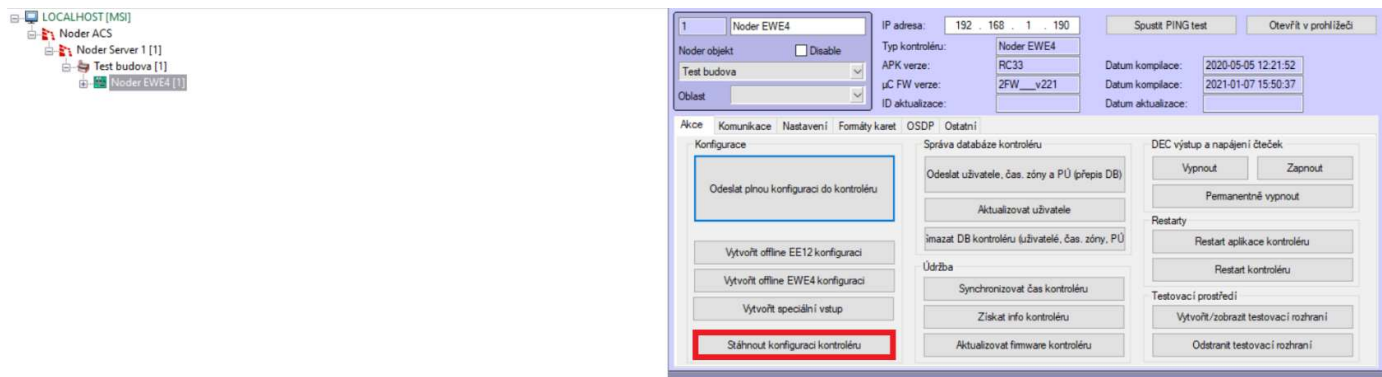
Nastavení skupiny výtahů KONE (pouze pokud se používá integrace s KONE):

KONE skupina výtahů – Vyberte jednu skupinu Kone Elevator, kterou chcete spravovat z tohoto kontroléru.

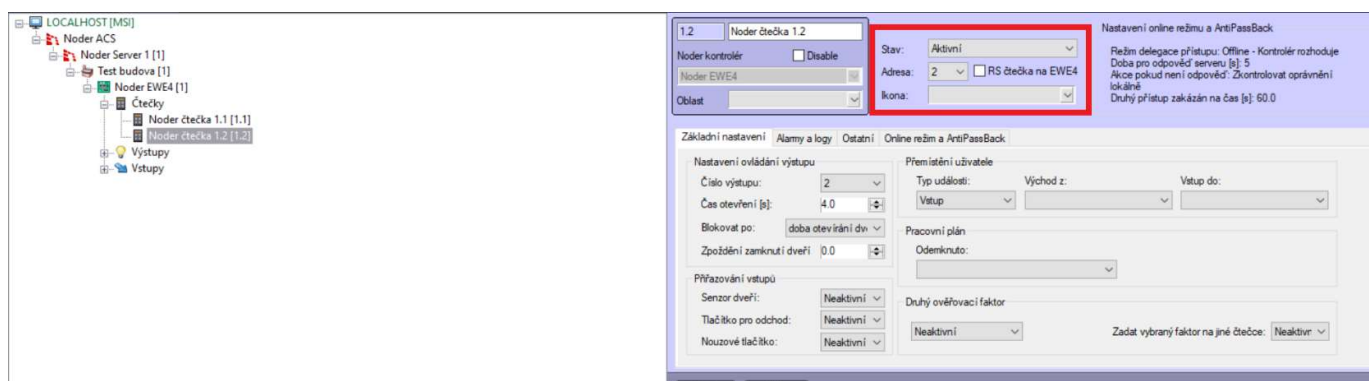
Odesílat masky – Pokud je zaškrtnuto, kontrolér odesílá masky specifikované ve skupině KONE Elevator.

3.5 Čtečky

Při prvním spuštění kontroléru si musíte kliknutím stáhnout jeho spouštěcí konfiguraci **Stáhnout konfiguraci kontroléru**.



Po stažení konfigurace z kontroléru se vytvoří vstupy a čtečky. 12 čteček a 20 vstupů pro EE12 a 4 čtečky a 16 vstupů pro EWE4. Čtečky a vstupy je nutné nakonfigurovat podle potřeb systému. **Nepoužité je třeba odstranit a poté odeslat konfiguraci do kontroléru** (tlačítko „Odeslat plnou konfiguraci do kontroléru“). Pro připojení ke čtečce je nutné nakonfigurovat její stav, adresu a typ:



Stav:

Neaktivní – toto je stav nastavený, když má být zařízení vypnuto pro systém.

Aktivní – toto je stav nastavený pro normální provoz systému.

Zamknutý – je nastaven tak, aby blokoval činnost čtečky.

Adresa – v rozevíracím seznamu jsou k dispozici volné adresy v rozsahu 1-12. Čtečky lze adresovat programovacími kartami, které přiřadí adresu z rozsahu 1-4. Adresy pro kontrolér EE12 jsou převedeny následovně:

<i>Adresa čtečky</i>	<i>Port</i>	<i>Logická adresa v kontroléru</i>
1	1	1
2	1	2
3	1	3
4	1	4
1	2	5
2	2	6
3	2	7
4	2	8
1	3	9
2	3	10
3	3	11
4	3	12

V případě EWE4 je možné připojit až čtyři čtečky (jak Wiegand, tak RS-485 v libovolné konfiguraci: např. 1 čtečka Wiegand a 3 čtečky RS-485). Čtečky Noder by měly být adresovány programovacími kartami (MD-R/MDK-R pomocí 1-4 programovacích karet k adresované čtečce a klíčům pro nahrávání, MD-W pomocí 1 programovací karty adresy k nahrávání klíčů).

Ikona – ikona, která bude představovat čtečku na mapovém podkladu.

RS čtečka na EWE4 – tato možnost by měla být zvolena, když je čtečka RS-485 (Noder MD-R/MDK-R) na kontroléru EWE4.

3.5.1 Záložka Základní nastavení

Karta se používá ke konfiguraci otevření dveří. Umožňuje přiřadit čtečce vstupy a výstupy.



Nastavení ovládání výstupu:

Číslo výstupu – relé, které je přiřazeno čtečce. Pro EWE4 zvolte relé 1-6, pro EE12 zvolte relé 1-16.

Čas otevření [s] – doba, po kterou kontrolér po udělení přístupu sepne výstup odpovídající dané čtečce.

Blokovat po – vstup lze zablokovat po **době otevření dveří**, **otevření dveří** nebo **zavření dveří**. Pro parametry **otevření dveří** a **zavření dveří**, k zablokování dveří dojde po **době otevření dveří**, když na něm neproběhne žádná akce.

Zpoždění zamknutí dveří [s] – umožňuje nastavení dodatečného časového zpoždění pro parametry otevírání a zavírání dveří. Maximální hodnota je 2s.

Přiřazování vstupů:

Senzor dveří – číslo vstupu, ke kterému je připojeno čidlo dveří.

Tlačítko pro odchod – číslo vstupu, ke kterému je připojeno odchodové tlačítko.

