



PORTIER A BOUTON

Manuel de Configuration

Applicable Models: R20A/R20B/R26C/R26P/E11R/E12/E21A/E21V

Version : 1.0|Date: Juin.2021

A propos de ce manuel

Nous vous remercions d'avoir choisi le portier Akuvox série R20A/R20B/R26C/R26P/E11R/E21A/E21V/E12W. Ce manuel est destiné aux administrateurs qui doivent configurer correctement le portier. Ce manuel s'applique à la version 220.30.2.104 , 110.30.1.216 , 226.30.2.10 , 221.30.1.106, 12.30.1.103, et il fournit toutes les configurations pour les fonctions et caractéristiques du portier Akuvox. Veuillez visiter le forum Akuvox ou consulter le support technique pour toute nouvelle information ou les derniers firmwares.

Introduction des icônes et des



Attention :

- **Respectez toujours ces informations afin d'éviter que les personnes ne se blessent.**



Attention :

- **Respectez toujours ces informations afin d'éviter d'endommager l'appareil.**



Note :

- **Informations et conseils sur l'utilisation efficace de l'appareil.**



Conseil :

- **Informations utiles pour une utilisation rapide et efficace de l'appareil.**

Documentation

Il est conseillé de se référer aux documents connexes pour plus d'informations techniques via le lien ci-dessous :

<http://knowledge.akuvox.com>

Pour contacter le support technique en France contactez Akuvox France sur support@akuvox-france.fr

Documentation

Table des matières

1. Aperçu des produits	1
2. Journal des modifications	2
3. Spécifications du modèle	3
4. Introduction au menu de configuration	5
5. Accéder à l'appareil	7
5.1. Obtenir l'adresse IP du dispositif	7
5.2. Accéder aux paramètres de l'appareil sur l'interface Web	8
6. Réglage de la langue et de l'heure	9
6.1. Réglage de la langue	9
6.2. Réglage de l'heure	9
7. Réglage des LED	11
7.1. Réglage des LED infrarouges	11
7.2. État de l'affichage LED	12
7.3. Configurer un écran LED à partir d'une URL HTTP	13
7.4. Réglage des LED sur la zone du lecteur de carte	13
7.5. Réglages des LED sur le clavier	15
8. Configuration du volume et de la tonalité	16
8.1. Configuration du volume	16
8.2. Configuration de la tonalité de porte ouverte	17
8.3. Télécharger les fichiers de tonalité	18
8.3.1. Télécharger la sonnerie de rappel	18
8.3.2. Télécharger la tonalité de porte ouverte	18
9. Paramètres du réseau	20
9.1. Statut du réseau	20
9.2. Configuration du réseau de dispositifs	20
9.3. Déploiement des dispositifs dans le réseau	21
9.4. Configuration RTP locale du dispositif	22
9.5. Réglage du NAT	23
9.6. Réglage du WIFI	24
10. Configuration des appels intercom	25
10.1. Appel IP & Configuration de l'appel IP	25
10.2. Appel SIP & Configuration de l'appel SIP	25
10.3. Enregistrement du compte SIP	26
10.4. Configuration du serveur SIP	27
10.5. Configurer le serveur proxy sortant	27
10.6. Configurer le type de transmission des données	28
10.7. Configurer la fonction d'appel	29
10.7.1. DND	29
10.7.2. Appel par bouton-poussoir	30
10.7.3. Robin Call	31
10.7.4. Appel Web	31

10.7.5. Réponse automatique.....	32
10.7.6. Multicast.....	33
10.7.7. Configurer la durée maximale d'un appel.....	34
10.7.8. Durée maximale de la composition.....	34
11. Configuration des codecs audio et vidéo pour les appels SIP	36
11.1. Configuration du codec audio.....	36
11.2. Configuration du Cod Cod Cod Vidéo.....	37
11.3. Configurer la transmission des données DTMF.....	38
12. Configuration de la liste blanche d'accès	39
12.1. Gestion du groupe de contacts.....	39
12.2. Gestion des contacts.....	40
13. Réglage du relais	41
13.1. Réglage du commutateur de relais.....	41
13.2. Sélectionner le relais de la cloche du carillon.....	42
13.3. Réglage du relais Web.....	42
14. Gestion des horaires d'accès aux portes.....	45
14.1. Configurer le calendrier d'accès aux portes.....	45
14.1.1. Gestion des horaires d'accès aux portes.....	45
15. Configuration du déverrouillage des portes	48
15.1. Configurer le format de la carte d'accès.....	48
15.2. Configurer la carte d'accès pour le déverrouillage de la porte.....	49
15.3. Importation et exportation de données de cartes de contrôle d'accès.....	50
15.4. Configurer le relais ouvert via HTTP pour le déverrouillage de porte.....	51
15.5. Configurer le bouton de sortie pour le déverrouillage de la porte.....	52
16. Sécurité	54
16.1. Réglage de l'alarme de sabotage.....	54
16.2. Détection de mouvement.....	54
16.2.1. Configurer la détection de mouvement.....	55
16.3. Réglage de la notification de sécurité.....	56
16.3.1. Réglage de la notification par courriel.....	56
16.3.2. Paramètres de notification FTP.....	57
16.3.3. Réglage de la notification d'appel SIP.....	58
16.3.4. Configuration de la notification d'URL HTTP.....	58
16.3.5. Réglage de la notification TFTP.....	59
16.4. Configuration des actions de sécurité.....	59
16.4.1. Configurer l'action du bouton poussoir.....	59
16.4.2. Configurer l'action de mouvement.....	60
16.4.3. Configurer l'action d'entrée.....	60
16.5. Cryptage de la voix.....	61
16.6. Agent de l'utilisateur.....	62
17. Moniteur et image	63
17.1. Surveillance des cours d'eau RTSP.....	63
17.1.1. Paramètres de base de RTSP.....	63
17.1.2. Réglage du flux RTSP.....	64

17.2. Capture d'images MJPEG	66
17.3. ONVIF	68
17.4. Stream en direct.....	69
18. Bûches.....	70
18.1. Journaux d'appels.....	70
18.2. Bûches de porte	71
19. Déboguer.....	73
19.1. Journal des événements.....	73
19.2. Journal du système	74
19.3. PCAP.....	75
20. Mise à jour du micrologiciel.....	77
21. Sauvegarde.....	78
22. Auto-provisionnement via le fichier de configuration	79
22.1. Principe du provisionnement.....	79
22.2. Fichiers de configuration pour l'auto-provisionnement.....	80
22.3. Programme AutoP	81
22.4. Configuration PNP	82
22.5. Configuration de l'approvisionnement statique	82
23. Intégration avec un dispositif tiers	84
23.1. Intégration via Wiegand	84
23.2. Intégration via l'API HTTP	85
24. Modification du mot de passe.....	88
24.1. Modifier le mot de passe de l'interface Web de l'appareil.....	88
24.2. Configurer la déconnexion automatique de l'interface Web.....	88
25. Redémarrage et réinitialisation du système.....	89
25.1. Redémarrage	89
25.2. Réinitialiser	89
26. Abréviations	90
27. FAQ	92
28. Nous contacter	95

















1. Aperçu du produit

La sécurité qui découle de la possibilité de contrôler qui entre dans votre bâtiment et de confirmer verbalement et visuellement son identité est incommensurable. L'Akuvox R20A/R20B/R26C/R26P/E11R/E21A/E21V/E12W est un portier compatible SIP, mains libres et vidéo (en option). Il peut être connecté aux moniteurs intérieurs Akuvox pour contrôler et surveiller l'accès à distance. Les utilisateurs peuvent communiquer avec les visiteurs via des appels audio et vidéo, et déverrouiller la porte en cas de besoin. Le portier vous permet de surveiller facilement une porte d'entrée ou un portail et vous donne la tranquillité d'esprit de savoir que votre installation est plus sécurisée.

2. Journal des modifications

Le journal des modifications sera mis à jour ici en fonction des changements apportés à la nouvelle version du logiciel.

3. Spécifications du modèle

Modèle et caractéristiques	R20A	R20B	R26C	R26P	E11R	E21V	E21A	E12W
       								
Bouton	1 Bouton physique	5 Boutons physiques	1 Bouton physique	1 Bouton physique	1 Bouton physique	1 Bouton physique	1 Bouton physique	1 Bouton physique
Logement Matériau	Aluminium	Aluminium	Aluminium	Aluminium	Aluminium	Aluminium	Aluminium	Plastique
Appareil photo	2 Mégapixels, éclairage automatique	2 Mégapixels, éclairage automatique	2 Mégapixels, éclairage automatique	2 Mégapixels, éclairage automatique	2 Mégapixels, éclairage automatique	2 Mégapixels, éclairage automatique	X	2 Mégapixels, éclairage automatique
Entrée du relais	2	2	3	3	2	2	2	2
Relais Out	2	2	2	2	2	2	2	1
RS485	√	√	√	√	√	X	X	√
PoE	√	√	√	√	√	√	√	√
RAM	64MB	64MB	128MB	128MB	64MB	128MB	128MB	128MB
ROM	128MB	128MB	16MB	16MB	128MB	128MB	128MB	16MB
Carte Lecteur	√	√	√	X	√	X	X	√
IP Classement	IP65	IP65	IP65	IP65	X	IP65	IP65	IP65
IK Classement	X	X	X	X	X	X	IK10	X

Mur Montag e	√	√	√	√	√	X	X	√
Chasse d'eau	√	√	√	√	X	√	√	X

Mountin g								
--------------	--	--	--	--	--	--	--	--

4. Introduction au menu de configuration

- **Statut** : cette section vous donne des informations de base telles que les informations sur le produit, les informations sur le réseau, les informations sur le compte, etc.
- **Compte** : cette section concerne le compte SIP, le serveur SIP, le serveur proxy, le type de protocole de transport, le codec audio&vidéo, le DTMF, la minuterie de session, etc.
- **Réseau** : cette section traite principalement du paramétrage de l'IP statique et du DHCP, du paramétrage du port RTP, du déploiement des périphériques, etc.
- **Intercom** : cette section couvre les paramètres de l'intercom, le journal des appels, etc.
- **Surveillance** : cette section couvre la détection de mouvement, RTSP, MJPEG, ONVIF, Live stream.
- **Contrôle d'accès** : cette section couvre le contrôle d'entrée, le relais, les paramètres de carte, le paramètre de reconnaissance faciale, le code PIN privé, la connexion Wiegand, etc.
- **Locataires** : cette section concerne la gestion des locataires et le plan de dialogue.
- **Appareil** : cette section comprend les paramètres de l'éclairage, l'affichage des onglets et des boutons, les paramètres LCD et les paramètres vocaux.
- **Paramètres** : cette section comprend l'heure et la langue, les paramètres d'action, les paramètres de porte, la programmation du contrôle d'accès.
- **Mise à niveau** : cette section couvre la mise à niveau du micrologiciel, la réinitialisation et le redémarrage de l'appareil, l'auto-provisionnement du fichier de configuration et le diagnostic des erreurs.
- **Sécurité** : cette section est destinée à la modification du mot de passe.
- **Sélection du mode** :

1. **Mode découverte** : Il s'agit d'un mode de configuration "plug and play". Les appareils Akuvox se configurent automatiquement lorsque les utilisateurs les mettent sous tension et les connectent au réseau. C'est un mode qui permet de gagner beaucoup de temps.

et il apportera un grand confort aux utilisateurs en réduisant les opérations manuelles. Ce mode ne nécessite aucune configuration préalable par l'administrateur.

2. **Mode Cloud** : Akuvox Cloud est un système de gestion tout-en-un. Akuvox Cloud est le service mobile qui permet le contrôle de l'audio, de la vidéo et de l'accès à distance entre les téléphones intelligents et les interphones Akuvox. Toutes les configurations de l'appareil seront émises automatiquement à partir du nuage. Si les utilisateurs décident d'utiliser le service Akuvox Cloud, veuillez contacter le support technique d'Akuvox, qui vous aidera à configurer les paramètres correspondants avant de les utiliser.
3. **Mode SDMC** : Le mode SDMC (**SIP Device Management Controller**) est un mode de gestion simple et efficace.

logiciel complet pour la gestion des bâtiments. Il fournit une topographie pour une communauté tout en vous offrant une interface de configuration graphique pour l'accès aux portes, l'interphone, la surveillance, l'alarme, etc. Il s'agit d'un outil pratique pour le gestionnaire immobilier pour gérer, exploiter et entretenir la communauté.

