



AKUVOX A15 ACCESS CONTROL

Návod pro administrátory

Děkujeme, že jste si vybrali zařízení pro řízení přístupu Akuvox A15. Tento manuál je určen pro administrátory, kteří potřebují zařízení správně nakonfigurovat. Tento manuál se vztahuje na verzi 1115.30.10.408 a obsahuje všechny konfigurace funkcí a funkcí A15. Pro nové informace nebo nejnovější firmware navštivte prosím fórum Akuvox nebo se obraťte na technickou podporu na www.akuvox.cz.

Obsah

Přehled produktu.....	10
Specifikace modelu.....	11
Přístup k zařízení	12
Počáteční nastavení.....	12
Přístup k Nastavení zařízení.....	14
Přístup k webovým nastavením zařízení	15
Vyhledejte požadovaná nastavení	19
Úvod do konfiguračního menu	20
Jazyk a čas.....	22
Jazyk	22
Vlastní jazyk	22
Čas.....	23
Hlasitost a tón.....	25
Ovládání hlasitosti.....	25
Nahrávání hlasových náповěd.....	26
Nastavení vyzvánění.....	27
Nastavení LED diod	29
Nastavení infračervených LED	29
LED bílé světlo	30
Zobrazení na obrazovce	32

Zobrazení na domovské obrazovce	32
Výchozí téma	32
V režimu vícefaktorové autentizace	34
Configure Screensaver	36
Nahrajte spořič obrazovky.....	39
Zobrazení textového promptu pro otevření dveří	40
Zobrazení možností odemčení	41
Nastavení sítě	43
Nasazení zařízení v síti	45
Nastavení NAT.....	46
Nastavení HTTP na webu zařízení	47
Lokální RTP konfigurace zařízení.....	47
Nastavení SNMP	48
Konfigurace hovorů interkomu.....	49
Konfigurace IP hovorů	49
Konfigurace SIP hovoru	49
Registrace SIP účtu	50
Konfigurace SIP serveru	51
Výběr SIP účtu	52
Odchozí proxy server.....	52
Typ přenosu dat.....	53

Prevence SIP hackingu	54
Nastavení hovoru	55
Automatické přijímání hovorů	55
Skupinový hovor.....	56
Sekvenční volání	56
Maximální doba vytáčení	58
Maximální doba trvání hovoru.....	58
Zavěšení hovoru po otevření dveří	59
Typ video transportu	60
Konfigurace audio a video kodeků	61
Audio kodek	61
Video kodek	62
Zařízení podporuje kodek H264, který poskytuje lepší kvalitu videa při mnohem nižší datové rychlosti a odlišné kvalitě videa a užitečném zatížení.	62
Video kodek pro IP hovory	62
Nastavení relé	64
Místní štafeta.....	64
Bezpečnostní relé.....	66
Web Relay	68
Správa časové harmonogramu řízení přístupu.....	71
Vytvořte harmonogram přístupu ke dveřím.....	71
Plán importu a exportu přístupu ke dveřím	72

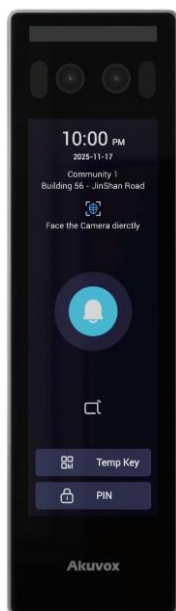
Harmonogram relé.....	72
Program pro svátky	73
Sváteční rozvrh Import/Export	75
Konfigurace otevírání dveří.....	76
Odemknutí pomocí veřejného PIN kódu	76
Uživatelsky specifické metody přístupu.....	76
Odemknout pomocí soukromého PIN	77
Odemknout pomocí QR kódu.....	77
Odemknutí pomocí RF karty	79
Odemknout podle registrační značky	80
Odemknout pomocí rozpoznávání obličeje	81
Odemknutí pomocí Bluetooth	83
Nastavení přístupu	84
Import/export uživatelských dat	85
Odemčení pomocí NFC	86
Mifare Card.....	87
Odemknutí pomocí DTMF kódu	88
DTMF Bílý seznam	89
Přenos dat DTMF	89
Odemknutí pomocí HTTP příkazů	91
Odemknout tlačítkem Exit	92
Monitor a obraz.....	94

Zachycení obrázků v MJPEG.....	94
RTSP monitorování.....	96
Nastavení RTSP streamu.....	96
ONVIF	98
Živý přenos	100
Režim kamery	100
Typ přenosu dat pro kamery třetích stran.....	101
Bezpečnost.....	103
Alarm proti manipulaci	103
Nastavení pro odzbrojení.....	104
Správa účtu.....	105
Nastavení klientského certifikátu	107
Certifikát webového serveru	107
Klientský certifikát	107
Detekce pohybu.....	109
Bezpečnostní oznámení.....	111
E-mailové upozornění.....	111
FTP oznámení.....	112
Oznámení o SIP hovorech.....	112
Action URL	113
Šifrování hlasu.....	116

User Agent.....	117
Monitorování v reálném čase.....	117
Nouzová akce	118
Automatické odhlášení webového rozhraní	118
Režim vysoké bezpečnosti.....	118
Logování.....	121
Logy hovorů	121
Logy přístupu ke dveřím.....	121
Záznamy událostí	122
Integrace se zařízením třetích stran.....	124
Integrace přes Wiegand	124
Integrace přes HTTP API.....	126
Napájecí výstup.....	128
Integrace přes RS485.....	129
Integrace s třetími stranami pro řízení přístupu	131
Ovládání výtahu	135
Aktualizace firmwaru	137
Automatické nastavení přes konfigurační soubor	138
Princip provisioningu	138
Konfigurační soubory pro automatický provisioning	139
AutoP rozvrh	140

Statický provisioning	141
DHCP Provisioning.....	142
PNP konfigurace	145
Debug.....	146
Systémový log pro ladění.....	146
PCAP pro ladění.....	146
Vzdálený ladicí server.....	147
Ping	148
Web Call	148
Záloha	149
Úprava hesla	150
Upravit heslo k webovému rozhraní	150
Upravit bezpečnostní otázky.....	151
Upravit administrátorské přihlašovací údaje.....	151
Restart a reset systému	153
Reboot	153
Reset.....	154

Přehled produktu



Akuvox A15S je ultra-tenké zařízení pro řízení přístupu, které integruje ovladač dveří a čtečku karet do jednoho kompaktního zařízení, což pomáhá snížit složitost instalace a celkové náklady na nasazení.

Navržen pro scénáře řízení přístupu s omezeným prostorem, poskytuje pohodlné řešení pro správu přístupu ke vstupu.

A15S podporuje více autentizačních metod, včetně rozpoznávání obličeje, PIN kódů, QR kódů, Bluetooth, NFC a RFID karet, a nabízí flexibilní a bezpečné možnosti přístupu pro různé uživatelské požadavky.

Specifikace modelu

Model	A15
Dotyková obrazovka	✓
Reléový port	2x
Vstupní port	4x
Napájení	PoE nebo 12VDC 2A
Napětí a odběr	12VDC 0,5A(max.) pokud vstup PoE+ 12VDC 1A(max.) pokud DC vstup
Wiegand	✓
RS485	✓
Výkon	✓
Tlačítko reset	✓
Bluetooth	✓
Wi-Fi	X
Mikrofon	1x
Mluvčí	1x

Přístup k zařízení

Přístup k systémovým nastavením zařízení buď přímo na něm, nebo v jeho rozhraní.

Počáteční nastavení

Před konfigurací zařízení se ujistěte, že je správně nainstalováno a připojeno k běžné síti.

Během počátečního nastavení budete vedeni k výběru jazyka zařízení, nastavení administrátorských přihlašovacích údajů (PIN a/nebo karta) a výběru časového pásma.

Administrátorské přihlašovací údaje se používají k přístupu k systémovým nastavením zařízení. Vyberte alespoň jednu metodu a nakonfigurujte ji.

- **PIN:** 6 až 8 číslic.

<

Step 1/2

Set Administrator Credentials

Set up at least one method (one or both):

• Password

• Card



PIN



Card

Next

<

Admin PIN

* Admin PIN

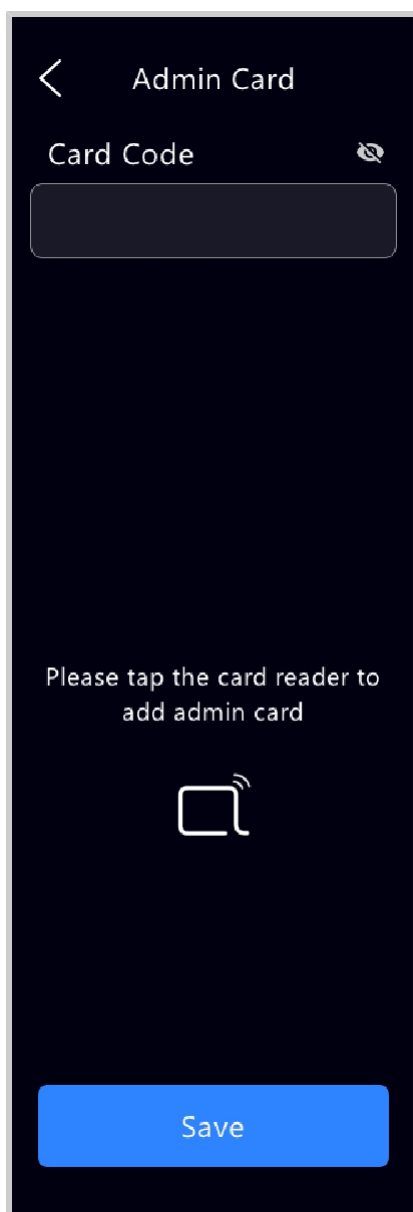
* Confirm PIN

Please enter the confirm PIN.

Save

www.akuvox.cz

13

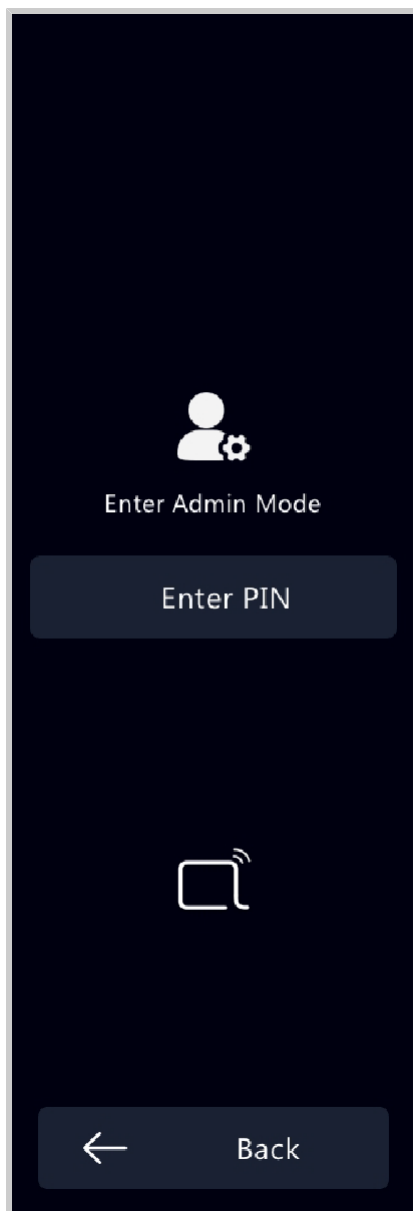


Tip

Viz kapitola [Úprava hesel](#) pro úpravu administrátorských údajů.

Přístup k Nastavení zařízení

Dlouhým stiskem na jakékoli místo domovské obrazovky přibližně pět sekund, poté zadejte admin PIN nebo přejed'te administrátorskou kartou.

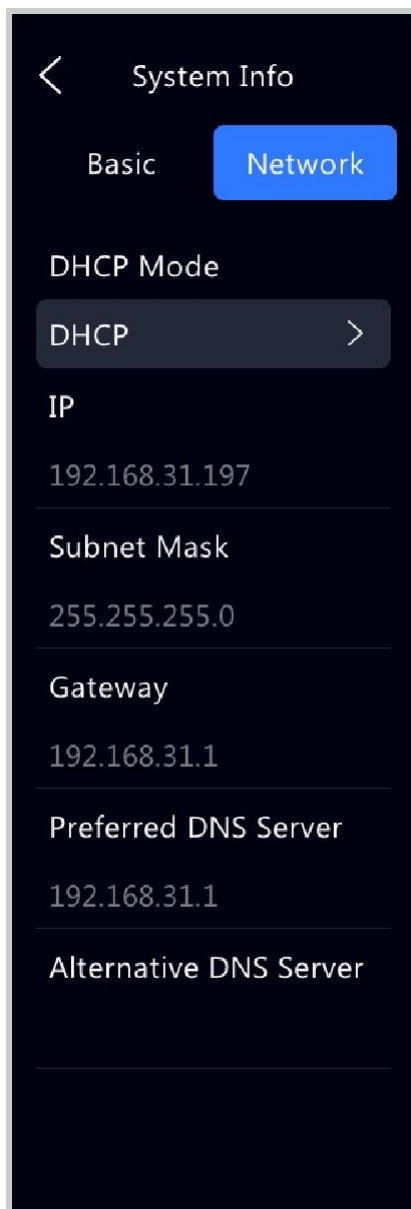


Přístup k webovým nastavením zařízení

Můžete zadat IP adresu zařízení v prohlížeči a přihlásit se do webového rozhraní, kde můžete nastavit a upravit parametry.



Zkontrolujte IP zařízení na obrazovce **Nastavení > System Info > Network** nebo použijte nástroj Akuvox IP Scanner k vyhledání IP adresy zařízení na stejné LAN.



Poznámka

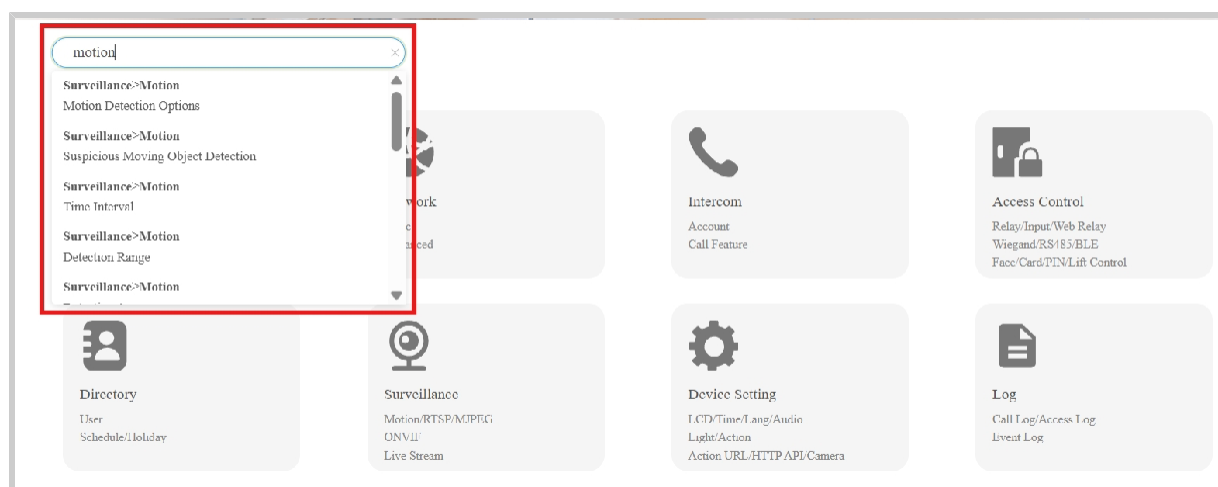
- Stáhněte IP skener:
<https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP>
- Viz podrobný návod:
<https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner>
- Prohlížeč Google Chrome je důrazně doporučován.
- **Počáteční uživatelské jméno i heslo je admin.**
- Váš počítač by měl být ve stejné síti jako zařízení.

Vyhledejte požadovaná nastavení

Zařízení podporuje vyhledávání funkcí ve svém webovém rozhraní.

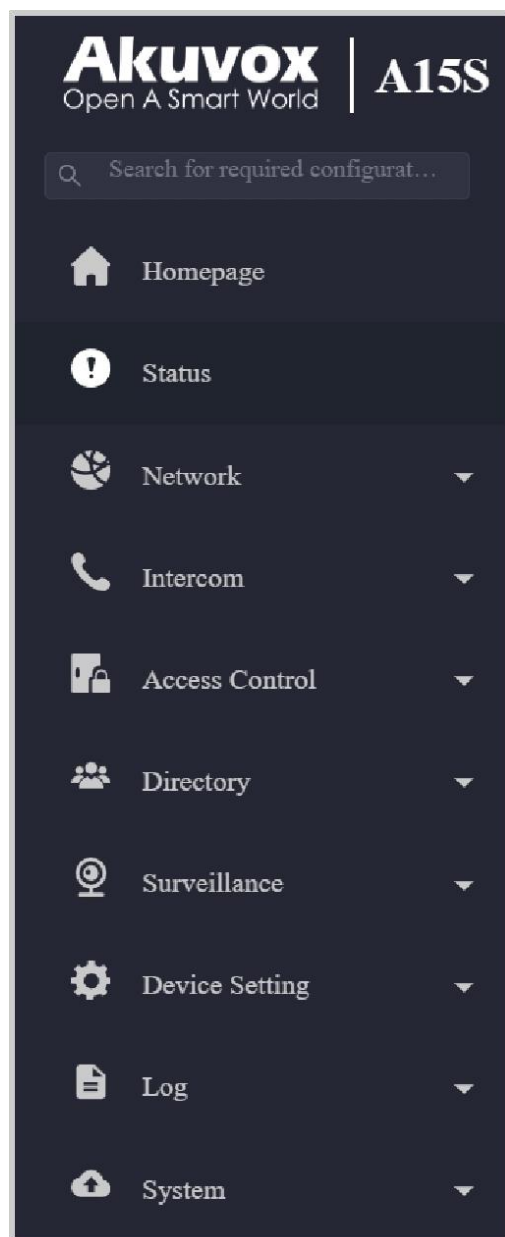
Například pokud chcete vyhledávat detekci pohybu, zadejte hodnotu do vyhledávacího pole.

Poté vyberte požadovanou možnost pro přesměrování na konfigurační rozhraní.



Úvod do konfiguračního menu

- **Stav:** Základní informace, jako jsou informace o produktu, síti, účtu atd.
- **Síť:** Tato sekce se hlavně zabývá nastavením DHCP a statické IP adresy, nastavením RTP portů, nasazením zařízení atd.
- **Interkom:** Tato část se týká nastavení účtu a funkcí hovoru.
- **Řízení přístupu:** Tato sekce pokrývá ovládání vstupu, relé, nastavení karet, rozpoznávání obličeje, soukromé PIN kódy, připojení k Wiegand atd.
- **Adresář:** Tato sekce se týká správy uživatelů.
- **Sledování:** Tato sekce pokrývá detekci pohybu, RTSP, MJPEG, ONVIF, živé vysílání atd.
- **Nastavení zařízení:** Nastavení světla, zobrazení záložek a tlačítek, nastavení LCD a zvuková nastavení.
- **Log:** Zahrnuje záznamy hovorů, přístupové záznamy a záznamy událostí.
- **Systém:** Zahrnuje aktualizaci firmwaru, automatické nastavení, údržbu zařízení atd.



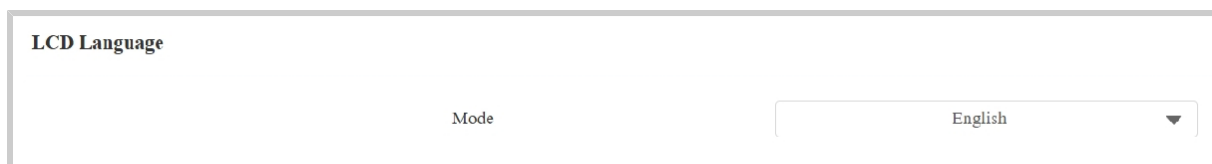
Jazyk a čas

Jazyk

Pro výběr jazyka zařízení přejděte do **Nastavení zařízení > Time/Lang > rozhraní jazyka LCD**.

LCD zařízení podporuje následující jazyky:

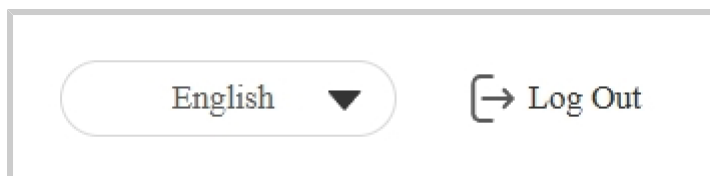
- Angličtina, zjednodušená čínština, tradiční čínština, čeština, portugalština, španělština, italština, nizozemština, francouzština, němčina, hebrejštiny, polština a arabština.



V pravém horním rohu můžete přepnout webový jazyk zařízení.

Web zařízení podporuje následující jazyky:

- Angličtina, zjednodušená čínština, tradiční čínština, **čeština**, portugalština, španělština, italština, nizozemština, francouzština, němčina, hebrejštiny, polština a arabština.



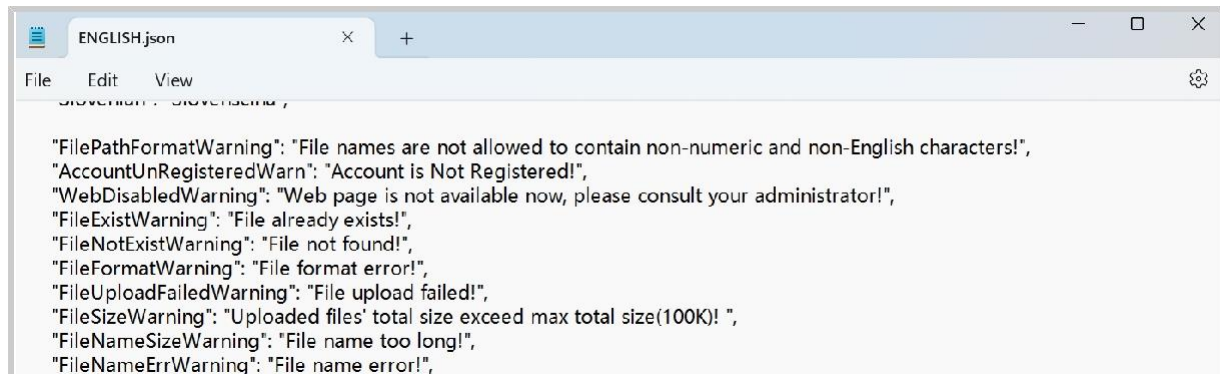
Vlastní jazyk

Můžete si upravit názvy konfigurací a texty na zařízení a jeho webovém portálu, například varování před chybou názvu souboru.

Exportujte .json soubor pro úpravy. Můžete ho upravovat pomocí poznámkového bloku na počítači.

Importujte .json soubor a jeho velikost by měla být menší než 1 MB.

Příklad souboru:



Nastavte to v **nastavení zařízení > rozhraní Time/Lang > Custom Language**.

Type	File Status	File Name	Import	Export	Reset
Web	Default	ENGLISH.json	Import	Export	Reset
LCD	Default	strings.xml	Import	Export	Reset

Čas

Časová nastavení ve webovém rozhraní umožňuje nastavit adresu NTP serveru pro automatickou synchronizaci času a data. Jakmile je časové pásmo vybráno, zařízení upozorní NTP server na zvolené časové pásmo, což mu umožní synchronizovat nastavení časového pásma na vašem zařízení.

Pro nastavení přejděte do **Nastavení zařízení > rozhraní Time/Lang > Time**.

Time

Automatic Date&Time

☒

Time Zone

GMT+0:00 GMT

▼

Date Format

2026-07-03

▼

Time Format

24 Hour

▼

NTP Server

0.pool.ntp.org

Update Interval

3600

(>=3600Sec)

System Time

02:52:17

- **Automatické datum a čas:** Automatické datum a čas je zapnuté ve výchozím nastavení, což umožňuje automatické nastavení a synchronizaci data a času s výchozím časovým pásmem a serverem Network Time Protocol (NTP). Můžete to také nastavit ručně vypnutím automatického data a zadáním času a data.
- **NTP server:** Adresa NTP serveru pro aktualizaci času. Výchozí adresa NTP serveru je 0.pool.ntp.org.
- **Interval aktualizace:** Nastavte interval časové aktualizace. Například pokud ho nastavíte na 3600 sekund, zařízení pošle požadavek na NTP server na časovou aktualizaci každých 3600 sekund.
- **Systémový čas:** Zobrazit aktuální čas zařízení.

Hlasitost a tón

Konfigurace hlasitosti a vyzvánění zahrnují hlasitost mikrofonu, hlasitost reproduktorů, hlasitost budíků a další. Navíc můžete nahrát tóny otevírání dveří, které obohatí uživatelský osobní zážitek.

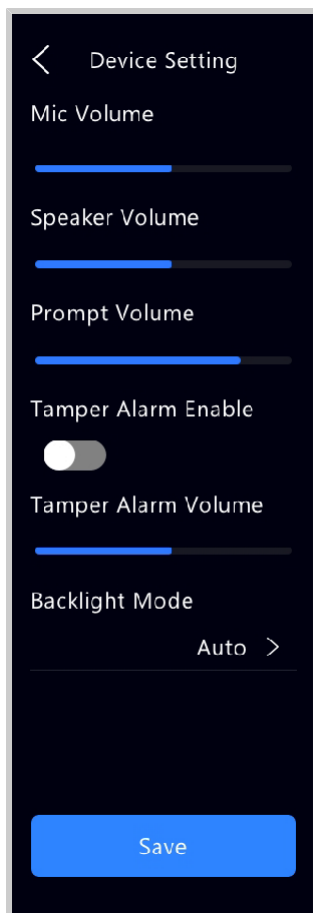
Ovládání hlasitosti

Nastavte hlasitost v nastavení zařízení > audio rozhraní. Klikněte na **Testovat** pro přehrávání zvuku na aktuální hlasitost.

Volume Control			
Mic Volume	8	(1~15)	
Speaker Volume	8	(1~15)	<button>Test</button>
Tamper Alarm Volume	8	(1~15)	<button>Test</button>
Prompt Volume	12	(0~15)	<button>Test</button>
Key Pressed Volume	8	(0~15)	<button>Test</button>

- **Hlasitost mikrofonu:** Hlasitost mikrofonu. Výchozí je 8.
- **Hlasitost reproduktorů:** Hlasitost reproduktorů. Výchozí je 8.
- **Hlasitost alarmu proti manipulaci:** Nastavte hlasitost při spuštění alarmu proti manipulaci . Výchozí je 8.
- **Objem promptů:** Různé výzvy, včetně úspěchu a neúspěchu při otevírání dveří. Výchozí je 12.
- **Stisknutá hlasitost:** Zvuk ťukání ikony. Výchozí je 8.

Hlasitost můžete také upravit na obrazovce **Nastavení > Nastavení zařízení**.



Nahrávání hlasových náповěd

Můžete si na zařízení přizpůsobit a nahrát různé hlasové výzvy. Pro nastavení přejděte do **Nastavení zařízení** > rozhraní **Audio** > **Tone Upload**.

ID	Tone	Import	Reset	Play	Enabled
1	Greetings	Import	Reset	Play	☒
2	Relay A - Access Granted	Import	Reset	Play	☒
3	Relay B - Access Granted	Import	Reset	Play	☒
4	Input A - Access Granted	Import	Reset	Play	☒
5	Input B - Access Granted	Import	Reset	Play	☒
6	Input C - Access Granted	Import	Reset	Play	☒
7	Input D - Access Granted	Import	Reset	Play	☒
8	Access Denied	Import	Reset	Play	☒
9	Close Door	Import	Reset	Play	☒
10	Pin Page	Import	Reset	Play	☒
11	APT+PIN	Import	Reset	Play	☒
12	Calling	Import	Reset	Play	☒
13	QR Code	Import	Reset	Play	☒

- **Přístup udělen (vstup):** Tón se přehraje, když se dveře otevřou stiskem výstupního tlačítka připojeného ke vstupu zařízení.
- **Zavřít dveře:** Zvuk zavření dveří funguje pro relé nastavené na **bistabilní** režim.
- **PIN stránka:** Tón se přehraje při vstupu do PIN obrazovky.
- **APT+PIN:** Tón se přehraje při zadávání čísla bytu a PIN kódu pro přístup ke dveřím.
- **Volání:** Tón se zazní při vstupu na obrazovku Hovor.
- **QR kód:** Tón se přehraje při vstupu do dočasné obrazovky pro skenování QR kódů.

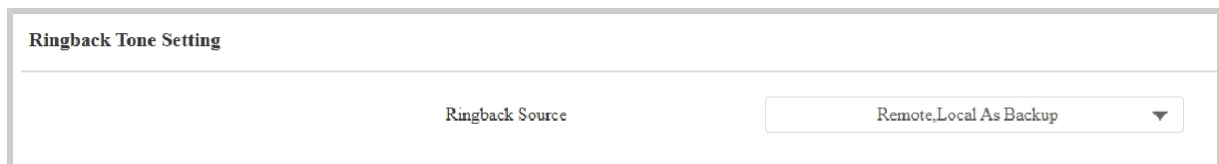
Poznámka

Formát souboru: wav; Velikost: < 200KB; Vzorkovací frekvence: 16000; Hloubka bitu: 16 bitů.