Nouzové tlačítko – číslo vstupu, ke kterému je připojeno tlačítko nouzového odchodu.

Přemístění uživatele:

Typ události – jsou možné následující možnosti: **Vstup, Exit, Obchodní vchod/východ, Soukromý vchod/východ, Příjezd, Odchod, Hlídka**. Jedná se o události, které systém zaznamená při načítání karty ze čtečky a průchodu dveřmi.

Východ z / Vstup do – jedná se o regiony, které systém AntiPassBack využívá k logickému mapování systému a řízení přítomnosti uživatele v daném regionu a možnosti jeho průchodu pouze do sousedních regionů. Bez nastavení těchto regionů není možné používat globální AntiPassBack.

Pracovní plán:

Odemknuto – volba umožňuje přiřazení plánu vytvořeného v Správci přístupu. Během ní dojde k odblokování průchodu.

Druhý ověřovací faktor:

Neaktivní – druhý autentizační faktor je neaktivní.

PIN kód – po zvolení této možnosti bude systém čekat na zadání PIN na čtečce za kartou.

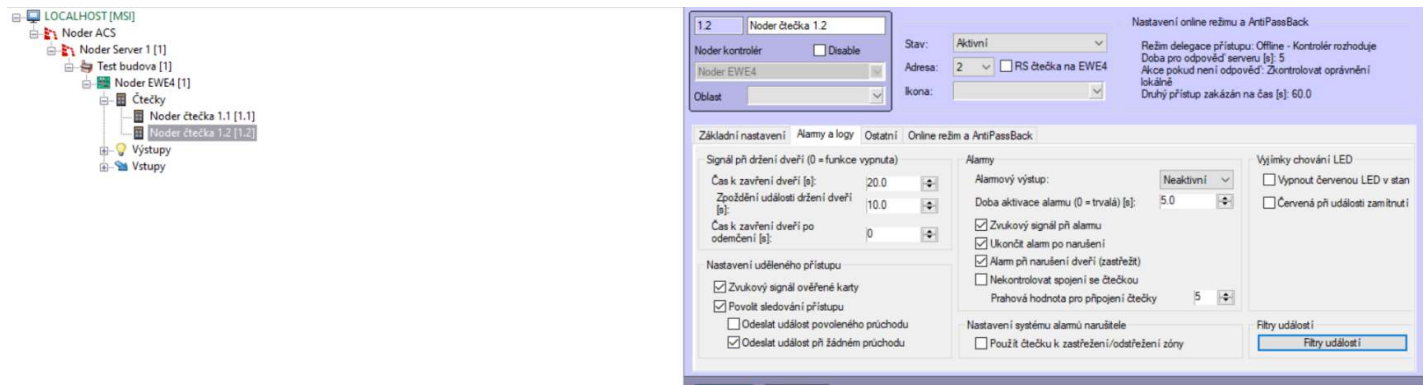
Číslo karty – po této volbě bude systém čekat na zadání stejného čísla karty, ale na jiné čtečce zvolené v parametru „Zadat druhý faktor na jiné čtečce“. Pokud není vybrána druhá čtečka, druhý autentizační faktor je neaktivní.

Zadat vybraný faktor na jiné čtečce:

- **Neaktivní** – výsledkem je, že systém očekává zadání PIN kódu na stejné čtečce, kde byla karta zaregistrována.
- **1-12** – adresa jiné čtečky připojené ke kontroléru.
- **13** – výsledkem je upozornění systému, že by měl očekávat potvrzení ze speciálního RS portu na EE12 používaného pro spojení se speciálními zařízeními (např. biometrické čtečky obličeje nebo otisků prstů připojené přes převodník Wiegand na RS485).

3.5.2 Záložka Alarmy a logy

Záložka slouží k nastavení alarmu po narušení nebo příliš dlouhém otevření dveří.



Signál při držení dveří:

Čas k zavření dveří [s] – doba, po kterém systém vygeneruje varovný alarm uživatele (událost, která se v systému ještě nevygenerovala) o držení otevřených dveří. Uživatel by měl zavřít dveře nebo se znovu autorizovat kartou na čtečce v době „Zpoždění události držení dveří“, aby se zabránilo generování poplachové události. Pro hodnotu 0 je funkce neaktivní.

Zpoždění události držení dveří [s] – doba zpoždění, po které se vygeneruje událost v systému a alarm na čtečce, pokud byly dveře otevřeny příliš dlouho. Pro hodnotu 0 je alarm generován ihned po "Čas zavření dveří". Pokud je však tato hodnota jiná, alarm bude o tuto dobu zpožděn.

Čas k zavření dveří po odemčení [s] – doba, po které systém začne generovat poplach pro obsluhu po otevření dveří s funkcí trvalého odemknutí. Pro hodnotu 0 je funkce neaktivní.

Nastavení uděleného přístupu:

Zvukový signál ověřené karty – zrušením této volby se autorizace při registraci platné karty na čtečce projeví pouze změnou barvy LED diody na zelenou. Zvuková signalizace bude pouze v případě neoprávněné karty nebo alarmu.

Povolit sledování přístupu – je-li tato možnost deaktivována, ihned po přiložení karty je vygenerována událost „Vstup“. Když je možnost povolena, událost „Vstup“ je generována pouze po fyzickém otevření dveří. Pokud je tato funkce povolena, jsou také možná dvě další nastavení:

- **Odeslat událost povoleného průchodu** – pokud je vybrána tato možnost, po přiložení karty se uživateli vygeneruje událost „Přístup udělen“.
- **Odeslat událost při žádném průchodu** – pokud je vybrána tato možnost, po přiložení schválené karty, pokud se dveře neotevřou, po době otevření dveří [s] bude vygenerována událost „Po udělení přístupu není průchod“.

Alarmy:

Alarmový výstup – číslo relé, které bude pracovat v souvislosti s poplachovou událostí (vynucený průchod nebo pokud jsou dveře otevřeny příliš dlouho).

Doba aktivace výstupu [s] – parametr určuje dobu, po kterou čtečka signalizuje poplachovou situaci (blikání diody a zvuková signalizace) – nucené nebo dlouhé otevření dveří. Pokud příčina alarmu neustane, akustická signalizace se bude opakovat každých 24 hodin. Vizualní indikace je zachována, dokud není odstraněna příčina alarmu. Signalizace je následující:

- **V případě narušení dveří** – nepřetržitý tón, LED bliká oranžově s frekvencí přibližně 2/3 Hz;
- **V případě dlouze otevřených dveří** – čas počítaný od okamžiku otevření dveří uživatelem, po kterém se spustí zvuková signalizace na čtečce (přerušovaný signál o frekvenci 0,5Hz) a oranžově bliká dioda na stejné frekvenci. Jeho účelem je upozornit uživatele, aby zavřel dveře před spuštěním alarmu.

Zvukový signál při alarmu – pokud není tato volba zaškrtnuta, alarm na čtečce je indikován pouze oranžovým blikáním LED.