● Sélection des outils

Akuvox dispose de nombreux outils de configuration pour vous permettre de configurer les appareils de manière plus pratique. Voici une liste des outils les plus courants. Si vous avez besoin d'un outil, veuillez contacter votre administrateur pour l'obtenir.

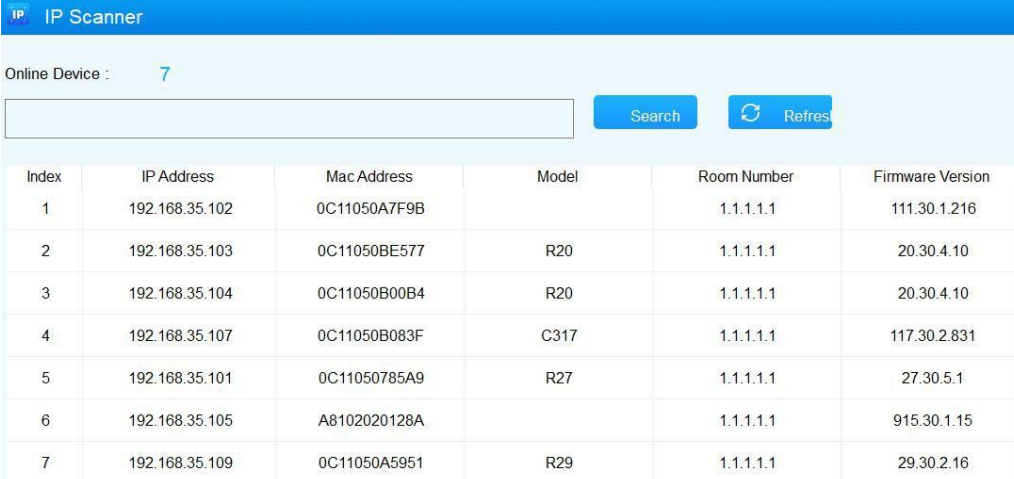
1. **SDMC** : SDMC est adapté à la gestion de grandes communautés de dispositifs Akuvox, y compris le contrôle d'accès, l'information des résidents, le contrôle à distance des dispositifs, etc.
2. **Outil de mise à niveau d'Akuvox** : Mise à niveau des dispositifs Akuvox par lots sur un **réseau local** (LAN).
3. **Akuvox PC Manager** : Distribuez tous les éléments de configuration en lot sur un réseau local.
4. **Scanner IP** : il est utilisé pour rechercher les adresses IP des dispositifs Akuvox sur un réseau local.
5. **FacePro** : Gérer les données du visage en lot pour le portier sur un réseau local.

5. Accéder à l'appareil

Les paramètres du système des séries R20A/R20B/R26C/R26P/E11R/E21V/E21A/E12W sont accessibles sur l'interface web du dispositif.

5.1. Obtenir l'adresse IP du dispositif

Vérifiez l'adresse IP de l'appareil en maintenant le bouton poussoir pendant 5s. Ou recherchez l'adresse IP de l'appareil à l'aide du scanner IP dans le même réseau LAN. Il suffit de cliquer sur l'onglet **Scan** dans le scanner IP pour vérifier l'IP du dispositif.



The screenshot shows the 'IP Scanner' interface. At the top, it says 'Online Device : 7'. Below this is a search bar and two buttons: 'Search' and 'Refresh'. A table lists the following data:

Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.35.102	0C11050A7F9B		1.1.1.1.1	111.30.1.216
2	192.168.35.103	0C11050BE577	R20	1.1.1.1.1	20.30.4.10
3	192.168.35.104	0C11050B00B4	R20	1.1.1.1.1	20.30.4.10
4	192.168.35.107	0C11050B083F	C317	1.1.1.1.1	117.30.2.831
5	192.168.35.101	0C11050785A9	R27	1.1.1.1.1	27.30.5.1
6	192.168.35.105	A8102020128A		1.1.1.1.1	915.30.1.15
7	192.168.35.109	0C11050A5951	R29	1.1.1.1.1	29.30.2.16

**Note :**

- Pour le R20B, il suffit de maintenir le premier bouton poussoir pendant 5s pour obtenir l'adresse IP.

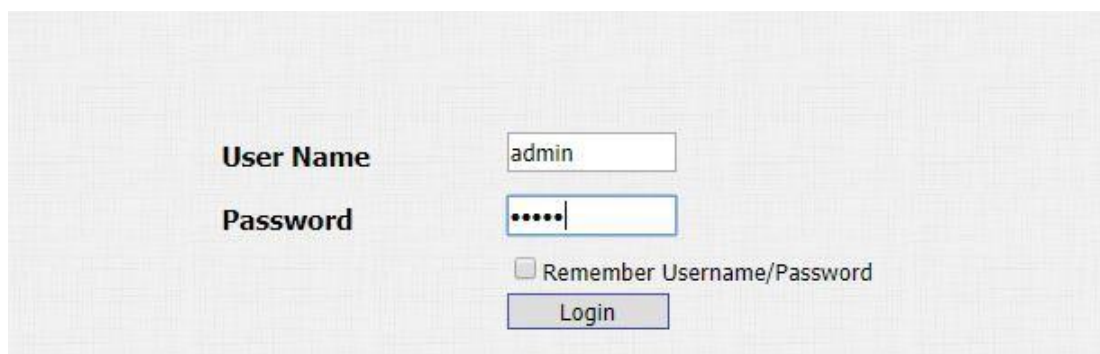
5.2.

Accès à l'

interface

DeviceSetting sur le Web

Saisissez l'adresse IP de l'appareil sur le navigateur Web afin de vous connecter à l'interface Web de l'appareil où vous pouvez configurer et régler les paramètres, etc. Le nom d'utilisateur et le mot de passe initiaux sont tous "admin". Veuillez respecter la casse des noms d'utilisateur et des mots de passe saisis.



User Name: admin

Password:

Remember Username/Password

Login



Co

- Vous pouvez également obtenir l'adresse IP de l'appareil en utilisant l'Akuvox IP pour se connecter à l'interface web du dispositif. Veuillez vous référer à l'URL ci-dessous pour l'application du scanner IP : [http://wiki.akuvox.com/doku.php?id=tool:ip_scanner&s\[\]=ip&s\[\]](http://wiki.akuvox.com/doku.php?id=tool:ip_scanner&s[]=ip&s[])



Note

- Le navigateur Google Chrome est fortement

6. Réglage de la langue et de l'heure

6.1. Réglage de la langue

Lorsque vous configurez l'appareil pour la première fois, il se peut que vous deviez régler la langue en fonction de vos besoins ou vous pouvez le faire plus tard si nécessaire. La langue peut être configurée sur l'interface Web de l'appareil, **Phone > Time/Lang > Web Language**, selon vos préférences.



Web Language

Type English ▼

Réglage des paramètres :

- **Type** : choisissez une langue web appropriée. Normalement, l'anglais est la langue web par défaut.



Note :

- Pour E12, le chemin d'accès est le suivant : **Setting > Time/Lang > Web Language**.

6.2. Réglage de l'heure

La configuration de l'interface Web de l'appareil est identique à celle de l'appareil, mais elle vous permet de configurer l'adresse du serveur NTP que vous avez obtenu pour synchroniser automatiquement votre heure et votre date. Et lorsque votre fuseau horaire est sélectionné, l'appareil notifie automatiquement son fuseau horaire au serveur NTP afin que ce dernier puisse synchroniser la configuration du fuseau horaire sur votre appareil.

NTP	
Time Zone	GMT+0:00 GMT ▼
Primary Server	0.pool.ntp.org
Secondary Server	1.pool.ntp.org
Update Interval	3600 (>= 3600s)
System Time	03:25:12

Réglage des paramètres :

- **Fuseau horaire** : sélectionnez le fuseau horaire spécifique en fonction de l'endroit où l'appareil est utilisé, puis appuyez sur l'onglet **Confirmer** pour la confirmation. Le fuseau horaire par défaut est **GMT+0.00**.
- **Primary/Secondary Server** : le serveur de fuseau horaire, normalement il obtiendra automatiquement l'heure lors de la connexion au réseau. Le serveur secondaire prend effet lorsque le serveur primaire est invalide.
- **Update Interval** : pour configurer l'intervalle entre deux requêtes NTP consécutives.

Vous pouvez également configurer l'heure manuellement, en cochant la case **Manuel**, et en saisissant les données relatives à l'heure.

Type	
<input checked="" type="radio"/> Manual	
Date	<input type="text"/> Year <input type="text"/> Mon <input type="text"/> Day
Time	<input type="text"/> Hour <input type="text"/> Min <input type="text"/> Sec
<input type="radio"/> Auto	

7. Réglage de la LED

7.1. Réglage des LED infrarouges

La LED infrarouge est utilisée dans les environnements sombres dans lesquels un résident peut ne pas être en mesure de voir clairement un visiteur via la vidéo du portier. Si la LED infrarouge est désactivée, le portier passe en mode nuit pour que vous puissiez voir clairement le visiteur.

LED	
LED Type	Auto ▾
Min Photoresistor	20
Max Photoresistor	45

Réglage des paramètres :

- **Type de LED** : sélectionnez **"Auto"** si vous souhaitez que la lumière LED infrarouge s'allume automatiquement en fonction du réglage. sélectionnez **"Always ON"** pour permettre à la lumière LED infrarouge de rester allumée en permanence. sélectionnez **"Always OFF"** pour éteindre la lumière LED infrarouge. Le mode LED est réglé sur **"Always OFF" (Toujours éteint)** par défaut. sélectionnez **"Schedule" (Calendrier)** pour allumer la LED infrarouge en fonction de l'horaire prévu.
- **Photorésistance Min/Max** : définissez la valeur minimale et maximale de la photorésistance en fonction de la valeur réelle actuelle de la photorésistance détectée pour contrôler **l'allumage et l'extinction de** la lumière LED. Vous pouvez définir la valeur maximale de la photorésistance pour que la LED IR s'allume et la valeur minimale pour qu'elle s'éteigne. Par défaut, les valeurs minimale et maximale de la photorésistance vont respectivement de **"0"** minimum à **"1000"** maximum.
- **Heure de début** : définissez l'heure de début de l'allumage de la LED infrarouge.
- **End Time (Heure de fin)** : définissez l'heure à laquelle la LED infrarouge doit s'éteindre.

Note :

- L'heure de début et l'heure de fin ne seront pas affichées, sauf si vous sélectionnez **Temps spécifique** pour votre mode LED.

7.2. État de l'affichage LED

Le réglage de l'affichage LED est utilisé pour afficher les changements de lumière du bouton d'appel dans les six états : normal (inactif), hors ligne, appelant, parlant et recevant un appel. L'utilisateur peut également vérifier le mode actuel du dispositif grâce à l'état des LED. Pour le configurer sur l'interface web **Intercom > LED Setting** de l'appareil.

LED Status

State	Color Off	Color On	Blink Mode
NORMAL ▼	OFF ▼	Blue ▼	Always On ▼
OFFLINE ▼	OFF ▼	Red ▼	2500/2500 ▼
CALLING ▼	OFF ▼	Blue ▼	2500/2500 ▼
TALKING ▼	OFF ▼	Green ▼	Always On ▼
RECEIVING ▼	OFF ▼	Green ▼	2500/2500 ▼

L'état par défaut de l'affichage LED :

État des LED		Description
Bleu	Toujours en cours	Statut normal
	Clignotant	Appel à
Rouge	Clignotant	Le réseau est indisponible
Vert	Toujours sur	Parler lors d'un appel
	Clignotant	Réception d'un appel
Rose	Clignotant	Mise à jour de

Configuration des paramètres :

- **État** : il existe cinq états : **Normal, Hors ligne, Appeler, Parler et Recevoir.**

- **Couleur désactivée** : l'état par défaut est **désactivé**.
- **Couleur activée** : il peut prendre en charge trois couleurs : **Rouge, Vert, Bleu**.
- **Mode de clignotement** : pour configurer les différentes fréquences de clignotement.