Nastavení vyzvánění.

Nastavení tónu vyzvánění, které upřednostňuje přehrávání místních vyzváněcích tónů a určuje, jaké typy náhledů může volající přijímat.

Pro nastavení přejděte do rozhraní **Interkom > Call Feature**.



Ringback Tone Setting

Ringback Source

Remote, Local As Backup ▼

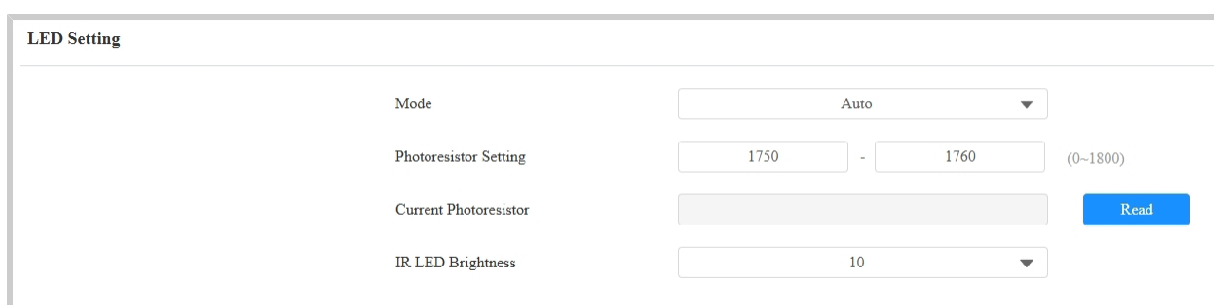
- **Zdroj zpětného vyzvánění:**
 - **Vzdálené, lokální jako záloha:** Bude přehrán místní vyzváněcí tón.
 - Když zařízení volá jiné zařízení, například Akuvox vnitřní monitor, a SIP server vrátí ne-183, vnitřní monitor nebude mít žádný interkomový náhled.
 - Pokud SIP server vrátí 183, vnitřní monitor přijme video náhled bez hlasu.
 - **Lokální:** Bude přehrán místní vyzváněcí tón. Ať už SIP server vrátí 183 nebo ne, volající nebude mít žádný interkom náhled.
 - **Dálkové řízení:**
 - Pokud SIP server vrátí verzi ne-183, přehraje se místní vyzvánění a volaný nebude mít žádný interkom náhled.
 - Pokud SIP server vrátí 183, bude přehrán vyzváněcí tón SIP serveru a volaný obdrží video náhled bez hlasu.

Nastavení LED diod

Nastavení infračervených LED

Infračervené LED je primárně navrženo k zesílení světla v noci nebo ve tmě.

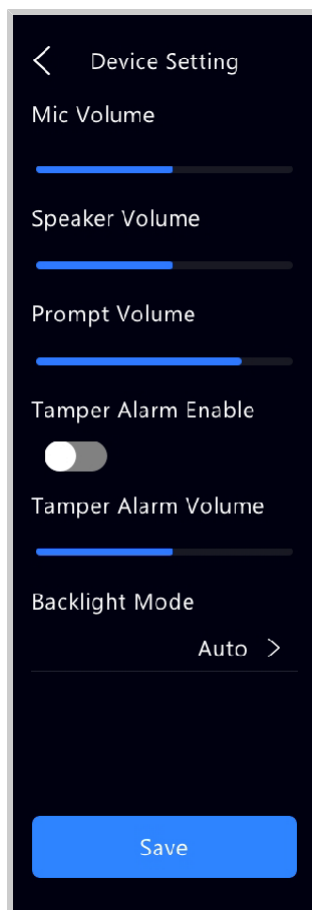
Nastavte to na webovém rozhraní **Nastavení zařízení > LED Setting**.



LED Setting	
Mode	Auto
Photoresistor Setting	1750 - 1760 (0~1800)
Current Photoresistor	Read
IR LED Brightness	10

- **Režim:**
 - **Auto:** Automaticky zapínáte infračervenou LED na základě minimální a maximální hodnoty fotorezistoru.
 - **Vždy zapnuté:** Zapněte infračervenou LED.
 - **Vždy vypnuto:** Vypněte infračervenou LED.
 - **Plán:** Zapněte infračervenou LED diodu podle plánu. Při výběru této možnosti zadejte čas začátku a konec. Kromě harmonogramu zařízení přechází do režimu Auto.
- **Nastavení fotorezistoru:** Nastavte minimální a maximální hodnotu fotorezistoru tak, aby automaticky ovládaly ZAPNUTO-VYPNUTÍ LED doplňkového světla. Čím vyšší hodnota, tím jasnější je světlo. Pokud je hodnota fotorezistoru nižší než minimální práh, zapněte doplňovací světlo. Pokud je větší než maximální práh, vypněte ho.
- **Aktuální fotorezistor:** Klikněte na **Číst** pro získání aktuální hodnoty fotorezistoru.
- **Jas IR LED:** Nastavte jas IR LED z úrovně 0 na úroveň 10. Výchozí hodnota je 10. Čím vyšší úroveň, tím jasnější je.

Režim podsvícení můžete také zvolit na obrazovce **Nastavení > Nastavení zařízení**.



LED bílé světlo

LED bílé světlo se používá především k zesílení osvětlení pro přístup pomocí QR kódů a pro lepší viditelnost návštěvníků při sledování snímků z vnitřního prostoru ve tmě.

Nastavte to na webovém rozhraní **Nastavení zařízení > Bílé světlo**.

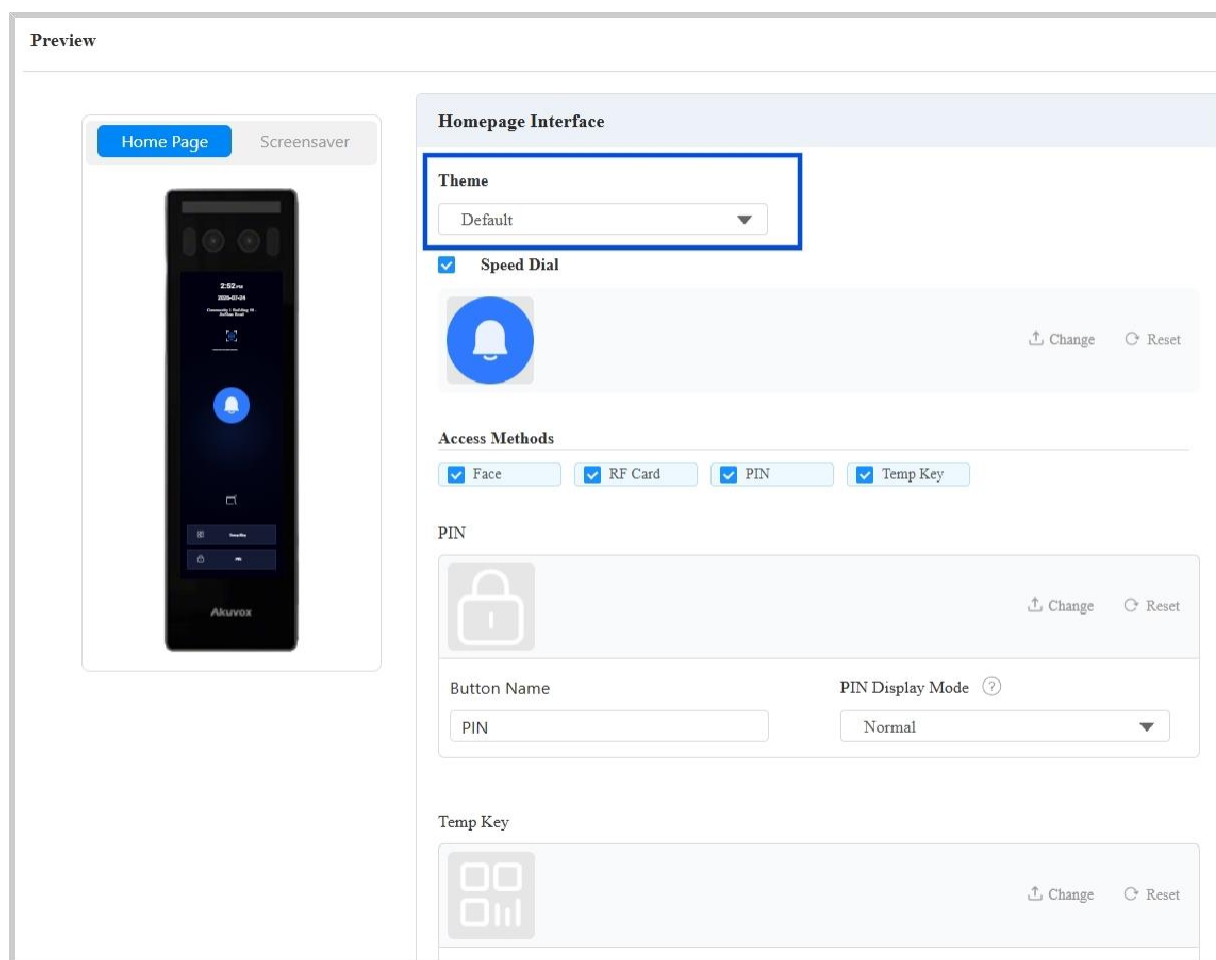
White Light	
Mode	Auto ▼
Max White Light Value	3 ▼
<button>Test</button>	

- **Režim:** Vyberte **Automatické** nebo **VYPNUTO**. Pokud zvolíte **Automatické**, bílé světlo se rozsvítí pouze tehdy, když jsou splněny všechny podmínky: probíhá rozpoznávání obličeje nebo skenování QR kódů, noční režim je detekován a pohyb je detekován radarem.
- **Maximální hodnota bílého světla:** Nastavte úroveň jasu. Vyšší hodnoty zvyšují jas. Kliknutím na **Test** se světlo na aktuální úrovni rozsvítí na 3 sekundy.

Zobrazení na obrazovce

Zobrazení na domovské obrazovce

Zařízení podporuje **výchozí a vícefaktorové ověřování**. Pro změnu režimu přejděte do **nastavení zařízení > rozhraní LCD > Theme**.



Výchozí téma

Zde můžete kdykoli nahrát vlastní obrázky ikon nebo obnovit výchozí ikony pro **Speed Dial**, **Temp Key** a **PIN**.

Klikněte na **Změnit** pro nahrání a na **Resetovat** pro obnovení.

Preview

Home Page Screensaver



Homepage Interface

Theme
Default: ▼

☒ Speed Dial



[Change](#)
[Reset](#)

Access Methods

☒ Face
 ☒ RF Card
 ☒ PIN
 ☒ Temp Key

PIN



[Change](#)
[Reset](#)

Button Name: PIN PIN Display Mode: ? Normal ▼

Temp Key



[Change](#)
[Reset](#)

Button Name

Temp Key

☒ Background



[Change](#)
[Reset](#)

- **Změna ikony:** Maximální velikost souboru: 200KB; Formát: .jpg, .png, .bmp, .jpeg; Doporučené rozlišení pro ikonu rychlé volby: 120x120; pro ostatní ikony: 80x80.

- **Rychlá volba:** Povolte/vypněte ikonu **rychlé volby** na domovské obrazovce pro volání hovorů. Viz kapitola [Nastavení hovoru](#) konfigurace čísla rychlé volby.
- **Metody přístupu:** Určete dostupné přístupové metody na domovské obrazovce. Když je způsob přístupu zakázán, jeho ikona je skryta a odpovídající autentizační metoda se stane nedostupnou.
- **PIN:**
 - **Název tlačítka:** Pokud je potřeba, upravte název tlačítka. Název nemění atribut tlačítka.
 - **Režim zobrazení PIN:** Dostupný, když je povolen přístup k PINu.
 - **Normální:** Číslice jsou zobrazeny ve standardním pořadí.
 - **Nepořádek:** Číslice jsou zobrazeny v náhodném pořadí.
- **Dočasný klíč:**
 - **Název tlačítka:** Pokud je potřeba, upravte název tlačítka. Název nemění atribut tlačítka.
- **Pozadí:** Přizpůsobte pozadí domovské obrazovky. Pozadí je viditelné, když **je autentizace obličeje na domovské obrazovce zakázána**.
 - Maximální velikost: 200KB; Formát: .jpg, .png, .bmp, .jpeg; Doporučené rozlišení: 320x960.

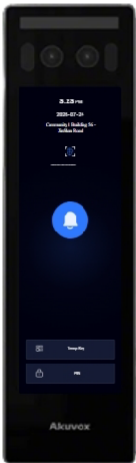
V režimu vícefaktorové autentizace

V tomto režimu se na domovské obrazovce zobrazují pouze vybrané metody autentizace. Možnosti autentizace a související nastavení jsou automaticky upravovány podle zvoleného režimu.

Pro záložky **Speed Dial** a **Temp Key** můžete kdykoli nahrát vlastní obrázky ikon nebo obnovit výchozí ikony.

Preview

Home Page Screensaver



Homepage Interface

Theme
Multi-factor Authentication

☒ Speed Dial



Change Reset

Authentication Mode
Face+PIN

☐ Entry Restriction

PIN



Change Reset

Button Name PIN PIN Display Mode ? Normal

Temp Key



Change Reset

Button Name

Temp Key

☒ Background



Change Reset

- **Změna ikony:** Maximální velikost souboru: 200KB; Formát: .jpg, .png, .bmp, .jpeg; Doporučené rozlišení ikony rychlé volby: 120x120; pro ostatní ikony: 80x80.

- **Rychlá volba:** Povolte/vypněte ikonu **rychlé volby** na domovské obrazovce pro volání hovorů. Viz kapitola [Nastavení hovoru](#) konfigurace čísla rychlé volby.
- **Režim autentizace:** Vyberte metodu dvoufaktorového ověřování : Face + PIN, Face + RF karta nebo RF karta + PIN. První autentizační metoda musí být úspěšně dokončena, než se přejde k druhé.
- **Omezení vstupu:** Povolte nebo vypněte opakovaná omezení přístupu pro stejného uživatele. Po zapnutí musí uživatel počkat na nastavenou dobu omezení, než dveře znovu odemkne. Toto omezení platí pouze pro stejného uživatele. Ostatní oprávnění uživatelé mohou dveře stále odemykat normálně.
- **PIN:**
 - **Název tlačítka:** Pokud je potřeba, upravte název tlačítka. Název nemění atribut tlačítka.
 - **Režim zobrazení PIN:** Dostupný, když je povolen přístup k PINu.
 - **Normální:** Číslice jsou zobrazeny ve standardním pořadí.
 - **Nepořádek:** Číslice jsou zobrazeny v náhodném pořadí.
- **Dočasný klíč:**
 - **Název tlačítka:** Pokud je potřeba, upravte název tlačítka. Název nemění atribut tlačítka.
- **Pozadí:** Přizpůsobte pozadí domovské obrazovky. Pozadí je viditelné, když **je autentizace obličeje na domovské obrazovce zakázána**.
 - Maximální velikost: 200KB; Formát: .jpg, .png, .bmp, .jpeg; Doporučené rozlišení: 320x960.

Configure Screensaver

Můžete nastavit délku spořiče obrazovky i časování vypnutí obrazovky pro ochranu i snížení spotřeby energie.

Pro nastavení přejděte do **Nastavení zařízení > LCD rozhraní**.

Standby Interface

Screensaver

✓

Akuvox

Open A Smart World

✕

Akuvox

Open A Smart World

✕

Akuvox

Open A Smart World

✕

Akuvox

Open A Smart World

✕

+

Screensaver Interval(Sec)

5 Seconds

Screensaver Time

30 Seconds

Sleep

15 Seconds

Wake Up Mode

Auto

Schedule

1001:Always ✕

- Rozhraní: Nastavit, zda je spořič obrazovky povolen.
- **Interval spořiče obrazovky (sekundy):** Interval přepínání mezi spořiči obrazovky (1 až 120 sekund). Výchozí interval je 5 sekund.
- **Čas spořiče obrazovky:** Nastavte dobu trvání spořiče obrazovky (5 sekund až 30 minut, nebo navždy).
- **Spánek:** Čas pro spuštění režimu spořiče obrazovky (5 sekund až 30 minut). Výchozí je 15 sekund. Například pokud je nastaven na 15 sekund, zařízení přejde do režimu spořiče obrazovky, když po dobu 15 po sobě jdoucích sekund nezaznamená žádnou funkci nebo nepřibližující se objekt. Když je režim spořiče obrazovky vypnutý, obrazovka zařízení se

vypne přímo během 15 sekund.

- **Režim probuzení:**
 - **Auto:** Obrazovka se probudí, když se někdo přiblíží, aniž by se jí někdo dotkl.
 - **Rozvrh:** Vyberte rozvrh, kdy se obrazovka může automaticky probudit. Mimo čas je potřeba ji probudit ručně. Nastavte rozvrh v **rozvrhu** Directory > Schedule.
 - **Manuál:** Uživatelé se musí dotknout a probudit obrazovku.

Nahrajte spořič obrazovky

Obrázky spořiče obrazovky můžete nahrát do zařízení přes webové rozhraní, čímž zlepší vizuální zážitek nebo slouží k propagaci.

Nastavte to na webu rozhraní **Device > LCD**. Klikněte na ikonu přidat +.

Standby Interface

Screensaver

✓

✕

✕

✕

✕

Screensaver Interval(Sec)

5 Seconds

Screensaver Time

30 Seconds

Sleep

15 Seconds

Wake Up Mode

Auto

Schedule

1001:Always ✕

Poznámka

- Nahrané obrázky by měly být ve formátu JPG s maximálně 2 miliony pixelů.
- Doporučené rozlišení je 320×960.
- Pokud nahraný obrázek duplikuje existující ID obrázku, bude existující obrázek přepsán.

Zobrazení textového promptu pro otevření dveří

Můžete povolit textovou výzvu k otevírání a zavírání dveří.

Pro nastavení přejděte do rozhraní **Access Control > Relay > Open Door Text Prompt**.

Open Door Text Prompt	
Open Door Outside Succeeded Text Prompt	☒
Open Door Inside Succeeded Text Prompt	☒
Open Door Failed Text Prompt	☒
Display User Info	☒

- **Otevření dveří venku – úspěšná textová výzva:** Zobrazí textovou výzvu poté, co jsou dveře otevřeny metodami přístupu podporovanými zařízením, kromě tlačítka výstupu. Výchozí výzva je "Přístup udělen". Výzvu si můžete přizpůsobit s maximálně 63 znaky.
- **Otevřít dveře uvnitř Úspěšná textová výzva:** Zobrazí textovou výzvu po otevření dveří stisknutím výstupního tlačítka (vstup je spuštěn). Výchozí výzva je "Přístup udělen". Můžete si výzvu přizpůsobit s maximálně 63 znaky.
- **Text výzva "Otevřít dveře selhalo":** Po neúspěšném otevření dveří zobrazte textovou výzvu. Výchozí výzva je "Přístup zamítnut". Výzvu můžete přizpůsobit maximálně 63 znaky.
- **Zobrazit uživatelské informace:** Zobrazit uživatelské informace po rozpoznání obličeje nebo přejetí RF kartou. Například pokud rozpoznávání obličeje uspěje, na obrazovce zařízení se objeví textová výzva "Přístup udělen" s uživatelským ID a jménem. Pokud selže, zobrazí se textová výzva "Přístup zamítnut".

Zobrazení možností odemčení

Uživatelé si mohou zvolit dveře, které se otevřou, když je zařízení připojeno k více než jednomu zámku dveří.

Klikněte [zde](#) pro zobrazení detailů funkce.

Pro zobrazení možností odemčení přejděte do **Kontroly přístupu > Relay > Možnosti odemčení**.

Unlock Options	
Unlock Options	Visible ▼

Nastavení sítě

Pro zajištění normálního fungování se ujistěte, že zařízení má správně nastavenou IP adresu nebo ji automaticky získává ze serveru DHCP.

Pro nastavení přejděte do Rozhraní **Network > Basic**.

LAN Port	
Network Mode	☐ DHCP ☒ Static IP
IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Preferred DNS Server	8.8.8.8
Alternative DNS Server	

- **DHCP:** Výchozí síťové připojení je režim DHCP. Pokud je zvolen režim DHCP, zařízení bude automaticky přiřazeno IP adrese, maskou podsítě, výchozí bránou a adresou DNS serveru.
- **Statická IP:** Když je zvolen statický IP režim, měla by být IP adresa, maska podsítě, výchozí brána a adresa DNS serveru nastaveny podle síťového prostředí.
- **IP adresa:** Nastavte IP adresu, když je zvolen statický IP režim. Pro přístup k webovým nastavením zařízení by měl být váš počítač ve stejné lokální síti jako zařízení.
- **Maska podsítě:** Maska podsítě říká vašemu zařízení, které IP adresy jsou součástí vaší lokální sítě a které ne. Například pokud je maska podsítě 255.255.255.0, znamená to, že zařízení s podobnými počátečními IP adresami (například 192.168.1.x) jsou ve stejné síti.
- **Výchozí brána:** Brána je jako most mezi vaším zařízením a dalšími sítěmi, například internetem. Obvykle je to IP adresa vašeho routeru.

- **Preferovaný/alternativní DNS server:** Systém doménových jmen (DNS) je celkový systém nebo síť, která zajišťuje překlad doménových jmen (jako `www.example.com`) na IP adresy (například `192.0.2.1`), které počítače používají k vzájemné identifikaci v síti. Zařízení se připojí k alternativnímu DNS serveru, když primární server není k dispozici.

Síť si můžete také nastavit na obrazovce **Nastavení** > **Ethernet**.

< Ethernet

DHCP

☒

* IP Address

192.168.31.197

* Subnet Mask

255.255.255.0

* GateWay

192.168.31.1

* Preferred DNS Server

192.168.31.1

Alternative DNS Server

Save

Nasazení zařízení v síti

Pro usnadnění ovládání a správy zařízení konfiguruje interkomové zařízení Akuvox s detaily jako poloha, režim provozu, adresa a čísla linky.

Pro nastavení přejděte do rozhraní **Web Network > Advanced > Connect Settings**.

Connect Setting					
Connect Type	None				
Device Address	1	1	1	1	1
Device Extension	1				
Device Location	Access Control				

- **Typ připojení:** Automaticky se nastavuje podle připojení zařízení ke konkrétnímu serveru v síti, například SDMC, Cloud nebo None.
 - **Žádné:** Žádné je výchozí tovární nastavení, což znamená, že zařízení není v žádném typu serveru. Zařízení se připojují přímo k sobě navzájem nebo v rámci lokální sítě (LAN) bez závislosti na externích serverech.
 - **Cloud:** Zařízení je připojeno ke SmartPlus Cloud, cloudovému systému zjednodušujícímu správu přístupu k nemovitostem. Cloudový režim umožňuje zařízením inteligentně komunikovat mezi sebou a mobilní aplikací SmartPlus, zálohovat data denně a na různých hostitelích. Vyhovuje projektům vyžadujícím chytré, flexibilní a bezpečné nasazení a správu.
 - **SDMC:** Zařízení je připojeno k SDMC, platformě pro správu navrženou pro on-premise projekty. Režim SDMC spravuje a zálohuje data na dálku v lokální síti. Také se pyšní mnoha funkcemi vhodnými pro projekty vyžadující vysokou ochranu soukromí, nižší náklady a centralizovanou správu.
- **Adresa zařízení:** Dostupná pro serverový režim None. Lze ji použít k volání zařízení. Zadejte adresu zařízení zadáním informací o poloze zařízení zleva doprava: Komunita, Budova, Jednotka, Patro a Místnost v pořadí.

- **Rozšíření zařízení:** Dostupné pro serverový režim None. Číslo rozšíření zařízení se pohybuje od 0 do 10.
- **Umístění zařízení:** Místo, kde je zařízení instalováno a používáno .

Nastavení NAT

Překlad síťových adres (NAT) umožňuje zařízením v privátní síti používat jednu veřejnou IP adresu k přístupu k internetu nebo jiným veřejným sítím. NAT ukládá omezené veřejné IP adresy a skrývá interní IP adresy a porty před vnějším světem.

Pro registraci SIP účtů na serverech třetích stran v síti Wide Area Network (WAN) je potřeba povolit funkci RPort na interkomových zařízeních, abyste navázali stabilní připojení.

Pro povolení NAT přejděte do rozhraní **Interkom > Account > NAT**.

The screenshot shows the NAT configuration page. It has a title 'NAT' at the top left. Below it, there are several settings:

- STUN Enabled:** A checkbox that is currently unchecked.
- STUN Server IP:** A text input field that is empty.
- Port:** A text input field containing the value '3478'. To its right, in smaller text, is the range '(1024~65535)'.
- UDP Keep Alive Messages:** A checkbox that is checked with a blue square.
- UDP Alive Messages Interval:** A text input field containing the value '30'. To its right, in smaller text, is the range '(5~60Sec)'.
- RPort:** A checkbox that is currently unchecked.

- **IP STUN serveru:** Zadejte adresu serveru, když je zařízení v širokopásmové síti (WAN).
- **Port:** Server port.
- **UDP Keep Alive zprávy:** Pokud je zařízení zapnuto, odešle zprávu na SIP server, který rozpozná, zda je zařízení online.
- **UDP Alive Messages Interval:** Nastavte interval odesílání zpráv od 5 do 60 sekund. Výchozí je 30 sekund.
- **RPort:** Povolte RPort, když je SIP server ve WAN.

Nastavení HTTP na webu zařízení

Tato funkce spravuje přístup na webové stránky zařízení. Zařízení podporuje dva způsoby vzdáleného přístupu: HTTP a HTTPS (šifrování).

Nastavte to na rozhraní **Network > Advanced > Web Server**.

Web Server		
Protocol	☒ HTTP	☒ HTTPS
HTTP Port	80	(80,1024-65535)
HTTPS Port	443	(443,1024-65535)

- **Protokol:** HTTP a HTTPS jsou ve výchozím nastavení povoleny.
- **HTTP/HTTPS port:** Specifikujte port webového serveru pro přístup k webovému rozhraní zařízení přes HTTP/HTTPS.

Lokální RTP konfigurace zařízení

Protokol pro přenos v reálném čase (RTP) umožňuje zařízením streamovat audio a video data přes síť v reálném čase.

Pro použití RTP potřebují zařízení řadu portů. Port je jako kanál pro data v síti. Nastavením RTP portů na zařízení a routeru můžete předejít rušení sítě a zlepšit kvalitu zvuku a obrazu.

Pro nastavení přejděte na rozhraní **Network > Advanced > Local RTP**.

Local RTP		
Starting RTP Port	11800	(1024-65535)
Max RTP Port	12000	(1024-65535)

- **Počáteční RTP port:** Hodnota portu pro stanovení výchozího bodu pro exkluzivní rozsah přenosu dat.

- **Max RTP port:** Hodnota portu pro určení koncového bodu pro exkluzivní rozsah přenosu dat.

Nastavení SNMP

Simple Network Management Protocol (**SNMP**) je protokol pro správu IP síťových zařízení. Umožňuje správcům sítě monitorovat zařízení a přijímat upozornění na situace, které stojí za pozornost. SNMP poskytuje proměnné popisující konfiguraci systému, organizované do hierarchií a popisované Management Information Bases (MIB).

Pro nastavení přejděte do rozhraní **Network > Advanced > SNMP**.

SNMP	
Enabled	☐
Port	(1024–65535)
Trusted IP	

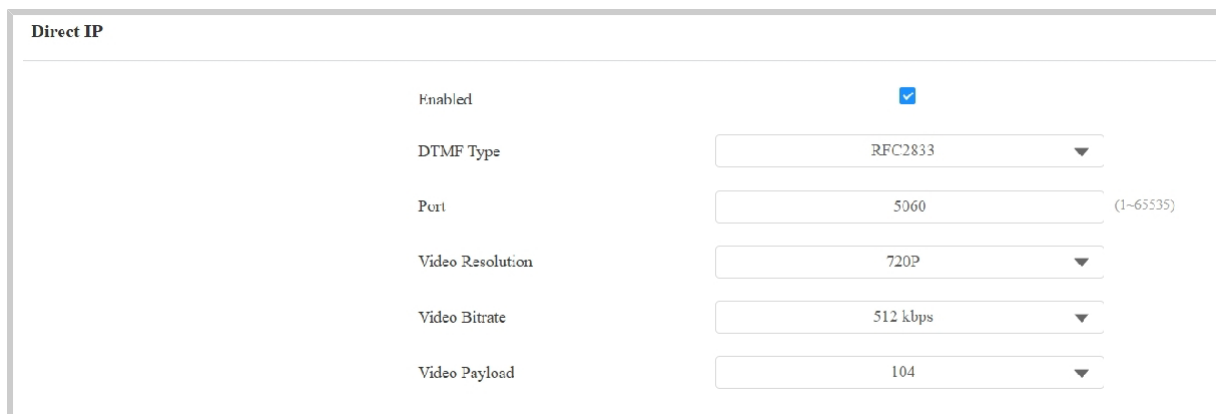
- **Port:** Nastavte specifický port pro přenos dat od 1024 do 65535.
- **Důvěryhodná IP:** Povolená adresa SNMP serveru. Může to být IP adresa nebo jakékoliv platné URL doménové jméno.

Konfigurace hovorů interkomu

Konfigurace IP hovorů

IP hovor je přímý hovor mezi dvěma interkomovými zařízeními používajícími jejich IP adresy, bez serveru nebo ústředny. IP hovory fungují, když jsou zařízení ve stejné síti.