Ukončit alarm po narušení – v případě poplachu (nuceně nebo dlouho otevřené dveře) akustická a vizualní signalizace bude smazána ihned po odstranění příčiny poplachu (zavření dveří). V opačném případě je zvukový alarm signalizován časem aktivace alarmu [s]. Pokud tato možnost není zvolena, LED na čtečce bude po uplynutí času alarmu nadále blikat oranžově, dokud nebude na čtečku přiložena autorizovaná karta.

- **Možnost povolena v případě narušení dveří** – nepřetržitě pípání, LED bliká oranžově s frekvencí přibližně 2/3 Hz. Po ukončení narušení se zvuková a světelná signalizace zastaví;
- **Možnost povolena v případě dlouze otevřených dveří** – audio signál je přerušovaný na frekvenci asi 2,5 Hz a LED dioda bliká oranžově na stejné frekvenci. Po zavření dveří se zvuková a světelná signalizace zastaví.
- **Možnost zakázána v případě narušení dveří** – nepřetržitě pípání, LED bliká oranžově s frekvencí přibližně 2/3 Hz. Po odeznění narušení pokračuje zvuková a světelná signalizace podle času aktivace alarmového výstupu. Po uplynutí této doby zvuková signalizace ustane, ale LED na čtečce stále bliká oranžově s frekvencí cca 2 / 3 Hz, a to až do okamžiku přiložení platné karty ke čtečce, použití výstupního tlačítka nebo otevření dveří operátorem.
- **Možnost zakázána v případě dlouze otevřených dveří** – audio signál je přerušovaný na frekvenci asi 2,5 Hz a LED dioda bliká oranžově na stejné frekvenci. Po zavření dveří zvuková a světelná signalizace

pokračuje podle času aktivace alarmového výstupu. Po uplynutí této doby zvuková signalizace ustane, ale LED na čtečce stále bliká oranžově s frekvencí cca 2,5 Hz, dokud uživatel nepřiloží ke čtečce autorizovanou kartu, použije výstupní tlačítko nebo neotevře dveře.

Alarm při narušení dveří (zastřežit) – tato volba umožňuje vypnout/zapnout generování poplachu v případě neoprávněného otevření dveří. Funkce signalizace příliš dlouhého otevření dveří bude pokračovat.

Nekontrolovat spojení se čtečkou – možnost pro zařízení připojená přes Wiegand. Pokud je zařízení napájeno z jiného zdroje, než je nakonfigurovaný port, kontrolér nebude mít potvrzení komunikace se zařízením. Výběr této možnosti umožňuje trvale nastavit normální stav zařízení na mapě.

Prahová hodnota pro připojení čtečky – umožňuje nastavit aktuální úroveň, pro kterou je detekována čtečka Wiegand na EWE4. Detekce je založena na aktuální spotřebě na portu, proto nemusí být čtečky s nízkou spotřebou detekovány, pokud tato možnost není korektně nastavena.

Nastavení systému alarmů narušitele:

Použit čtečku pro zastřežení/odstřežení zóny – Tato možnost se používá v IAS systémech. Umožňuje zastřežit zónu, která je přiřazena čtečce. Pro zastřežení zóny musíte použít autorizovanou kartu na čtečce dvakrát během 2,5 sekundy. Pro odstřežení zóny musíte jednou použít autorizovanou kartu na čtečce. Zastřežení zóny je signalizováno 2x pípnutím čtečky a blikáním oranžové LED každé 2 sekundy.

Výjimky chování LED:

Vypnout červenou LED v standby režimu – volba umožňuje zhasnutí červené diody při normálním stavu čtečky.

Červená při události zamítnutí – volba umožňuje změnit barvu z oranžové na červenou pro signalizaci neoprávněné karty.

Filtry událostí – volba umožňuje zakázat generování a ukládání některých událostí do databáze.

3.5.3 Záložka Ostatní

Karta slouží ke konfiguraci dalších nastavení čtečky.



Popisy – jedná se o pole, která umožňují přiřadit čtečkám určité popisy, např. inventární číslo, umístění a další.

Filtrování:

Ignorovat události zamítnutí přístupu pro karty – Funkce umožňuje zadání čísel karet (oddělených středníkem), u kterých systém nezaregistruje událost načtení neoprávněné karty.

KONE nastavení skupiny výtahů (pouze pokud se používá integrace s KONE):

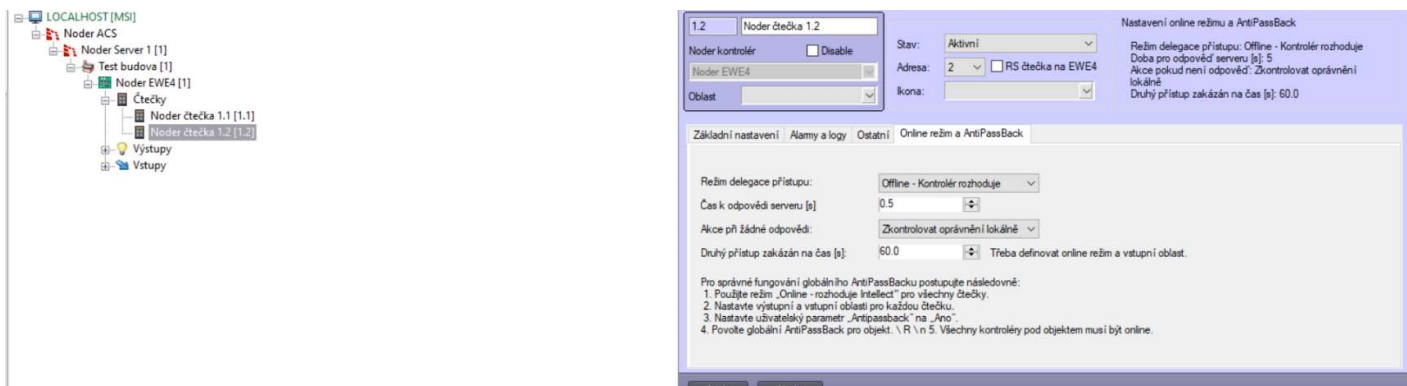
Související DOP nebo COP – přiřadit čtečku ke konkrétnímu cílovému ovládacímu panelu nebo ovládacímu panelu automobilu

Protokol – komunikační protokol:

- **GCAC (ELI)** – protokol pro správu přístupu z DOP nebo COP.
- **RCGIF (Home floor)** – protokol pro volání výchozího patra.

3.5.4 Záložka Online režim a AntiPassBack

Záložka slouží k nastavení režimu, ve kterém má čtečka pracovat.



Režim delegace přístupu:

Offline – Kontrolér rozhoduje – přístupové dotazy budou směřovány do interní databáze kontroléru. Povolením těchto funkcí zakážete provoz globálního AntiPassBack na této čtečce (funkce musí být povolena také pro uživatele).

Online – Intellect rozhoduje – přepne čtečku do online režimu práce. O udělení přístupu po použití karty rozhodne server automaticky. Povolení těchto funkcí umožní provoz globálního AntiPassBack na této čtečce (funkce musí být povolena také pro uživatele).