 **Note :**

- L'élément Status et Color off ne peut pas être modifié.
- La LED du mode de mise à niveau ne peut pas être ajustée.
- E12W supporte trois couleurs : **Rouge, Bleu et Violet**.

7.3. Configurer un écran LED à partir d'une URL HTTP

Les portiers Akuvox permettent d'utiliser l'URL HTTP pour contrôler à distance l'état de l'affichage LED. Vous pouvez entrer l'URL HTTP dans le navigateur pour gérer la couleur et la fréquence des LED.



Configuration des paramètres :

- **Format de l'URL HTTP :**
`http://PhoneIP/fcgi/do?action=LedAction&State=1&Color=1&Mode=2500`
- **Statut** : 1=En attente ; 2=Défaut de ligne ; 3=Appel ; 4=Parole ; 5=Réception ; **Couleur** : 1=Vert ; 2=Bleu ; 3=Rouge ; **Mode** : 0=Toujours allumé ; 1=Toujours éteint ; 500/1000/1500/2000/25000/3000

7.4. Réglage des LED sur la zone du lecteur de cartes

Vous pouvez activer ou désactiver l'éclairage LED sur la zone du lecteur de cartes selon vos besoins sur l'interface web. Si vous ne souhaitez pas que le voyant lumineux de la zone du lecteur de cartes reste allumé, vous pouvez également

définir le moment exact où il sera allumé.

période pendant laquelle la lumière LED peut être désactivée afin de réduire la consommation d'énergie électrique.

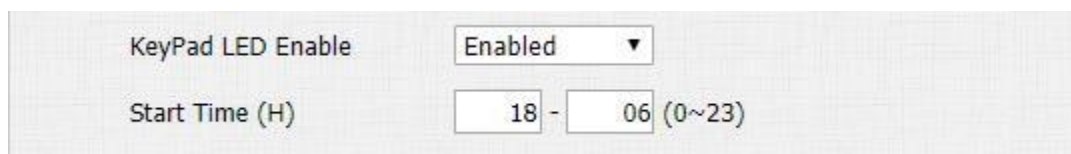
Card LED Enable	Enabled ▼
Start Time (H)	18 - 06 (0~23)

Configuration des paramètres :

- **Activé** : Cochez la case si vous souhaitez activer l'éclairage de la LED du lecteur de carte et vice versa.
- **Heure de début - Heure de fin (H)** : entrez l'intervalle de temps pendant lequel l'éclairage LED sera valide, par exemple, si l'intervalle de temps est réglé de **8-0 (Heure de début - Heure de fin)**, cela signifie que la lumière LED restera allumée pendant l'intervalle de temps de **8:00 à 12:00** pendant une journée (24 heures).

7.5. Réglages des LED sur le clavier

Vous pouvez activer ou désactiver l'éclairage LED du clavier selon vos besoins sur l'interface web. Si vous préférez que l'éclairage LED du clavier ne reste pas allumé, vous pouvez également définir la durée exacte pendant laquelle l'éclairage LED peut être activé afin de réduire la consommation d'énergie électrique, etc.



KeyPad LED Enable	Enabled ▼
Start Time (H)	18 - 06 (0~23)

Réglage des paramètres :

- **Activation de la LED du clavier** : Cliquez pour activer ou désactiver l'éclairage de la LED du clavier.
- **Heure de début (H)** : Entrez la durée de validité de l'éclairage LED. Par exemple, si l'intervalle de temps est de 18-22, cela signifie que la lumière LED restera allumée pendant la période allant de 18h00 à 22h00 au cours d'une journée.

8. Configuration du volume et de la tonalité

La configuration du volume et de la tonalité dans le portier Akuvox fait référence au volume du microphone, au volume du haut-parleur, au volume de l'alarme tempérée, à la tonalité de rappel et à la configuration de la tonalité de porte ouverte. En outre, vous pouvez télécharger la tonalité que vous aimez pour enrichir votre expérience utilisateur personnalisée.

8.1. Configuration du volume

Pour configurer les volumes, vous pouvez le faire sur l'interface web de l'appareil, **Phone > Voice**.

Mic Volume	
Mic Volume	<input type="text" value="8"/> (1~15)

Speaker Volume	
Speaker Volume	<input type="text" value="8"/> (1~15)

Tamper Alarm Volume	
Tamper Alarm Volume	<input type="text" value="8"/> (1~15)

Ringback Volume	
Ringback Volume	<input type="text" value="8"/> (1~15)

Voice Prompt Volume	<input type="text" value="15"/> (1~15)
---------------------	--

Configuration des paramètres :

- **Volume du micro** : Réglez le volume du micro selon vos besoins.
- **Volume du haut-parleur** : Réglez le volume du haut-parleur selon vos besoins.

- **Volume de l'alarme d'autoprotection** : Réglez le volume de l'alarme d'autoprotection.

- **Volume du retour d'appel** : Réglez le volume de la sonnerie de rappel.
- **Volume de l'invite vocale** : Réglez le volume de l'invite vocale.

**Note :**

- Pour E12W, le chemin d'accès est le suivant : **Appareil > Voix > Contrôle du volume**.
- **Le volume de l'invite vocale ne peut être configuré que sur le E12W.**

8.2. Configuration de la tonalité de porte ouverte

Vous pouvez non seulement activer ou désactiver la tonalité de porte ouverte mais aussi contrôler les mots d'invite qui accompagnent la tonalité sur l'interface web **Intercom > Voice**.

Open Door Warning	
Open Door Succ Warning	Enabled ▼
Open Door Failed Warning	Enabled ▼

Open Door Tone Setting	
Open Door Inside Tone Enabled	<input type="checkbox"/>
Open Door Outside Tone Enabled	<input type="checkbox"/>

Configuration des paramètres :

- **Avertissement de réussite de la porte ouverte** : cliquez sur le champ **Activé** ou **Désactivé selon** que vous souhaitez entendre les mots d'invite qui accompagnent la tonalité de **réussite de la porte ouverte**.
- **Avertissement en cas d'échec de la porte ouverte** : cliquez sur le champ **Activé** ou **Désactivé selon** que vous souhaitez entendre les mots d'invite qui accompagnent la tonalité d'**échec de la porte ouverte**.
- **Open Door Inside Tone Enabled** : cochez la case pour activer la tonalité de porte ouverte à l'intérieur.

- **Open Door Outside Tone Enabled** : cochez la case pour activer la tonalité de porte ouverte à l'extérieur.

**Note :**

- Pour E12W, le chemin d'accès est le suivant : **Dispositif > Voix**

8.3. Télécharger les fichiers de tonalité

8.3.1. Télécharger la sonnerie de rappel

Vous pouvez personnaliser la sonnerie d'appel si vous le souhaitez. Veuillez suivre les instructions concernant la taille et le format du fichier.

RingBack Upload

Choose File No file chosen Upload Delete Export

File Format: wav, size: < 200KB, samplerate: 16000,
Bits: 16

8.3.2. Télécharger la tonalité de porte ouverte

Vous pouvez personnaliser la tonalité d'ouverture de la porte si vous le souhaitez. La tonalité extérieure est utilisée pour ouvrir la porte par carte ou DTMF. La tonalité intérieure est utilisée pour ouvrir la porte via l'interface d'entrée déclenchée. Veuillez suivre les instructions concernant la taille et le format du fichier.

Opendoor Outside Tone Upload

No file chosen

File Format: wav, size: < 200KB, samplerate: 8k/16k, Bits: 16

Opendoor Inside Tone Upload

No file chosen

File Format: wav, size: < 200KB, samplerate: 8k/16k, Bits: 16

9. Paramètres du réseau

9.1. État du réseau

Pour vérifier l'état du réseau sur le Web **État > Informations sur le réseau** interface.

Network Information	
LAN Port Type	DHCP Auto
LAN Link Status	Connected
LAN IP Address	192.168.1.3
LAN Subnet Mask	255.255.255.0
LAN Gateway	192.168.1.1
LAN DNS1	192.168.1.1
LAN DNS2	192.168.1.1

9.2. Configuration du réseau de l'appareil

Vous pouvez vérifier les informations relatives à la connexion réseau du portier et configurer le mode DHCP (**Dynamic Host Configuration Protocol**) par défaut et la connexion IP statique de l'appareil sur l'interface web **Network > Basic** de l'appareil.

LAN Port

DHCP
 Static IP

IP Address	<input type="text" value="192.168.1.100"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.1"/>
LAN DNS1	<input type="text" value="8.8.8.8"/>
LAN DNS2	<input type="text"/>

Réglage des paramètres :

- **DHCP** : sélectionnez le mode **DHCP** en déplaçant le commutateur à bascule vers la droite. Le mode DHCP est la connexion réseau par défaut. Si le mode DHCP est activé, le serveur DHCP attribue automatiquement au portier une adresse IP, un masque de sous-réseau, une passerelle par défaut et une adresse de serveur DNS.
- **IP statique** : sélectionnez le mode IP statique en cochant la case DHCP. Lorsque le mode IP statique est sélectionné, l'adresse IP, le masque de sous-réseau, la passerelle par défaut et l'adresse des serveurs DNS doivent être configurés manuellement en fonction de votre environnement réseau actuel.
- **Adresse IP** : configurez l'adresse IP si le mode IP statique est sélectionné.
- **Masque de sous-réseau** : configurez le masque de sous-réseau en fonction de votre environnement réseau actuel.
- **Passerelle par défaut** : configurez la passerelle par défaut correcte en fonction de l'adresse IP de la passerelle par défaut.
- **LAN DNS1/2** : configurez le serveur DNS (**Domain Name Server**) préféré ou alternatif selon votre environnement réseau actuel. Le serveur DNS préféré est l'adresse du serveur DNS primaire tandis que le serveur DNS alternatif est l'adresse du serveur secondaire. Le portier se connecte au serveur alternatif lorsque le serveur DNS primaire est indisponible.

9.3. Déploiement des dispositifs dans le réseau

Les portiers doivent être déployés avant d'être correctement configurés dans l'environnement réseau en termes d'emplacement, de mode de fonctionnement,

et les numéros de poste, contrairement à d'autres appareils, pour le contrôle des appareils et la commodité de la gestion. Vous pouvez donc le faire sur l'interface web **Network > Advanced > Connect Setting**.

Connect Setting	
Server Type	SDMC
Discovery Mode	Disabled
Device Address	1 . 1 . 1 . 1 . 1
Device Extension	1
Device Location	Door Unit

Réglage des paramètres :

- **Type de serveur** : il est automatiquement configuré en fonction de la connexion réelle de l'appareil avec un serveur spécifique du réseau, tel que **SDMC** ou **Cloud et Aucun**. **Aucun** est le paramètre d'usine par défaut qui indique que l'appareil n'est connecté à aucun type de serveur. Vous pouvez donc choisir Cloud, SMDC en mode découverte.
- **Mode de découverte** : cliquez sur "**Activer**" pour activer le mode de découverte de l'appareil afin qu'il puisse être découvert par d'autres appareils du réseau, et cliquez sur "**Désactiver**" si vous souhaitez dissimuler l'appareil afin qu'il ne soit pas découvert par d'autres appareils.
- **Adresse du dispositif** : spécifiez l'adresse du dispositif en saisissant les informations de localisation du dispositif de gauche à droite : **Communauté, Unité, Escalier, Étage, Pièce** dans l'ordre.
- **Extension du dispositif** : saisissez le numéro d'extension du dispositif que vous avez installé.
- **Emplacement du dispositif** : saisissez l'emplacement dans lequel le dispositif est installé et utilisé.

9.4. Configuration RTP locale du dispositif

Pour la transmission de données sur le réseau, le dispositif doit être configuré avec une gamme de ports RTP (**Real-time Transport Protocol**) pour établir une gamme exclusive de transmission de données sur le réseau.

Local RTP		
Min RTP Port	<input type="text" value="11800"/>	(1024~65535)
Max RTP Port	<input type="text" value="12000"/>	(1024~65535)

Réglage des paramètres :

- **Starting RTP Port (Port RTP de départ)** : entrez la valeur du port afin d'établir le point de départ de la plage de transmission exclusive des données.
- **Port RTP maximum** : saisissez la valeur Port afin d'établir le point final de la plage de transmission exclusive des données.