Povolte nebo deaktivujte funkci přímého IP hovoru v **Interkom > Call Feature > rozhraní Direct IP**.



Direct IP	
Enabled	☒
DTMF Type	RFC2833
Port	5060 (1~65535)
Video Resolution	720P
Video Bitrate	512 kbps
Video Payload	104

- **Port:** Nastavte port pro přímé IP hovory. Výchozí je 5060 s rozsahem od 1 do 65535. Pokud zadáte hodnotu v tomto rozsahu jinou než 5060, zajistěte konzistenci s odpovídajícím zařízením pro přenos dat.

Konfigurace SIP hovoru

Protokol zahájení relace (**SIP**) je protokol pro přenos signálu používaný k iniciaci, udržování a ukončení hovorů.

SIP hovor využívá SIP k odesílání a přijímání dat mezi SIP zařízeními a může využívat internet nebo místní síť k nabídce vysoce kvalitní a bezpečné komunikace. Zahájení SIP hovoru vyžaduje SIP účet, SIP adresu pro každé zařízení a konfiguraci SIP nastavení na zařízeních.

Registrace SIP účtu

Každé zařízení potřebuje SIP účet pro uskutečňování a přijímání SIP hovorů.

Interkomová zařízení Akuvox podporují konfiguraci dvou SIP účtů, které lze registrovat pod dvěma nezávislými servery.

Klikněte [zde](#) pro zobrazení příkladu registrace SIP účtu.

Zaregistrujte SIP účet v rozhraní **Interkom > Účet**.

The screenshot shows the 'SIP Account' configuration page. At the top, there is a breadcrumb 'Intercom» Account' and two tabs: 'Account1' (selected) and 'Account2'. Below the tabs, the title 'SIP Account' is displayed. The main configuration area contains a table with the following fields:

Status	Disabled
Account Enabled	☐
Display Label	
Display Name	
Register Name	
Username	
Password	

- **Účet 1/Účet 2:** Zařízení podporuje 2 SIP účty.
 - Účet 1 je výchozí účet pro zpracování hovorů. Také bude využit, když bude aktivována cloudová služba Akuvox SmartPlus.
 - Systém přepne na účet 2, pokud účet 1 není registrován.
- **Stav:** Uveďte, zda je účet SIP registrovaný nebo ne.
- **Štítek displeje:** Štítek zařízení.
- **Zobrazovací jméno:** Označení účtu 1 nebo 2 se zobrazí na obrazovce volajícího zařízení.
- **Název registru:** Stejný jako uživatelské jméno z PBX serveru.

- **Uživatelské jméno:** Stejně jako uživatelské jméno z PBX serveru pro autentizaci.
- **Heslo:** Stejně jako heslo z PBX serveru pro autentizaci.

Poznámka

- Pro přidání zařízení do cloudu vyberte **jeho typ zařízení** jako **Door Phone**. Výběrem **Kontroly přístupu** se deaktivují všechny funkce interkomu zařízení.
- Když je zařízení připojeno ke SmartPlus Cloudu, zobrazovací štítek, název registru a uživatelské jméno zobrazí jeho SIP číslo.

Konfigurace SIP serveru

SIP servery umožňují zařízením navazovat a spravovat hovorové relace s jinými interkomovými zařízeními pomocí protokolu SIP. Mohou to být servery třetích stran nebo vestavěné ústředny v Akuvox indoor monitoru.

Pro nastavení přejděte na webové rozhraní **Interkom > Účet**.

Preferred SIP Server		
Server IP		
Port	5060	(1024~65535)
Registration Period	1800	▼ (30~65535Sec)

Alternative SIP Server		
Server IP		
Port	5060	(1024~65535)
Registration Period	1800	▼ (30~65535Sec)

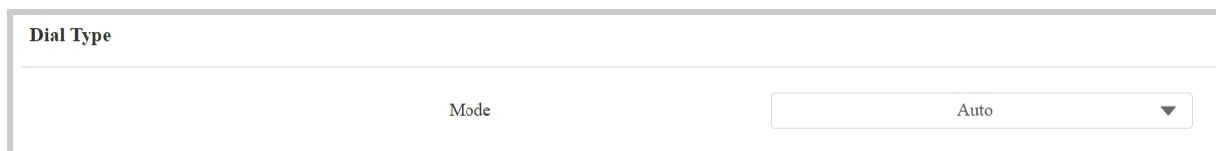
- **IP serveru:** Zadejte IP adresu serveru nebo jeho doménové jméno.
- **Port:** Specifikujte port SIP serveru pro přenos dat.

- **Registrační období:** Definujte časový limit pro registraci SIP účtu . Automatická reregistrace se spustí, pokud registrace účtu selže v této stanovené lhůtě.

Výběr SIP účtu

Funkce Typ vytočení určuje, který výchozí účet pro SIP hovory uskutečňuje. Platí pro hovory stisknutím kontaktů a zadáním SIP čísel na klávesnici zařízení.

Výchozí účet si můžete vybrat v rozhraní **Interkom > Call Feature > Dial Type**.



- **Režim:**
 - **Auto:** Zařízení použije registrovaný účet k provádění SIP hovorů. Pokud jsou oba zaregistrována, výchozí je účet 1.
 - **Účet 1:** Volat lze pouze kontaktům účtu 1.
 - **Účet 2:** Volat lze pouze kontaktům účtu 2.

Odchozí proxy server

Odchozí proxy server se používá k přijímání všech iniciačních požadavků a jejich směrování na určený SIP server za účelem navázání hovorové relace prostřednictvím přenosu dat na portu.

Pro nastavení přejděte na rozhraní **Interkom > Account > Outbound Proxy Server**.

Outbound Proxy Server		
Outbound Enabled	☐	
Preferred Server IP		
Port	5060	(1024-65535)
Alternative Server IP		
Port	5060	(1024-65535)

- **Preferovaná IP adresa serveru:** Zadejte IP adresu SIP proxy serveru.
- **Port:** Nastavte port pro navázání volání přes odchozí proxy server.
- **Alternativní IP serveru:** Zadejte IP adresu SIP proxy, která se použije, když hlavní proxy server selže.
- **Port:** Nastavte proxy port pro navázání hovorové relace přes záložní odchozí proxy server.

Typ přenosu dat

Interkomová zařízení Akuvox podporují čtyři protokoly přenosu dat: **User Datagram Protocol (UDP)**, **Transmission Control Protocol (TCP)**, **Transport Layer Security (TLS)** a **DNS-SRV**.

Vyberte typ přenosu dat na rozhraní **Interkom > Account > Transport Type**.

Transport Type	
Type	UDP

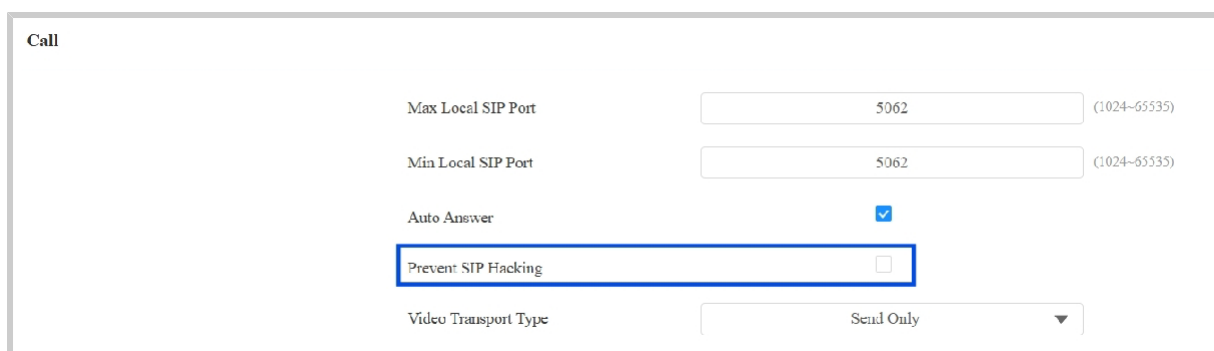
- **UDP:** Nespolehlivý, ale velmi efektivní protokol transportní vrstvy. Je to výchozí transportní protokol.
- **TCP:** Méně efektivní, ale spolehlivý protokol transportní vrstvy.
- **TLS:** Šifrovaný a bezpečný protokol transportní vrstvy. Vyberte tuto možnost, pokud chcete šifrovat SIP zprávy pro zvýšení bezpečnosti, nebo pokud server druhé strany používá TLS. Pro jeho použití je potřeba [nahrát certifikáty pro autentizaci](#).

- **DNS-SRV:** DNS servisní záznam definuje umístění serverů. Tento záznam obsahuje název hostitele a číslo portu serveru, stejně jako priority a váhy, které určují pořadí a frekvenci používání serveru.

Prevence SIP hackingu

Odposlech internetových telefonů je síťový útok, který umožňuje neoprávněným stranám zachytit a přistupovat k obsahu komunikačních relací mezi uživateli interkomu. To může útočníkům odhalit citlivé a důvěrné informace. Ochrana proti SIP hackingu je technika, která chrání SIP hovory před kompromitací na internetu.

Zapněte prevenci SIP hackování na rozhraní **Interkom > Account > Call**.



Call

Max Local SIP Port	5062	(1024-65535)
Min Local SIP Port	5062	(1024-65535)
Auto Answer	☒	
Prevent SIP Hacking	☐	
Video Transport Type	Send Only	▼

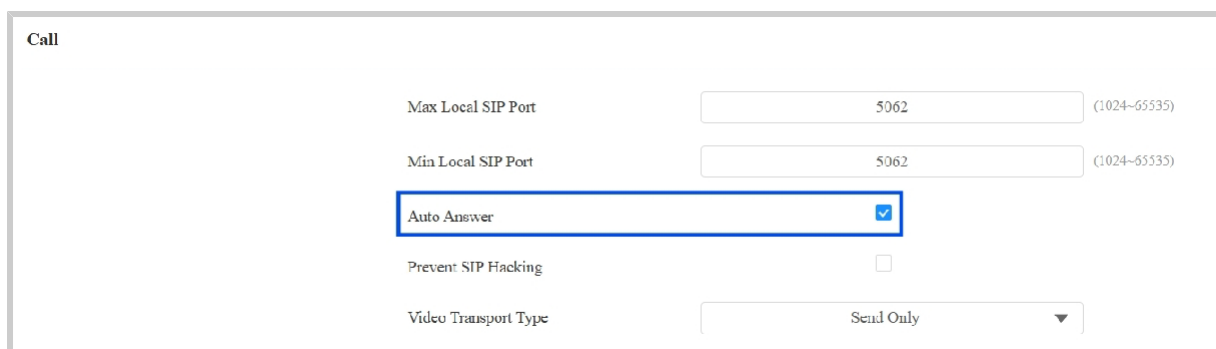
- **Zabránit SIP hackingu:** Aktivujte tuto funkci tak, abyste přijímali hovory pouze od kontaktů z bílé listiny. To chrání soukromé a tajné informace uživatelů před potenciálními hackery během SIP hovorů.

Nastavení hovoru

Automatické přijímání hovorů

Funkce automatického přijímání umožňuje zařízení automaticky přijímat příchozí hovory bez jakéhokoli manuálního zásahu. Tuto funkci si můžete také přizpůsobit nastavením doby automatického přijímání a volbou režimu komunikace mezi zvukem a obrazem.

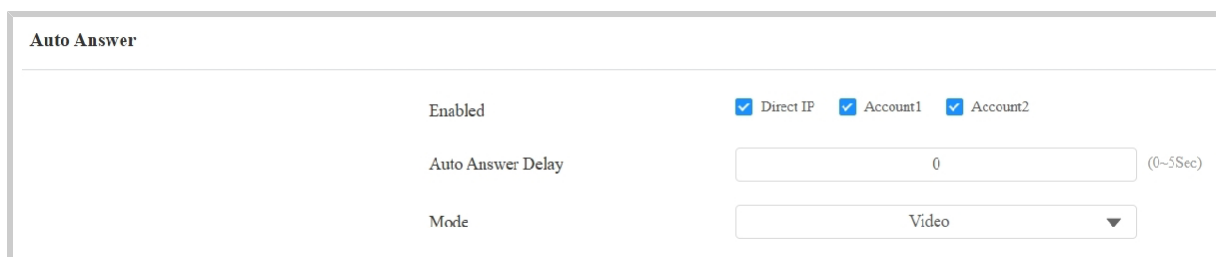
Pro povolení automatické přijímání hovorů přejděte do rozhraní **Interkom > Účet**.



Call

Max Local SIP Port	5062	(1024~55535)
Min Local SIP Port	5062	(1024~55535)
Auto Answer	☒	
Prevent SIP Hacking	☐	
Video Transport Type	Send Only	▼

Pro nastavení přejděte do **Interkomu > Call Function > rozhraní Auto Answer**.



Auto Answer

Enabled	☒	☒ Direct IP	☒ Account1	☒ Account2
Auto Answer Delay	0	(0~5Sec)		
Mode	Video	▼		

- **Zpoždění automatického přijetí:** Nastavte časový interval, kdy bude hovor automaticky přijat po vyzvání. Například pokud nastavíte zpoždění na 5 sekund, zařízení automaticky přijme hovor po 5 sekundách.
- **Režim:** Určit, zda hovor automaticky přijmeme jako video nebo zvukový hovor.

Skupinový hovor

Tato funkce umožňuje uživatelům volat skupinu kontaktů jedním stiskem. Zařízení podporuje místní a skupinové hovory s funkcí SmartPlus. Pro podrobnější konfiguraci klikněte [zde](#).

Pro nastavení přejděte do rozhraní **Interkom > Call Feature**.

The screenshot shows a configuration window titled "Speed Dial". It contains the following fields and options:

- Call Type:** A dropdown menu currently set to "Group Call".
- When Refused:** A dropdown menu currently set to "End This Call Only".
- Label:** A text field currently containing "Reception".
- Group Call Number (Local):** A numeric keypad with four rows of four digits each, used for entering a 16-digit group call number.

- **Typ hovoru:** Vyberte skupinový hovor.
- **Když je odmítnuto:**
 - **Ukončit všechny hovory:** Zařízení přestane volat.
 - **Ukončit tento hovor pouze** – zařízení bude dál volat na další číslo.
- **Štítek:** Text zobrazený na obrazovce zařízení, když zařízení volá cílová čísla. Výchozí je "Příjem".
- **Skupinové volací číslo (místní):** Zadejte cílová čísla.

Sekvenční volání

Sequence Call je funkce, která vám umožňuje vytáčet skupinu čísel v předem definovaném pořadí, dokud jedno z nich neodpoví. Tuto funkci podporuje Akuvox SmartPlus, který poskytuje sadu sekvenčních čísel hovorů pro tuto aplikaci. Klikněte prosím [zde](#) pro podrobnou konfiguraci.

Můžete také nastavit lokální sekvenční čísla hovorů v rozhraní Interkom > Call Feature.

Speed Dial

Call Type	Sequence Call ▼
Time Out (Sec)	20 ▼
When Refused	Do Not Call Next ▼
Label	Reception
Sequence Call Number	
Sequence Call Number 1	
Sequence Call Number 2	
Sequence Call Number 3	
Sequence Call Number 4	
Sequence Call Number 5	
Sequence Call Number 6	
Sequence Call Number 7	
Sequence Call Number 8	
Sequence Call Number 9	
Sequence Call Number 10	

- **Typ hovoru:** Vyber sekvenční volání.
- **Timeout(Sec):** Určete dobu trvání před zavoláním na další číslo, pokud předchozí hovor není přijat.
- **Když odmítnuto:** Rozhodněte se, zda vyvolat další, pokud byl hovor odmítnut dříve volanou stranou.
 - **Nevolat příště:** Sekvenční volání se zastaví, když je hovor odmítnut.
 - **Zavolejte dál:** Zařízení zavolá další číslo v pořadí, kdy je hovor odmítnut.
- **Štítek:** Text zobrazený na obrazovce zařízení, když zařízení volá cílová čísla. Výchozí je "Příjem".
- **Číslo volacího signálu:** Zadejte cílová čísla.

Maximální doba vytáčení

Maximální doba vytáčení je časový limit pro příchozí a/nebo odchozí hovory na zařízení. Pokud je nakonfigurováno, zařízení automaticky ukončí hovor, pokud nikdo neodpoví v přednastaveném čase, ať už je příchozí nebo odchozí.

Pro nastavení přejděte do funkce **Interkom > Call > rozhraní Max Dial Time**.

Max Dial Time		
Max SIP/IP Dial In Time	60	(30~120Sec)
Max SIP/IP Dial Out Time	60	(30~120Sec)

- **Maximální doba SIP/IP vytáčení:** Určete maximální dobu trvání příchozího hovoru. Zařízení automaticky ukončí příchozí hovor, pokud není přijat v přednastaveném čase.
- **Maximální doba SIP/IP výstupu:** Určete maximální dobu trvání odchozího hovoru. Zařízení automaticky ukončí volání, pokud příjemce v přednastaveném čase neodpoví.

Poznámka

Maximální doba vytáčení je ovlivněna maximální dobou vytáčení SIP serveru při uskutečňování SIP hovorů. Maximální doba hovoru by neměla přesahovat dobu vytáčení SIP serveru.

Maximální doba trvání hovoru

Zařízení umožňuje nastavit délku hovoru pro příjem hovoru z volajícího zařízení, protože volající může zapomenout interkom zavěsit. Když je dosaženo doby hovoru, zařízení hovor automaticky ukončí.

Pro nastavení přejděte do **Interkom > Call Feature > rozhraní Max Call Time**.

Max Call Time	
Max SIP/IP Call Time	5 (2~30min)

- **Maximální doba hovoru SIP/IP:** Určete maximální délku všech hovorů. Zařízení hovor automaticky ukončí, jakmile je časový limit dosažen.

Poznámka

Maximální doba hovoru je ovlivněna maximální dobou hovoru SIP serveru při uskutečňování SIP hovorů. Maximální doba hovoru by neměla přesahovat délku hovoru SIP serveru.

Zavěšení hovoru po otevření dveří

Tato funkce automaticky ukončí hovor po otevření dveří, což umožňuje bezproblémový příjem dalších hovorů.

Pro nastavení přejděte do **Interkomu > Call Function > Ukončit po otevření dveří**.

Hang Up After Opening Door	
Enabled	☒
Type	Only DTMF
Time Out (Sec)	5 (0~15Sec)

- **Typ:** Specifikujte způsob otevírání dveří. Pokud je tato konkrétní metoda použita k uvolnění dveří během hovoru, zařízení ukončí hovor po dosažení přednastaveného času zavěšení.
- **Timeout(Sec):** Určete časový limit pro zavěšení. Zařízení automaticky ukončí hovor, jakmile dosáhne konkrétního času po otevření dveří.

Typ video transportu

Typ video přenosu pro náhled SIP hovoru můžete zvolit na rozhraní **Intercom > Account**. Toto nastavení se nevztahuje na IP hovory.

The screenshot shows the 'Call' settings page. It includes fields for 'Max Local SIP Port' and 'Min Local SIP Port', both set to 5062. There are checkboxes for 'Auto Answer' (checked) and 'Prevent SIP Hacking' (unchecked). The 'Video Transport Type' dropdown menu is highlighted with a blue border and shows 'Send Only' as the selected option.

- **Typ přenosu videa:** Ve výchozím nastavení je **pouze odesílaný**.
 - **Neaktivní:** Funkci deaktivovat.
 - **Pouze odesílat:** Zařízení odesílá video stream druhé straně.
 - **Pouze přijímání:** Zařízení přijímá video stream pouze od druhé strany.
 - **Odesílat a přijímat:** Zařízení může odesílat a přijímat video streamy mezi druhou stranou a zpět.

Konfigurace audio a video kodeků

Audio kodek

Zařízení podporuje tři typy kodeků (PCMU, PCMA a G722) pro kódování a dekódování zvukových dat během hovoru. Každý typ kodeku se liší kvalitou zvuku. PCMU a PCMA jsou dobře přizpůsobeny tradiční telefonii a prostředí s omezenou šířkou pásma, zatímco G722 poskytuje lepší kvalitu zvuku pro modernější komunikační potřeby.

Můžete si vybrat konkrétní kodek podle skutečného síťového prostředí.

Nastav to přes rozhraní **Interkomu > Účet**.

The screenshot shows a web interface titled "Audio Codescs". It features two main panels. The left panel, labeled "0 item Disabled Codescs", contains a "No Data" message with a folder icon. The right panel, labeled "3 items Enabled Codescs", lists three items: PCMU, PCMA, and G722, each with an unchecked checkbox. Between the panels are left and right arrow buttons. To the right of the "Enabled Codescs" panel are up and down arrow buttons.

Typ kodeku	Spotřeba šířky pásma	Vzorkovací frekvence
PCMA	64 kbit/s	8 kHz
PCMU	64 kbit/s	8 kHz
G722	64 kbit/s	16 kHz

Video kodek

Zařízení podporuje kodek H264, který poskytuje lepší kvalitu videa při mnohem nižší datové rychlosti a odlišné kvalitě videa a užitečném zatížení.

Nastavte to na webovém rozhraní **Interkom > Účet** .

Video Codec	
Name	☒ H.264
Resolution	720P
Bitrate	320 kbps
Payload	104

- **Název:** Zkontrolujte povolení formátu video kodeku H264 pro video stream zařízení.
- **Rozlišení:** Vyberte rozlišení z dostupných možností. Výchozí rozlišení je 720P(1280×720 pixelů).
- **Přenosový tok:** Přenosový tok video streamu se pohybuje od 128 do 2048 kbps. Čím vyšší je přenosový tok, tím více dat se přenáší za sekundu a tím čistší bude video. Výchozí datový tok kódu je 320.
- **Náklad:** Užitečné zatížení se pohybuje od 90 do 119 pro konfiguraci audio/video konfiguračních souborů. Výchozí hodnota je 104.

Video kodek pro IP hovory

Kvalitu videa pro IP hovor můžete zvolit správným rozlišením kodeku podle stavu sítě.

Nastavte to na webovém interkomu > **Call Feature > rozhraní Direct IP** .

Direct IP

Enabled	☒
DTMF Type	RFC2833
Port	5060 (1-65535)
Video Resolution	720P
Video Bitrate	512 kbps
Video Payload	104

- **Rozlišení videa:** Vyberte rozlišení z dostupných možností. Výchozí rozlišení je 720P (1280×720 pixelů).
- **Přenosový tok videa:** Přenosový tok video streamu se pohybuje od 128 do 2048 kbps. Výchozí přenosový tok je 512.
- **Video náklad:** Užitečné zatížení se pohybuje od 90 do 119 pro konfiguraci audio/video konfiguračních souborů. Výchozí hodnota je 104.

Nastavení relé

Místní štafeta

Lokální relé je výstup relé zabudovaný v interkomovém zařízení. Může přímo ovládat připojená zařízení, jako jsou zámky dveří, spouštěním akcí na základě uživatelského vstupu nebo autorizace.

Můžete nastavit přepínač relé a DTMF pro přístup ke dveřím na webovém rozhraní **Access Control > Relay**.

Relay ID	RelayA	RelayB
Relay Type	Default Status ▼	Default Status ▼
Mode	Monostable ▼	Monostable ▼
Trigger Delay(Sec)	0 ▼	0 ▼
Hold Delay(Sec)	5 ▼	5 ▼
DTMF Mode	1 Digit DTMF ▼	1 Digit DTMF ▼
1 Digit DTMF	0 ▼	1 ▼
2~4 Digits DTMF	010	012
Relay Status	Relay A: Low	Relay B: Low
Relay Name	RelayA	RelayB
Door Sensor	None ▼	None ▼ ?
Alarm Door Opened	☐	☐ ?
Door Opened Timeout	60	60 (1~300Sec)
Break-in intrusion	☐	☐ ?
Access Method	☒ PIN ☒ Face ☒ RF Card ☒ BLE ☒ NFC ☒ LPR Camera	☒ PIN ☒ Face ☒ RF Card ☒ BLE ☒ NFC ☒ LPR Camera
	Test	Test

- **Typ relé:** Určte interpretaci stavu relé ohledně stavu dveří:
 - **Výchozí stav:** Stav "Nízký" v poli Stav relé znamená zavřené dveře, zatímco "Vysoký" znamená, že jsou otevřené.
 - **Invert Status:** Stav "Nízký" v poli Relay Status znamená otevřené dveře, zatímco "High" znamená zavřené.
- **Režim:** Specifikujte podmínky pro automatické resetování stavu relé.
 - **Monostabilní:** Stav relé se automaticky resetuje během zpoždění relé po aktivaci.
 - **Bistabilní:** Stav relé se resetuje při opětovném spuštění relé .
- **Zpoždění spouště (Sec):** Nastavte čas zpoždění před aktivací relé. Například pokud je to nastaveno na 5 sekund, relé se aktivuje 5 sekund po stisknutí tlačítka Odemknutí.
- **Zpoždění (Sek):** Určete, jak dlouho relé zůstává aktivováno. Například pokud je relé nastaveno na 5 sekund, zůstává otevřené 5 sekund, než se zavře.
- **DTMF režim:** Nastavte číslice DTMF kódu.
- **1 číslice DTMF:** Definujte jednociferný DTMF kód v rozsahu (0-9 a *,#), když je režim DTMF nastaven na 1 číslici.
- **2~4 číslice DTMF:** Nastavte DTMF kód na základě počtu vybraných číslic v DTMF režimu.
- **Stav relé:** Označuje stavy relé, které jsou normálně otevřeno a zavřené. Ve výchozím nastavení ukazuje nízký pro normálně zavřený (NC) a vysoký pro normálně otevřený (NO).
- **Název relé:** Přiřadte odlišné jméno pro účely identifikace.
- **Senzor dveří:** Určete, které vstupní rozhraní je připojeno ke senzoru dveří.
- **Otevření alarmových dveří:** Pokud jsou aktivovány, při překročení limitu se spustí alarm.
 - **Timeout na otevření dveří:** Časový limit pro otevření dveří.
- **Vloupání:** Aktivujte alarm, když jsou dveře násilně nebo nelegálně otevřeny. Klikněte [zde](#) pro více informací o této funkci.
- **Přístupová metoda:** Zkontrolujte metodu(y) pro spuštění relé.

- **Test:** Klikněte na **Test** , abyste relé spustili ručně.

Bezpečnostní relé

Bezpečnostní relé, známé jako Akuvox SR01, je produkt navržený k posílení bezpečnosti přístupu tím, že zabraňuje neoprávněným pokusům o násilné vniknutí. Instalován uvnitř dveří přímo řídí mechanismus otevírání dveří, čímž zajišťuje, že dveře zůstanou bezpečné i v případě poškození zařízení.



Klikněte [zde](#) pro zobrazení způsobu, jak nastavit bezpečnostní relé.

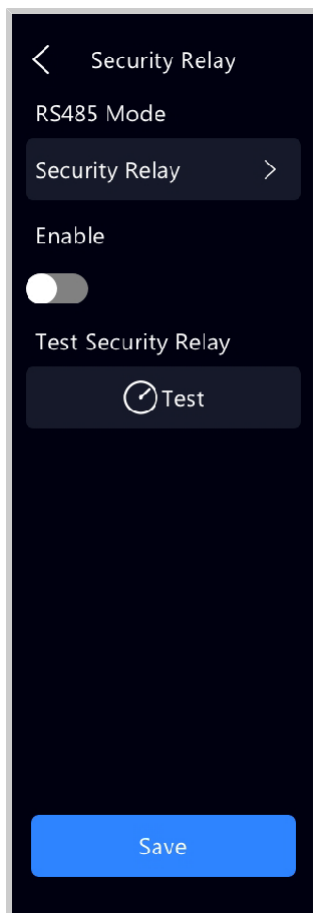
Pro nastavení bezpečnostního relé přejděte do **Access Control > Relay > Security Relay** rozhraní.

Security Relay

Relay ID	Security Relay
Connect Type	RS485
Trigger Delay(Sec)	0
Hold Delay(Sec)	5
1 Digit DTMF	2
2~4 Digits DTMF	012
Relay Name	Security Relay
Access Method	☒ PIN ☒ Face ☒ RF Card ☒ BLE ☒ NFC ☒ LPR Camera
Enabled	☐
Test	

- **Typ připojení:** Typ připojení je ve výchozím nastavení RS485. Pro použití SR01 by měl být režim RS485 nastaven na **Security Relay** na rozhraní **Access Control > RS485**.
- **Zpoždění spouštění (Sek):** Nastavte čas zpoždění před aktivací relé. Například pokud je relé nastaveno na 5 sekund, aktivuje se 5 sekund po stisknutí tlačítka Odemknutí.
- **Držení zpoždění(Sek):** Určete, jak dlouho relé zůstává aktivováno. Například pokud je relé nastaveno na 5 sekund, zůstane otevřené 5 sekund před uzavřením.
- **1-místný DTMF:** Definujte jednociferný DTMF kód v rozsahu (0-9 a *,#), když je režim DTMF v sekci Relé výše nastaven na 1-číslici.
- **2~4 číslice DTMF:** Nastavte DTMF kód na základě počtu vybraných číslic v DTMF režimu.
- **Název relé:** Pojmenujte bezpečnostní relé. Název lze zobrazit v logech otevírání dveří. Při připojení ke SmartPlus Cloudu Cloud server automaticky přiřadí název relé.
- **Metoda přístupu:** Zkontrolujte způsob přístupu, který může spustit bezpečnostní relé.
- **Test:** Klikněte pro odeslání signálu do SR01. Když se zařízení a SR01 párují, klikněte na **Test** pro dokončení párování.