Online – Operátor rozhoduje – přepne čtečku do online režimu práce. O udělení přístupu po přiložení karty se rozhodne zobrazením předem připraveného rozhraní pro operátora. Povolení těchto funkcí umožní provoz globálního AntiPassBack na této čtečce (funkce musí být povolena také pro uživatele).

Čas k odpovědi serveru [s] – čas, po který musí kontrolér čekat na odpověď serveru.

Akce při žádné odpovědi – v případě nepřítomnosti odezvy serveru provede kontrolér jednu z následujících možností:

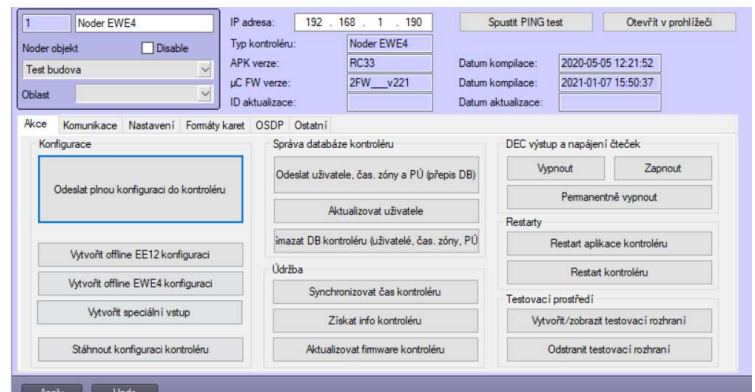
- **Zamítnout přístup** – po ztrátě spojení se serverem a použití karty uživatel automaticky nezíská přístup, i když je jeho karta platná.
- **Zkontrolovat oprávnění lokálně** – po ztrátě spojení se serverem a použití karty bude přístup udělen po kontrole oprávnění uživatele v interní databázi kontroléru.

Druhý přístup zakázán na čas – čas, po kterém může uživatel znovu vstoupit do zóny. Aby funkce korektně fungovala, musí být možnost „Povolit vícenásobný přístup“ v uživatelských oprávněních označena jako „Ne“ a kontrolér musí být v režimu online.

3.6 Vstupy

Stažením konfigurace z kontroléru se automaticky vytvoří 16 vstupů pro EWE4 a 20 vstupů pro EE12 ve vypnutém stavu. Chcete-li vytvořit speciální vstupy, vyberte možnost Vytvořit speciální vstupy na kartě Akce kontroléru.

Kromě přiřazení vstupního čísla čtečky za účelem indikace její funkce v systému (např. jazyčkový spínač nebo výstupní tlačítko), by měla být také odpovídajícím způsobem nakonfigurována. Nejprve definujte, zda má vstup pracovat v logice NO nebo NC.



Speciální vstupy nelze volně konfigurovat a používat, například jako výstupní tlačítko. Typy povolené pro tyto vstupy jsou Vypnuto, Speciální – NC a Speciální – NO. Účel speciálních vstupů:

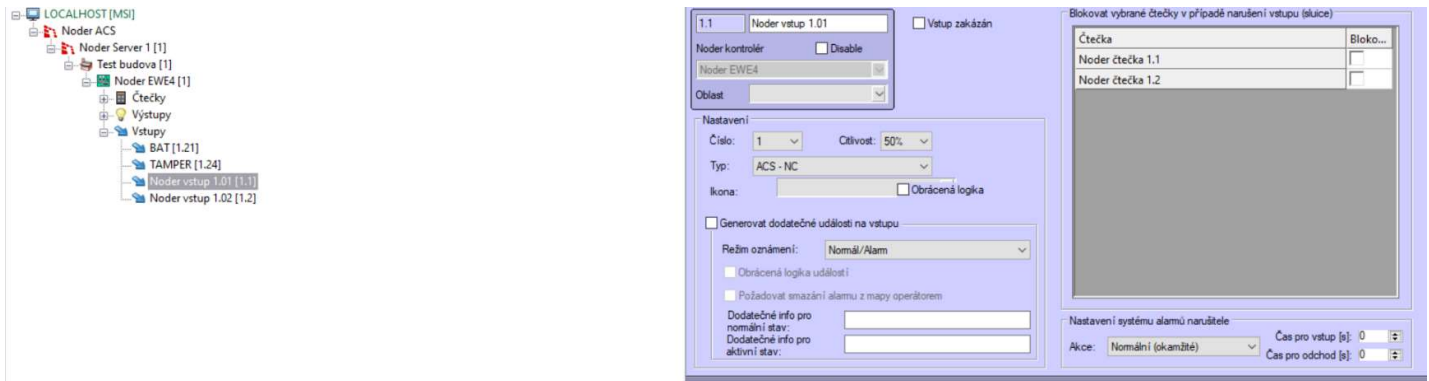
BAT – signál vybitých baterií.

AC – žádné napájení 230 V.

TMP – Poškození zdroje 12V DC,

DR – sériové připojení všech dveří tamper skříně a montáž na stěnu.

3.6.1 Konfigurace vstupů



Vstup zakázán – aktivace vstupu není v systému zaznamenána.

Nastavení:

Číslo – číslo vstupu kontroléru.

Citlivost – volba umožňuje nastavení času od aktivace vstupu po jeho registraci v systému pomocí úrovní 10-100%.

Typ – typ vstupu. Z dostupného rozevíracího seznamu. Pokud vstup používá pouze systém kontroly přístupu, vyberte typ vstupu „ACS“. Pokud je vstup používán pouze systémem Intruder Alarm System, vyberte typ vstupu „IAS“. Pokud vstup používá systém kontroly přístupu a systém alarmu narušení, vyberte typ vstupu „ACS + IAS“. Typy vstupů:

- Off
- ACS – NO
- ACS – NC
- ACS – EOL/NO
- IAS – NO
- IAS – NC
- IAS – EOL/NO
- ACS – EOL/NO
- IAS – 2EOL/NO
- IAS – 2EOL/NC
- ACS + IAS – NO
- ACS + IAS – NC
- ACS + IAS – EOL/NO
- ACS + IAS – EOL/NC
- ACS + IAS – 2EOL/NO
- ACS + IAS – 2EOL/NC
- Special – NO
- Special – NC

Ikona – ikona, která bude reprezentovat vstup na vizualizaci.

Obrácená logika – výběr této možnosti způsobí, že ikona na vizualizaci zobrazí opak skutečného signálu.

Generovat dodatečné události na vstupu – výběr této možnosti vygeneruje v systému další událost

Režim oznámení:

- Vypnuto/Aktivní
- Normální/Alarm
- Normální/Selhání

Obrácená logika – výběr této možnosti obrátí logiku událostí generovaných systémem ve vztahu ke skutečnému stavu vstupu.

Požadovat smazání alarmu z mapy operátorem – výběr této možnosti způsobí zachování stavu alarmu pomocí ikony na mapě, dokud jej operátor nesmaže, i když se fyzický vstup vrátí do normálního stavu

Dodatečné info pro normální/aktivní stav – toto jsou textová pole, která umožňují připojit k události trvalý komentář. Jsou zobrazeny v prohlížeči událostí v části Dodatečné info.