9.5. Paramètre NAT

Le NAT (**Network Address Translation**) permet aux hôtes de l'intranet privé d'une organisation de se connecter de manière transparente aux hôtes du domaine public. Il n'est pas nécessaire que les hôtes internes aient des adresses Internet enregistrées. C'est un moyen de traduire l'adresse IP du réseau privé interne en une technologie d'adresse IP du réseau légal. Pour ce faire, il faut configurer sur le site Web **Account > Advance > NAT** interface.

NAT		
UDP Keep Alive Messages	<input type="text" value="Enabled"/>	▼
UDP Alive Msg Interval	<input type="text" value="30"/>	(5~60s)
RPort	<input type="text" value="Enabled"/>	▼

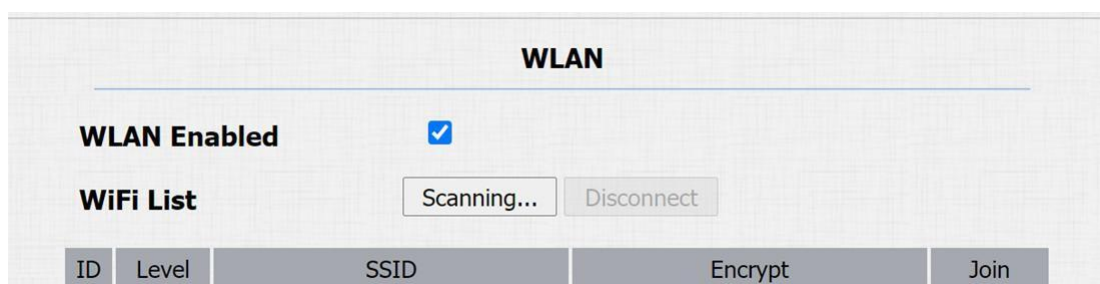
Réglage des paramètres :

- **Messages UDP Keep Alive** : Si cette option est activée, l'appareil enverra le message au serveur SIP afin que ce dernier puisse reconnaître si l'appareil est en ligne.
- **UDP Alive Msg Interval** : définit l'intervalle de temps d'envoi des messages entre 5 et 60 secondes, la valeur par défaut est 30 secondes.

- **RPort** : activer le Rport lorsque le serveur SIP est en WAN (**Wide Area Network**).

9.6. Réglage du WIFI

En plus de la connexion filaire, l'appareil prend également en charge la connexion Wi-Fi. Vous pouvez définir le Wi-Fi sur l'écran de l'appareil **Réseau > Basique > WLAN**. Cliquez sur Scanning pour rechercher les WIFI disponibles, choisissez-en un et entrez les informations d'authentification pour vous connecter si l'AP WIFI a besoin d'un mot de passe.



Configuration des paramètres :

- **WLAN Enable** : active la fonction WIFI.

10. Configuration des appels intercom

L'appel intercom dans l'appareil peut être configuré pour vous permettre d'effectuer une variété d'appels intercom personnalisés tels que l'appel IP et l'appel SIP pour différents scénarios d'application.

10.1. Appel IP & Configuration de l'appel IP

L'appel IP peut être effectué directement sur le dispositif d'interphone en entrant le numéro IP sur le dispositif. Vous pouvez également désactiver l'appel IP direct si vous ne souhaitez pas que l'appel IP soit effectué sur le dispositif.

Direct IP	Enabled ▾
Direct IP AutoAnswer	Enabled ▾
Direct IP Port	5060 (1~65535)

Configuration des paramètres :

- **Appel IP direct** : cliquez sur "**Activer**" ou "**Désactiver**" pour activer ou désactiver l'appel IP direct. Par exemple, si vous n'autorisez pas les appels IP directs sur l'appareil, vous pouvez cliquer sur "**Désactiver**" pour mettre fin à la fonction.
- **Direct IP AutoAnswer** : cliquez sur "**Enable**" ou "**Disable**" pour activer ou désactiver l'appel direct IP lorsque le téléphone répond automatiquement à l'appel entrant.
- **Port IP direct** : configure le port d'appel direct IP, 5060 est le port par défaut.

10.2. Appel SIP & Configuration de l'appel SIP

Vous pouvez passer des appels SIP (**Session Initiation Protocol**) de la même manière que pour les appels IP sur l'appareil. Toutefois, les paramètres d'appel SIP liés au compte, au serveur et au type de transport doivent être configurés avant que vous puissiez passer des appels sur l'appareil.

10.3. Enregistrement du compte SIP

Les portiers Akuvox prennent en charge deux comptes SIP qui peuvent tous être enregistrés en fonction de vos applications. Vous pouvez, par exemple, passer de l'un à l'autre si l'un des comptes échoue et devient invalide. Le compte SIP peut être configuré sur l'appareil et sur l'interface de l'appareil. Pour effectuer le réglage du compte SIP sur l'interface **Compte Web > Basique > Compte SIP**.

SIP Account	
Status	UnRegistered
Account	Account 1
Account Active	Disabled
Display Label	
Display Name	
Register Name	
User Name	
Password

Réglage des paramètres :

- **Statut** : vérifie si le compte SIP est enregistré ou non.
- **Compte actif** : cliquez sur **Activer** ou **Désactiver** pour activer ou désactiver le compte SIP enregistré.
- **Nom d'affichage** : configurez le nom, par exemple le nom de l'appareil qui doit être affiché sur l'appareil appelé.
- **Nom d'utilisateur** :
indiquez le nom d'utilisateur obtenu auprès de l'administrateur du compte SIP.
- **Compte** : sélectionnez le compte exact (Compte 1&2) à configurer.
- **Afficher l'étiquette** : configurez l'étiquette du dispositif à afficher sur l'écran du dispositif.
- **Nom du registre** : entrer le nom du registre du compte SIP obtenu auprès de l'administrateur du compte SIP.

passé obtenu à partir du compte SIP.

10.4. Configuration du serveur SIP

Les serveurs SIP peuvent être configurés pour les appareils afin d'établir une session d'appel via le serveur SIP entre les appareils d'interphonie. Cette configuration s'effectue également sur l'interface Web **Account > Basic > SIP Server**.

SIP Server 1		
Server IP	<input type="text" value="192.168.35.11"/>	Port <input type="text" value="5060"/>
Registration Period	<input type="text" value="1800"/>	(30~65535s)

SIP Server 2		
Server IP	<input type="text"/>	Port <input type="text" value="5060"/>
Registration Period	<input type="text" value="1800"/>	(30~65535s)

Réglage des paramètres :

- **Serveur SIP préféré** : entrez le numéro d'adresse IP du serveur primaire ou son URL.
- **Serveur SIP alternatif** : entrez l'adresse IP du serveur SIP de secours ou son URL.
- **Port** : configure le port du serveur SIP pour la transmission des données.
- **Période d'enregistrement** : définit la période d'enregistrement du compte SIP. Le réenregistrement SIP commencera automatiquement si l'enregistrement du compte échoue pendant la période d'enregistrement. La période d'enregistrement par défaut est "1800", allant de **30-65535s**.

10.5. Configurer le serveur proxy sortant

Un serveur proxy sortant est utilisé pour recevoir tous les messages de demande d'initialisation et les acheminer vers le serveur SIP désigné afin d'établir une

session d'appel via une transmission de données basée sur le port. Pour le configurer sur le **compte** Web de l'appareil, procédez de la manière suivante :
Compte >

Basic > Interface du serveur proxy sortant.

Outbound Proxy Server			
Enable Outbound	<input type="text" value="Enabled"/>		
Server IP	<input type="text" value="112.39.22.140"/>	Port	<input type="text" value="5060"/>
Backup Server IP	<input type="text"/>	Port	<input type="text" value="5060"/>

Réglage des paramètres :

- **Enable Outbound** : cliquez sur "Enable" et "Disable" pour activer ou désactiver le serveur proxy sortant.
- **Preferred Server IP** : entrez l'adresse SIP du serveur proxy primaire de sortie.
- **Port** : entrez le numéro de port pour établir une session d'appel via le serveur proxy sortant primaire.
- **Alternate Server IP** : configurer l'IP du serveur de secours pour le serveur proxy sortant de secours.
- **Port** : entrez le numéro de port pour établir une session d'appel via le serveur proxy sortant de secours.

10.6. Configurer le type de transmission des données

Le message SIP peut être transmis dans trois protocoles de transmission de données : **UDP (User Datagram Protocol)**, **TCP (Transmission Control Protocol)**, **TLS (Transport Layer Security)** et **DNS-SRV**. Entre-temps, vous pouvez également identifier le serveur d'où proviennent les données. Pour ce faire, il faut configurer l'interface Web **Account > Basic > Transport Type**.

Transport Type	
Transport Type	<input type="text" value="UDP"/>

Réglage des paramètres :

- **UDP** : sélectionnez "**UDP**" pour un protocole de couche de transport peu fiable mais très efficace. UDP est le protocole de transport par défaut.
- **TCP** : sélectionnez "**TCP**" pour Protocole de couche de transport fiable mais moins efficace.
- **TLS** : sélectionnez "**TLS**" pour le protocole de couche de transport sécurisé et fiable.
- **DNS-SRV** : sélectionnez "**DNS-SRV**" pour obtenir un enregistrement DNS permettant de spécifier l'emplacement des serveurs. Et **SRV** n'enregistre pas seulement l'adresse du serveur mais aussi le port du serveur. De plus, SRV peut également être utilisé pour configurer la priorité et le poids de l'adresse du serveur.

10.7. Configurer la fonction d'appel

10.7.1. DND

Le paramètre DND (**Do not disturb**) vous permet de ne pas être dérangé par des appels SIP entrants non désirés. Vous pouvez configurer correctement les paramètres relatifs à la fonction DND sur l'interface Web **Téléphone > Fonctionnalité d'appel de l'appareil** afin de bloquer les appels SIP auxquels vous n'avez pas l'intention de répondre. Dans le même temps, vous pouvez également définir le code à envoyer au serveur SIP lorsque vous souhaitez rejeter l'appel.

DND	
Account	All Account ▼
DND	Disabled ▼
Return Code When DND	486(Busy Here) ▼
DND On Code	<input type="text"/>
DND Off Code	<input type="text"/>

Réglage des paramètres :

- **Compte** : sélectionnez "**Compte1**", "**Compte2**" ou "**Tous les comptes**" pour

l'application DND.

- **DND** : active ou désactive la fonction DND. La fonction DND est désactivée par défaut.

- **Code de retour en cas de DND** : sélectionnez le code qui doit être envoyé au dispositif appelant via le serveur SIP. **404** pour "Not found" ; **480** pour "Temporary unavailable" **486** pour "busy here".
- **DND On Code** : **activer le DND** on server en utilisant le code obtenu. Le DND on Code est **78** par défaut.
- **Code de désactivation du DND** : désactivez le DND sur le serveur à l'aide du code obtenu. Le code de désactivation du DND est **79** par défaut.
- **Code de retour en cas de refus** : sélectionnez le code à envoyer à l'appelant via le serveur SIP lorsque vous avez rejeté l'appel entrant.



Note :

- Pour l'E12W, le chemin d'accès est le suivant : **Interphone > Fonction d'appel**

10.7.2. Appel par bouton-poussoir

Des boutons poussoirs qui sont utilisés pour lancer des appels. Chaque bouton poussoir peut être lié à 6 numéros sip ou adresses IP au maximum, ce qui signifie que les utilisateurs peuvent appeler 6 numéros en même temps en appuyant sur le bouton poussoir.

Push Button						
Key	Number1	Number2	Number3	Number4	Number5	Number6
Push Button 1	111	112	113	114	115	116
Push Button 2	192.168.1.4	192.168.1.5	192.168.1.6			
Push Button 3						
Push Button 4						
Push Button 5						

**Note**

:

a 2/3/4/5 pous boutons

R20A/R26C/R26P/E11

R/E21A/E21V/E12Whasonlyonepush
bouton.

10.7.3. Robin Call

Le robin call est utilisé pour appeler plusieurs numéros configurés dans le bouton poussoir, un par un. Si l'appelant précédent ne répond pas dans le délai du robin call, l'appel sera transféré au suivant. Si l'appel est répondu par l'un des destinataires, l'appel ne sera plus transféré.