Bezpečnostní relé můžete také zapnout na obrazovce **Nastavení > Security > Security Relay**.



Web Relay

Webové relé má vestavěný webový server a může být ovládáno přes internet nebo lokální síť. Zařízení může použít webové relé buď k ovládání lokálního relé, nebo vzdáleného relé někde jinde v síti.



Klikněte [zde](#) a zjistěte, jak nastavit webové relé.

Pro nastavení přejděte do **Access Control > rozhraní Web Relay**.

Web Relay

Type

Disabled

Authorization Mode

None

IP Address

Username

Password

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
01			
02			
03			
04			
05			
06			

- **Typ:** Určit typ relé aktivovaného při použití metod vstupu ke dveřím.
 - **Zakázáno:** Aktivujte pouze lokální relé.
 - **Pouze webové relé:** Aktivujte pouze webové relé.

- **Lokální i webové relé:** Aktivujte jak lokální relé, tak webové relé. Obvykle se nejprve spustí lokální relé, následované webovým relé.
- **IP adresa:** IP adresa webového relé poskytovaná výrobcem webového relé.
- **Uživatelské jméno:** Uživatelské jméno poskytnuté výrobcem webového relé.
- **Heslo:** Autentizační klíč poskytnutý výrobcem pro webové relé. Autentizace probíhá přes HTTP. Ponechat pole Heslo prázdné znamená nepoužití HTTP autentizace. Heslo můžete definovat pomocí HTTP GET v poli Web Relay Action.
- **Akce webového relé:** Nastavte akce, které má webové relé provádět při spuštění. Zadejte výrobcem poskytnuté URL adresy pro různé akce až s 50 příkazy.

POZNÁMKA

Pokud URL obsahuje celý HTTP obsah (např. `http://admin:admin@192.168.1.2/state.xml?relayState=2`), nezávisí na IP adrese, kterou jste zadali výše. Pokud je však URL jednodušší (např. `state.xml?relayState=2`), relé používá zadanou IP adresu.

- **Klíč pro webové relé:** Určte metody aktivace webového relé na základě toho, zda je DTMF kód vyplněn.
- Vyplnění s nakonfigurovaným DTMF kódem omezuje aktivaci pouze na přejetí karty a DTMF.
 - Ponechání prázdného umožňuje všechny způsoby otevírání dveří.
 - **Rozšíření Web Relay:** Specifikujte interkom zařízení a metody, které může použít k aktivaci webového relé během hovorů.
 - Když je specifikována IP/SIP interkomového zařízení, pouze toto zařízení může během hovorů spustit webové relé (kromě přejetí karty nebo DTMF).
 - Pokud je volba prázdná, všechna zařízení mohou během hovorů spustit relé.

Správa časové harmonogramu řízení přístupu

Harmonogram přístupu ke dveřím vám umožňuje rozhodnout, kdo a kdy může dveře otevřít. Platí jak pro jednotlivce, tak pro skupiny, což zajišťuje, že uživatelé v rámci rozvrhu mohou dveře otevřít autorizovanou metodou pouze v určených časových obdobích.

Vytvořte harmonogram přístupu ke dveřím

Můžete si vytvořit rozpisy přístupu ke dveřím pro denní, týdenní nebo vlastní časová období.

Nastavte to ve webovém rozhraní **Directory > Schedule**. Můžete přidat 100 lokálních rozvrhů.

The screenshot shows the 'Schedule' management page. At the top, there are buttons for 'Search', '+ Add', 'Import', and 'Export'. Below is a table with the following columns: Index, Schedule ID, Source, Mode, Name, Date, Day of Week, Time, and Edit. Two schedules are listed: Index 1 (Schedule ID 1002, Local, Daily, Never, --, --, --) and Index 2 (Schedule ID 1001, Local, Daily, Always, --, --, 00:00-23:59:59). At the bottom, there are controls for 'Selected: 0/2', 'Delete', 'Delete All', 'Total: 2', 'Prev', '1/1', 'Next', 'Go To Page 1', and 'Go'.

Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
1	1002	Local	Daily	Never	--	--	--	
2	1001	Local	Daily	Always	--	--	00:00-23:59:59	

The screenshot shows the 'Add Schedule' modal form. It includes fields for 'Mode' (set to 'Normal'), 'Name', 'Start Date - End Date' (20260703 ~ 20260703), 'Day' (checkboxes for Mon, Tue, Wed, Thur, Fri, Sat, Sun, with 'Check All' option), 'Start Time - End Time' (00:00 - 23:59), and 'Holiday Exemption' (checkbox). 'Cancel' and 'Submit' buttons are at the bottom.

- **Režim:**
 - **Normální:** Nastavte rozvrh podle měsíce, týdne a dne. Používá se pro dlouhodobý rozvrh.
 - **Týdenně:** Nastavte rozvrh podle týdne.
 - **Denně:** Nastavte si rozvrh podle 24 hodin denně.
- **Název programu:** Uved'te rozvrh.
- **Osvobození od svátků:** [Sváteční rozvrh](#) je vyšší přednost před harmonogramem přístupu, který omezuje uživatele v otevírání dveří. Pokud chtějí uživatelé otevírat dveře během svátků v rámci harmonogramu přístupu, musíte tuto možnost zaškrtnout.

Plán importu a exportu přístupu ke dveřím

Kromě samostatného rozvrhu přístupu ke dveřím můžete také pohodlně importovat nebo exportovat rozvrhy, abyste maximalizovali efektivitu správy rozvrhu přístupu ke dveřím.

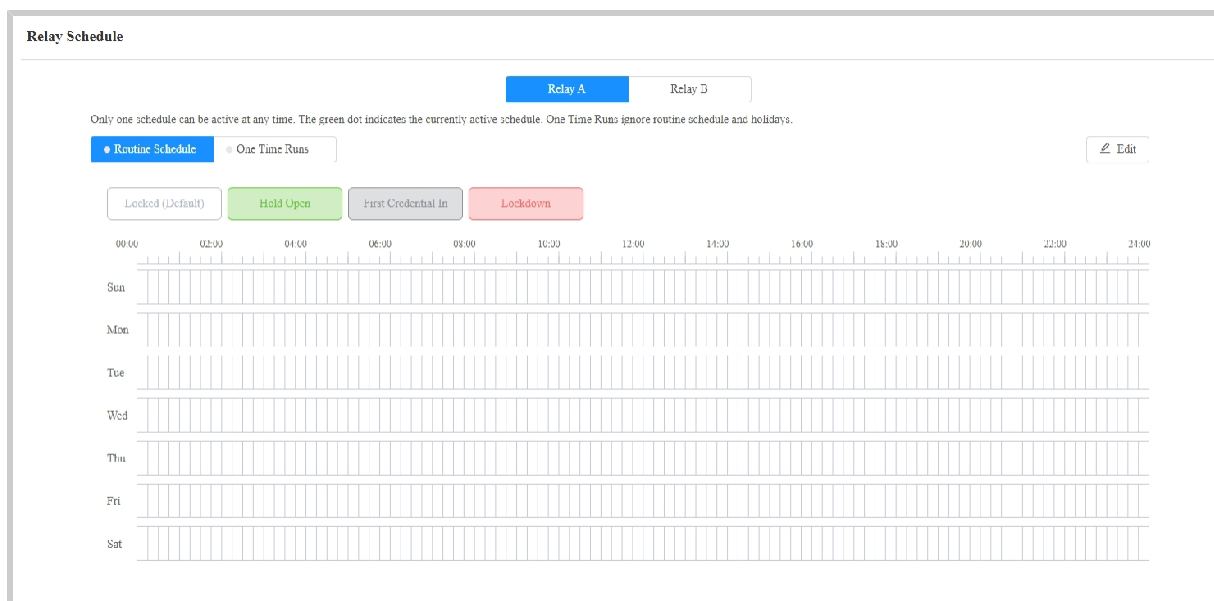
Pro nastavení přejděte do rozhraní **Directory > Schedule**. Importovaný soubor by měl být ve **formátu XML**.

Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
1	1002	Local	Daily	Never	--	--	-	
2	1001	Local	Daily	Always	--	--	00:00:00-23:59:59	

Harmonogram relé

Rozvrh relé umožňuje nastavit konkrétní relé, které se vždy otevírá v určitou dobu. To je užitečné v situacích, jako je ponechat bránu otevřenou po škole nebo otevřenou během pracovní doby.

Pro nastavení rozvrhu relé přejděte do rozhraní **Access Control > Relay > Relay Schedule**.



- **Typ opakování:**
 - **Rutinní rozvrh:** Rozvrh se opakuje každý týden. Klikněte na **Upravit** vpravo pro nastavení.
 - **Jednorázové běhy:** Nastavte denní nebo týdenní rozvrh, který se opakuje během definovaného období.
- **Režim rozvrhu:**
 - **Držet otevřeno:** Dveře zůstávají otevřené po plánovanou dobu.
 - **První přihlašovací údaje:** Dveře zůstávají otevřené po plánovaném čase po prvním použití přihlašovacích údajů uživatelem.
 - **Uzamčení:** Dveře zůstávají zavřené během plánované doby.

Poznámka

Klikněte [zde](#) pro zobrazení podrobné konfigurace každého režimu jízdního plánu.

Program pro svátky

Můžete definovat svátky, kdy uživatelé nemohou otevírat dveře, aby se zvýšila bezpečnost kontroly přístupu. Můžete také nastavit pracovní dobu tak, aby oprávnění uživatelé mohli otevírat dveře.

Nastavte si ji v rozhraní **Directory > Holiday** . Můžete si vybrat, zda chcete zobrazit místní svátky, SmartPlus Cloud svátky, nebo obojí.

Klikněte na **+Přidat** pro nastavení místního svátečního rozvrhu.

Holiday

All

Search

+ Add

Import

Export

	Index	Source	Name	Repeat By Year	Edit
No Data					

Selected:0/0

Delete

Delete All

Total 0

Prev

1/1

Next

Go To Page 1

Go

Calendar

Holiday Name

Repeat By Year

Year 2026

Working Hours

Clear

January	February	March	April	May	June
Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
July	August	September	October	November	December
Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29	Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

- **Název svátku:** Zadejte název svátku.
- **Opakujte podle roku:** Opakujte rozvrh každý rok.
- **Rok:** Stanovte rok a datum svátku.
- **Pracovní doba:** Když je zapnuta, určete čas, kdy mohou oprávnění uživatelé otevírat dveře.

Sváteční rozvrh Import/Export

Rozvrhy svátků můžete importovat nebo exportovat pro rychlé nastavení v rozhraní **Directory > Holiday > Import/Export Holiday**.

Formát import/export souboru je .xml.

Holiday

All

Search

+ Add

Import

Export

☐	Index	Source	Name	Repeat By Year	Edit
No Data					

Selected 0/0

Delete

Delete All

Total:0

Prev

1/1

Next

Go To Page

1

Go

Konfigurace otevírání dveří

Odemknutí pomocí veřejného PIN kódu

Existují dva typy PIN kódů pro přístup ke dveřím: veřejné a soukromé. Soukromý PIN je jedinečný pro každého uživatele, zatímco veřejný je sdílen obyvateli stejné budovy nebo komplexu. Můžete vytvářet a upravovat jak veřejné, tak soukromé PIN kódy.

Nastavte to na webovém rozhraní **Access Control > PIN > rozhraní Public Key**.

Public Key	
Enabled	☒
PIN Code	***** (5~8 digits)

- **PIN kód:** Nastavte 5 až 8 číslic pro otevírání dveří. Výchozí je 33333333.

Uživatelsky specifické metody přístupu

Soukromý PIN kód, RF karta, obličej a registrační značka by měly být přiřazeny konkrétnímu uživateli pro otevírání dveří.

Při přidávání uživatele můžete také upravit nastavení, například definovat harmonogram přístupu ke dveřím, abyste určili, kdy je kód platný, a specifikovat, který relé otevřít.

Pro přidání uživatele přejděte do **adresáře > uživatelského** rozhraní a klikněte na **+Přidat**.

User Basic	
User ID	1
Name	

- **Uživatelské ID:** Jedinečné identifikační číslo přiřazené uživateli.
- **Jméno:** Jméno tohoto uživatele.

Odemknout pomocí soukromého PIN

Uživatelé mohou otevírat dveře zadáním svých soukromých PIN kódů na klávesnici.

V **adresáři** > **uživatelském** > **+Add** rozhraní přejděte do sekce **Soukromý PIN**.

Private PIN	
Code	
	

- **Kód:** Nastavte 2–8místný PIN kód výhradně pro použití tohoto uživatele. Každému uživateli může být přiřazen pouze jeden PIN kód.

Použití soukromého PIN kódu můžete povolit/vypnout na webovém nastavení **Access Control** > **PIN** > rozhraní **Private PIN**. Je to ve výchozím nastavení povoleno.

Private PIN	
Enabled	☒

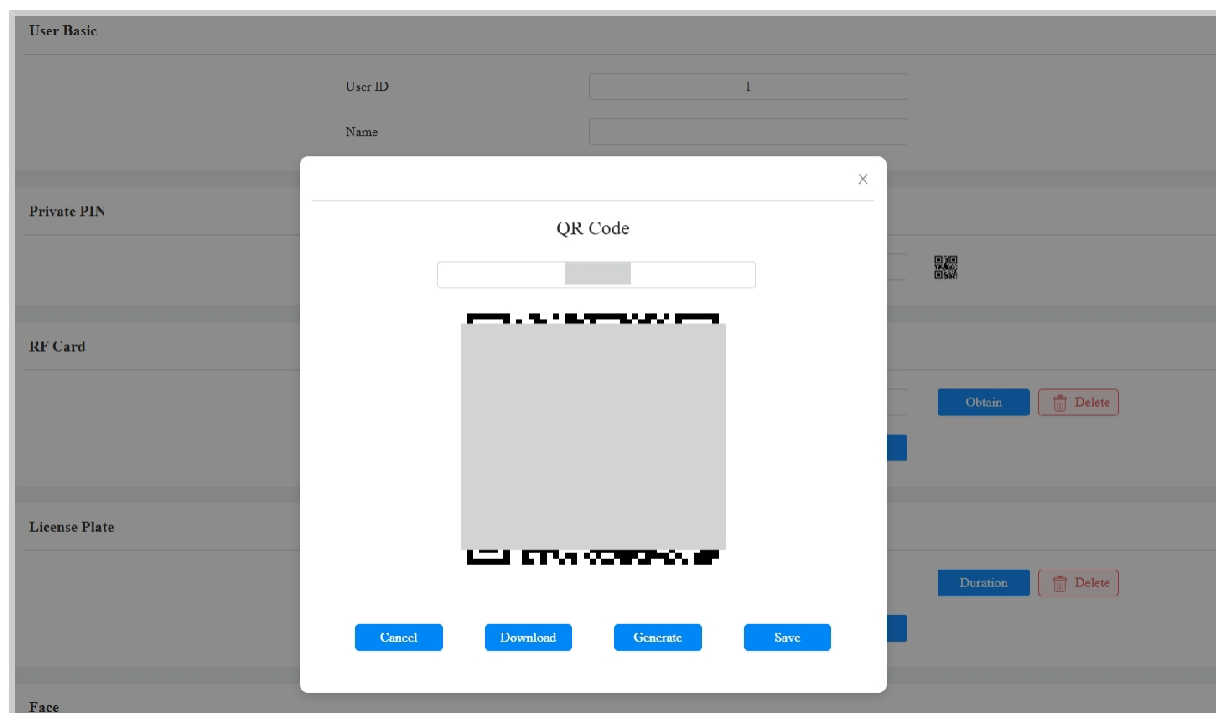
Odemknout pomocí QR kódu

Zařízení podporuje skenování QR kódů generovaných přímo na místě a **generovaných SmartPlus Cloud pomocí cloudu**.

Na **Adresář** > **uživatelský** > **+Add** rozhraní, posuňte se na **Soukromý PIN** sekce. Klikněte na ikonu QR kódu.

Private PIN	
Code	
	

Klikněte na **Generovat** pro vygenerování QR kódu s 8místným PINem.



- **Zrušit:** Klikněte pro návrat do uživatelského rozhraní pro úpravy. QR kód a PIN kód nebudou uloženy.
- **Stažení:** Klikněte pro uložení QR kódu do vašeho počítače.
- **Vygenerovat:** Klikněte pro vygenerování dalšího QR kódu a PIN kódu.
- **Uložit:** Klikněte pro návrat do uživatelského editačního rozhraní a uložte kódy.

Používání QR kódu povolíte nebo zakážete v rozhraní **Access Control > Relay > Open Relay Methods**.

Je to ve výchozím nastavení povoleno.

Relay Methods

Via HTTP
Enabled
☐

Via QR Code
Enabled
☒

Via DTMF
Enabled
☒

Assigned The Authority For

Only Contacts List

Odemknutí pomocí RF karty

V **adresáři** > **uživatelském** > **+Add** rozhraní přejděte do sekce **RF Card** .

RF Card

Code

Obtain

Delete

Add

- **Kód:** Číslo karty, které čtečka karet čte.

Poznámka:

- Každý uživatel může mít přidáno maximálně 5 karet.
- Zařízení umožňuje přidat 5 000 uživatelů.
- RF karty pracující na frekvencích 13,56 MHz jsou kompatibilní se zařízením pro přístup.

Používání RF karet můžete povolit a vypnout v rozhraní **Access Control** > **Card Settings**.

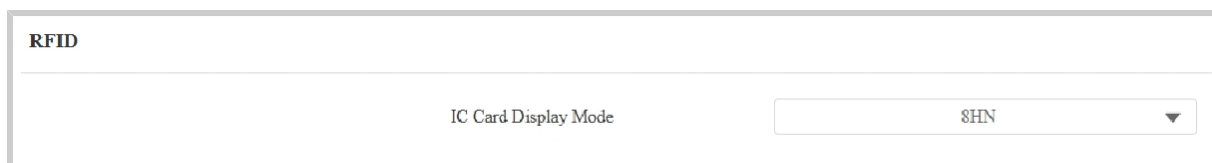
Card Type

Enabled
☒ IC Card
☒ NFC

Formát kódu RF karty

Pro integraci přístupu k dveřím RF karty s interkomovým systémem třetí strany je potřeba sladit formát kódu RF karty s tím, který používá třetí stranový systém.

Pro nastavení přejděte do **Nastavení přístupu > karty > RFID** rozhraní.



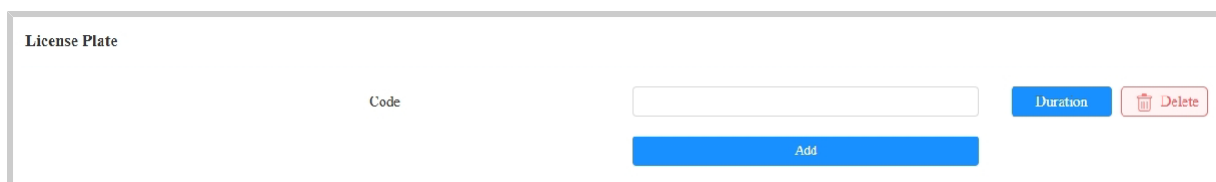
- **Režim zobrazení karty IC:** Nastavte formát čísla karty z dostupných možností.

Odemknout podle registrační značky

Akuvox nabízí dva hlavní způsoby, jak identifikovat vozidla a otevírat brány.

- Použijte [kameru třetí strany LPR \(rozpoznávání registračních značek\)](#) k rozpoznání registrační značky vozidla.
- Použijte [dlouhodobou čtečku karet Akuvox ACR-CPR12](#) k rozpoznání UHF karty připevněné na čelním skle vozidla.

Pro přiřazení registrační značky uživateli najděte část **Registrační značka** v **adresáři > uživatelském > +Add**.



- **Přidat:** Uživatel může mít až 5 registračních značek.
- **Doba trvání:** Povolit/vypnout dlouhodobé vozidlo. Je to ve výchozím nastavení povoleno. Pokud je deaktivováno, uveďte, kdy může vozidlo vstoupit nebo vystoupit z parkoviště.

Odemknout pomocí rozpoznávání obličeje

V **adresáři > uživatelském > + Add** rozhraní přejděte do sekce **Obličej** .
Klikněte na **Import** pro nahrání obrázku a **Reset** pro její odstranění .

Face	
Status	Unregistered
Face	Import + Obtain Reset

- **Import:** Klikněte pro nahrání fotografie obličeje.
- **Získáte:** Klikněte pro zahájení zápisu obličeje na straně zařízení.
- **Resetovat:** Klikněte pro odstranění registrovaného obrázku obličeje.

Poznámka

Formát podpory: jpg, png. Velikost: maximálně 2 MB.

Nastavení rozpoznávání obličeje

Zařízení umožňuje upravovat přesnost rozpoznávání obličeje, intervaly rozpoznávání a další pro zlepšení uživatelského zážitku.

Pro nastavení přejděte do rozhraní **Nastavení Přístupové kontroly > Face Settings**.

Face Basic	
Facial Recognition Enabled	☒
Offline Learning Enabled	☒
Facial Recognition Matching Level	Normal ▼
Anti-Spoofing Option	High ▼
Facial Recognition Interval(Sec)	5 ▼
Visitor Friendly Mode	☐ ?
No Face Detected Interval (sec)	1 ▼
Face Detection Distance (M)	3 ▼

- **Rozpoznávání obličeje zapnuto:** Zapnout/vypnout funkci rozpoznávání obličeje.
 - **Offline učení:** Přesnost rozpoznávání obličejů se zlepšuje s rostoucím počtem rozpoznávání obličejů.
 - **Úroveň rozpoznávání obličeje:** Zjistěte, jak přísný je systém rozpoznávání obličeje při porovnávání obličeje osoby s nahranými daty o obličeji. Každá úroveň umožňuje odlišný rozdíl v zakrývání obličeje (**s výjimkou oblasti úst**), aby prošel rozpoznáním.
- Nízká: Povolit mírné rozdíly oproti nahraným datům o obličeji, s malým pokrytím obličeje.
- Nejvyšší: Vyžadovat, aby obličej byl identický s nahraným tělem, s minimálním nebo žádným zakrytím.
- Další dvě úrovně jsou někde mezi tím.
- **Možnost proti falšování:** Nastavte přísnost systému v prevenci falešných tváří.
- Zavřít: Deaktivovat funkci anti-spoofing obličeje. Ověření obličeje lze provést pomocí neživých náhrad za obličej oprávněné osoby, například fotografie.
- Nejvyšší: Systém nelze oklamat žádnými neživými náhradami za tvář oprávněné osoby.
- Ostatní tři úrovně jsou někde mezi tím.
- **Interval rozpoznávání obličeje (Sec):** Upravte časový interval mezi jednotlivými pokusy o rozpoznání obličeje, v rozmezí od 1 do 8 sekund.
 - **Režim přátelský k návštěvám:** Nastavit, zda při selhání rozpoznání dát zvukové nebo vizuální pokyny. Výchozí deaktivace.
 - **Interval(sek) bez detekce obličeje:** Upravte časový interval mezi jednotlivými detekcemi v rozmezí od 1 do 8 sekund.
 - **Vzdálenost detekce obličeje (M):** Upravte detekční vzdálenost v rozsahu od 1 do 3 metrů.

Odemknutí pomocí Bluetooth

Zařízení podporuje otevírání dveří pomocí Bluetooth aplikace My MobileKey nebo SmartPlus. Uživatelé mohou dveře otevřít s aplikacemi v kapse, nebo mávat telefonem směrem k zařízení, když se přibližují ke dveřím.

Poznámka

Před použitím Bluetooth k otevírání dveří je potřeba povolit funkci Bluetooth na rozhraní **Access Control > BLE**.

Odemknout přes My MobileKey

V **adresáři > uživatelském rozhraní > +Add** přejděte do **sekce BLE Settings**.

BLE Setting	
Authentication Code	Generate Delete
Status	Unpaired
Pairing Valid Until	N/A

- **Autentizační kód:** Klikněte na **Generovat** pro vygenerování 6místného ověřovacího kódu.

Nastavení odemykání přes Bluetooth

Nastavte funkci odemykání přes Bluetooth v rozhraní **Access Control > BLE**.

BLE Basic

Enable BLE Function
☒

Enable Hands Free Mode
☒

RSSI Threshold
(-85~-50db)

Unlock Interval For Same User (Sec)
(5~900Sec) ?

Unlock Interval For Different Users (Sec)
(5~900Sec) ?

- **Zapnout režim hands-free: Pokud je povolen, uživatelé mohou získat přístup ke dveřím bez použití ruky. Pokud je režim vypnutý, musí uživatelé mávat rukama u zařízení, aby otevřeli dveře.**
- **RSSI práh: Nastavte sílu přijímaného signálu. Vyšší hodnoty znamenají silnější signál, což usnadňuje příjem Bluetooth signálu.**
- **Odemknutí intervalu pro stejného uživatele(sek):** Nastavte časový interval mezi po sobě jdoucími pokusy o přístup přes Bluetooth ke dveřím pro jednoho uživatele.
- **Odemknutí intervalu pro různé uživatele(sek):** Nastavte časový interval mezi po sobě jdoucími pokusy o přístup přes Bluetooth u různých uživatelů.

Poznámka

Pro podrobné kroky konfigurace různých přístupových metod založených na Bluetooth klikněte na následující články.

- [Odemkněte přes Bluetooth přes aplikaci My MobileKey.](#)
- [Odemkněte přes Bluetooth přes aplikaci SmartPlus.](#)

Nastavení přístupu

Můžete si přizpůsobit nastavení přístupu, například definovat rozvrh přístupu ke dveřím, abyste zjistili, kdy je kód platný, a specifikovat, který relé otevřít.

V rozhraní **Directory > User > +Add** přejděte do sekce **Nastavení přístupu**.

- **Povolit otevření:** Povolte otevření dveří.
- **První přihlašovací údaje:** To rozhoduje, zda uživatel může udržet dveře otevřené po **plánovaném čase** po jejich aktivaci.
- **Obcházení uzamčení:** To rozhoduje, zda uživatel může otevřít dveře, když jsou zamčené v **plánovaném čase**.
- **Patro č. :** Zadejte uživateli přístupné patro pomocí výtahu.
- **Web Relay:** Zadejte ID příkazů k akci webového relé, které jste nastavili v rozhraní Web Relay. Výchozí hodnota 0 znamená, že webové relé nebude spuštěno.
- **Plán:** Umožněte uživateli otevřít určené dveře během přednastavených období přesunem požadovaného rozvrhu(ů) z levého pole do pravého. Kromě vlastních rozvrhů existují 2 výchozí možnosti:
 - **Vždy:** Umožňuje otevírání dveří bez omezení počtu otevřených dveří během platné doby.
 - **Nikdy:** Zakazuje otevírání dveří.

Import/export uživatelských dat

Zařízení podporuje sdílení uživatelských dat o řízení přístupu mezi zařízeními Akuvox prostřednictvím importu a exportu.

Klikněte [zde](#) pro zobrazení způsobu, jak importovat a exportovat uživatelská data mezi zařízeními Akuvox.

Pro nastavení přejděte do **uživatelského** rozhraní **Directory** > .
Zařízení podporuje až 5 000 uživatelů.

Import/Export User	
User Data	Import Export ▼

- **Import:** Podporovaný formát je TGZ.
- **Export:** Podporovaný formát je CSV nebo XML.

Odemčení pomocí NFC

NFC (Near Field Communication) je oblíbený způsob přístupu ke dveřím. Využívá rádiové vlny pro přenos dat. Zařízení lze odemknout pomocí NFC. Mobilní telefon můžete držet blíže k zařízení pro přístup ke dveřím.

Pro nastavení přejděte do rozhraní **Nastavení** > **karty** > **Card Control** rozhraní.

Card Type
Enabled ☒ IC Card ☒ NFC

Poznámka

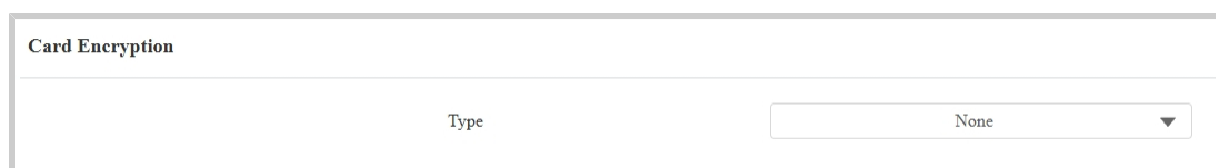
- Funkce NFC není na iPhonech dostupná.
- Klikněte [zde](#) a zjistěte, jak otevírat dveře přes NFC.

Mifare Card

Zařízení dokáže číst šifrované Mifare karty pro vyšší bezpečnost. Když je tato funkce zapnuta, čte data z určených sektorů a bloků karet, nikoli z UID.

Klikněte [zde](#) pro zobrazení detailů šifrování a čtení karet Mifare.

Pro nastavení přejděte do **Nastavení přístupu > Card Settings > rozhraní šifrování Mifare karet**.