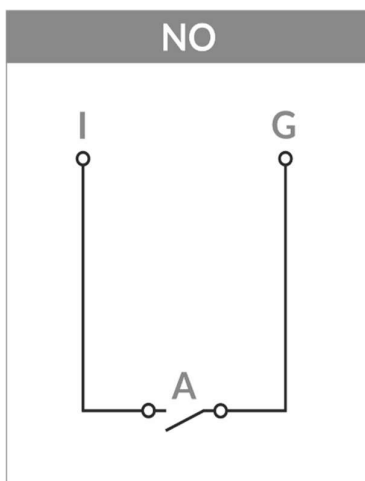
Blokovat vybrané čtečky po narušení vstupu (sluice) – zde označené čtečky budou po dobu aktivace vstupu zablokovány.

Nastavení systému alarmů narušitele – funkce bude platná, pokud je typ vstupu nakonfigurován jako „IAS“ nebo „ACS+IAS“.

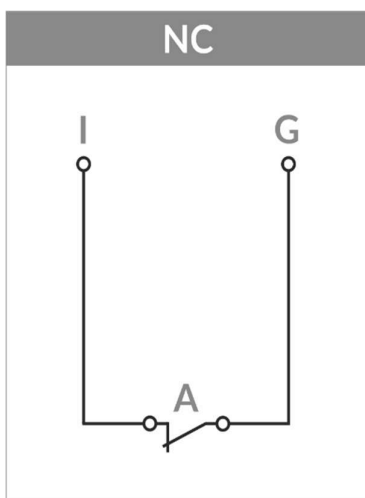
Akce – z dostupného rozevíracího seznamu můžete vybrat, kdy se spustí alarm:

- **Normální (okamžitě)** – po aktivaci zóny a aktivaci vstupu
- **Vstup/Odchod** – když je zóna aktivována po aktivaci vstupu, má uživatel čas pro vstup (s) (čas do deaktivace) /čas pro opuštění (s) této zóny. Po uplynutí této doby se aktivuje alarm.
- **24h** – každou aktivací vstupu (i když je zóna odstřežena).
- **24h silent alarm** – každá aktivace vstupu generuje tichý poplach (i když je zóna odstřežena). Čtečky a výstupy nezmění svůj stav.
- **Panika** – každá aktivace vstupu generuje poplach Panika (i když je zóna odstřežena).
- **Tichá panika** – každá aktivace vstupu generuje tichý poplach Panika (i když je zóna odstřežena). Čtečky a výstupy nezmění svůj stav.
- **Technický – selhání AC napájení** – každá aktivace vstupu generuje tichý alarm výpadku střídavého napájení (i když je zóna odstřežena). Čtečky a výstupy nezmění svůj stav.
- **Technický – selhání baterie** – každá aktivace vstupu generuje tichý alarm selhání baterie (i když je zóna odstřežena). Čtečky a výstupy nezmění svůj stav.
- **Zastřežení** – aktivace vstupu zastřeží zónu.
- **Odstřežení** – aktivace vstupu odstřeží zónu.
- **Reset alarmu**

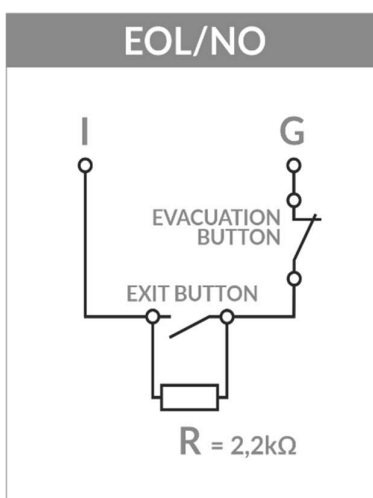
3.6.2 Diagramy zapojení vstupů v přístupovém systému



Vstup nakonfigurovaný jako NO se používá pro tlačítko odchodu. Po jeho stisknutí se sepne relé a je přijata událost „Otevření odchodovým tlačítkem“.

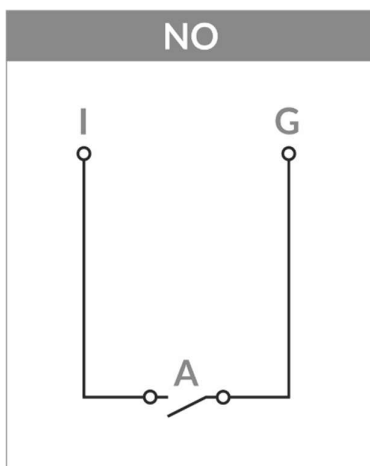


Vstup nakonfigurovaný jako NC se používá pro dveřní sensor nebo tlačítko nouzového východu. Dveřní sensor informuje o aktuálním stavu dveří. Po stisknutí tlačítka nouzového východu je přijata událost „Stisknuto tlačítko nouzového východu“.

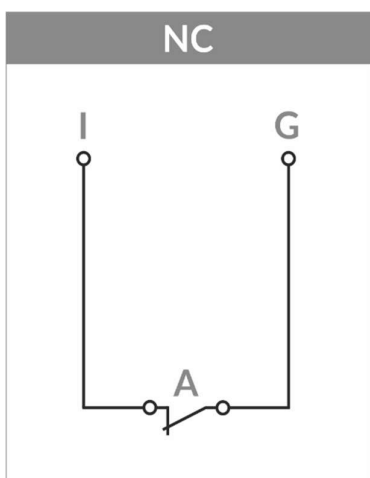


Vstup v konfiguraci NO s koncovým rezistorem (2,2kOhm). Po stisku tlačítka exit se aktivuje relé a je přijata událost „Otevření tlačítkem odchodu“. Po stisknutí evakuačního tlačítka je přijata událost „Nouzové tlačítko je stisknuto“.

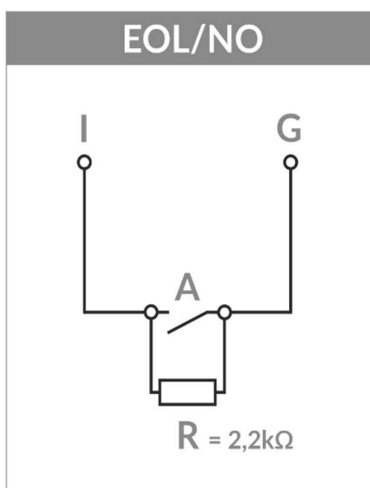
3.6.3 Diagramy zapojení vstupu v zabezpečovacím systému



Detektor s normálně otevřeným vstupem. Uzavření okruhu spustí alarm. Nedostáváme informace o sabotáži (událost Alarm není generována) nebo závadě (událost Alarm není generována).

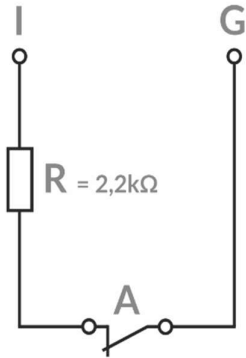


Detektor s normálně uzavřeným vstupem. Otevření okruhu spustí alarm. Nedostáváme informace o sabotáži („generuje se událost Alarm“) nebo závadě („událost Alarm“ se negeneruje).