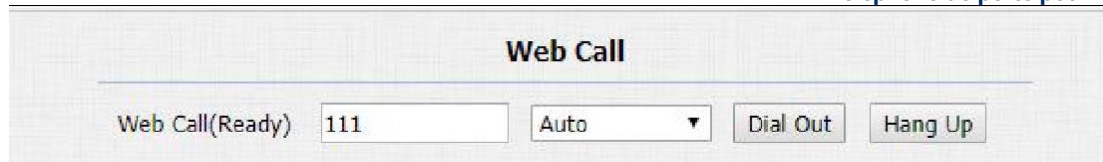
Robin Call	
Robin Call Enable	Disabled ▼
Robin Call Timeout	60 ▼

Configuration des paramètres :

- **Activation du robinet** : Activez ou désactivez la fonction de robin call. Elle est désactivée par défaut.
- **Robin Call Timeout** : Valeur du temps d'appel pour chaque numéro, entre 5 et 60 secondes.

10.7.4. Appel Web

En plus d'effectuer des appels IP/SIP directement sur l'appareil, vous pouvez également effectuer des appels sur l'interface web de l'appareil sans vous approcher physiquement de l'appareil à des fins de test, etc.



Web Call

Web Call(Ready) 111 Auto ▼ Dial Out Hang Up

Configuration des paramètres :

- **Auto/Account1/Account2** : Pour choisir un compte SIP approprié pour effectuer un appel Web. Si vous appelez en utilisant l'adresse IP, il n'est pas nécessaire de choisir le compte.

10.7.5. Réponse automatique

Vous pouvez définir la vitesse à laquelle le portier doit répondre à un appel SIP/IP entrant en configurant les paramètres relatifs au temps. En outre, vous pouvez également définir le mode de réponse aux appels (mode vidéo ou mode audio). Pour activer cette fonction sur l'interface Web **Account > Advanced**, vous pouvez définir les paramètres correspondants sur Web **Phone > Call Feature**.



Auto Answer Enabled ▼

Auto Answer Delay 0 (0~5s)

Auto Answer Mode Video ▼

Configuration des paramètres :

- **Réponse automatique** : Activez la fonction de réponse automatique en cliquant sur "Activer".
- **Délai de réponse automatique** : **Définissez** le délai (de 0 à 5 secondes) avant que l'appel puisse être répondu automatiquement. Par exemple, si vous définissez un délai de 1 seconde, l'appel sera répondu automatiquement en 1 seconde.
- **Mode de réponse automatique** : **Configurez** le mode vidéo ou audio que vous préférez pour répondre automatiquement à l'appel.



Note :

- Pour E12W, le chemin d'accès est **Intercom > Call Feature**.

10.7.6. Multicast

La multidiffusion utilise le mode un-à-plusieurs pour communiquer dans un rayon. Le téléphone de porte peut être un auditeur et recevoir l'audio de la partie écoutée.

Multicast Setting

Paging Barge

1 ▼

Paging Priority Active

Enabled ▼

Priority List

IP Address	Listening Address	Label	Priority
1 IP Address	<input type="text" value="224.1.6.11:1200"/>	<input type="text" value="Akuvox"/>	1
2 IP Address	<input type="text"/>	<input type="text"/>	2
3 IP Address	<input type="text"/>	<input type="text"/>	3
4 IP Address	<input type="text"/>	<input type="text"/>	4
5 IP Address	<input type="text"/>	<input type="text"/>	5
6 IP Address	<input type="text"/>	<input type="text"/>	6
7 IP Address	<input type="text"/>	<input type="text"/>	7
8 IP Address	<input type="text"/>	<input type="text"/>	8
9 IP Address	<input type="text"/>	<input type="text"/>	9
10 IP Address	<input type="text"/>	<input type="text"/>	10

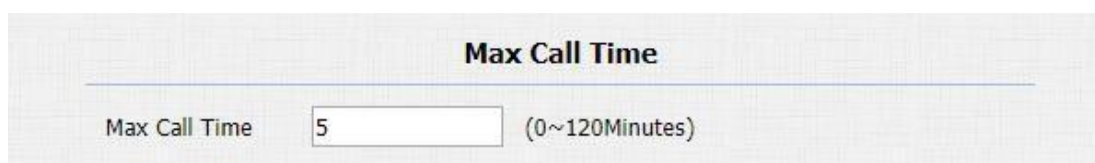
Configuration des paramètres :

- **Paging Barge** : multicast ou combien d'appels multicast sont plus prioritaires que l'appel SIP, si vous désactivez l'activation de la priorité Paging, l'appel SIP aura une priorité élevée.
- **Paging Priority Active** : les appels multicast sont appelés par ordre de priorité ou non.
- **Adresse d'écoute** : Entrez l'adresse IP de multidiffusion que vous voulez écouter. L'adresse IP de multidiffusion doit être la même que la partie écoutée et le port de multidiffusion ne peut pas être le même pour chaque adresse IP. L'adresse IP de multidiffusion est comprise entre 224.0.0.0 et

- **Étiquette** : Entrez l'étiquette pour chaque adresse d'écoute.

10.7.7. Configurer la durée maximale de l'appel

Le téléphone de porte vous permet de configurer la durée de l'appel pour recevoir l'appel du dispositif appelant, car l'appelant peut oublier de raccrocher le dispositif intercom. Lorsque la durée de l'appel est atteinte, le portier met automatiquement fin à l'appel.



Configuration des paramètres :

- **Durée maximale de l'appel** : Entrez la durée de l'appel en fonction de vos besoins (de 0 à 120 minutes). La durée d'appel par défaut est de 5 minutes.

Note

Si vous utilisez un compte SIP pour passer un appel, veuillez faire attention au temps d'appel maximum du serveur SIP. Si le temps d'appel maximum du serveur SIP est plus court...

10.7.8. Durée maximale de la composition

La durée maximale de composition se compose de la durée maximale d'entrée en communication et de la durée maximale de sortie en communication. La durée maximale d'entrée en communication correspond à la durée maximale

avant que le portier ne raccroche si l'appel n'est pas pris par le portier. A l'inverse, le temps maximum d'appel sortant correspond au temps maximum avant que le portier ne raccroche l'appel si celui-ci ne répond pas.

durée avant que le portier ne raccroche automatiquement lorsque l'appel du portier n'est pas répondu par le dispositif d'interphone appelé.

Max Dial Time		
Dial In Time	<input type="text" value="60"/>	(1~120Sec)
Dial Out Time	<input type="text" value="60"/>	(1~120Sec)

Configuration des paramètres :

- **Durée d'appel** : Entrez la durée d'appel de votre portier (entre 30 et 120 secondes). Par exemple, si vous définissez la durée d'appel de votre portier à 60 secondes, le portier raccrochera automatiquement l'appel entrant si le portier ne répond pas à l'appel dans les 60 secondes. Par défaut, la durée de composition du numéro est de 60 secondes.
- **Temps d'appel** : Entrez la durée de l'appel pour votre portier (de 5 à 120 secondes). Par exemple, si vous réglez la durée de l'appel à 60 secondes, le portier raccrochera automatiquement l'appel s'il ne répond pas à l'appareil appelé.



Note

Si vous utilisez un compte SIP pour passer un appel, veuillez faire attention au temps de composition maximal du serveur SIP. Si le temps de composition maximum du serveur SIP est inférieur à

11. Configuration des codecs audio et vidéo pour les appels SIP

11.1. Configuration du codec audio

Le téléphone de porte Akuvox prend en charge quatre types de codecs (PCMU, PCMA, G729, G722) pour coder et décoder les données audio pendant la session d'appel. Chaque type de codec varie en termes de qualité sonore. Vous pouvez sélectionner le codec spécifique avec une bande passante et un taux d'échantillonnage différents de manière flexible en fonction de l'environnement réseau réel. Pour effectuer la configuration sur le **compte** web de l'appareil > Interface **avancée**.

The screenshot shows the 'SIP Account' configuration page. At the top, there is a dropdown menu for 'Account' set to 'Account 1'. Below this is the 'Codecs' section, which is divided into two columns: 'Disabled Codecs' and 'Enabled Codecs'. The 'Enabled Codecs' list contains four items: PCMU, PCMA, G722, and G729. The 'Disabled Codecs' list is currently empty. Between the two lists are two buttons: '>>' and '<<'. To the right of the 'Enabled Codecs' list are two buttons: an upward arrow and a downward arrow.

Veillez vous référer à la consommation de bande passante et au taux d'échantillonnage pour les quatre types de codecs ci-dessous :

Type de codec	Bande passante Consommation	Taux d'échantillonnage
PCMA	64 kbit/s	8kHz
PCMU	64 kbit/s	8kHz
G729	8 kbit/s	8kHz
G722	64 kbit/s	16kHz

11.2. Configuration du codec vidéo

Le téléphone de porte Akuvox supporte le codec H264 qui fournit une meilleure qualité vidéo à un débit binaire beaucoup plus faible avec une qualité vidéo et une charge utile différentes. Pour configurer le codec vidéo sur le **compte** web > interface **avancée**.

Video Codec

Codec Name	<input checked="" type="checkbox"/> H264
Codec Resolution	4CIF ▼
Codec Bitrate	2048 ▼
Codec Payload	104 ▼

Réglage des paramètres :

- **Nom du codec** : Cochez pour sélectionner le format de codec vidéo H264 pour le flux vidéo du portier. H264 est le codec vidéo par défaut.
- **Résolution du codec** : sélectionnez la résolution du code pour la qualité vidéo parmi quatre options : "QCIF", "CIF", "VGA", "4CIF" et "720P" en fonction de votre environnement réseau réel. La résolution du code par défaut est 4CIF.
- **Codec Bitrate** : sélectionnez le débit binaire du flux vidéo (de 320 à 2048). Plus le débit binaire est élevé, plus la quantité de données transmises par seconde est importante et plus la vidéo est claire. Alors que le bitrate du code par défaut est de 2048.

- **Charge utile du codec** : sélectionnez le type de charge utile (de 90 à 118) pour

configurer le fichier de configuration audio/vidéo. La charge utile par défaut est 104.

11.3. Configurer la transmission de données DTMF

Afin de réaliser l'accès à la porte via un code DTMF ou d'autres applications, vous devez configurer correctement la fonction DTMF dans **Compte Web > Avancé > DTMF** afin d'établir une transmission de données basée sur DTMF entre le portier et un autre dispositif d'interphone pour l'intégration d'un tiers.

DTMF	
Type	<input type="text" value="RFC2833"/>
How To Notify DTMF	<input type="text" value="Disabled"/>
DTMF Payload	<input type="text" value="101"/> (96~127)

Réglage des paramètres :

- **Type** : sélectionnez le mode DTMF parmi cinq options : "**Inband**", "**RFC2833**", "**Info+Inband**" et "**Info+RFC2833**" en fonction du type de transmission DTMF spécifique du dispositif tiers avec lequel il faut établir une correspondance pour la réception des données du signal.
- **Comment notifier le DTMF** : **select** parmi quatre types : "**Disable**" " **DTMF**" "**DTMF-Relay**" "**Telephone-Event**" selon le type spécifique adopté par le dispositif tiers. Vous devez le configurer uniquement lorsque le dispositif tiers avec lequel vous souhaitez vous associer adopte le mode "**Info**".
- **DTMF Payload (charge utile DTMF)** : définit la charge utile en fonction de la charge utile spécifique de transmission de données convenue entre l'émetteur et le récepteur pendant la transmission de données.

12. Configuration de la liste blanche d'accès

Le portier Akuvox permet de stocker jusqu'à 500 contacts qui peuvent donner une autorisation d'accès au moniteur intérieur ou à d'autres dispositifs. La liste blanche d'accès comprend la configuration des groupes et la configuration et la gestion des contacts. Pour la configurer sur le web, **accédez à Whitelist > Access Whitelist**.

12.1. Gestion du groupe de contacts

Saisissez le nom du groupe dans la colonne Nom et configurez l'anneau et les informations de description du groupe pour ajouter un nouveau groupe. Vérifiez et gérez les groupes existants dans la liste des groupes.

Index	Name	Ring	Description	<input type="checkbox"/>
1	test1	Auto	akuvox group	<input type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>

Group

Group Setting

Name

Ring

Description

Réglage des paramètres :

- **Nom** : le nom du groupe.
- **Sonnerie** : la sonnerie des appels entrants pour le groupe.
- **Description** : les informations remarquées pour le groupe.