Card Encryption	
Type	None ▼

- **Klasika:**
 - **Sektor/blok:** Určete místo, kde jsou uložena šifrovaná data karty . Mifare karta má 16 sektorů (očíslovaných od 0 do 15) a každý sektor má 4 bloky (očíslované od 0 do 3).
 - **Blokový klíč:** Nastavte heslo pro přístup k datům uloženým v předdefinovaném sektoru/bloku.
- **Navíc:** Můžete nastavit tři možnosti. To znamená, že můžete použít tři typy karet Mifare Plus. Při přejetí kartou, pokud jedna z možností odpovídá jejímu SL klíči, bude vytištěn kód karty v bloku, který jste zadali.
 - **Blok:** Určete blok(y), které mají být čteny.
 - **SL1:** Klíčové číslo v rámci 32 bitů.
 - **SL3:** Klíčové číslo v rámci 32 bitů.
- **DESFire:**
 - **ID aplikace:** 6místné hexadecimální číslo
 - **ID souboru:** ID zašifrovaného souboru aplikace, které může mít číslo od 0 do 16.
 - **Krypto:** Šifrovací metoda.
 - **Klíč:** Souborový klíč.
 - **Index klíče:** Indexové číslo klíče, které může být číslo od 0 do 11.

Odemknutí pomocí DTMF kódu

Dvoutónové vícefrekvenční signalizace (**DTMF**) je způsob přenosu signálů přes telefonní linky pomocí různých frekvenčních pásem. Uživatelé mohou pomocí funkce DTMF odemknout dveře návštěvníkům během hovoru buď zadáním DTMF kódu na softwarové klávesnici, nebo klepnutím na záložku odemykání s DTMF kódem na obrazovce.

Pro konfiguraci DTMF kódů přejděte do rozhraní **Access Control > Relay**.

Relay ID	RelayA	RelayB
Relay Type	Default Status	Default Status
Mode	Monostable	Monostable
Trigger Delay(Sec)	0	0
Hold Delay(Sec)	5	5
DTMF Mode	1 Digit DTMF	1 Digit DTMF
1 Digit DTMF	0	1
2-4 Digits DTMF	010	012
Relay Status	Relay A: Low	Relay B: Low
Relay Name	RelayA	RelayB
Door Sensor	None	None
Alarm Door Opened	☐	☐
Door Opened Timeout	60	60 (1~300Sec)
Break-in intrusion	☐	☐

- **DTMF režim:** Nastavte počet číslic pro DTMF kód.
- **1 číslice DTMF:** Definujte jednociferný DTMF kód v rozsahu (0-9 a *,#), když je režim DTMF nastaven na 1 číslici.
- **2-4místný DTMF:** Nastavte DTMF kód podle počtu vybraných číslic v DTMF režimu.

Poznámka

Pro otevření dveří pomocí DTMF musí interkomová zařízení, která odesílají a přijímají příkaz k odemýkání, používat stejný režim a kód. Jinak může odemčení DTMF selhat. Podrobné [kroky konfigurace DTMF](#) naleznete zde.

DTMF Bílý seznam

Pro zabezpečení přístupu ke dveřím pomocí DTMF kódů můžete nastavit DTMF whitelist na rozhraní zařízení **Web Access Control > Relay > Relay Methods**, takže pouze čísla volajících, která jste v zařízení zadali, mohou použít DTMF kód k získání přístupu ke dveřím.

Relay Methods	
Via HTTP	Enabled ☐
Via QR Code	Enabled ☒
Via DTMF	Enabled ☒
Assigned The Authority For: Only Contacts List ▼	

- **Přidělena pravomoc k:** Specifikujte kontakty oprávněné otevírat dveře přes DTMF:
 - **Pouze seznam kontaktů:** Dveře lze otevřít přidáním čísel do seznamu kontaktů zařízení stisknutím tlačítka.
 - **Všechna čísla:** Jakákoli čísla lze odemknout pomocí DTMF.

Přenos dat DTMF

Pro dosažení přístupu ke dveřím pomocí DTMF kódu nebo jiných aplikací je nutné správně nakonfigurovat DTMF, aby bylo možné navázat přenos dat založený na DTMF mezi zařízením a ostatními interkomy.

Rozdíly mezi typy DTMF:

Inband	DTMF signály jsou přenášeny ve stejném audio kanálu jako hlasová data. Jednoduchá implementace, ale u vysoce komprimovaných kodeků (např. G.729) může dojít ke zkreslení signálu.
RFC2833	Přenáší DTMF jako speciální událostní pakety přes RTP (Real-Time Transport Protocol), známý jako off-of-band transmission. Spolehlivé a neovlivněné kodeky.
Informace	Odesílá DTMF signály přes SIP (Session Initiation Protocol) signalizační kanál. Oddělené od hlasového přenosu, což zajišťuje kvalitu zvuku.
Info+Inband	Kombinuje informace a metody Inband.
Info+RFC2833	Kombinuje metody Info a RFC2833.
Info+Inband+RFC2833	Všechny tři metody se používají současně.

Nastavte to na rozhraní **Interkom > účet > DTMF**.

DTMF

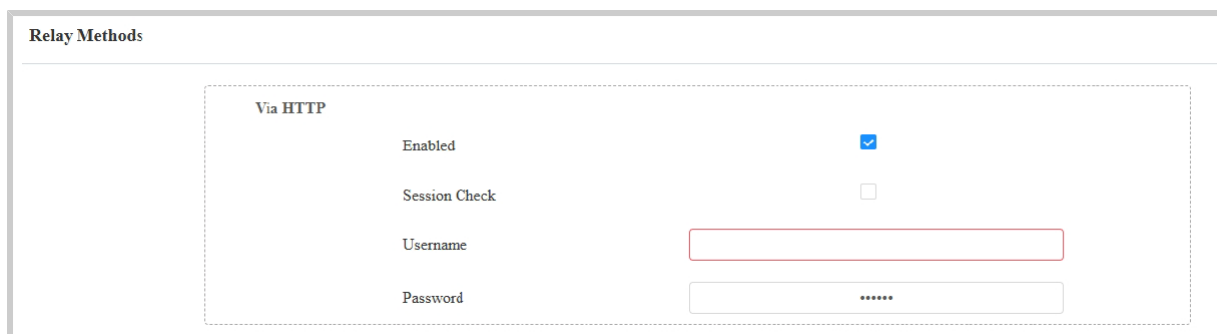
Type	Info+Inband+RFC2833	▼
How To Notify DTMF	Disabled	▼
Payload	101	(96-127)

- **Typ:** Vyberte z následujících možností: **Inband**, **RFC2833**, **Info**, **Info+Inband**, **Info+RFC2833**, na základě konkrétního typu DTMF přenosu zařízení třetí strany, které má být spárováno jako strana pro příjem signálních dat.
- **Jak informovat DTMF:** Vyberte **Disabled**, **DTMF**, **DTMF-Relay** nebo **Telephone-Event** podle konkrétního typu zařízení třetí strany. Nastavit ji musíte pouze tehdy, když zařízení třetí strany, které chcete spárovat, přejde do režimu **Info**.
- **Užitečné zatížení:** Nastavte užitečné zatížení podle konkrétního přenosového zatížení dat, na kterém se odesílatel a příjemce dohodnou během přenosu dat.

Odemknutí pomocí HTTP příkazů

Zařízení podporuje vzdálené odemykání dveří pomocí HTTP příkazu. Jednoduše tuto funkci povolte a zadejte HTTP příkaz (URL) pro zařízení. Tím se spustí relé a dveře se otevřou, i když jsou uživatelé od zařízení pryč.

Nastavte to na rozhraní **Access Control > Relay > Open Relay Methods**.



The screenshot shows the 'Relay Methods' configuration interface. A dashed box highlights the 'Via HTTP' section. Inside this section, there are four settings: 'Enabled' with a checked checkbox, 'Session Check' with an unchecked checkbox, 'Username' with an empty text input field, and 'Password' with a masked text input field (displayed as '*****').

- **Kontrola relace:** Povolte pro zvýšení bezpečnosti přenosu dat.
- **Uživatelské jméno:** Nastavte uživatelské jméno pro autentizaci v HTTP příkazových URL adresách.
- **Heslo:** Nastavte heslo pro autentizaci v HTTP příkazových URL.

Tip

Zde je příklad HTTP URL pro spouštění relé.

Device's IP
http://192.168.35.127/fcgi/do? action=OpenDoor&

Preset credentials for authentication
UserName=admin&Password=123458

ID of Relay to be triggered
DoorNum=1

Poznámka

HTTP formát pro spouštění relé se liší podle toho, zda je zařízení zapnutý režim vysokého zabezpečení. Pro více informací se prosím podívejte na tento návod [Opening the Door via HTTP Command](#).

Odemknout tlačítkem Exit

Když uživatelé potřebují otevřít dveře zevnitř stisknutím tlačítka Výstup, je potřeba nastavit vstupní terminál odpovídající tlačítku Výstup, aby aktivoval relé pro přístup ke dveřím.

Klikněte [zde](#) pro sledování instruktážního videa.

Pro nastavení přejděte do rozhraní **Access Control > Input**.

Input ID	Input A	Input B	Input C	Input D
Enabled	☒	☒	☒	☒
Trigger Electrical Level	Low	Low	Low	Low
Action to Execute	☐ FIP ☐ SIP Call ☐ Email ☐ HTTP	☐ FIP ☐ SIP Call ☐ Email ☐ HTTP	☐ FIP ☐ SIP Call ☐ Email ☐ HTTP	☐ FIP ☐ SIP Call ☐ Email ☐ HTTP
HTTP URL				
Action Delay	0	0	0	0 (0-300Sec)
Action Delay Mode	Unconditional Execution	Unconditional Execution	Unconditional Execution	Unconditional Execution
Door Sensor Associated Relay	None	None	None	None
Execute Relay	None	None	None	None
Door Status	High	High	High	High

- **Povoleno:** Pro použití specifického vstupního rozhraní.
- **Spustit elektrickou úroveň:** Nastavte vstupní rozhraní tak, aby spouštělo nízkou nebo vysokou elektrickou úroveň.
- **Akce k vykonání:** Nastavte požadované akce, které nastanou, když je spuštěno konkrétní vstupní rozhraní.
 - **FTP:** Pošlete screenshot na přednastavený [FTP server](#).
 - **E-mail:** Pošlete screenshot předkonfigurované [E-mail Adresa](#) .
 - **SIP hovor:** Zavolejte přednastavené [číslo](#) při spuštění.
 - **HTTP:** Po spuštění lze HTTP zprávu zachytit a zobrazit v odpovídajících paketech. Pro využití této funkce povolte HTTP server a zadejte obsah zprávy do určeného pole níže.
- **HTTP URL:** Zadejte HTTP zprávu, pokud jako akci pro spuštění zvolíte HTTP. Formát je obsah IP/zprávy [http://HTTP serveru](http://HTTP_serveru).
- **Zpoždění akce:** Určete, o kolik sekund zpoždovat provádění přednastavených akcí.
- **Režim zpoždění akce:**
 - **Bezpodmínečné provedení:** Akce bude provedena ve chvíli, kdy je vstup spuštěn.
 - **Spustit, pokud je vstup stále spuštěn:** Akce bude provedena, když vstup zůstane aktivovaný. Například pokud dveře zůstanou otevřené po spuštění vstupu, bude odeslána akce, například e-mail, aby upozornila příjemce.
- **Relé přidružené ke senzoru dveří:** To indikuje relé připojené k vstupu, když je vstup nastaven jako **senzor dveří**. Zobrazuje **Žádné**, pokud vstup není spojen s žádným relé.
- **Spustit relé:** Specifikovat, že relé se aktivuje při spuštění vstupu. To není kompatibilní s funkcí průniku. Stejný vstup nemůže fungovat jak pro senzor dveří, tak pro tlačítko pro výstup.
- **Stav dveří:** Zobrazit stav vstupního signálu.

Monitor a obraz

MJPEG a RTSP jsou hlavní typy monitorovacích proudů diskutované v této kapitole.

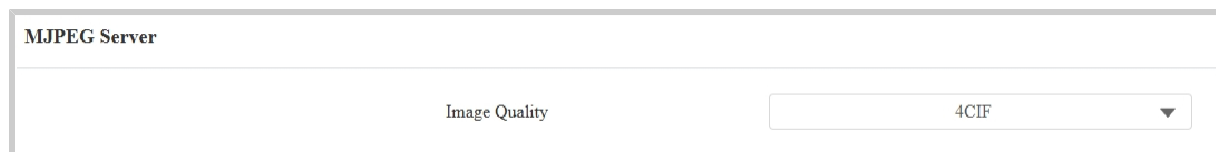
MJPEG, neboli Motion JPEG, je formát komprese videa, který používá JPEG obrázky pro každý video snímek. Zařízení Akuvox zobrazují živé přenosy na webovém rozhraní a pořizují monitorovací snímky ve formátu MJPEG. Nastavení související s MJPEG určují kvalitu videa a stav zapnutí/vypnutí funkce živého přenosu.

RTSP znamená Real Time Streaming Protocol (Protokol pro streamování v reálném čase). Lze jej použít ke streamování videa a zvuku z kamer třetích stran do zařízení. Stream kamery můžete přidat přidáním jeho URL. URL formát zařízení Akuvox je rtsp://Device's IP/live/ch00_0

ONVIF je fórum pro otevřené síťové video rozhraní. Umožňuje zařízení skenovat a objevovat kamery nebo interkomy s aktivovanými funkcemi ONVIF. Živé přenosy získané přes ONVIF jsou v podstatě ve formátu RTSP.

Zachycení obrázků v MJPEG

Funkce MJPEG je ve výchozím nastavení zapnutá. Kvalitu obrazu si můžete zvolit v rozhraní **Surveillance > MJPEG**.



The screenshot shows a web interface titled "MJPEG Server". Below the title bar, there is a label "Image Quality" and a dropdown menu. The dropdown menu is currently set to "4CIF", with a small downward arrow indicating it can be expanded.

Zadáním konkrétní URL do prohlížeče lze z kamery zobrazit buď obrázek, nebo video.

Tip

- Pro zobrazení dynamického streamu použijte URL http://device_IP:8080/video.cgi.
- Pro pořízení snímku obrazovky použijte následující URL, přičemž formáty obrázků se podle toho liší:
 - http://device_IP:8080/picture.cgi
 - http://device_IP:8080/picture.jpg
 - http://device_IP:8080/jpeg.cgi
- Například pokud chcete zachytit obrázek zařízení ve formátu jpg s IP adresou 192.168.1.104, můžete zadat <http://192.168.1.104:8080/picture.jpg> do webového prohlížeče.

- **Kvalita obrazu:** Specifikujte rozlišení obrazu, které se pohybuje od nejnižšího CIF (352×288 pixelů) po nejvyšší 720P (1280 × 720 pixelů). Výchozí hodnota je 4CIF (704×576 pixelů).

Pro nastavení autentizace MJPEG přejděte na rozhraní **Surveillance > RTSP > RTSP Basic**.

- **Povolena autorizace MJPEG:** Po povolení je přístup k obrazu nebo videu zařízení v reálném čase zadáním URL do prohlížeče nutný ověřit autentizační režim, uživatelské jméno RTSP a heslo RTSP.

RTSP monitorování

Funkce RTSP umožňuje vnitřním monitorům Akuvox nebo zařízením třetích stran přijímat živý přenos z tohoto zařízení.

Můžete nastavit RTSP autentizační údaje a video parametry.

Pro nastavení přejděte do rozhraní **Surveillance > RTSP > RTSP Basic**.

The screenshot shows the 'RTSP Basic' configuration page. It contains several settings:

- Enabled:** A checkbox that is checked (blue square with a white checkmark).
- RTSP Authorization Enabled:** A checkbox that is unchecked (empty square).
- MJPEG Authorization Enabled:** A checkbox that is checked (blue square with a white checkmark).
- Authentication Mode:** A dropdown menu currently set to 'Digest'.
- Username:** A text input field containing the value 'admin'.
- Password:** A text input field containing a series of dots (password mask).

- **Povoleno autorizace RTSP:** Po povolení nastavte RTSP autentizační režim, uživatelské jméno RTSP a heslo RTSP. Tyto přihlašovací údaje jsou vyžadovány pro přístup k RTSP streamu zařízení z jiných interkomových zařízení, jako jsou vnitřní monitory.
- **Autorizační režim:** Digest je výchozí autentizační typ, který používá hashování místo snadno vratného kódování v Base64. Pro ověření se používá token.
- **Uživatelské jméno:** Nastavte uživatelské jméno pro autorizaci.
- **Heslo:** Nastavte heslo pro autorizaci.

Nastavení RTSP streamu

RTSP stream může používat H.264 jako video kodek. Rozlišení videa, datovou rychlost a další nastavení můžete upravit na webovém rozhraní **Surveillance > RTSP > H.264 Video Parameters**.

H.264 Video Parameters	
Video Resolution	720P ▼
Video Framerate	25fps ▼
Video Bitrate	2048kbps ▼
2nd Video Resolution	VGA ▼
2nd Video Framerate	25fps ▼
2nd Video Bitrate	2048kbps ▼

- **Rozlišení videa:** Zadejte rozlišení obrazu, které se pohybuje od nejnižšího QCIF (176×144 pixelů) až po nejvyšší 1080P (1920×1080 pixelů). Výchozí je 720P.
- **Video snímková frekvence:** Snímky za sekundu označují, kolik snímků je zobrazeno v jedné sekundě videa. Výchozí snímková frekvence je 25 fps.
- **Přenosová rychlost videa:** Množství video dat přenesených během určitého časového období. Vyšší datová rychlost videa znamená vyšší možnou kvalitu, ale také větší velikost souborů a větší šířku pásma. Výchozí hodnota je 2048 kbps.
- **2. rozlišení videa:** Určete rozlišení obrazu pro druhý kanál video streamu.
- **2. snímková frekvence videa:** Nastavte snímkovou frekvenci pro druhý kanál video streamu.
- **2. datová rychlost videa:** Nastavte datovou rychlost pro druhý kanál video streamu.

Tip

Pro zobrazení audio a video streamu pomocí RTSP:

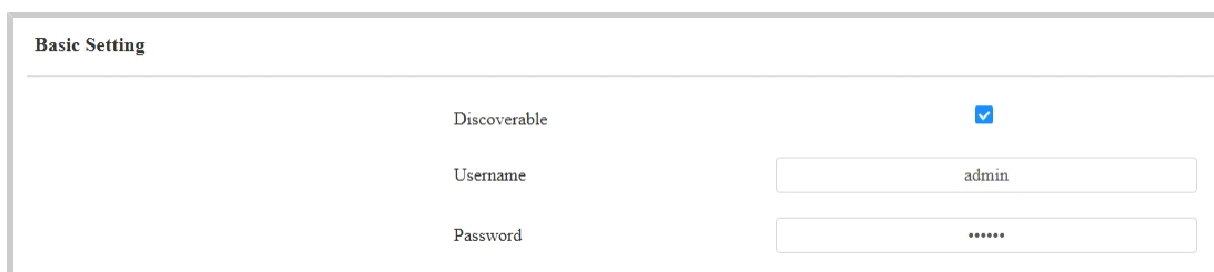
- První kanál: rtsp://Device's IP/live/ch00_0
- Druhý kanál: rtsp://Device's IP/live/ch00_1

ONVIF

K video v reálném čase můžete přistupovat z kamery zařízení pomocí vnitřního monitoru Akuvox nebo jiných zařízení třetích stran, jako je Network Video Recorder (**NVR**). Zapnutí a nastavení funkce ONVIF na zařízení umožní vidět jeho video na jiných zařízeních.

Klikněte [zde](#) pro zobrazení příkladu použití funkce ONVIF: integrace se systémem Uniview NVR.

Pro nastavení přejděte na webové rozhraní **Surveillance > ONVIF**.



Basic Setting	
Discoverable	☒
Username	admin
Password	*****

- **Objevitelné:** Po zapnutí je video z kamery zařízení vyhledáváno jinými zařízeními.
- **Uživatelské jméno:** Nastavte uživatelské jméno potřebné pro přístup k video streamu zařízení na jiných zařízeních. Ve výchozím nastavení je to administrátor.
- **Heslo:** Nastavte heslo potřebné pro přístup k video streamu zařízení na jiných zařízeních. Ve výchozím nastavení je to administrátor.

Tip

Jakmile jsou nastavení nastavena, pro přístup k video streamu na zařízení třetí strany stačí zadat URL ONVIFu:

IP:80/onvif/device_service http://Device.

Některé NVR mohou odesílat požadavky na otevírání dveří zařízení a ovládat otevírání dveří. Funkci lze povolit nebo vypnout zapnutím nebo vypnutím spínače na stejném rozhraní jako funkce ONVIF.

Advanced Setting

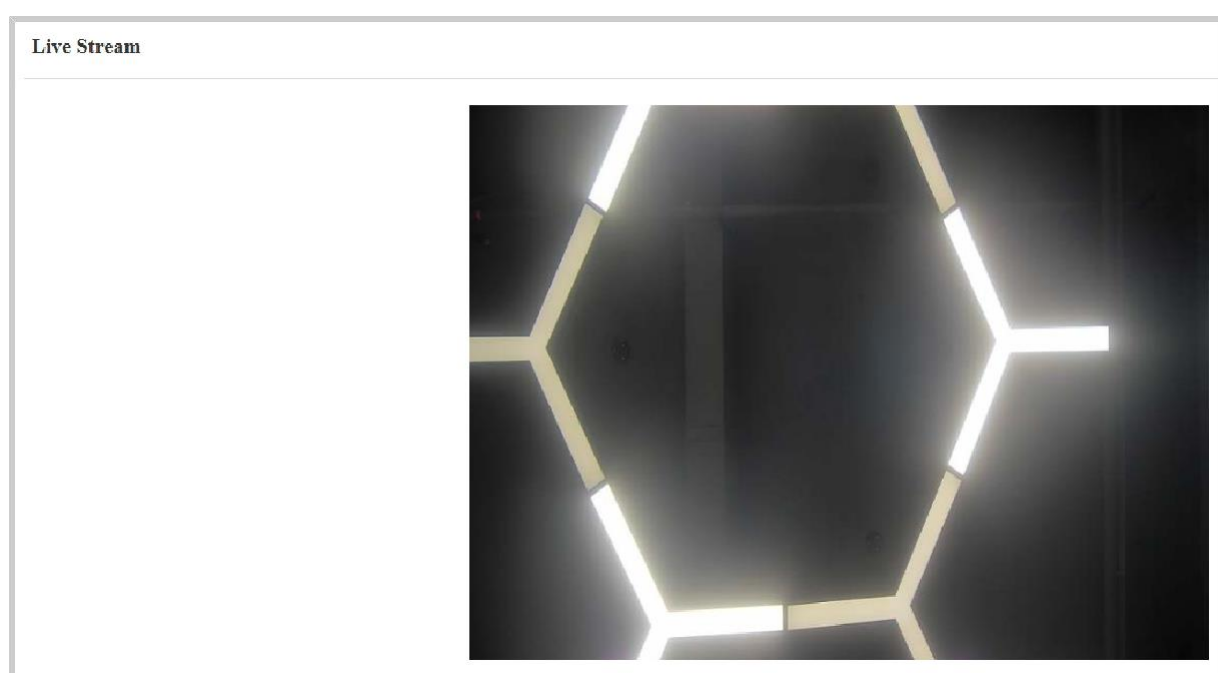
Milestone



Živý přenos

Existují dva způsoby, jak zkontrolovat video v reálném čase ze zařízení. Jedním je jít do webového rozhraní zařízení a video si tam prohlédnout. Druhým je zadat správnou URL adresu do webového prohlížeče a přistupovat k videu přímo.

Pro zařízení je cesta **Surveillance > Live Stream**.



Režim kamery

- Vysoký dynamický rozsah (HDR) je technologie používaná ve fotografii, videografii a zobrazovacích zařízeních ke zlepšení kvality obrazu zachycováním širšího rozsahu jasu a barev.
- Lineární označuje přímočaré zobrazení jasu na obrázcích. Lineární obrazy se běžně používají v prostředí s řízeným osvětlením, například v interiérových scénách, kde je přítomen stálý jas.

Režim fotoaparátu můžete nastavit mezi HDR a Linear v **nastavení zařízení** > rozhraní fotoaparátu. Ve výchozím nastavení je HDR.

Camera Mode	
Mode	HDR ▼
Anti-Flicker	
Anti-Flicker Mode	Auto ▼
Anti-Flicker Frequency	50HZ ▼
Framerate	
Sensor Framerate	25fps ▼

- **Režim proti blikání:** Funkce proti blikání snižuje nebo eliminuje blikání na obrázcích či videích způsobené různými zdroji světla.
 - **Auto:** Zařízení automaticky přepne mezi frekvencí proti blikání 50Hz a 60Hz.
 - **Manuální:** Manuálně vyberte frekvenci proti blikání.
 - **Vypnuto:** Deaktivujte funkci proti blikání.
- **Frekvence proti blikání:** Vyberte frekvenci proti blikání mezi 50Hz a 60Hz.
- **Snímková frekvence senzoru:** Upravte snímkovou frekvenci kamery.
 - **30fps:** Lepší pro aplikace vyžadující vyšší plynulost.
 - **25fps:** Vhodné pro standardní nahrávání videa a přehrávání, zejména při frekvenci 50Hz pro minimalizaci blikání.

Typ přenosu dat pro kamery třetích stran

Můžete zvolit typ přenosu dat mezi zařízením a kamerou třetí strany, když je připojena ke SmartPlus Cloud.

Pro nastavení přejděte na rozhraní **Surveillance > RTSP > Third Party Camera**.

Third Party Camera	
Transport Type	TCP

- **UDP:** Nespolehlivý, ale velmi efektivní protokol transportní vrstvy.
- **TCP:** Méně efektivní, ale spolehlivý protokol transportní vrstvy. Je to výchozí transportní protokol.

Bezpečnost

Alarm proti manipulaci

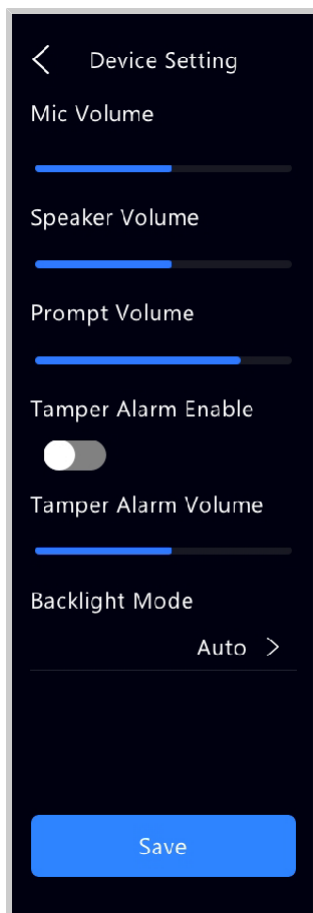
Funkce alarmu proti manipulaci zabraňuje komukoliv zařízení bez povolení odstranit. Zařízení Akuvox podporují dva typy ochrany proti manipulaci: detekci gravitace a detekci stavu tlačítek.

Klikněte [zde](#) pro zobrazení typu, který typ zařízení podporuje, a zjistěte podrobnosti o funkci.

Nastavte to v rozhraní **System > Security > Tamper Alarm**. Klikněte na **Zneškodnit** pro vyčištění alarmu.

Tamper Alarm	
Enabled	☒
Disarm	

Také můžete zapnout/vypnout Alarm pro manipulaci na **obrazovce nastavení > zařízení**.

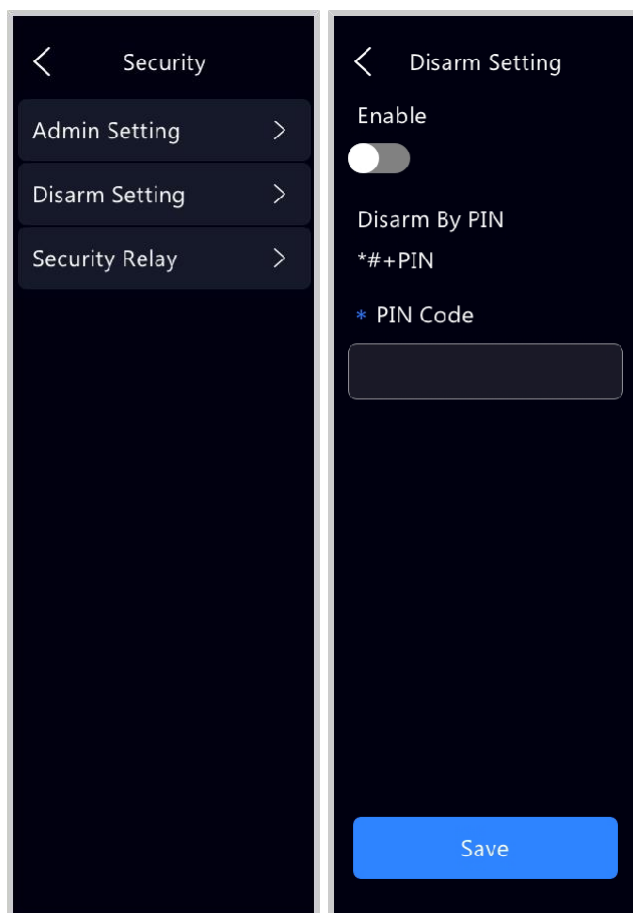


Nastavení pro odzbrojení

Kód pro deaktivaci si můžete nastavit na webovém rozhraní **System > Security > Disarm Setting**.