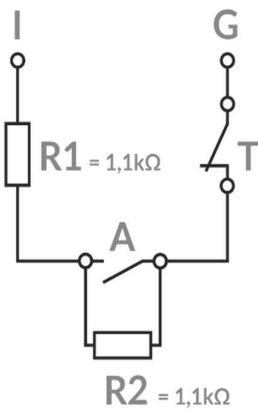
Detektor v konfiguraci s koncovým rezistorem (2,2kΩm). Uzavření okruhu spustí alarm. Dostáváme informace o sabotáži („vygeneruje se událost „Tamper“) a nedostáváme informace o poruše („vygeneruje se událost Alarm“).

EOL/NC



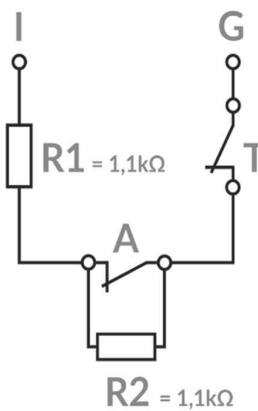
Detektor v konfiguraci s koncovým rezistorem (2,2kOhm). Otevření okruhu spustí alarm. Nedostáváme informace o sabotáži („generuje se událost Alarm“) a dostáváme informace o poruše („generuje se událost Porucha“).

2EOL/NO



Detektor v konfiguraci se 2 koncovými rezistory (2x1,1kOhm). Uzavření okruhu spustí alarm. Dostáváme informace o sabotáži („vygeneruje se událost „Tamper““) a („vygeneruje se událost „Selhání““).

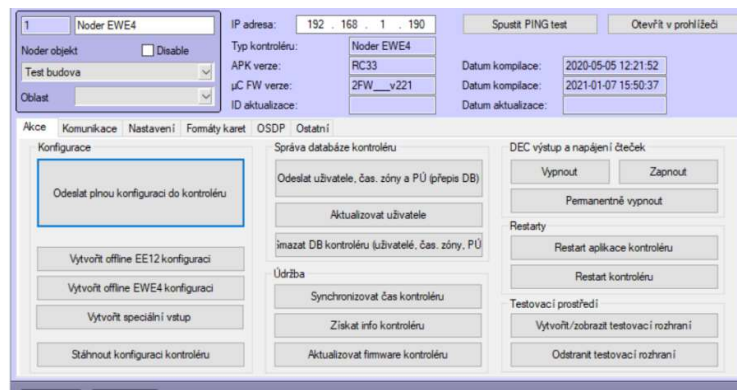
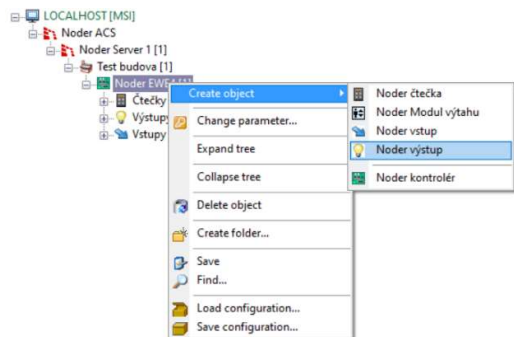
2EOL/NC



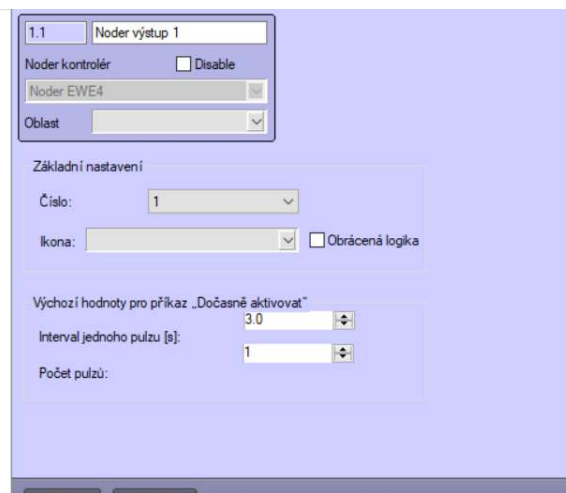
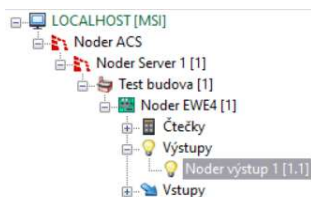
Detektor v konfiguraci se 2 koncovými rezistory (2x1,1kOhm). Otevření okruhu spustí alarm. Dostáváme informace o sabotáži („vygeneruje se událost „Tamper““) a („vygeneruje se událost „Selhání““).

3.7 Výstupy

Chcete-li vytvořit výstup, klikněte pravým tlačítkem na kontrolér a vyberte Noder výstup. Po zadání názvu a čísla výstupu se otevře okno nastavení.



Objekt může být použit v Intruder Alarm System (po vytvoření bude viditelný v nastavení IAS Zone) k aktivaci při poplachu nebo pouze k ovládání relé z mapy, makra nebo skriptu.



Základní nastavení:

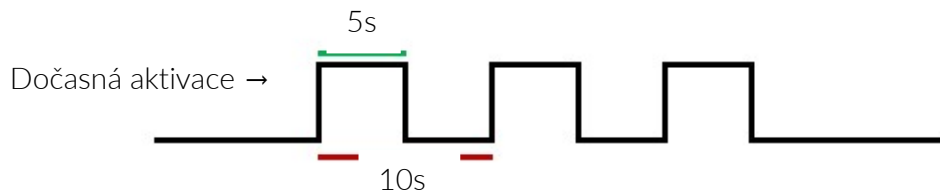
Číslo – číslo relé kontroléru.

Ikona – ikona, která bude reprezentovat výstup na vizualizaci.

Výchozí hodnoty pro příkaz „Dočasně aktivovat“:

Interval jednoho pulzu [s] – doba trvání jednoho pulzu (v příkladu níže Doba trvání jednoho pulzu [s] = 5).

Počet pulzů – počet pulzů po příkazu „Dočasně aktivovat“ (v příkladu níže Počet pulzů = 3).



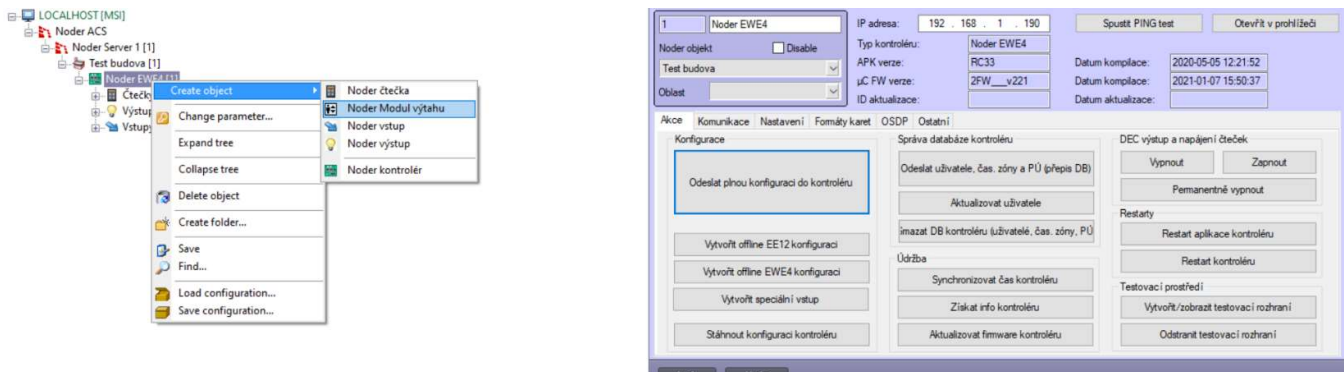
Obrácená logika – výběr této možnosti obrátí logiku ikony na mapě ve vztahu ke skutečnému stavu výstupu.