12.2. Gestion des contacts

Vous pouvez rechercher, créer, afficher, modifier et supprimer les contacts de votre répertoire téléphonique.

Contact

Search

Index	Name	Phone Num	Group	Ring	<input type="checkbox"/>
1	Aku..	112425	test1	Auto	<input type="checkbox"/>
2					<input type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
9					<input type="checkbox"/>
10					<input type="checkbox"/>

Page 1 ▾

Move To

Contact Setting

Name

Group

Phone Num

Ring

Paramètres d'installation :

- **Nom** : saisissez le nom du contact, qui est obligatoire.
- **Téléphone** : saisissez le numéro de téléphone du contact, qui est obligatoire.
- **Groupe** : cliquez sur l'onglet vert pour sélectionner le nom du groupe que vous avez créé. Vous ne pouvez pas sélectionner le nom du groupe si aucun nom de groupe n'a été créé.
- **Compte** : sélectionnez le compte SIP qui sera utilisé pour appeler. Si vous utilisez l'appel direct IP, il n'est pas disponible.
- **Priorité d'appel** : jusqu'à 3 numéros dans un groupe et configuration de la séquence d'appel pour ces numéros.

13. Réglage du relais

13.1. Réglage du commutateur de relais

Vous pouvez configurer le(s) commutateur(s) relais et le DTMF pour l'accès à la porte sur l'interface web **Intercom > Relay**.

The screenshot shows a configuration page titled "Relay" with two columns for "RelayA" and "RelayB". The settings are as follows:

Parameter	RelayA	RelayB
Relay ID	RelayA	RelayB
Relay Type	Default state	Default state
Relay Delay(sec)	3	3
DTMF Option	1 Digit DTMF	
DTMF	0	0
Multiple DTMF	<input type="checkbox"/>	<input type="checkbox"/>
Relay Status	RelayA: Low	RelayB: Low

Réglage des paramètres :

- **Relay Delay (Sec)** : définit le délai de déclenchement du relais (de 1 à 10 secondes). Par exemple, si vous définissez le délai à "5" secondes, le relais ne se déclenchera pas avant 5 secondes après avoir appuyé sur l'onglet "unlock".
- **Option DTMF** : sélectionnez le nombre de chiffres DTMF pour le contrôle d'accès de la porte (**de 1 à 4 chiffres**). Par exemple, vous pouvez sélectionner un code DTMF à 1 chiffre ou un code DTMF à 2 chiffres, selon vos besoins.
- **DTMF** : réglez le code DTMF à un chiffre dans la gamme (**0-9 et *,#**).
- **DTMF multiple** : définissez le code DTMF en fonction du paramètre de l'**option DMTP**. Par exemple, vous devez définir le code DTMF à 3 chiffres si le **mode DTMF** est réglé sur 3 chiffres.

- **État du relais** : l'état du relais est faible par défaut, ce qui signifie que normalement, l'état du relais est faible.

fermé(NC) Si l'état du relais est élevé, alors il est en état Normalement Ouvert(NO).

**Note :**

- Seuls les dispositifs externes connectés au commutateur de relais doivent être alimentés par des adaptateurs de puissance, car le commutateur de relais ne fournit pas de puissance.

**Note :**

- Si le mode DTMF est réglé sur "**1 Digit DTMF**", vous ne pouvez pas modifier le code DTMF dans le champ **DTMF 2~4 Digits**. Et si vous réglez le mode DTMF de 2 à 4 dans le champ "**2~4 Digits DTMF**", vous ne pouvez pas modifier le code DTMF dans le champ "**1 Digit DTMF**".

13.2. Sélectionner le relais de la cloche du carillon

Cette fonction est utilisée pour déclencher un relais lors d'un appel. Elle est souvent utilisée dans certains scénarios spécifiques.

ChimeBell Setting

Apply Setting to

Configuration des paramètres :

- **Appliquer le réglage à :** trois options peuvent être choisies : "Aucun", "Relais A", "Relais B". Celle qui est choisie sera déclenchée après avoir appuyé sur le bouton d'appel.

13.3. Réglage du relais Web

En plus du relais qui est connecté au portier, vous pouvez également

contrôler l'accès à la porte en utilisant le relais web basé sur le réseau sur le dispositif et sur l'interface web du dispositif.

Le relais Web doit être configuré sur l'interface Web **Phone > WebRelay** où vous devez remplir des informations telles que l'adresse IP du relais, le mot de passe, l'action du relais Web, etc. avant de pouvoir accéder à la porte via le relais Web.

Web Relay

Type	Disabled ▼
IP Address	<input type="text"/>
UserName	<input type="text"/>
Password	••••••

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 02	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 03	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 04	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 05	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 06	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 07	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 08	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 09	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 10	<input type="text"/>	<input type="text"/>	<input type="text"/>

Réglage des paramètres :

- **Type** : sélectionnez parmi trois options "**Disabled**" (désactivé), "**WebRelay**" (relais Web) et "**Both**" (les deux). Sélectionnez "**Webrelay**" pour activer le relais Web. Sélectionnez "**Disable**" pour désactiver le relais Web. Sélectionnez "**Both**" pour activer à la fois le relais local et le relais Web.
- **Adresse IP** : entrez l'adresse IP du relais Web fournie par le fabricant du relais Web.
- **Nom d'utilisateur** : entrez le nom d'utilisateur fourni par le fabricant du relais Web.
- **Mot de passe** : entrez le mot de passe fourni par le fabricant du relais web. Les mots de passe sont authentifiés via HTTP et vous pouvez définir les mots de passe en utilisant "**http get**" dans Action.
- **Action du relais Web** : entrez la commande d'action spécifique du relais Web

en ajoutant ip, username, pwd, vous pouvez remplir la commande HTTP dans l'action de relais web, ainsi vous pouvez configurer plusieurs relais web

- **Clé de relais Web** : elle peut être nulle ou entrer le code DTMF configuré, lorsque la porte est déverrouillée par le code DTMF, la commande d'action sera envoyée au relais Web automatiquement.
- **Web Relay Extension (Extension de relais Web)** : il peut être nul ou entrer les informations de l'extension de relais, qui peut être un nom d'utilisateur de compte SIP d'un dispositif d'interphone tel qu'un moniteur intérieur, de sorte que la commande d'action spécifique sera envoyée lorsque le déverrouillage est effectué sur le dispositif d'interphone, alors que ce paramètre est facultatif. Veuillez vous référer à l'exemple ci-dessous :

<http://admin:admin@192.168.1.2/state.xml?relayState=2>.

**Note :**

- Pour l'E12W, le chemin d'opération est **Contrôle d'accès > Relais Web**.

14. Gestion des horaires d'accès aux portes

Vous devez configurer et programmer l'accès aux portes par l'utilisateur via une carte RF, un code PIN privé et une reconnaissance faciale.

14.1. Configurer le calendrier d'accès aux portes

Vous pouvez créer des programmes d'accès aux portes afin qu'ils puissent être appliqués ultérieurement au contrôle d'accès aux portes destiné à un utilisateur individuel ou à un groupe d'utilisateurs créé. En outre, vous pouvez modifier votre programmation d'accès aux portes si nécessaire.

14.1.1. Gestion des horaires d'accès aux portes

Vous pouvez créer le programme d'accès aux portes sur une base quotidienne ou mensuelle et vous pouvez également créer un programme qui vous permet de planifier sur une plus longue période en plus de l'exécution du programme d'accès aux portes sur une base quotidienne ou mensuelle. Pour ce faire, configurez l'interface Web **Intercom > Schedules**.

Schedule Setting

Schedule Type

Schedule Name

Date Time : - :

Schedule Manage

Index	Type	Name	Date	Day of Week	Time	
1	Daily	Test	-	-	04:00-18:00	<input type="checkbox"/>
2						<input type="checkbox"/>
3						<input type="checkbox"/>
4						<input type="checkbox"/>
5						<input type="checkbox"/>
6						<input type="checkbox"/>
7						<input type="checkbox"/>
8						<input type="checkbox"/>
9						<input type="checkbox"/>
10						<input type="checkbox"/>

Page:

Configuration des paramètres :

- **Schedule Type (Type de programme) :** définissez le type de période de temps. Vous avez le choix entre trois types : quotidien, hebdomadaire et normal. La valeur par défaut est Quotidien.
- **Nom de l'horaire :** définissez le nom de la période de temps.
- **Date Heure :** définissez la période correspondante.
- **Jour de la semaine :** sélectionnez le jour de la semaine correspondant. Ce champ ne s'affiche que lorsque les types Semaine et Normal sont sélectionnés.
- **Plage de dates :** définissez la date correspondante. Ce champ ne s'affiche que lorsque le type Normal est sélectionné.



Note :

- Pour E12W, le chemin d'accès est le suivant : **Setting > Schedule.**

15. Configuration du déverrouillage des portes

Le portier Akuvox vous offre de nombreux types d'accès. Vous pouvez les configurer sur le dispositif et l'interface web. De plus, vous pouvez importer ou exporter les fichiers configurés pour maximiser l'efficacité de la configuration de votre carte RF.

15.1. Configurer le format de la carte d'accès

Si vous souhaitez vous intégrer à un système d'interphonie tiers en termes d'accès aux portes par carte RF, vous pouvez modifier le format du code de la carte RF pour qu'il soit identique à celui appliqué dans le système tiers. Vous pouvez effectuer cette configuration sur l'interface web **Intercom > Advanced**.



The screenshot shows a configuration window titled "RFID". It contains three rows, each with a label and a dropdown menu:

RFID	
ICCARD Display Mode	8HN ▼
IDCARD Display Mode	8HN ▼
WIEGAND Display Mode	8HN ▼

Configuration des paramètres :

- **Mode d'affichage ICCARD** : Sélectionnez le format du code de la carte à **puce** pour l'accès à la porte parmi cinq options de format : **8H10D** ; **6H3D5D(W26)** ; **6H8D** ; **8HN** ; **8HR**. Le format de code de carte est 8HN par défaut dans le portier.
- **Mode d'affichage de la carte d'identité** : Sélectionnez le format de la carte d'**identité** pour l'accès à la porte parmi cinq options de format : **8H10D** ; **6H3D5D(W26)** ; **6H8D** ; **8HN** ; **8HR**. Le format du code de la carte est 8HN par défaut dans le portier.
- **Mode d'affichage WIEGAND** : **Sélectionnez** le format de la **carte WIEGAND** pour l'accès à la porte parmi cinq options de format : **8H10D** ; **6H3D5D(W26)** ; **6H8D** ; **8HN** ; **8HR**. Le format du code de la carte est 8HN par défaut dans le portier.

15.2. Configurer la carte d'accès pour le déverrouillage de la porte

Vous pouvez gérer le numéro de la carte et les paramètres correspondants sur le web. **Intercom > Interface de paramétrage de la carte.**

ID/IC Enabled

IC Enabled

ID Enabled

Card Status

Card Status

Card Setting

IC Key DoorNum RelayA RelayB

IC Key Tags

IC Key Name

IC Key Code

Schedule Management

All Schedules

Enable Schedules

>> <<

Configuration des paramètres :

- **IC/ID Enable** : pour activer le type de carte IC ou ID.
- **Statut de la carte** : sélectionnez "**émission de voiture**" dans le champ avant d'ajouter la carte RFID et remettez le statut sur "**normal**" après l'ajout de la carte.
- **Clé IC DoorNum** : sélectionne le commutateur de relais disponible pour

l'accès à la porte de la carte RIFD.

- **IC Key Tags** : sélectionnez la fréquence de validité de la carte RFID pour l'accès à la porte parmi trois options : "Par exemple, si vous sélectionnez "**Autorisé**", la carte est toujours valide pour un accès illimité à la porte selon vos paramètres. Si vous sélectionnez "Schedule", vous devez définir l'heure spécifique de validité de l'accès par carte RFID. Si vous sélectionnez "Interdit", la carte RFID ne sera jamais valide pour l'accès à la porte.
- **Fréquence** : si vous sélectionnez les étiquettes comme "calendrier", vous devez également définir la fréquence d'utilisation, c'est-à-dire le nombre de fois que la carte peut être utilisée pendant une période donnée.
- **Code de la clé IC** : trouver le code de la carte RFID dans le champ.
- **Gestion des horaires** : sélectionnez un horaire disponible pour la carte, de Tous les horaires à Activer les horaires.