Disarm Setting	
Enabled	☐
PIN Code	***** (Enter *# + PIN to disarm)

Kód si můžete také nastavit na obrazovce **Nastavení > Bezpečnost > Nastavení odzbrojení**.



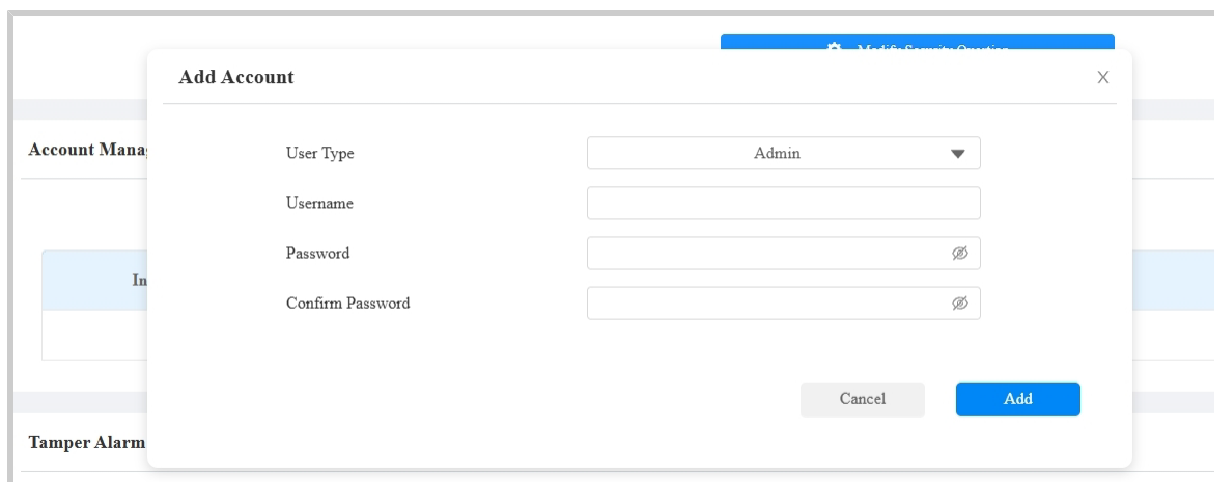
Správa účtu

Můžete přidat uživatelské účty pro přístup k webovému rozhraní zařízení a přiřadit různá přístupová oprávnění pro kontrolu dostupných nastavení pro každý účet.

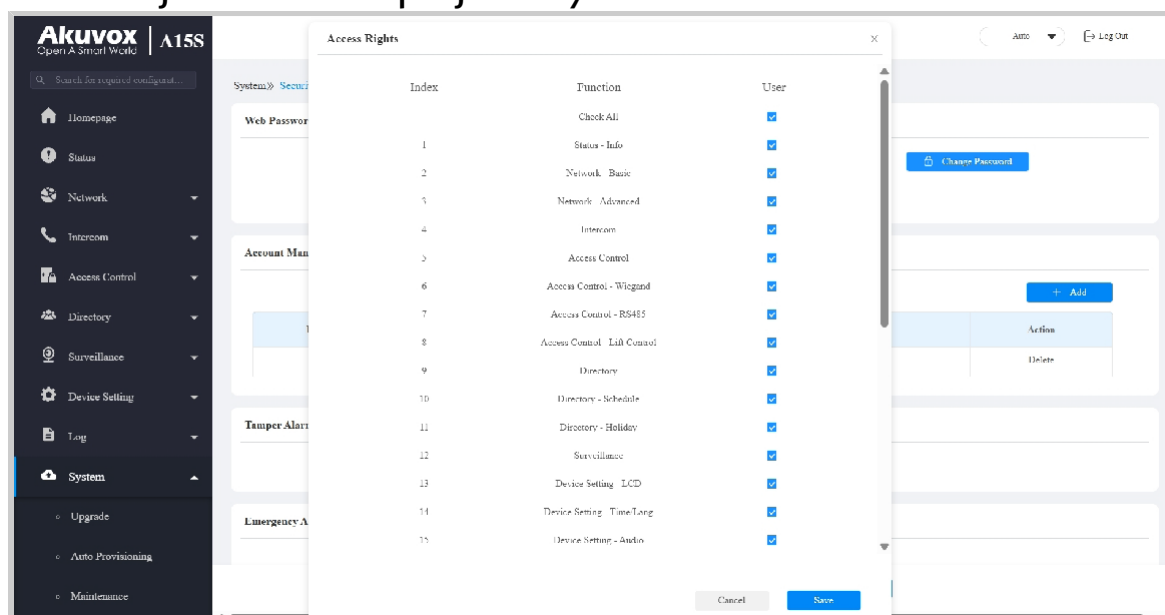
Pro nastavení přejděte do rozhraní **System > Security > Account Management**. Výchozí administrátorský účet nelze smazat.

Klikněte na **+Přidat** pro vytvoření nového účtu.

Account Management				
				+ Add
Index	Type	Username	Access Rights	Action
1	Admin	admin	Full Access	Delete



- **Typ uživatele:** Typ účtu.
 - **Admin:** Administrátorský účet má plný přístup k webovým nastavením zařízení.
 - **Uživatel:** Uživatelský účet má přístup pouze k nastavením, která jsou zvolena při jeho vytvoření.



- **Uživatelské jméno:** Uživatelské jméno používané k přihlášení do webového rozhraní zařízení .
- **Heslo:** Heslo používané k přihlášení do webového rozhraní zařízení .

Nastavení klientského certifikátu

Certifikáty zajišťují integritu a soukromí komunikace. Pro použití SSL protokolu je nutné nahrát správné certifikáty k ověření.

Certifikát webového serveru

Jedná se o certifikát zasílaný klientovi k autentizaci, když klient požádá o SSL spojení se zařízením Akuvox. Prosím, nahrajte certifikáty v akceptovaných formátech.

Nahrajte certifikát do rozhraní **System > Certificate**.

Web Server Certificate				
Upload		 Upload		
Index	Issue To	Issuer	Expire Time	Delete
1	akweb	AKUVOX	Sun Dec 31 00:00:00 2099	 Delete

Klientský certifikát

Konfigurujte nastavení TLS a certifikáty používané pro bezpečnou SIP komunikaci. Můžete specifikovat verzi TLS, nastavit ověřování serverových certifikátů a spravovat certifikáty potřebné pro SIP TLS připojení.

Nahrajte certifikát do webového rozhraní **System > Certificate**.

SIP TLS Certificate

TLS Version

TLS 1.2

CA Certificate

Verify SIP Server CA Certificate

☐

?

Index

Auto

Upload

Upload

	Index	Issue To	Issuer	Expire Time
No Data				

Delete

Delete All

Client Certificate

Upload

Upload

Index	Issue To	Issuer	Expire Time	Delete
1	akpbx	cloud.akuvox.com	Sun Sep 10 03:21:52 2049	Delete

- **Verze TLS:** TLS 1.2 poskytuje silnější zabezpečení díky moderním šifrovacím algoritmům a doporučuje se pro bezpečnou komunikaci. TLS 1.0 je zastaralý protokol s proslulými zranitelnostmi a měl by se mu vyhýbat, pokud není nezbytný pro kompatibilitu s legacy.
- **Ověřte certifikát SIP Server CA:** Po povolení zařízení ověří certifikát SIP serveru pomocí nahraného CA certifikátu před navázáním TLS spojení. Připojení bude odmítnuto, pokud certifikát není důvěryhodný.
- **Index:** Vyberte požadovanou hodnotu z rozbalovacího seznamu Index. Pokud zvolíte Auto, nahraný certifikát se zobrazí v číselném pořadí. Pokud vyberete hodnotu od 1 do 10, nahraný certifikát se zobrazí podle čísla.
- **Nahrávání certifikátů v Kalifornii:** Podporované formáty: .pem, .der, .cer, .crt.
- **Nahrávání klientského certifikátu:** podporované formáty: .pem, .cer, .crt.

Detekce pohybu

Detekce pohybu je funkce, která umožňuje nepozorované video sledování a automatické alarmy. Detekuje jakékoli změny v obrazu zachyceném kamerou, například když někdo prochází kolem nebo je čočka posunuta, a aktivuje systém pro provedení příslušné činnosti.

Nastavte detekci pohybu na rozhraní **Surveillance > Motion**.

Motion Detection Options	
Suspicious Moving Object Detection	Radar Detection ▼
Time Interval	10 (0~120Sec)
Detection Range	3 (m) ▼

- **Detekce podezřelých pohybujících se objektů:** Funkce využívá hlavní kameru k detekci.
 - **Zakázáno:** Vypněte funkci.
 - **Detekce videa:** Když videokamera detekuje pohybující se objekty, spustí se přednastavené akci. Zaměřte se na analýzu vizuálních informací zachycených kamerami.
 - **Detekce radaru:** Když radar detekuje pohybující se objekty, spustí se přednastavené akci. Nabízí delší dosah a lepší detekci při špatné viditelnosti.
 - **Video + radar:** Detekujte pohyb kombinací videokamery a radaru.
- **Časový interval:** Určete, jak zpozdit a spustit detekci pohybu.
 - Časový interval mezi 1–3 sekundami: Stačí 1 detekce během tohoto intervalu k spuštění akcí.
 - Časový interval > 3 sekundy (např. 10 sekund): Pro provedení akcí je potřeba druhé zjištění v posledních 3 sekundách intervalu (např. mezi 7–10 sekundami u 10sekundového intervalu) po prvním zjištění.
 - Výchozí interval je 10 sekund.

- **Přesnost detekce:** Není dostupná pro radarovou detekci. Citlivost detekce. Čím vyšší hodnota, tím větší citlivost. Výchozí hodnota přesnosti detekce je 3.
- **Detekční dosah:** Nastavte vzdálenost, ve které je radarová detekce aktivována. Vzdálenost zahrnuje 1, 2 a 3 metry.
- **Detekční oblast:** Kliknutím a podržením tlačítka myši vyberte až tři detekční oblasti. Když je v těchto oblastech detekován pohyb, provedou se přednastavené akce.
- **Akce k provedení:** Nastavte požadované kroky, které nastanou, když je zjištěn podezřelý pohyb.
 - **FTP:** Pošlete screenshot na přednastavený [FTP server](#).
 - **E-mail:** Pošlete screenshot předkonfigurované [E-mail Adresa](#) .
 - **SIP hovor:** Zavolejte přednastavené [číslo](#) při spouštění.
 - **HTTP:** Po spuštění lze HTTP zprávu zachytit a zobrazit v odpovídajících paketech. Pro využití této funkce povolte HTTP server a zadejte obsah zprávy do určeného pole níže.
 - **HTTP URL:** Zadejte HTTP zprávu, pokud jako akci pro spuštění zvolíte HTTP. Formát je obsah IP/zprávy http://HTTP serveru.
 - **Spustit relé:** Relé lze odemknout detekcí pohybu. Sjed'te dolů a

můžete nastavit rozvrh detekce pohybu.

Motion Detect Time Setting

Day

☒ Mon
 ☒ Tue
 ☒ Wed
 ☒ Thur
 ☒ Fri
 ☒ Sat
 ☐ Sun
 ☐ Check All

Start Time - End Time

00:00
 -
 23:59

Bezpečnostní oznámení

Bezpečnostní oznámení informuje uživatele nebo bezpečnostní pracovníky o jakémkoli narušení nebo hrozbě, kterou zařízení detekuje. Například pokud zařízení detekuje něco neobvyklého, systém odešle upozornění uživatelům nebo bezpečnostním složkám prostřednictvím e-mailu, telefonátů nebo jiných metod.

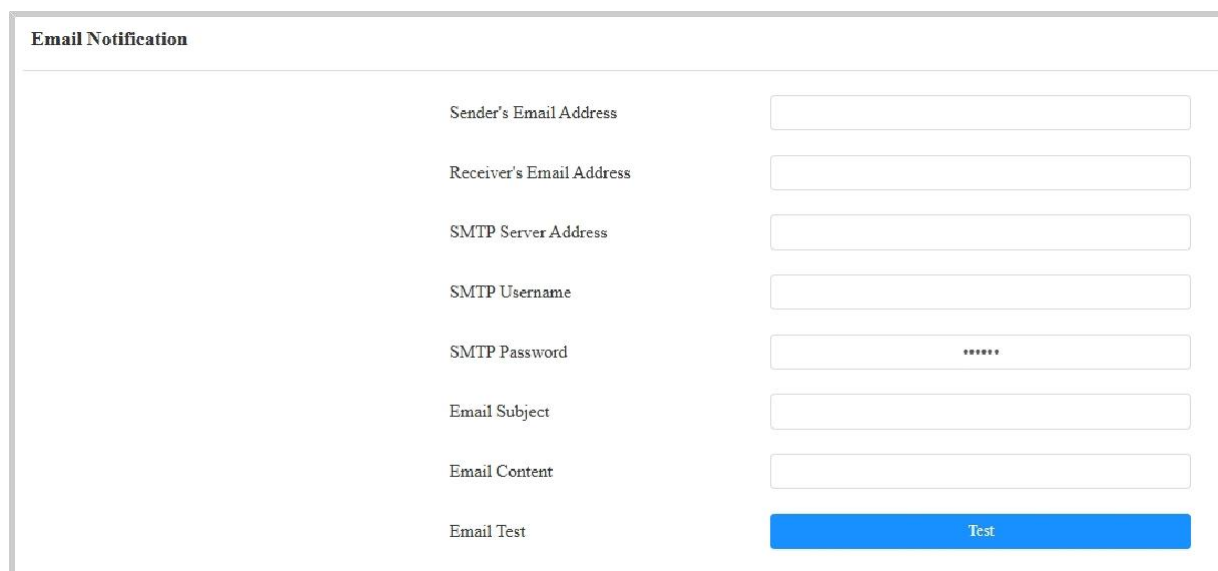
Pro nastavení bezpečnostních oznámení přejděte do rozhraní **Nastavení zařízení > Akce**.

E-mailové upozornění

Nastavte e-mailová upozornění, abyste dostávali screenshoty neobvyklého pohybu ze zařízení.

Klikněte [zde](#) a zjistěte, jak tuto funkci nastavit.

Nastavte ji v`všechny sekci **E-mailová upozornění**.



The screenshot shows a web form titled "Email Notification". It contains several input fields for configuration: "Sender's Email Address", "Receiver's Email Address", "SMTP Server Address", "SMTP Username", "SMTP Password" (with a masked password "*****"), "Email Subject", and "Email Content". At the bottom, there is a "Test" button next to the "Email Test" label.

- **Adresa SMTP serveru:** Adresa SMTP serveru odesílatele.
- **SMTP uživatelské jméno:** Uživatelské jméno SMTP je obvykle stejné jako e-mailová adresa odesílatele.
- **SMTP heslo:** Heslo SMTP služby je stejné jako e-mailová adresa odesílatele.

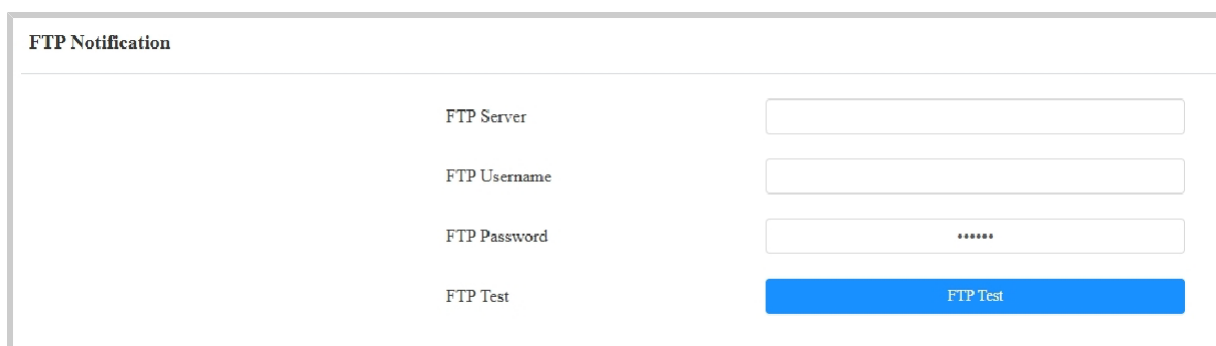
FTP oznámení

Pro získání notifikací přes FTP server je potřeba nastavit FTP nastavení. Zařízení nahraje screenshot do určené FTP složky, pokud zaznamená nějaký neobvyklý pohyb.

Klikněte [zde](#) pro zobrazení konfiguračních

kroků. Nastavte to v **sekci FTP**

Notification.



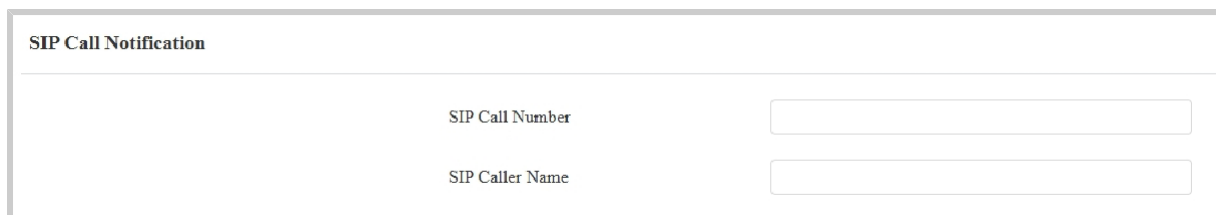
The screenshot shows a configuration window titled "FTP Notification". It contains four input fields: "FTP Server", "FTP Username", and "FTP Password" (with masked characters "*****"). Below these fields is a blue button labeled "FTP Test".

- **FTP server:** Nastavte adresu (URL) FTP serveru.
- **FTP uživatelské jméno:** Zadejte uživatelské jméno pro přístup k FTP serveru.
- **FTP heslo:** Zadejte heslo pro přístup na FTP server.

Oznámení o SIP hovorech

Kromě FTP a e-mailových notifikací může zařízení také uskutečnit SIP hovor, když je aktivována nějaká akce.

Nastavte to v sekci **SIP Call Notification**.



The screenshot shows a configuration window titled "SIP Call Notification". It contains two input fields: "SIP Call Number" and "SIP Caller Name".

- **Zobrazovací jméno:** Název zařízení zobrazený v oznámení.

Action URL

Zařízení můžete použít k odeslání specifických HTTP URL příkazů HTTP serveru pro určité akce. Tyto akce se spustí, když se změní stav relé, vstupní stav, PIN kód nebo přístup k RF kartě.

Akuvox Action URL:

Událost	Formát parametrů	Příklad
Zavolejte	\$remote	Http://server IP / Číslo hovoru = \$remote
Zavěs	\$remote	Http://server IP / Číslo hovoru = \$remote
Zadaný platný kód	\$code	Http://server ip / validcode = \$code
Zadán neplatný kód	\$code	Http://server ip / invalidcode = \$code
Platná karta zadaná	\$card_sn	Http://server ip / validcard = \$card_sn
Zadaná neplatná karta	\$card_sn	Http://server IP / invalidcard = \$card_sn
Alarm proti manipulaci	\$alarmstatus	Http://server ip / tampertri = \$alarmstatus
Relé spuštěno	\$relay 1 stav	Http://server IP / Relaytrigger = \$relay 1 stav
Relé uzavřeno	\$relay 1 stav	Http://server IP / relayclose = \$relay 1 stav

Vstup spuštěn	\$input 1 status	Http://server IP /vstupní spouštěč= \$input 1 status
Vstup uzavřen	\$input 1 status	Http://server ip /vstupní blízko= \$input 1 status
Poplach proti vloupání	\$input 1 status	Http://server IP /vstupní spouštěč= \$input 1 status
Rozpoznávání obličeje	\$unlocktype	Http://serverip/unlocktype= \$unlocktype

Například: `http://192.168.16.118/help.xml? mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn` Pro

nastavení přejděte do rozhraní **Device Setting > Action URL**.

Action URL

Enabled

☐

Type

GET

Authorization Mode

None

Make Call

Hang Up

Valid Code Entered

Invalid Code Entered

Valid Card Entered

Invalid Card Entered

Tamper Alarm

RelayA Triggered

RelayA Closed

RelayB Triggered

RelayB Closed

InputA Triggered

InputA Closed

Break In Alarm A	
InputB Triggered	
InputB Closed	
Break In Alarm B	
InputC Triggered	
InputC Closed	
Break In Alarm C	
InputD Triggered	
InputD Closed	
Break In Alarm D	
Valid Face Recognition	
Invalid Face Recognition	

Šifrování hlasu

Secure Real-time Transport Protocol (SRTP) je protokol odvozený z Real-time Transport Protocol (RTP). Zvyšuje bezpečnost přenosu dat tím, že poskytuje šifrování, autentizaci zpráv, zajištění integrity a ochranu před přehráváním.

Nastavte to na webovém rozhraní **Interkom > Účet**.

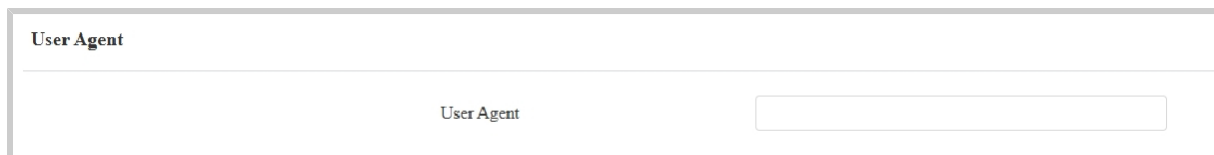
Encryption	
Voice Encryption(SRTP)	Disabled ▼

- **Hlasové šifrování (SRTP):** Zvolte Disabled, Optional nebo Compulsory for SRTP. Pokud **je zvoleno** Optional **nebo** Nuce, hlas během hovoru je zašifrován a můžete si RTP paket přečíst a zobrazit si ho.

User Agent

User agent se používá pro identifikaci při analýze SIP datového paketu.

Pro nastavení přejděte do rozhraní **Intercom > Account > User Agent**.



User Agent

User Agent

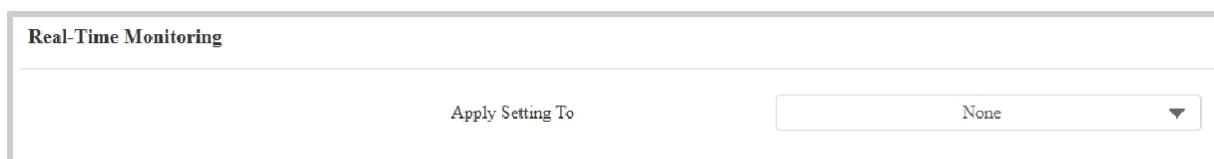
- **User Agent:** Akuvox je ve výchozím nastavení.

Monitorování v reálném čase

Tato funkce zobrazuje stav dveří, když je zařízení připojeno ke SmartPlus Cloudu. Správci nemovitostí a koncoví uživatelé mohou zkontrolovat stav dveří na platformě SmartPlus Property Manager a v aplikaci SmartPlus. Musíte specifikovat relé(y) nebo vstupy, které tuto funkci aplikují.

Klikněte [zde](#) pro podrobnou konfiguraci.

Pro nastavení přejděte do rozhraní **System > Security > Real-Time Monitoring**.



Real-Time Monitoring

Apply Setting To

None

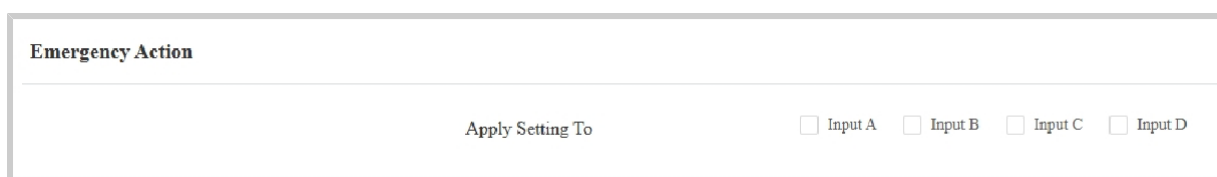
- **Aplikujte nastavení na:**
 - **Žádné:** Nezobrazuje stav dveří.
 - **Vstup:** Dveře se otevírají spuštěním vstupu.
 - **Relay:** Dveře se otevírají aktivací relé.

Nouzová akce

Tato funkce funguje s Akuvox SmartPlus Cloud. Udrží dveře otevřené, když nastane nouzová situace. Musíte zadat vstup, který tuto funkci aplikuje.

Klikněte [zde](#) pro zobrazení podrobné konfigurace této funkce.

Pro nastavení přejděte do rozhraní **System > Security > Emergency Action**. Vyberte vstup(y), které se spustí.

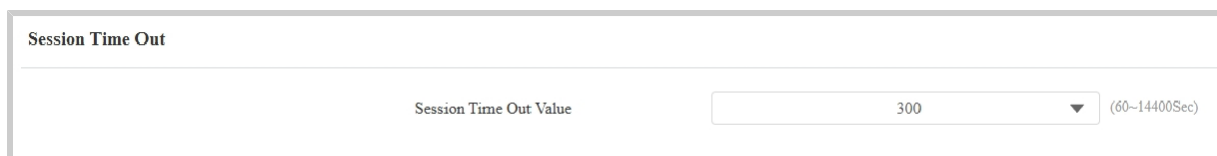


The screenshot shows the 'Emergency Action' configuration page. At the top, it says 'Emergency Action'. Below this, there is a section labeled 'Apply Setting To' followed by four checkboxes: 'Input A', 'Input B', 'Input C', and 'Input D'. All checkboxes are currently unchecked.

Automatické odhlášení webového rozhraní

Můžete nastavit automatické odhlášení webového rozhraní, které vyžaduje opětovné přihlášení zadáním uživatelského jména a hesel pro bezpečnostní účely nebo pro pohodlí provozu.

Pro nastavení přejděte do rozhraní **System > Security > Session Time Out**.



The screenshot shows the 'Session Time Out' configuration page. At the top, it says 'Session Time Out'. Below this, there is a section labeled 'Session Time Out Value' followed by a dropdown menu showing '300' and a range '(60~14400Sec)'.

Režim vysoké bezpečnosti

Režim vysoké bezpečnosti je navržen tak, aby zvýšil bezpečnost. Využívá šifrování v různých aspektech, včetně komunikačního procesu, příkazů k otevírání dveří, metod ukládání hesel a dalších.

Povolte ji v rozhraní **System > Security > High Security Mode**.

High Security Mode
Enabled ☒

Důležité poznámky

1. Režim vysoké bezpečnosti je ve výchozím nastavení vypnutý, když upgradujete zařízení z verze bez tohoto režimu na verzi s ním. Ale pokud zařízení resetujete na tovární nastavení, režim je ve výchozím nastavení zapnutý.

2. Tento režim způsobuje, že staré verze nástrojů nejsou kompatibilní. Musíte je upgradovat na následující verze nebo vyšší, abyste je mohli používat.

- PC Manager: 1.2.0.0
- IP Scanner: 2.2.0.0
- Nástroj pro upgrade: 4.1.0.0
- SDMC: 6.0.0.34

3. Podporovaný formát HTTP pro spouštění relé se liší podle toho, zda je režim vysokého zabezpečení povolen nebo vypnutý.

Pokud je režim zapnutý, zařízení přijímá nové HTTP formáty pouze pro otevírání dveří.

- `http://username:password@deviceIP/fcgi/OpenDoor?akce=OpenDoor&DoorNum=1`
- `http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1`

Pokud je režim vypnutý, zařízení může používat jak nové formáty výše, tak starý formát níže:

- `http://deviceIP/fcgi/do?action=OpenDoor&Username=username&Password=password&DoorNum=1`

4. Není povoleno importovat/exportovat konfigurační soubory v TGZ. Formátovat mezi zařízením s režimem vysoké bezpečnosti a jiným bez něj. Pro pomoc s přenosem souborů kontaktujte prosím technickou podporu Akuvox.

Logování

Logy hovorů

Pro kontrolu hovorů – včetně hovorů, přijatých a zmeškaných hovorů – v určitém období si můžete prohlédnout záznam hovorů na webovém rozhraní zařízení. Pokud je potřeba, můžete také exportovat záznam hovorů ze zařízení.

Zkontrolujte záznamy hovorů na webovém rozhraní **Log > Call Log**. Zařízení může uložit 500 záznamů hovorů.

Call Log

Save Call Log Enabled ☒

All Start Time End Time Name/Number Search Export

Index	Type	Status	Date	Time	Local Identity	Details
No Data						

Selected: 0/0 Delete Delete All Total: 0 Prev 1/1 Next Go To Page 1 Go

- **Všichni:** K dispozici jsou čtyři typy historie hovorů: Vše, vytočené, přijaté a Zmeškané.
- **Čas začátku a konce:** Konkrétní čas záznamů hovorů, které chcete vyhledávat, kontrolovat nebo exportovat.
- **Jméno/číslo:** Vyhledejte záznam hovorů podle jména nebo podle SIP či IP čísla.
- **Export:** Záznamy hovorů lze exportovat ve .csv formátu.

Logy přístupu ke dveřím

Pro vyhledávání a kontrolu různých typů historie přístupu ke dveřím stačí zkontrolovat záznamy dveří na webovém rozhraní zařízení.

Zkontrolujte záznamy dveří na webu **Log > rozhraní Access Log**. Zařízení může uložit 5 000 záznamů o dveřích.