3.8 Výtahové moduly

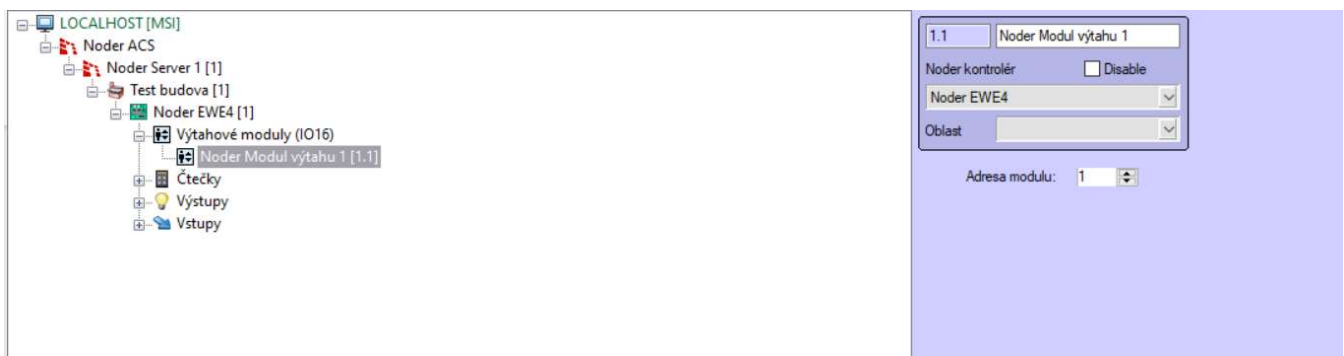
Po připojení a konfiguraci kontroléru může správce přidat modul IO16RS.

3.8.1 Konfigurace výtahového modulu

Chcete-li vytvořit objekt, klikněte pravým tlačítkem myši na kontrolér, ke kterému má být zařízení připojeno, a poté vytvořte objekt modulu Noder Modul výtahu.



Po výběru objektu se otevře okno, ve kterém je třeba přiřadit číslo a pojmenovat zařízení. Klikněte na Použít, objeví se okno s možnostmi modulu.



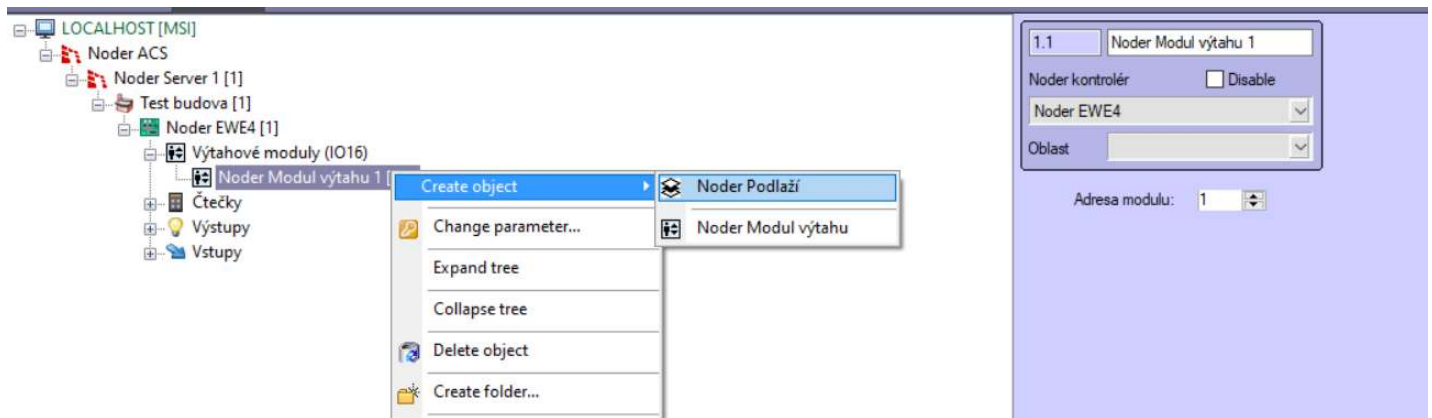
Adresa objektu musí být stejná jako adresa nastavená na DIP přepínači modulu (adresa je popsána v Noder TD-IO16RS). K jednomu kontroléru EE12 a EWE4 lze připojit 4 moduly. V případě EE12 připojte modul k rozšiřující sběrnici (port 4) a pro EWE4 ke sběrnici RS485. Jen jeden typ zařízení může pracovat na sběrnici RS485, proto při použití IO16RS na EWE4 jsou podporovány pouze čtečky na sběrnici Wiegand.

Po přiřazení adresy klikněte na Použít a klikněte na Odeslat konfiguraci do kontroléru v nastavení kontroléru. V tomto okamžiku by mělo zařízení navázat spojení. Kontrolky RX a TX komunikace na kontroléru a modulu by měly začít pravidelně s vysokou frekvencí blikat.

Pro kontrolu připojení můžete vytvořit testovací rozhraní. Pokud je připojení aktivní, prohlížeč událostí zobrazí událost „Připojeno“ a ikona modulu bude zelená.

3.8.2 Konfigurace podlaží

IO16RS má 16 relé, která by měla být přiřazena patřům budovy. Chcete-li vytvořit objekt podlaží, klikněte pravým tlačítkem na modul výtahu Noder a vyberte objekt Noder Podlaží. Měli byste přiřadit číslo a název objektu.



Po kliknutí na tlačítko Použít se objeví okno s možnostmi podlaží.



Čtečka – fyzická čtečka ve výtahu, ke které se aktivují relé modulu při přiložení autorizované karty do zařízení. Čtečka by měla být přiřazena do všech pater, která obsluhuje. Po přiložení autorizované karty se relé aktivují podle úrovně přístupu přidělené uživateli.

Číslo výstupu – relé modulu přiřazené k podlaží.