**Note :**

- La carte RF de 13,56 MHz et 125 KHz peut être appliquée au portier pour l'accès à la porte.

15.3. Contrôle de l'importation et de l'exportation de données de cartes d'accès

Les portiers Akuvox prennent en charge le partage des données de carte de contrôle d'accès entre les portiers Akuvox par le biais de l'importation et de l'exportation. Vous pouvez également exporter les données de carte hors du portier, puis les importer vers un dispositif tiers sur l'interface Web **Intercom > Card Setting**.

Import/Export Card Data(.xml)

No file chosen

Card AES Key

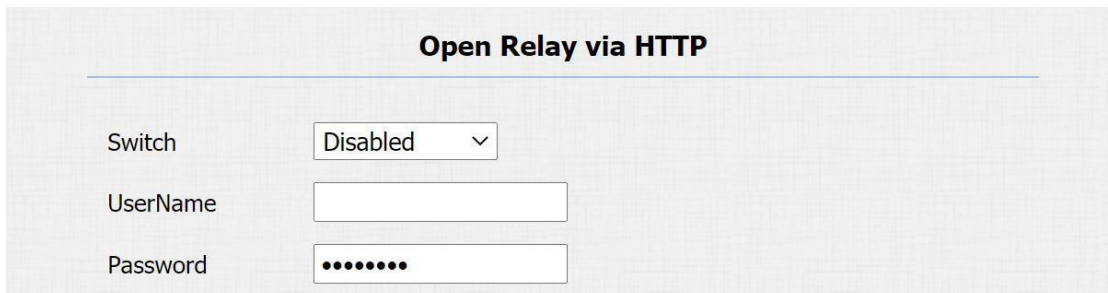
 **Note :**

- Pour E12W, le chemin d'accès est le suivant : **Contrôle d'accès > Réglage de la carte.**

15.4.

Configurer un relais ouvert via HTTP pour le déverrouillage des portes

Vous pouvez déverrouiller la porte à distance sans vous approcher physiquement du dispositif pour l'accès à la porte en saisissant dans le navigateur Web la commande HTTP (URL) créée pour déclencher le relais lorsque vous n'êtes pas disponible près de la porte pour l'accès à la porte. Pour ce faire, configurez l'interface Web **Intercom > Relay**.



Open Relay via HTTP

Switch

UserName

Password

Réglage des paramètres :

- **Activer** : activer la fonction de déverrouillage de la commande HTTP en cliquant sur **Activer**.
champ.
- **Nom d'utilisateur** : saisissez le nom d'utilisateur de l'interface Web de l'appareil, par exemple "**Admin**".
- **Mot de passe** : entrez le mot de passe pour la commande HTTP. Par exemple : "**12345**".

Veillez vous référer à l'exemple suivant :

<http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1>

**Note :**

- **DoorNum** dans la commande HTTP ci-dessus fait référence au relais numéro 1 à déclencher pour l'accès à la porte.
- Pour E12W, le chemin d'opération est **Contrôle d'accès > Relais**.

15.5. Configurer le bouton de sortie pour le déverrouillage de la porte

Lorsque vous devez ouvrir la porte de l'intérieur à l'aide du bouton de sortie installé près de la porte, vous pouvez configurer l'entrée du parlophone pour qu'elle déclenche le relais d'accès à la porte sur l'interface Web **Intercom > Input**.

Input A

Input Service: Disabled

Trigger Option: Low

Action to execute: FTP Email Sip Call HTTP

Http URL:

Action Delay: 0 (0~300 Sec)

Open Relay: None

Door Status: DoorA: High

Paramétrage :

- **Service de saisie** : Sélectionnez " **Enable** " pour pouvoir utiliser la fonction Input.
- **Option de déclenchement** : Sélectionnez les options de déclenchement en fonction de l'opération réelle sur le bouton de sortie.
- **Action à exécuter** : sélectionnez la méthode pour exécuter l'action parmi quatre options : FTP, Email, HTTP, TFTP.
- **Http URL** : entrez l'URL si vous sélectionnez le HTTP pour exécuter l'action.

- **Délai d'action** : paramétrez le délai d'exécution de l'action. Pour

Par exemple, si vous réglez le délai d'action à 5 secondes, les actions correspondantes seront exécutées 5 secondes après que vous ayez appuyé sur le bouton.

- **Relais ouvert** : configurez des relais qui seront déclenchés par l'entrée.
- **Door Status** : affiche l'état du signal d'entrée.

**Note :**

- Pour E12W, le chemin d'opération est **Contrôle d'accès > Entrée**.

16. Sécurité

16.1. Réglage de l'alarme de sabotage

La fonction d'alarme anti-sabotage sert de protection contre tout retrait non autorisé des appareils en déclenchant l'alarme tempérée tout en envoyant des appels à l'endroit désigné. L'alarme de sabotage se déclenche lorsque le portier modifie sa valeur de gravité par rapport à la valeur de gravité initiale définie lors de l'installation du dispositif.

Tamper Alarm	
Tamper Alarm	Disabled ▼
Gravity Sensor Threshold	32 (0~127)

Réglage des paramètres :

- **Tamper Alarm** : cliquez pour sélectionner "ON" dans le champ Tamper Alarm afin d'activer la fonction d'alarme antivol.
- **Gravity Sensor Threshold (seuil du capteur de gravité)** : définissez le seuil de sensibilité du capteur de gravité. Plus la valeur est faible, plus le capteur de gravité est sensible. La valeur du capteur de gravité est de 32 par défaut.

16.2. Détection de mouvement

La détection de mouvement est souvent utilisée pour la vidéo de surveillance sans surveillance et l'alarme automatique. Les images collectées par la caméra à différentes fréquences d'images seront calculées et comparées par le CPU selon un certain algorithme. Lorsque l'image change, si quelqu'un passe, l'objectif est déplacé, le nombre obtenu par le calcul et le résultat de la comparaison dépassera le seuil et indiquera que le système peut le traitement correspondant est fait automatiquement.

16.2.1. Configurer la détection de mouvement

Vous pouvez activer la détection de mouvement et configurer l'intervalle de détection de mouvement sur l'appareil.

Motion Detection Options

Motion Detection	<input type="text" value="Disabled"/>	
Time	<input type="text" value="10"/>	(0~120 Sec)

Motion Detect Time Setting

Mon	<input checked="" type="checkbox"/>	Tue	<input checked="" type="checkbox"/>	Wed	<input checked="" type="checkbox"/>	Thur	<input checked="" type="checkbox"/>
Fri	<input checked="" type="checkbox"/>	Sat	<input checked="" type="checkbox"/>	Sun	<input checked="" type="checkbox"/>	Check All	<input type="checkbox"/>
<input type="text" value="00"/>	:	<input type="text" value="00"/>	-	<input type="text" value="23"/>	:	<input type="text" value="59"/>	

Réglage des paramètres :

- **Détection de mouvement** : Pour activer ou désactiver la détection de mouvement.
- **Time (Temps)** : définit l'intervalle de temps pour la détection de mouvement. En supposant que nous définissons l'intervalle de temps comme "10", et que le premier mouvement capturé puisse être considéré comme le point de départ de la détection de mouvement, et si le mouvement se poursuit pendant 7 secondes de l'intervalle de 10 secondes, alors l'alarme sera déclenchée à 7 secondes (le premier point de déclenchement) et l'action de détection de mouvement peut être déclenchée (envoi d'une notification) n'importe où entre **7 et 10** secondes une fois le mouvement détecté. L'intervalle de "10" secondes correspond à un cycle complet de la détection de mouvement avant qu'elle ne commence un autre cycle du même intervalle de temps. Pour être plus précis, le premier point de déclenchement peut être calculé comme étant " **l'intervalle de temps moins trois** ".

16.3. Paramètres de notification de sécurité

16.3.1. Paramètres de notification par courriel

Si vous souhaitez recevoir la notification de sécurité par e-mail, vous pouvez configurer correctement la notification par e-mail sur l'interface web **Intercom > Action > Notification par e-mail**. La notification par courriel s'affichera comme les captures.

Email Notification	
Sender's email address	<input type="text" value="neil.fang1214@gmail.com"/>
Receiver's email address	<input type="text" value="neil.fang@akuvox.com"/>
SMTP server address	<input type="text" value="smtps://smtp.gmail.com"/>
SMTP user name	<input type="text" value="neil.fang1214@gmail.com"/>
SMTP password	<input type="password" value="••••••••"/>
Email subject	<input type="text" value="Test"/>
Email content	<input type="text" value="Only for Testing."/>
<input type="button" value="Email Test"/>	

Paramétrage :

- **Adresse e-mail de l'expéditeur** : saisissez l'adresse e-mail de l'expéditeur à partir de laquelle la notification par e-mail sera envoyée.
- **Adresse électronique du destinataire** : saisissez l'adresse électronique du destinataire.
- **Adresse du serveur SMTP** : saisissez l'adresse du serveur SMTP de l'expéditeur.
- **Nom d'utilisateur SMTP** : saisissez le nom d'utilisateur SMTP, qui est généralement le même que l'adresse électronique de l'expéditeur.
- **Mot de passe SMTP** : configurez le mot de passe du service SMTP, qui est le même que l'adresse e-mail de l'expéditeur.
- **Objet de l'e-mail** : saisissez l'objet de l'e-mail.

- **Contenu de l'e-mail** : compiler le contenu des e-mails en fonction de vos besoins.

**Note :**

- Pour E12W, le chemin d'accès est le suivant : **Setting > Action > Email Notification**.

16.3.2. Réglage de la notification FTP

Si vous souhaitez recevoir la notification de sécurité par FTP, vous pouvez configurer correctement la notification FTP sur le web **Intercom > interface > Notification FTP**.

FTP Notification	
FTP Server	<input type="text" value="192.168.1.155"/>
FTP User Name	<input type="text" value="admin"/>
FTP Password	<input type="password" value="....."/>
	<input type="button" value="FTP Test"/>

Paramétrage :

- **Serveur FTP** : saisissez l'adresse (URL) du serveur FTP pour la notification FTP.
- **Nom d'utilisateur FTP** : entrez le nom d'utilisateur du serveur FTP.
- **Mot de passe FTP** : entrez le mot de passe du serveur FTP.

**Note :**

- Pour E12W, le chemin d'accès est le suivant : **Setting > Action > FTP Notification**.

16.3.3. Réglage de la notification d'appel SIP

En plus de la notification par FTP et par e-mail, le portier peut également émettre un appel SIP lorsqu'une action est déclenchée. Pour configurer une notification d'appel SIP sur l'interface Web **Intercom > Action > Notification d'appel SIP**.

SIP Call Notification	
SIP Call Number	<input type="text" value="5101100010"/>
SIP Caller Name	<input type="text" value="Judy"/>

Réglage des paramètres :

- **Numéro d'appel SIP** : Pour configurer le numéro d'appel SIP.
- **Nom d'appel SIP** : Pour configurer le nom d'affichage du téléphone de porte.



Note :

- Pour l'E12W, le chemin d'accès est le suivant : **Setting > Action > SIP Call Notification**.

16.3.4. Configuration de la notification d'URL HTTP

Les portiers Akuvox permettent d'envoyer une notification HTTP à une tierce partie lorsque certaines fonctions sont déclenchées. La notification HTTP peut être configurée dans des chapitres spécifiques, veuillez consulter le chapitre 15.4. Le format de l'URL : **http://http adresse IP du serveur/toutes les informations**.

Action to execute	FTP <input type="checkbox"/>	Email <input type="checkbox"/>	Http URL <input type="checkbox"/>
Http URL:	<input type="text"/>		

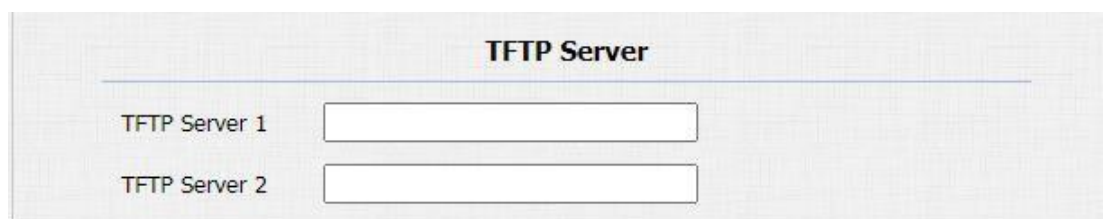
Réglage des paramètres :

- **Http URL** : cochez la case pour activer la notification d'URL HTTP.