The screenshot shows the 'Access Log' interface. At the top, there are three settings: 'Save Access Log Enabled' (checked), 'Save Picture Enabled' (checked), and 'Export Picture Enabled' (unchecked). Below these are filters for 'All' (selected), 'All' (selected), 'Start Time' ~ 'End Time', and 'Name/Code'. There are 'Search' and 'Export' buttons. Below the filters is a table with columns: Index, User ID, Name, Code, Reader, Door ID, Type, and Date. The table is empty, showing 'No Data'. At the bottom, there are buttons for 'Delete' and 'Delete All', and a 'Go To Page' dropdown set to 1.

- **Export obrázků povolen:** Když je povolen, můžete exportovat záznamy dveří s obrázky.

Záznamy událostí

Záznamy událostí zaznamenávají klíčové události, jako je změna stavu vstupu, relé, alarm manipulace atd. To pomáhá sledovat stav a změny zařízení.

Záznamy událostí můžete zkontrolovat v rozhraní **Log > Event Log**. Zařízení podporuje až 100 000 logů, které lze exportovat ve formátu CSV.

Type	Time	Event Type	Status
All	Start Time - End Time	Search	Export
	2025-07-27 02:15:39	Login	Account admin, Success; IP 192.168.31.157
	2025-07-27 02:15:36	Login Attempt	Account admin, Failed; IP 192.168.31.157
	2025-07-27 01:59:44	Login	Account admin, Success; IP 192.168.31.157
	2025-07-27 01:45:44	Login	Account admin, Success; IP 192.168.31.157
	2025-07-27 01:14:10	IP Change	IP Changed from 169.254.210.214 to 192.168.31.197
	2025-07-27 01:14:34	IP Change	IP Connection Lost
	2025-07-27 01:13:30	IP Change	IP Obtained - 169.254.210.214
	2025-07-27 01:13:19	Device State	Startup
	2025-07-24 12:25:43	IP Change	IP Changed from 192.168.31.197 to 169.254.210.75
	2025-07-24 12:25:10	IP Change	IP Connection Lost
	2025-07-24 10:27:01	Login	Account admin, Success; IP 192.168.31.157
	2025-07-24 08:58:50	Login	Account admin, Success; IP 192.168.31.157

Integrace se zařízením třetích stran

Integrace přes Wiegand

Funkce Wiegand umožňuje zařízení Akuvox fungovat jako ovladač nebo čtečka karet.

Nastavte to na webovém rozhraní **Access Control > Wiegand**.

The screenshot shows the 'Wiegand' configuration page. It contains several settings:

- Wiegand Display Mode:** A dropdown menu currently set to 'SHN'.
- Wiegand Card Reader Mode:** A dropdown menu currently set to 'Auto'.
- Wiegand Transfer Mode:** A dropdown menu currently set to 'Input'.
- Wiegand Input Data Order:** A dropdown menu currently set to 'Normal'.
- Wiegand Input Clear Time:** A dropdown menu currently set to '5'.
- Wiegand Open Relay:** Three checkboxes labeled 'Relay A', 'Relay B', and 'Security Relay', all of which are currently unchecked.

- **Režim zobrazení Wiegand:** Vyberte formát kódu karty Wiegand z následujících možností: 8H10D, 6H3D5D(W26), 6H8D, 8HN, 8HR, 6H3D5D-R(W26), 8HR10D a RAW.
- **Režim čtečky karet Wiegand:** Formát přenosu by měl být identický mezi A15 a zařízením třetí strany.
- **Wiegand Transfer Mode:**
 - **Vstup:** Zařízení slouží jako přijímač.
 - **Výstup:** Zařízení slouží jako odesílač a může přímo vyslat data, například kód karty.
 - **Převést na kartu č. Výstup:** Zařízení slouží jako odesílatel a nemůže přímo vynášet data, jako jsou data obličeje a otisky prstů.
- **Pořadí vstupních dat Wiegand:** Nastavte sekvenci vstupních dat Wiegand mezi normální a obrácenou. Pokud zvolíte Reversed, číslo vstupní karty bude obrácené.

- **Wiegand Output Basic Data Order:** Nastavte pořadí dat na kartě před konverzí do Wiegand a výstupem kódu karty.
Například pokud jsou data karty 0x11 0x22 0x33 0x44 a je zvolena **možnost Reversed**, data budou 0x44 0x33 0x22 0x11.
- **Pořadí výstupních dat Wiegand:** Určte pořadí dat z karet po převodu Wiegand.
Například pokud jsou data karty 0x11 0x22 0x33 0x44 0x55, budou 0x33 0x44 0x55 po Wiegandově konverzi (např. Wiegand 26). Pokud je **zvoleno Reversed**, data karty jsou 0x55 0x44 0x33.
- **Wiegand Output CRC povolen:** Je ve výchozím nastavení povolen pro inspekci dat Wiegand. Jeho vypnutí může vést k selhání integrace s zařízeními třetích stran.
- **Wiegand Input Clear Time:** Pokud interval mezi zadáním hesel překročí tento čas. Všechna zadaná hesla budou vymazána.
- **Ověření RF karty:** Dostupné při **výstupu** nebo **převodu na kartu č. Výstup** je vybrán. Po zapnutí zařízení ověří, zda je kód karty přiřazen uživateli. Pokud není, na obrazovce zařízení se objeví výzva "Otevření dveří selhalo". Po deaktivaci zařízení neprovede lokální ověření.
- **Ověření PIN/QR kódu:** Dostupné, když je **výstup** vybrán jako Wiegand Transfer Mode. Po zapnutí zařízení ověří, zda je přihlašovací karta přiřazena uživateli. Pokud není, na obrazovce zařízení se objeví výzva "Otevření dveří selhalo". Po deaktivaci zařízení neprovede lokální ověření.
- **Wiegand Open Relay:** Zkontrolujte, zda se relé spustí přes Wieganda.

Poznámka

Klikněte [zde](#) pro více informací o nastavení Wiegand, včetně:

- Akuvox zařízení fungují jako vstup/výstup Wiegand.
- Připojení k čtečce karet Wiegand.

Když je zařízení v režimu **výstupu Wiegand**, můžete nastavit formát výstupu kódu Wiegand PIN, který určuje, jak jsou data přenášena. Formát by měl být konzistentní s formátem zařízení třetí strany.

Convert To Wiegand Output	
PIN Output	Disabled ▼

- **8 bitů na číslici:** Když uživatel stiskne "1" na klávesnici, binární data budou přenášena v 8 bitech, tedy "11100001".
- **4 bity na číslici:** Když uživatel stiskne "1" na klávesnici, binární data budou přenášena ve 4 bitech, "0001".
- **Najednou:** Po zadání celého PIN kódu uživateli budou data přenášena podle režimu čtečky karet Wiegand. Například "123456" bude ve Wiegand 26 převedeno na "01e240".

Integrace přes HTTP API

HTTP API je navrženo tak, aby umožnilo síťovou integraci mezi zařízeními třetí strany a zařízeními Akuvox.

Pro nastavení přejděte do webových nastavení **Zařízení** > rozhraní **HTTP API**.

HTTP API

Enabled

☒

Authorization Mode

Allowlist ▼

Username

admin

Password

1st IP

2nd IP

3rd IP

4th IP

5th IP

- **Povoleno:** Povolit nebo zakázat funkci HTTP API pro integraci třetích stran. Pokud je funkce deaktivována, jakýkoli požadavek na zahájení integrace bude zamítnut a vrátí se stav HTTP 403 zakázaný.
- **Režim autorizace:** Vyberte jednu z následujících možností: Žádný, Seznam povolených, Základní, Digest a Token pro typ autorizace, který bude podrobně vysvětlen v následující tabulce.
- **Uživatelské jméno:** Zadejte uživatelské jméno, když je zvolen režim autorizace **Basic** nebo **Digest**. Výchozí uživatelské jméno je admin.
- **Heslo:** Zadejte heslo, když je zvolen režim autorizace Basic nebo Digest. Výchozí heslo je admin.
- **1. IP-5. IP:** Zadejte IP adresu zařízení třetích stran, když je pro integraci zvolena autorizace Allowlistu.

Prosím, podívejte se na následující popis autentizačního režimu:

Režim autorizace	Popis
Žádné	Není potřeba autentizace. Tento režim je určen pouze pro testování a není doporučen v produkčních prostředích.
Seznam povolených	Autentizuje požadavky na základě zdrojové IP adresy. Před odesláním požadavků přidejte IP adresu zařízení třetí strany do seznamu povolených služeb. Doporučuje se pro důvěryhodná LAN prostředí.
Základní	Ověřuje požadavky pomocí uživatelského jména a hesla. Přihlašovací údaje musí být kódovány v Base64 a zahrnuty v hlavičce autorizace.
Digest	Autentizuje požadavky pomocí autentizace HTTP Digest. Podporován je pouze algoritmus MD5.
Token	Vyhrazeno pro interní vývoj a testování Akuvoxu .

Napájecí výstup

Zařízení může sloužit jako zdroj napájení pro externí relé. Klikněte [zde](#) pro zobrazení požadavků na odběr energie.

Pro nastavení přejděte na webové rozhraní **Access Control > Relay > 12V Relay Output**.

12V Power Output	
12V Power Output	Disabled ?
Time Out (Sec)	3

- **12V výkon:**
 - **Vždy:** Poskytujte nepřetržité napájení zařízení třetí strany.
 - **Spouštěno otevřeným relé:** Poskytujte napájení zařízení třetí strany přes výstup 12 a rozhraní GND během timeoutu, kdy je stav relé změněn z nízkého na vysoký.

Integrace přes RS485

Zařízení můžete připojit k externímu zařízení, například SR01, nebo k čtečce karet založené na OSDP přes RS485. Pro efektivní připojení je potřeba zvolit správný režim RS485.

Klikněte [zde](#) pro zobrazení podrobné konfigurace funkce OSDP.

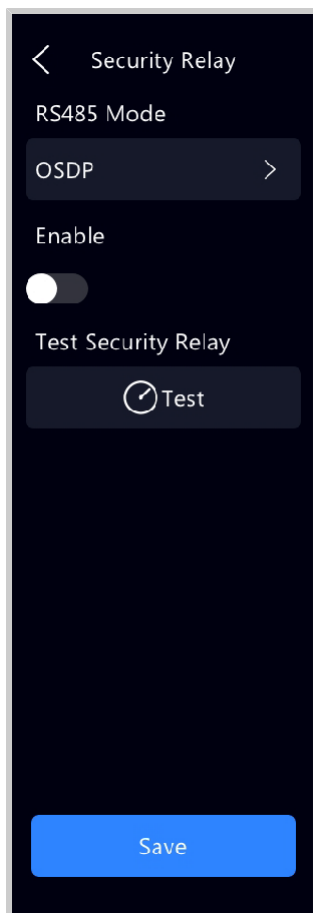
Aby bylo připojení efektivní, musíte nastavit RS485 na rozhraní **Access Control > RS485**.

RS485 Setting	
Apply RS485 Setting To	OSDP
OSDP Setting	
Encryption	☐
Baud Rate	9600
Transfer Mode	Input
SCBK Value	
OSDP Open Relay	☐ Relay A ☐ Relay B

- **Zakázáno:** Funkce RS485 je deaktivována.

- **OSDP:** Zařízení je připojeno k externímu zařízení založenému na OSDP, například čtečce karet.
 - **Šifrování:** Tuto možnost zaškrtněte při šifrování protokolu.
 - **Baud Rate:** Nastavte rychlost přenosu dat během komunikace. Výchozí hodnota je 9600, podporovaná zařízeními Akuvox.
 - **Přenosový režim:** Vyberte pracovní režim RS485: Výstup nebo vstup.
 - **Ověření lokálního relé:** Když je vybrán výstup, nastavte možnost ověření přístupových údajů. Pokud není zaškrtnuto, nezobrazí se výzvy k selhání otevírání dveří.
 - **SCBK hodnota:** Bezpečná komunikace klíčová hodnota.
 - Když je hodnota naplněna, OSDP použije tuto hodnotu pro šifrování a použije přizpůsobený protokol pro komunikaci.
 - Když je ponechán prázdný, OSDP použije pro komunikaci výchozí šifrovaný protokol.
 - **Adresa:** Adresa RS485, která odlišuje toto zařízení od ostatních.
 - **Bezpečnostní relé:** Tuto možnost zvolte, když zařízení pracuje se SR01.

Režim RS485 můžete také zvolit na obrazovce **Nastavení > Security > Security Relay**.



Integrace s třetími stranami pro řízení přístupu

Zařízení může přenášet přihlašovací data na server třetí strany bez jakéhokoli ověření. Generování a ověřování dat probíhá na serveru třetí strany.

Pro nastavení přejděte do rozhraní **Access Control > Relay > Third Party Integration**.

Third Party Integration

List	Customize ▼
Prompt On LCD	Return Value ▼
Remote Verification	☒ QR Code ☒ Card ☒ PIN ☒ Face
HTTP URL	
Device ID	
Success Parameter	1
Failed Parameter	0

- **Žádné:** Vypněte funkci.
- **Obecné:** Odesílejte HTTP URL propojenou s QR kódem metodou Akuvox .
 - **HTTP URL:** Zadejte formát HTTP příkazu poskytnutý poskytovatelem služeb třetí strany. Po načtení QR kódu HTTP příkaz automaticky přenese dynamické informace o QR kódu před odesláním na server QR kódu k ověření. Viz příklad: `http://{Server IP}:8090/api/visitor/scan?codeKey={QRCode} &deviceId={DeviceID}`.
 - **ID zařízení:** ID zařízení poskytuje třetí stranový server. Automaticky se přidá do HTTP příkazu při použití QR kódu pro přístup ke dveřím.
 - **Parametr úspěchu:** Přijetí této hodnoty znamená, že otevření dveří je úspěšné.
 - **Parametr selhání:** Přijetí této hodnoty znamená, že otevření dveří selhalo.
- **Přizpůsobení:** Přenos přístupových údajů o přihlašovacích údajích přizpůsobeným způsobem. Když **je Face** vybrán, zařízení nejprve provede lokální rozpoznávání obličeje. Pokud není zjištěna shodná tvář, autentizace selže. Pokud je nalezena shoda, příslušné **uživatelské ID** nebo **PIN** je odesláno na server třetí strany k dalšímu ověření.

- **Vzdálené ověření:** Určeně, které přístupové údaje budou ověřeny serverem třetí strany. Ve všech případech je specifikované přihlašovací oprávnění předáno serveru tak, jak je, bez lokální ověření na zařízení.

Dostupné možnosti závisí na **konfigurované**

zařízení motiv :

Téma	Dostupné možnosti
Výchozí stav	QR kód, karta, PIN, obličej
Vícefaktorové ověřování	QR kód, vícefaktorový

Když je zvoleno téma **vícefaktorové autentizace**, možnosti **vzdáleného ověřování** se chovají následovně:

Možnost	Popis
QR kód	Zařízení naskenuje QR kód a pošle jej přímo třetí straně Server.
Vícefaktorové	Zařízení nejprve zkontroluje, zda autentizační metoda odpovídá nakonfigurované metodě. Pokud není → spárováno uživatel je vyzván k použití správné metody. Pokud jsou shodné → Shromážděné přihlašovací údaje jsou odeslány serveru k ověření.

- **HTTP URL:** Zadejte formát HTTP příkazu poskytovaný poskytovatelem služeb třetí strany. Po skenování QR kódu, přejetí kartou, zadání PINu nebo rozpoznání obličeje zařízení automaticky nahradí proměnné v URL a odešle požadavek serveru.

Příklad formátu:

http://{Server IP}:8090/api/visitor/scan?codeKey={QRCode}/{Card}/{UserID}/{Pin}&deviceId={DeviceID}.

Pokud uživatel přejede kartou, URL bude

http://192.168.35.123:8090/api/visitor/scan?codeKey={QRCode}/123456/{UserID}/{Pin}&deviceId=1.

V tématu **vícefaktorové autentizace** závisí dostupné zástupné prvky na **zvoleném autentizačním režimu**.

Proměnná	Popis
{Token}	Přihlašovací údaje získané v aktuálním autentizačním kroku.
{Type}	Typ dvoufaktorové autentizace: 1 = RF karta + PIN 3 = Face + RF karta 4 = Obličej + PIN

- **ID zařízení:** ID zařízení poskytuje třetí stranový server. Bude automaticky přidáno do HTTP příkazu.
- **Parametr úspěchu:** Přijetí této hodnoty znamená, že otevření dveří je úspěšné.
- **Parametr selhání:** Přijetí této hodnoty znamená, že otevření dveří selhalo.

Ovládání výtahu

Zařízení lze připojit k ovladači výtahu Akuvox pro ovládání výtahu. Uživatelé mohou vyvolat výtah, aby sestoupil dolů do přízemí, když jim je umožněn přístup různými způsoby přístupu na zařízení.

Klikněte [zde](#) a podívejte se na ukázkové video konfigurace funkce ovládání zvedačky.

Pro nastavení přejděte na webové rozhraní **Access Control > Lift Control**.

Lift Control List	
Lift Control List	Akuvox ▼

General Setting	
Server 1 IP (Unlock)	
Port	
Server 2 IP (Execute)	
Port	

Action Setting	
Username	admin
Password	*****
Floor No. Parameter	\$floor
URL To Trigger Specific Floor	/cdor.cgi?open=0&door=\$floor
URL To Trigger All Floors	/cdor.cgi?open=8
URL To Close All Floors	/cdor.cgi?open=9
Floor Starts From	1 ▼
Ground Floor	▼
Device Location	None ▼

- **Seznam ovládacích prvků zvedání:** Vyberte Žádné pro deaktivaci funkce a vyberte Akuvox pro integraci zařízení s ovladačem Akuvox.
- **IP serveru 1 (Odemknutí):** IP adresa ovladače výtahu, který odemyká tlačítka výtahu. Podporuje až 10 serverových adres oddělených ";".
- **IP adresy serveru 2 (Execute):** IP adresa ovladače výtahu, který posílá příkazy pro řízení výtahu.
- **Port:** Serverový port serveru ovladače liftu.
- **Uživatelské jméno:** Uživatelské jméno ovladače výtahu pro autentizaci.
- **Heslo:** Heslo ovladače výtahu pro ověření.
- **Patro č. Parametr:** Zadejte parametr číslo patra poskytnutý Akuvoxem. Výchozí parametrový řetězec je "\$floor". Pokud je potřeba, můžete definovat svůj parametrový řetězec.
- **URL pro spuštění konkrétního patra:** Zadejte URL pro spuštění konkrétního patra v Akuvox výtahu. URL je /cdor.cgi?open=0&door=\$floor, ale řetězec "\$floor" na konci musí být totožný s parametrem, který jste definovali.
- **URL pro spuštění všech pater:** Zadejte URL Akuvoxu pro spuštění všech pater.
- **URL pro uzavření všech pater:** Zadejte URL Akuvoxu používanou pro uzavření všech pater, což znamená, že všechna tlačítka spuštěná pro příslušná patra se stanou neplatnými.
- **Patro začíná od:** Nastavte patro, od kterého začíná počet pater . Například pokud vyberete -3, třetí patro v suterénu bude považováno za první patro, spárované s relé #1 (první patro).
- **Přízemí:** Pokud jsou přízemí mezi -1 a 1 patry, nastavte tuto možnost.
- **Umístění zařízení:** Vyberte patro, kde je zařízení instalováno.

Aktualizace firmwaru

Zařízení Akuvox lze upgradovat přes webové rozhraní zařízení.

Aktualizujte firmware na webu **System > Upgrade** interface. Pokud chcete zařízení po upgradu resetovat, zaškrtněte políčko Reset.

Basic	
Firmware Version	1115.30.10.408
Hardware Version	1115.0
Upgrade	 Upgrade
Reset To Factory Setting	 Reset
Reset Configuration To Default State	 Reset
Reboot	 Reboot

Poznámka

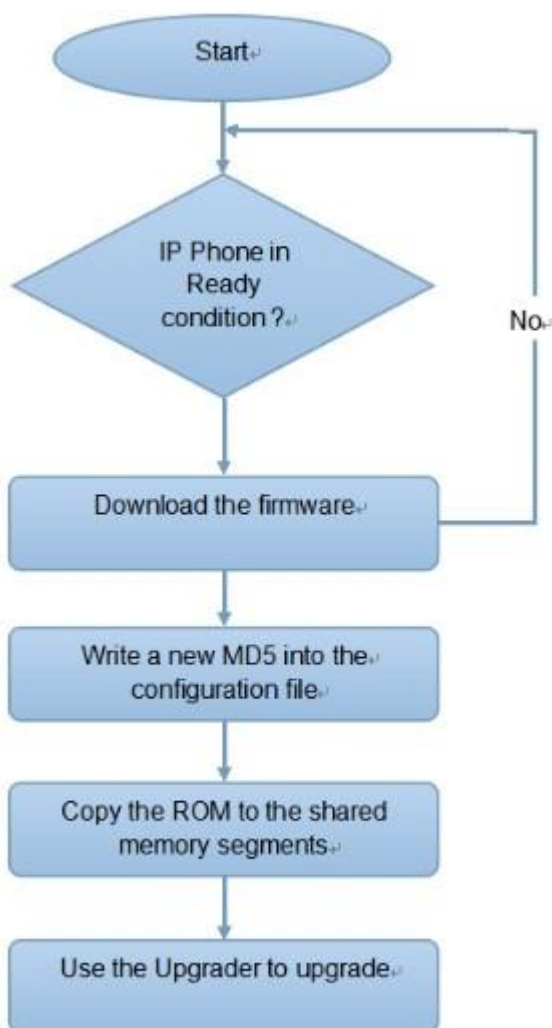
Firmware soubory by měly být ve .rom formátu pro upgrade.

Automatické nastavení přes konfigurační soubor

Princip provisioningu

Automatické nastavení je funkce používaná k hromadné konfiguraci nebo aktualizaci zařízení prostřednictvím serverů třetích stran. **DHCP, PNP, TFTP, FTP a HTTPS** jsou protokoly používané zařízeními Akuvox k přístupu k URL adresy serveru třetí strany, která ukládá konfigurační soubory a firmware, jež jsou následně použity k aktualizaci firmwaru a odpovídajících parametrů zařízení.

Podívejte se prosím na níže uvedený diagram:



Konfigurační soubory pro automatický provisioning

Konfigurační soubory pro automatické nastavení existují ve dvou formátech: obecné konfigurační soubory a MAC konfigurační soubory.

Rozdíly:

- **Obecné nastavení konfigurace:**

Obecný konfigurační soubor je uložen na serveru, který umožňuje všem souvisejícím zařízením stáhnout stejný soubor a aktualizovat parametry.

- **Nastavení konfigurace založené na MAC:**

MAC konfigurační soubory jsou specifické pro jednotlivá zařízení, identifikovaná podle jejich jedinečných MAC adres. Soubory pojmenované MAC adresou zařízení budou automaticky spárovány před stažením pro provisioning.

Poznámka

- Konfigurační soubory musí být ve formátu CFG.
- Název obecného konfiguračního souboru pro dávkové provisionování se liší podle modelu.
- MAC konfigurační soubor je pojmenován podle své MAC adresy.
- Zařízení nejprve přistupují k obecným konfiguračním souborům před těmi založenými na MAC, pokud jsou oba typy dostupné.

Můžete kliknout [zde](#) pro podrobný formát a kroky.

AutoP rozvrh

Akuvox vám poskytuje různé metody AutoP, které umožňují zařízení provádět provisioning podle plánu.

Nastavte to na webovém rozhraní **System > Auto Provisioning > Automatic AutoP**.

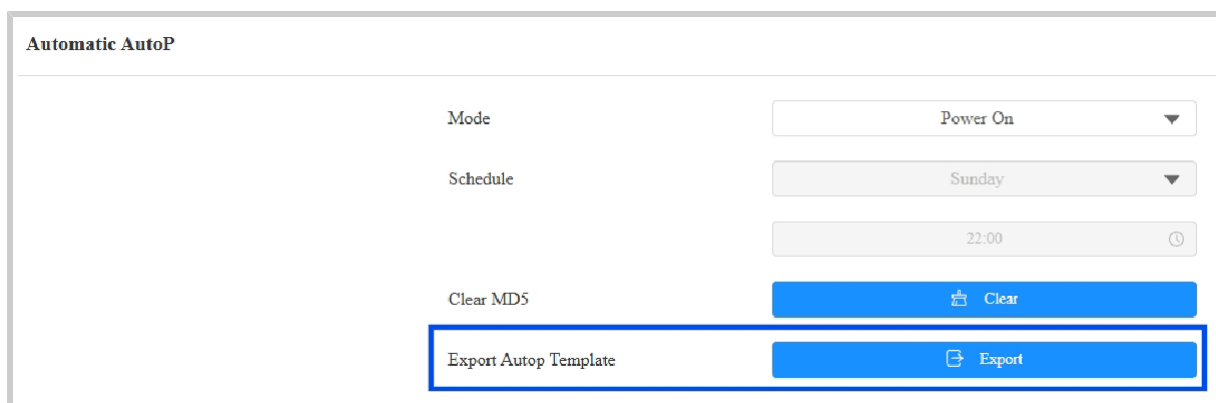
Automatic AutoP	
Mode	Power On
Schedule	Sunday
	22 (0~23Hour)
	0 (0~59Min)
Clear MD5	Clear
Export Autop Template	Export

- **Režim:**
 - **Zapnutí:** Nechte zařízení provádět Autop při každém spuštění při startu.
 - **Opakovaně:** Nechte zařízení provádět Autop podle plánu.
 - **Zapnutí + Opakovaně:** Kombinace režimů zapnutí a opakovaného zapnutí, což umožňuje zařízení provádět Autop pokaždé při spuštění nebo podle plánu.
 - **Hodinové opakování:** Nechte zařízení provádět Autop každou hodinu.
- **Plán:** Když je zvolen režim Zapnout + Opakovat, můžete zvolit konkrétní den a čas pro Autop.
- **Clear MD5:** Používá se ke srovnání existujícího autop souboru s autop souborem na serveru; pokud jsou soubory stejné, provisioning se zastaví, čímž se předejde zbytečnému automatickému provisioningu.

Statický provisioning

Můžete ručně nastavit konkrétní URL serveru pro stažení firmwaru nebo konfiguračního souboru. Pokud je nastaven automatický plán, zařízení provede automatické nastavení v určitý čas podle nastaveného harmonogramu. Navíc jsou protokoly TFTP, FTP, HTTP a HTTPS, které lze použít pro aktualizaci firmwaru a konfigurace zařízení.

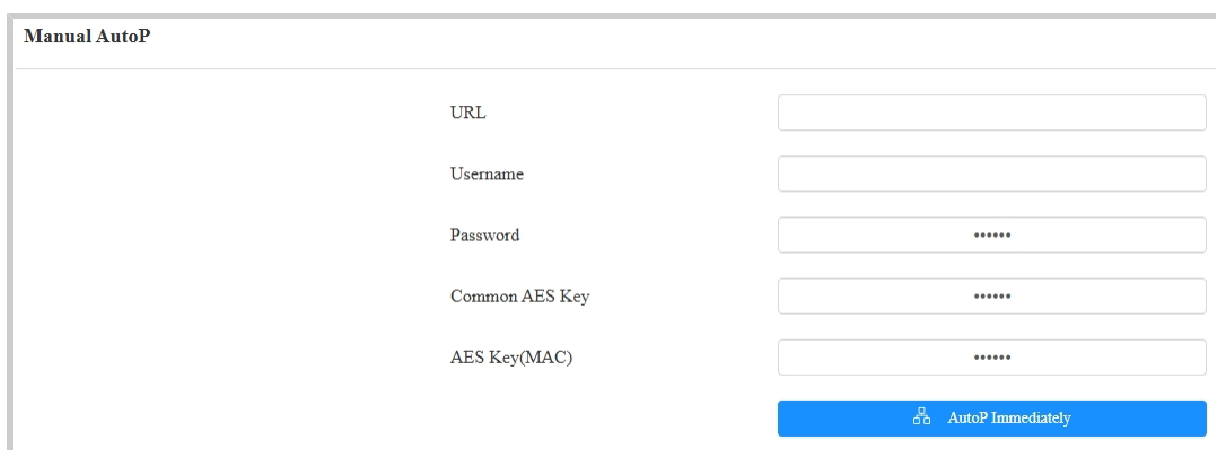
Stáhněte si šablonu Autop na rozhraní **System > Auto Provisioning > Automatic AutoP**.



Automatic AutoP

Mode	Power On ▼
Schedule	Sunday ▼
	22:00 ⌚
Clear MD5	Clear
Export Autop Template	Export

Nastavte AutoP server na **System > Auto Provisioning > manuální rozhraní AutoP**.



Manual AutoP

URL	
Username	
Password	
Common AES Key	
AES Key(MAC)	
	AutoP Immediately

- **URL:** Adresa TFTP, HTTP, HTTPS nebo FTP serveru pro provisioning.
- **Uživatelské jméno:** Nastavte uživatelské jméno, pokud server vyžaduje uživatelské jméno pro přístup.

- **Heslo:** Nastavte heslo, pokud server vyžaduje heslo pro přístup.
- **Běžný AES klíč:** Nastavte AES kód pro interkom, aby rozluštil obecný konfigurační soubor Auto Provisioning.
- **AES klíč (MAC):** Nastavte AES kód pro interkom, aby rozluštil konfigurační soubor automatického provisioningu založený na MAC.