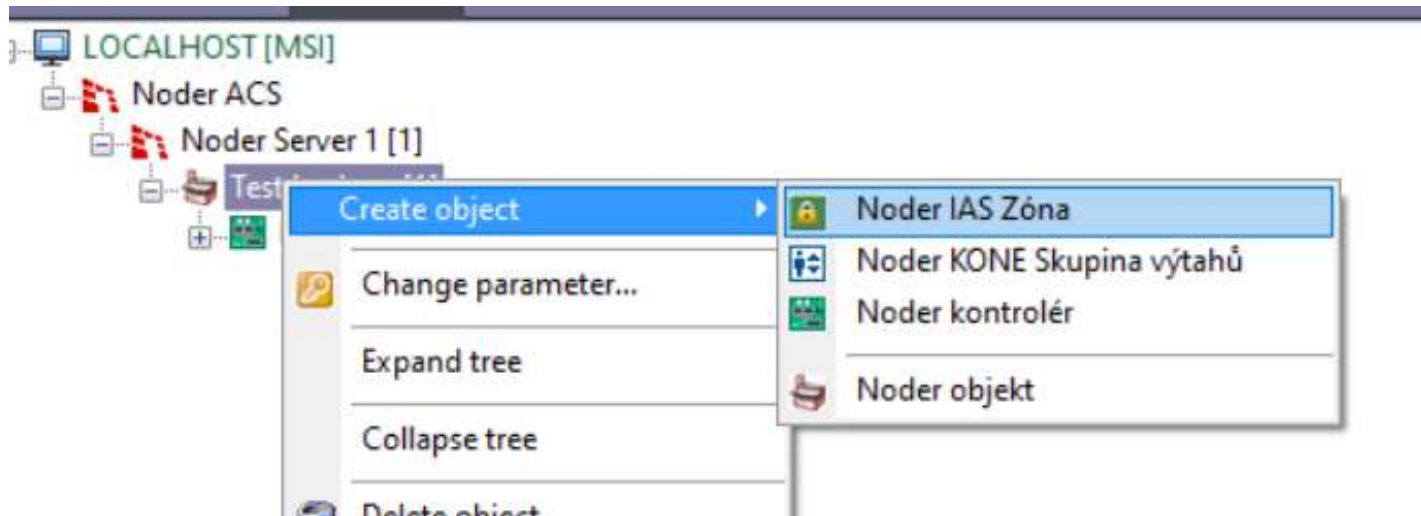
Otevírací doba výstupu – čas, kdy je relé modulu aktivováno po přiložení karty nebo operátor vydá příkaz "Dočasně otevřít".

Ikona – ikona zobrazená na mapě.

Po každé změně konfigurace by měla být potvrzena tlačítkem Použít a konfigurace odeslána do kontroléru kliknutím na Odeslat konfiguraci do kontroléru v jeho nastavení.

3.9 Noder IAS Zóna

Chcete-li vytvořit objekt, klikněte pravým tlačítkem na Noder Objekt, ke kterému bude zóna patřit, a vyberte Noder IAS Zóna. Měli byste přiřadit číslo a název objektu.

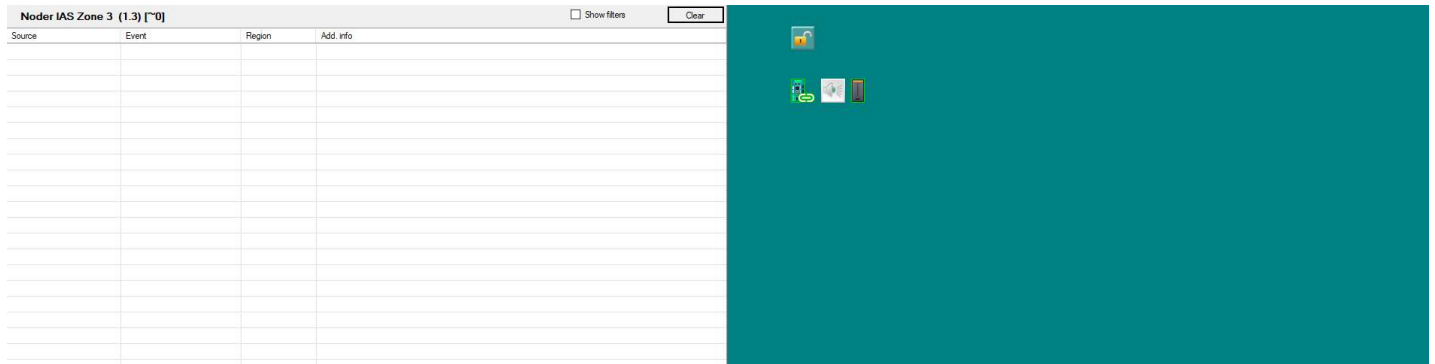


Po přidání objektu Noder IAS Zóna se zobrazí konfigurační rozhraní.



Odeslat konfiguraci – odešle aktuální nastavení zóny všem souvisejícím kontrolérům.

Vytvořit/zobrazit testovací rozhraní – vytvoří rozhraní kontroléru s prohlížečem událostí vztahujících se k dané zóně a mapou s ikonami zóny, všech kontrolérů, čteček, vstupů a výstupů dané zóny. Pokud bylo takové testovací rozhraní vytvořeno dříve, vyvolání této funkce aktualizuje mapu podle aktuální konfigurace a rozhraní zobrazení.



Odstranit testovací rozhraní – odstraní testovací rozhraní.

Vstupy – po výběru vstupů a odeslání konfigurace budou použity v zóně. Konfigurace je popsána v kapitole Vstupy.

Čtečky – po výběru čteček a odeslání konfigurace budou v zóně použity v případě poplachu (neplatí pro tichý poplach). Čtečku přiřazenou k zóně lze také použít k zastřežení nebo odstřežení zóny (musí být zaškrtnuta volba Použít čtečku k zastřežení/odstřežení zóny). Chování čtečky:

Zóna odstřežena – červená LED na čtečce.

Zóna zastřežena – červená LED bliká s frekvencí 0,5 Hz.

Zastřežování zóny – zvukové oznámení s frekvencí 2,5 Hz. Když se pokusíte zastřežit zónu, která není připravena k zastřežení, čtečka se na 1 sekundu rozsvítí oranžově LED a na 1 sekundu pípne.

Odstřežení zóny – zvukové oznámení s frekvencí 1Hz.

Alarm – bzučák po čas aktivace alarmu (nastavení čtečky) s frekvencí 2,5 Hz a červená LED s frekvencí 2,5 Hz.

Reset alarmu – bzučák po čas aktivace alarmu (nastavení čtečky) s frekvencí 2,5 Hz a červená LED s frekvencí 2,5 Hz po resetu alarmu → červená LED na čtečce.

Výstupy – po zvolení výstupů a odeslání konfigurace budou použity v zóně. V případě poplachu (neplatí pro tichý poplach), sabotáží (tamper nebo porucha) kontrolér spustí na omezenou dobu indikované relé. Konfigurace čísla a ikony relé je popsána v kapitole Výstupy.

4. Správa uživatelů

Správa uživatelů a úrovní přístupu je možná pomocí Správce přístupu. Je prvkem rozhraní. Pro správu uživatelů řízení přístupu by měl být vytvořen speciální uživatel s příslušnými oprávněními.

Podrobnosti o uživatelských službách a úrovních přístupu naleznete v dokumentu:

[Noder access control system operator's instruction](#)