Poznámka

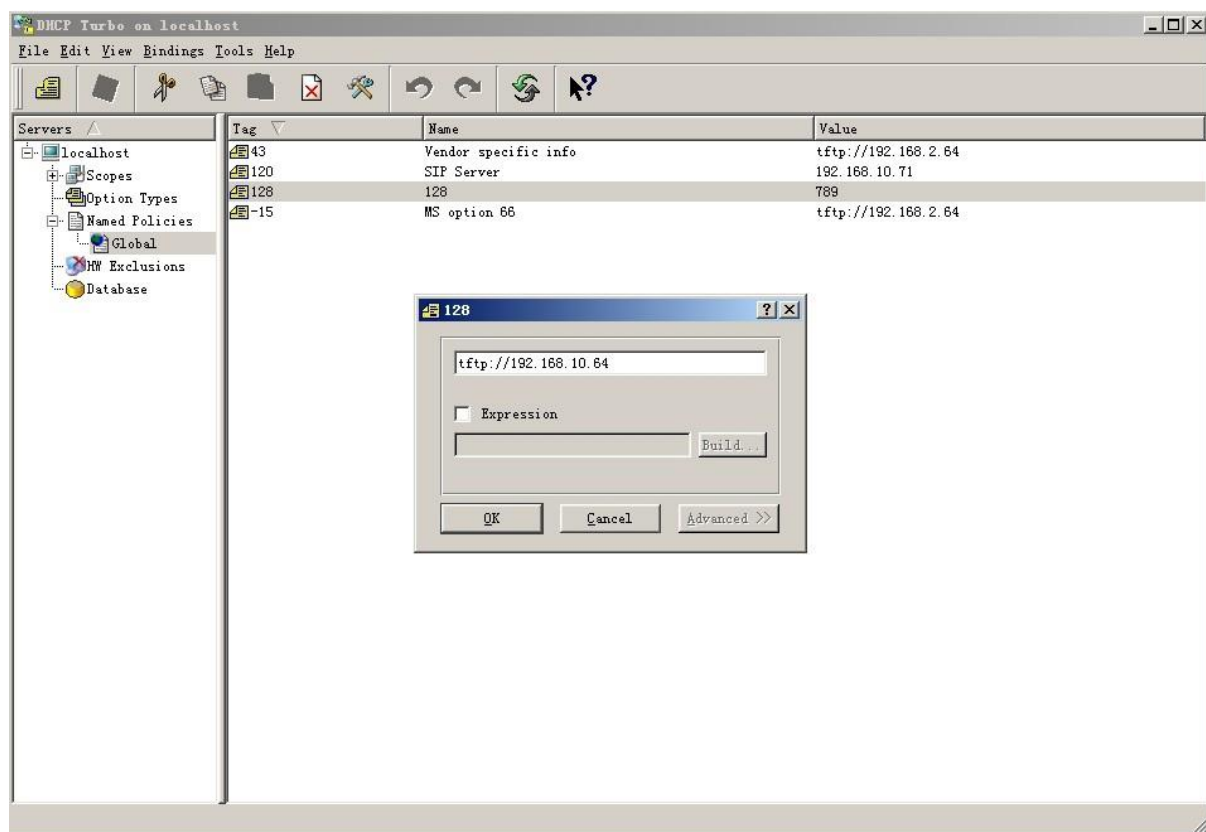
- AES jako jeden typ šifrování by měl být konfigurován pouze tehdy, když je konfigurační soubor zašifrován pomocí AES.
- Formát adresy serveru:
 - TFTP: tftp://192.168.0.19/
 - FTP: ftp://192.168.0.19/(umožňuje anonymní přihlášení)
ftp://username:password@192.168.0.19/(vyžaduje uživatelské jméno a heslo)
 - HTTP: http://192.168.0.19/(použijte výchozí port 80) http://192.168.0.19:8080/(použijte jiné porty, například 8080)

Tip

Akuvox neposkytuje uživatelsky specifikovaný server. Prosím, připravte si server TFTP/FTP/HTTP/HTTPS sami.

DHCP Provisioning

Automatické nastavení URL lze také získat pomocí možnosti DHCP, která umožňuje zařízení poslat požadavek na DHCP server na konkrétní kód DHCP volby. Pokud chcete použít **CustomOption**as definované uživateli s voličnými kódy v rozmezí 128-255), je nutné nastavit DHCP Custom Option na webovém rozhraní.



Poznámka

Typ Custom Option musí být řetězec. Hodnota je URL TFTP serveru.

Nastavte DHCP Autop v režimu Power On a exportujte šablonu AutoP pro úpravu konfigurace.

Stáhněte si šablonu Autop na rozhraní **System > Auto Provisioning > automatickém AutoP** .

Automatic AutoP

Mode	Power On ▼
Schedule	Sunday ▼
	22:00 ⌚
Clear MDS	Clear
Export AutoP Template	Export

Nastavte to na rozhraní **System > Auto Provisioning > DHCP Option** .

DHCP Option

Enabled	☒
Custom Option	(128~254)

(DHCP option 66/43 is enabled by default)

- **Vlastní možnost:** Zadejte DHCP kód, který odpovídá odpovídající URL, aby zařízení našlo konfigurační souborový server pro konfiguraci nebo upgrade.
- **DHCP Option 66:** Pokud není nic z výše uvedeného nastaveno, zařízení automaticky použije DHCP Option 66 k získání URL serveru pro upgrade. To se provádí v softwaru a uživatel to nemusí specifikovat. Aby to fungovalo, musíte nastavit DHCP server pro možnost 66 s aktualizovanou URL serveru.
- **DHCP Option 43:** Pokud zařízení nedostane URL z DHCP Option 66, automaticky použije DHCP Option 43. To se provádí v softwaru a uživatel to nemusí specifikovat. Aby to fungovalo, musíte nastavit DHCP server pro možnost 43 s aktualizovanou URL serveru.

PNP konfigurace

Plug and Play (PNP) je kombinace hardwarové a softwarové podpory, která umožňuje počítačovému systému rozpoznat a přizpůsobit se změnám konfigurace hardwaru s minimálním nebo žádným zásahem uživatele.

Klikněte [zde](#) pro sledování konfiguračního videa.

Zapni/vypněte to na webu v rozhraní **System > Auto Provisioning > PNP Option** .

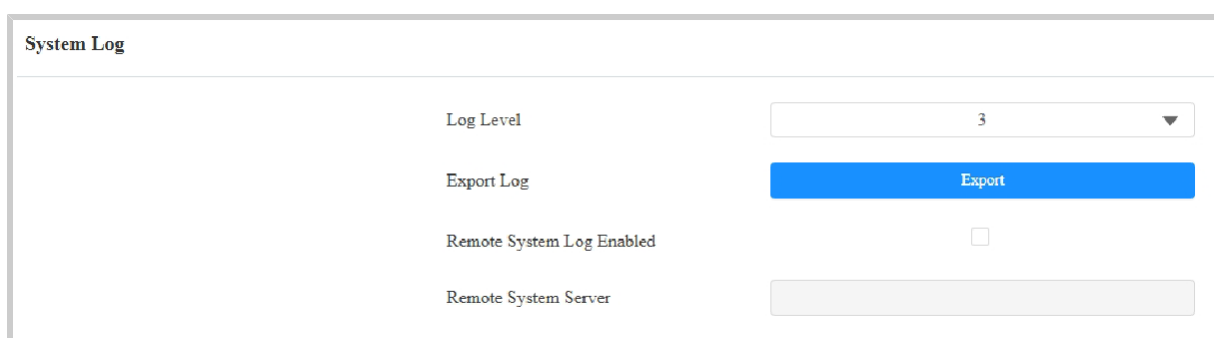
PNP Option
PNP Config Enabled ☒

Debug

Systémový log pro ladění

Systémové logy lze použít pro ladění.

Nastavte to na webovém rozhraní **System > Maintenance > System Log**.



The screenshot shows the 'System Log' configuration page. It contains four settings: 'Log Level' is a dropdown menu set to '3'; 'Export Log' is a blue button labeled 'Export'; 'Remote System Log Enabled' is an unchecked checkbox; and 'Remote System Server' is an empty text input field.

- **Úroveň logu:** Vyberte úroveň logu od 1 do 7. Technický tým Akuvoxu vás bude instruovat o konkrétní úrovni logu, která bude zadána pro účely ladění. Výchozí úroveň logu je 3. Čím vyšší je úroveň, tím je log úplnější.
- **Exportovat log:** Klikněte na záložku **Export**, abyste exportovali dočasný debug log soubor do lokálního počítače.
- **Aktivováno vzdálené systémové logování:** Nastavit, zda vzdálený server může přijímat záznam zařízení.

PCAP pro ladění

PCAP se používá k zachycení datového balíčku, který vstupuje a vychází ze zařízení, pro účely ladění a řešení problémů.

Nastavte to na webovém rozhraní **System > Maintenance > PCAP**.

PCAP

Specific Port

(1~65535)

PCAP

Start

Stop

Export

PCAP Auto Refresh Enabled

☐

- **Specifický port:** Vyberte konkrétní porty od 1 do 65535, aby bylo možné zachytit pouze datový paket z konkrétního portu. Pole můžete ve výchozím nastavení nechat prázdné.
- **PCAP:** Klikněte na záložku Start a Stop pro zachycení určitého rozsahu datových paketů, než kliknete na záložku Export, abyste datové pakety exportovali do svého lokálního počítače.
- **Automatické obnovování PCAP povoleno:** Pokud je povoleno, PCAP bude pokračovat v zachycování datových paketů i poté, co pakety dosáhnou maximální kapacity 1M. Pokud je deaktivován, PCAP zastaví zachycování datových paketů, jakmile zachycený paket dosáhne maximální kapacity 1MB.

Vzdálený ladicí server

Když má zařízení problém, můžete použít vzdálený ladicí server k vzdálenému přístupu k logu zařízení pro účely ladění.

Nastavte to na rozhraní **System > Maintenance > Remote Debug Server**.

Remote Debug Server

Enabled

☐

Connect Status

Disconnected

IP

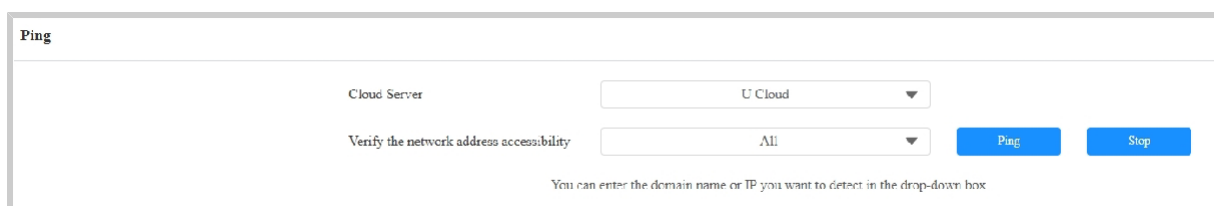
- **Stav připojení:** Zobrazit stav spojení mezi zařízením a serverem.
- **IP:** Zadejte IP adresu serveru.

Ping

Zařízení vám umožní ověřit přístupnost cílového serveru.

Nastavte to v rozhraní **System > Maintenance > Ping**. Klikněte na **Ping** pro spuštění detekce a výsledky se zobrazí na webu.

Můžete kliknout na **Exportovat** a stáhnout zprávu.



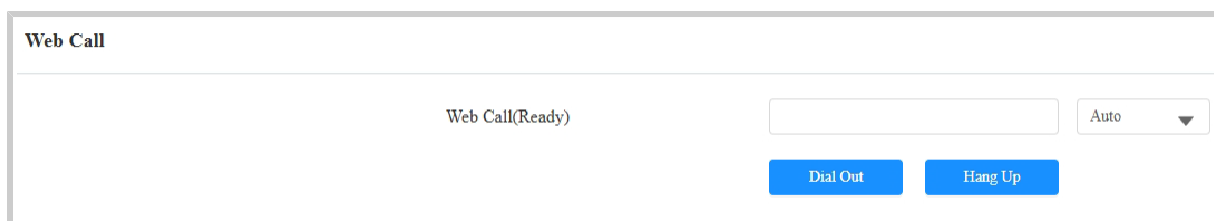
The screenshot shows the 'Ping' configuration window. It has a title bar 'Ping'. Below it, there are two dropdown menus. The first is labeled 'Cloud Server' and has 'U Cloud' selected. The second is labeled 'Verify the network address accessibility' and has 'All' selected. To the right of these dropdowns are two blue buttons: 'Ping' and 'Stop'. Below the buttons, there is a small text note: 'You can enter the domain name or IP you want to detect in the drop-down box'.

- **Cloud Server:** Server k ověření.
- **Ověřte přístupnost síťové adresy:** Typ služby zahrnuje TCP připojení, FTP službu, SIP službu atd. Můžete zvolit typ služby nebo jej zadat ručně.

Web Call

Funkce webových hovorů umožňuje volání přes webové rozhraní zařízení, které se běžně používá pro testování vzdálených hovorů.

Pro nastavení přejděte na webové rozhraní **System > Maintenance > Web Call**. Vyberte registrovaný SIP účet, zadejte IP/SIP číslo a klikněte na **Vytočit** pro uskutečnění hovoru.

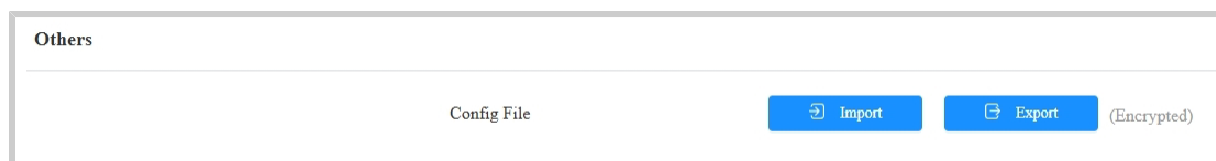


The screenshot shows the 'Web Call' interface. It has a title bar 'Web Call'. Below it, there is a text label 'Web Call(Ready)'. To the right of this label is a text input field and a dropdown menu with 'Auto' selected. Below these elements are two blue buttons: 'Dial Out' and 'Hang Up'.

Záloha

Můžete importovat nebo exportovat šifrované konfigurační soubory do svého lokálního počítače.

Nastavte to na webovém rozhraní **System > Maintenance > Others**. Importní soubor by měl být ve formátu .tgz/.conf/.cfg.



- **Konfigurační soubor:** Klikněte na **Exportovat** pro export konfiguračních položek jako šifrovaný soubor; klikněte na **Import** pro import konfiguračního souboru do zařízení. Konfigurační soubor slouží pouze k zálohování a obnově **nastavení konfigurace** zařízení. Neobsahuje uživatelská a kontaktní data.

Úprava hesla

Upravit heslo k webovému rozhraní

Můžete upravit přihlašovací heslo k webovému rozhraní zařízení jak pro administrátorské, tak uživatelské účty.

Přejděte do rozhraní **System > Security > Web Password Edit**. Vyberte administrátor pro administrátorský účet a uživatele pro uživatelský účet.

Klikněte na **Změnit heslo** pro úpravu hesla.

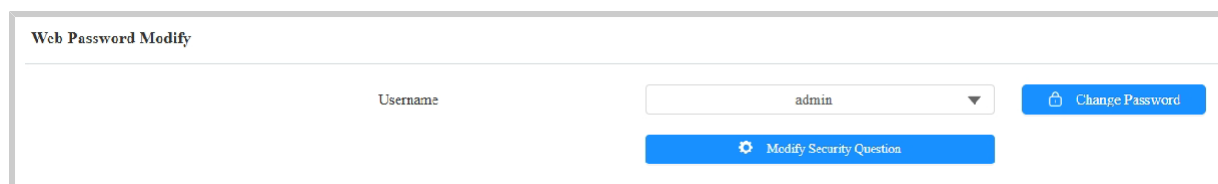
The screenshot displays the 'Web Password Modify' web interface. At the top, there is a header 'Web Password Modify'. Below it, a 'Username' dropdown menu is set to 'admin'. To the right of the dropdown is a blue button with a lock icon and the text 'Change Password'. Below the dropdown is another blue button with a gear icon and the text 'Modify Security Question'. A modal dialog titled 'Change Password' is open in the center. The dialog contains a message: 'The password must be at least eight characters long, containing at least one uppercase letter, one lowercase letter, and one number.' Below this message, there are three input fields: 'Username' (pre-filled with 'admin'), 'Current Password', 'New Password', and 'Confirm Password'. Each input field has a small circular icon with a diagonal line through it on the right side. At the bottom of the modal, there are two buttons: 'Cancel' and 'Change'. The background of the interface is dimmed, showing parts of the 'Account Manager' and 'Tamper Alarm' sections.

Upravit bezpečnostní otázky

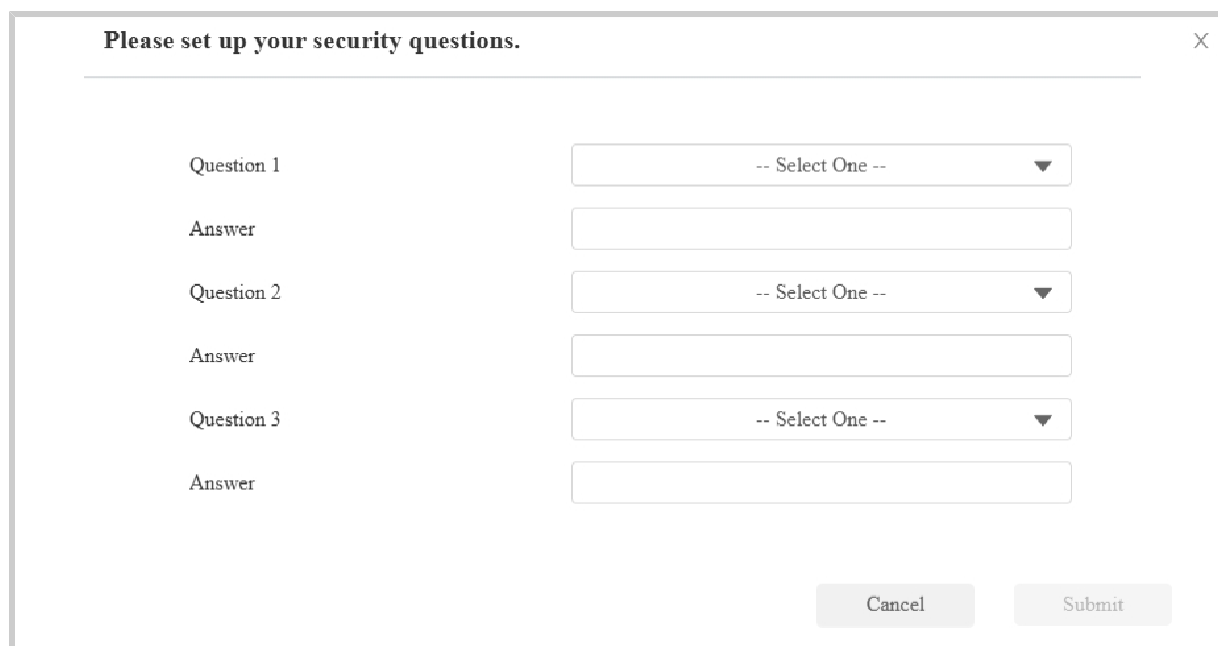
Bezpečnostní otázky vám umožní resetovat webové heslo, pokud ho zapomenete. Po nastavení bezpečnostních otázek můžete kliknout na "Zapomenout heslo" v přihlašovacím rozhraní, zadat odpovědi a zobrazí se okno pro reset hesla.

Pokud bezpečnostní otázky nenastavíte, kliknutím na "Odpovědět na bezpečnostní otázky" budete vyzváni k "Kontaktujte svého poskytovatele služeb".

Pro nastavení přejděte do rozhraní **System > Security > Web Password Edit**. Klikněte na **Upravit bezpečnostní otázky**.



Nejprve musíte zadat správné heslo pro ověření a poté nastavit bezpečnostní otázky.

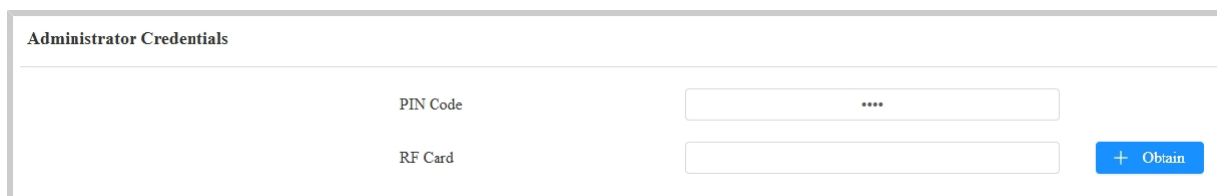


Upravit administrátorské přihlašovací údaje

Administrátorské přihlašovací údaje se používají k přístupu k

systémovým nastavením zařízení. Můžete nastavit oba (PIN a RF kartu) nebo si vybrat jedno.

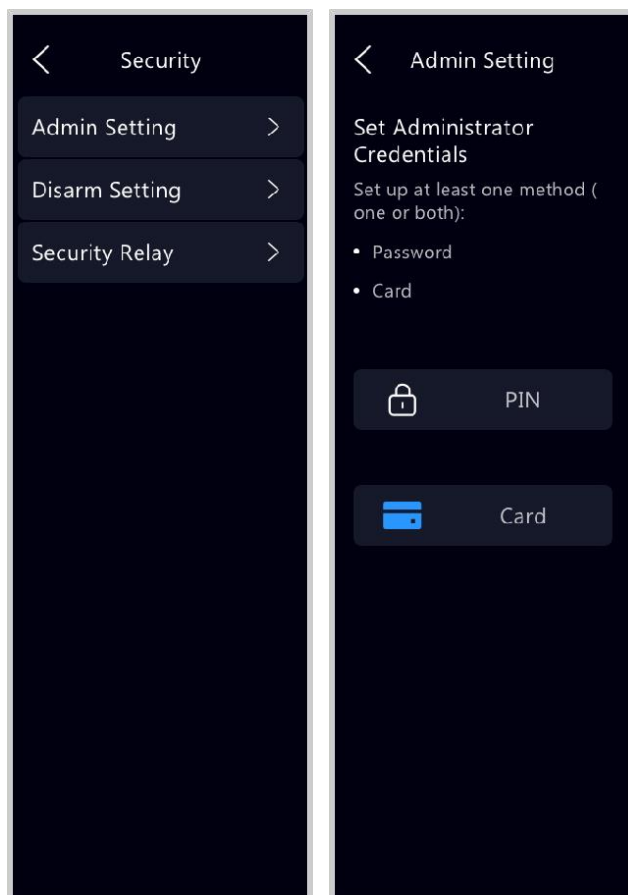
Pro nastavení přejděte do rozhraní **System > Security > Administrator Credentials**.



The image shows a web interface titled "Administrator Credentials". It contains two input fields: "PIN Code" with a masked value "****" and "RF Card". To the right of the "RF Card" field is a blue button labeled "+ Obtain".

- **PIN kód:** Nastavte 6 až 8 číslic.
- **RF karta:** Klikněte na **Získat** při vkládání karty do zařízení.

Přihlašovací údaje můžete také upravit na obrazovce **Nastavení > zabezpečení > Nastavení administrátorů**.



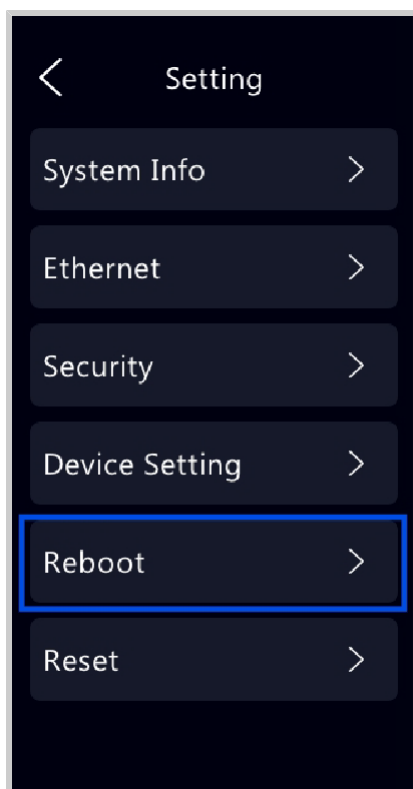
Restart a reset systému

Reboot

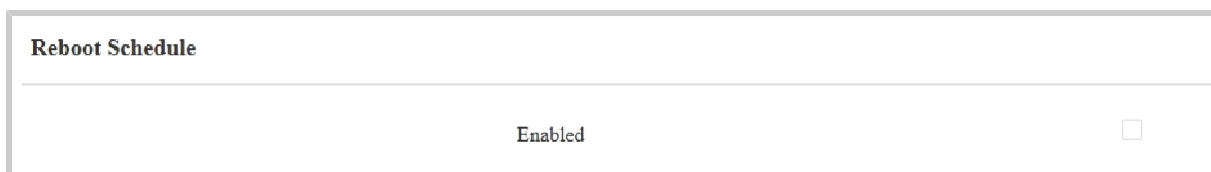
Restartujte zařízení na webovém rozhraní **System > Upgrade**.

Basic	
Firmware Version	1115.30.10.408
Hardware Version	1115.0
Upgrade	 Upgrade
Reset To Factory Setting	 Reset
Reset Configuration To Default State	 Reset
Reboot	 Reboot

Nebo ho restartuj na obrazovce **Nastavení**.



Plán restartu si můžete nastavit na webovém rozhraní **System > Auto Provisioning > Reboot Schedule**.

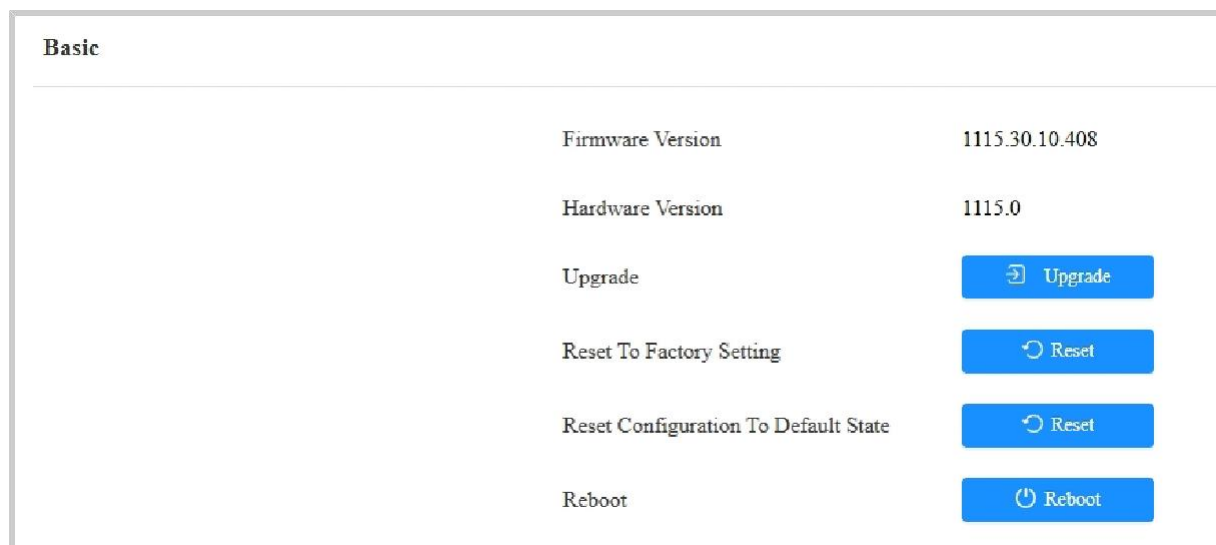


Reset

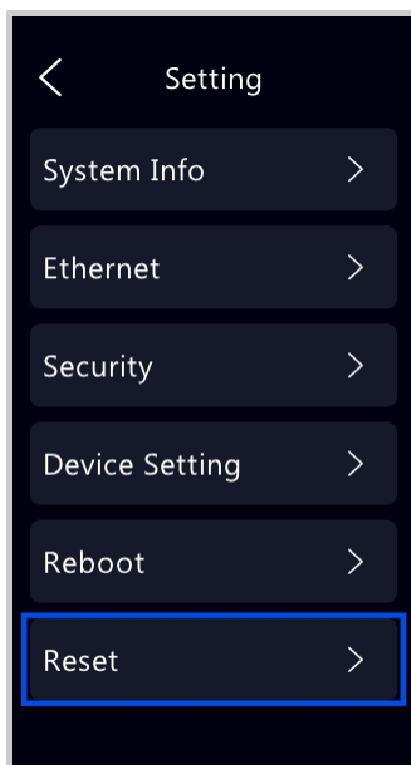
Zařízení nabízí dvě možnosti resetování:

- **Obnovit na tovární nastavení:** Obnovit všechna data na tovární nastavení.
- **Resetovat konfiguraci na výchozí stav:** Zachovat uživatelská data, jako jsou RF karty, data o obličeji, rozvrhy a záznamy hovorů.

Resetujte zařízení na webu **System > Upgrade** interface.



Nebo ho resetovat na obrazovce **Nastavení**.



Tip

Zařízení také podporuje resetování pomocí fyzického tlačítka na zadní straně.

- Stiskněte tlačítko a držte ho asi 3 sekundy.
- Podsvícení v oblasti čtečky karet a doplňovací kontrolka se rozsvítí, zařízení přejde do továrního resetu a restartu.