- **URL HTTP** : Si vous choisissez le mode HTTP, entrez le format de l'URL : **http://http adresse IP du serveur/toutes les informations.**

16.3.5. Réglage de la notification TFTP

Les portiers Akuvox permettent d'envoyer la capture via un serveur TFTP lors de l'utilisation de la détection de mouvement. Cette fonction doit fonctionner avec le serveur SDMC. Entrez l'adresse du serveur SDMC et vous pourrez obtenir l'image dans le serveur SDMC.



The screenshot shows a configuration window titled "TFTP Server". It contains two rows, each with a label and an empty text input field. The first row is labeled "TFTP Server 1" and the second row is labeled "TFTP Server 2".

Réglage des paramètres :

- **TFTP Server 1/2** : saisissez l'adresse du serveur TFTP. Vous pouvez entrer l'adresse du serveur SDMC dans le serveur 1, et l'adresse du moniteur intérieur qui se trouve dans la même maison dans le serveur 2. Lorsque la détection de mouvement est déclenchée, le SDMC et le moniteur intérieur recevront la capture en même temps.



Note :

- E12W ne permet pas d'envoyer la capture via un serveur TFTP.

16.4. Configuration des actions de sécurité

16.4.1. Configurer l'action du bouton poussoir

En appuyant sur le bouton poussoir, le portier déclenche le type d'action

préconfiguré, la notification peut être envoyée par e-mail, notification FTP ou appel SIP. Pour effectuer cette configuration sur le web **Intercom > Basic**

interface.

PushButton Action

Action to execute FTP Email Http URL

Http URL:

Réglage des paramètres :

- **Action à exécuter** : Pour choisir l'action à exécuter après le déclenchement.

16.4.2. Configurer l'action de mouvement

Lorsque la fonction de détection de mouvement fonctionne, vous pouvez faire en sorte qu'elle déclenche une action. Pour ce faire, configurez l'interface Web **Intercom > Motion**.

Action to execute

Action to execute FTP Email Sip Call HTTP

Http URL:

Réglage des paramètres :

- **Action à exécuter** : Pour choisir l'action à exécuter après le déclenchement.

**Note**

📁 Pour E12W, le chemin d'opération est **Surveillance > Modules**

5.4.3. Configurer l'action

Lorsque l'interface d'entrée fonctionne, elle peut également déclencher une action. Vous pouvez effectuer cette configuration sur le site Web **Intercom > Input** interface.

Action to execute FTP Email Sip Call HTTP

Http URL:

Action Delay (0~300 Sec)

Open Relay

Réglage des paramètres :

- **Action à exécuter** : Pour choisir l'action à exécuter après le déclenchement.

**Note :**

- Pour E12W, le chemin d'accès est le suivant : **Contrôle d'accès > Entrée**

16.5. Cryptage de la voix

SRTP(Secure Real-time Transport Protocol) est un protocole défini sur la base du protocole de transport en temps réel. Les données du protocole de transmission assurent le cryptage, l'authentification des messages, l'assurance de l'intégrité et la protection contre le rejeu. Pour configurer cette fonction sur l'interface Web **Account > Advanced > Encryption**.

Encryption

Voice Encryption(SRTP)

Réglage des paramètres :

- **Cryptage de la voix (SRTP)** : choisissez **Désactivé**, **Facultatif** ou **Obligatoire** pour SRTP. S'il est **optionnel** ou **obligatoire**, la voix pendant l'appel est cryptée, et vous pouvez saisir le paquet RTP pour visualiser les données.

16.6. Agent de l'utilisateur

Vous pouvez personnaliser le champ agent utilisateur dans le message SIP. Si l'agent utilisateur est défini sur une valeur spécifique, les utilisateurs peuvent voir les informations de PCAP. Si l'agent utilisateur est vide, par défaut, les utilisateurs peuvent voir le nom de la société "Akuvox", le numéro de modèle et la version du micrologiciel du PCAP.



The image shows a configuration interface for the 'User Agent' field. The title 'User Agent' is centered at the top. Below it, there is a horizontal line. On the left side, the text 'User Agent' is displayed. To the right of this text is an empty rectangular input box for entering a specific value.

Réglage des paramètres :

- **User Agent** : support pour entrer une autre valeur spécifique, Akuvox est par défaut.

17. Moniteur et image

17.1. Surveillance des cours d'eau RTSP

Les portiers Akuvox prennent en charge le flux RTSP qui permet aux dispositifs d'interphone tels que le moniteur intérieur ou l'unité de surveillance d'un tiers de surveiller ou d'obtenir l'audio/vidéo en temps réel (flux RTSP) du portier en utilisant l'URL correct.

17.1.1. RTSP Basic Setting

Vous devez configurer la fonction RTSP sur l'interface web **Intercom > RTSP > RTSP Basic** de l'appareil en termes d'autorisation RTSP, d'authentification et de mot de passe, etc. avant de pouvoir utiliser la fonction.

RTSP Basic	
RTSP Server Enabled	<input checked="" type="checkbox"/>
RTSP Authorization	<input type="checkbox"/>
MJPEG Authorization	<input type="checkbox"/>
RTSP Authentication Type	Basic ▾
RTSP User Name	admin
RTSP Password	•••••••

Réglage des paramètres :

- **RTSP Server Enable** : cliquez sur Enable et Disable dans le champ **RTSP Enable** pour activer ou désactiver la fonction RTSP.
- **RTSP Authorization (Autorisation RTSP)** : cliquez sur Enable (Activer) et Disable (Désactiver) dans le champ RTSP Authorization (Autorisation RTSP) pour activer ou désactiver l'autorisation RTSP. Si vous activez l'autorisation RTSP, vous devez entrer le type d'authentification RTSP, le nom d'utilisateur RTSP et le mot de passe RTSP sur le dispositif d'interphone tel que le moniteur intérieur pour l'autorisation.

- **Nom d'utilisateur RTSP** : entrez le nom utilisé pour l'autorisation RTSP.
- **Mot de passe utilisateur RTSP** : entrez le mot de passe pour l'autorisation RTSP.
- **Type d'authentification RTSP** : sélectionnez le type d'authentification RTSP entre " **Basic** " et " **Digest** ". "**Basic**" est le type d'authentification par défaut.

**Note :**

- Pour E12W, le chemin d'opération est **Surveillance > RTSP**.

17.1.2. Réglage du flux RTSP

Vous pouvez sélectionner le format de codec vidéo du flux RTSP pour la surveillance et configurer la résolution vidéo et le débit binaire, etc. en fonction de votre environnement réseau actuel sur l'interface Web **Intercom > RTSP > Flux RTSP**.

RTSP Stream	
RTSP Audio Enabled	<input type="checkbox"/>
RTSP Video Enabled	<input checked="" type="checkbox"/>
RTSP Video2 Enabled	<input checked="" type="checkbox"/>
RTSP Audio Codec	PCMU ▾
RTSP Video Codec	H.264 ▾

Paramétrage :

- **RTSP Audio Enabled** : **tick** pour activer l'audio RTSP qui signifie, le téléphone de porte peut également envoyer des informations audio au moniteur par RTSP.
- **RTSP vidéo activé** : **le portier** peut envoyer les informations vidéo au moniteur. Après avoir activé la fonction RTSP, la vidéo RTSP est activée par défaut et ne peut pas être modifiée.

- **RTSP Video2 Enabled** : **Akuvox** door phones supporte 2 flux RTSP, vous pouvez activer le second.
- **Codec audio RTSP** : **choisissez** un codec audio approprié pour l'audio RTSP.
- **Codec vidéo RTSP** : **choisissez** un codec vidéo approprié pour la vidéo RTSP.

H.264 And H.265 Video Parameters	
Video Resolution	720P ▼
Video Framerate	30 fps ▼
Video Bitrate	2048 kbps ▼
Video2 Resolution	VGA ▼
Video2 Framerate	30 fps ▼
Video2 Bitrate	512 kbps ▼

Réglage des paramètres :

- **Résolution vidéo** : sélectionnez les résolutions vidéo parmi sept options : "QCIF", "QVGA", "CIF", "VGA", "4CIF", "720P". La résolution vidéo par défaut est "4CIF". La vidéo du portier risque de ne pas pouvoir être affichée sur le moniteur intérieur si la résolution est supérieure à "4CIF".
- **Fréquence d'images vidéo** : "30fps" est la fréquence d'images vidéo par défaut.
- **Débit binaire vidéo** : sélectionnez le débit binaire vidéo parmi six options : "128 kbps", "256kbps", "512 kbps", "1024 kbps", "2048 kbps", "4096 kpbs" en fonction de votre environnement réseau. Le débit vidéo par défaut est de "2048 kpbs".
- **Résolution Video2** : sélectionnez la résolution vidéo pour le deuxième canal de flux vidéo. Alors que la solution vidéo par défaut est "VGA".
- **Video2 Framerate** : sélectionnez la fréquence d'images vidéo pour le deuxième canal de flux vidéo. "25fps" est la fréquence d'images vidéo par défaut pour le deuxième canal de flux vidéo.
- **Video2 Bitrate** : sélectionnez le débit binaire vidéo parmi les six options pour le deuxième canal de flux vidéo. Par défaut, le deuxième canal de flux vidéo est "512 kpbs".

17.2. Capture d'images MJPEG

Les portiers Akuvox vous permettent de capturer l'image de surveillance au format Mjpeg si nécessaire. Vous pouvez activer la fonction Mjpeg sur **Intercom > RTSP > RTSP Basic** et définir la qualité de l'image sur l'interface web **Intercom > RTSP > MJPEG Video Parameters**.

RTSP Basic	
RTSP Server Enabled	<input checked="" type="checkbox"/>
RTSP Authorization	<input type="checkbox"/>
MJPEG Authorization	<input type="checkbox"/>
RTSP Authentication Type	Basic ▾
RTSP User Name	admin
RTSP Password	••••••••

MJPEG Video Parameters	
Video Resolution	VGA ▾
Video Framerate	30 fps ▾
Video Quality	90 ▾

Réglage des paramètres :

- **Autorisation MJPEG** : à cocher pour accéder à la vidéo du dispositif ou aux captures d'écran en temps réel par le biais d'un navigateur (adresse http telle que : http://device IP:8080/video.cgi (vidéo dynamique), http://device IP:8080/jpeg.cgi (capture d'écran statique)).
- **Résolution vidéo** : sélectionnez les résolutions vidéo parmi sept options : "QCIF", "QVGA", "CIF", "VGA", "4CIF", "720P". La résolution vidéo par défaut est "4CIF". La vidéo du portier risque de ne pas pouvoir être affichée sur le moniteur intérieur si la résolution est supérieure à "4CIF".
- **Fréquence d'images vidéo** : "30fps" est la fréquence d'images vidéo par défaut.
- **Qualité vidéo** : le débit binaire de la vidéo, de 50 à 90.



Note :

- Pour E12W, le chemin d'opération est **Surveillance > RTSP > Paramètres vidéo MJPEG**

17.3. ONVIF

La vidéo en temps réel de la caméra du portier peut être recherchée et obtenue par le moniteur intérieur Akuvox ou par des dispositifs tiers tels que les NVR (**Network Video Recorder**). Vous pouvez configurer la fonction ONVIF sur l'interface web **Intercom > ONVIF** afin que d'autres dispositifs puissent voir la vidéo du portier.



Basic Setting

Onvif Mode: Discoverable

UserName: admin

Password:

Réglage des paramètres :

- **Discoverable** : cochez la case pour activer le mode ONVIF Discoverable. Si vous sélectionnez "**Discoverable**", la vidéo de la caméra du portier peut être recherchée par d'autres appareils.
- **Nom d'utilisateur** : saisissez le nom d'utilisateur. Le nom d'utilisateur est "**admin**" par défaut.
- **Mot de passe** : saisissez le mot de passe. Le mot de passe est "**admin**" par défaut.

Une fois le paramétrage terminé, vous pouvez entrer l'URL ONVIF sur l'appareil tiers pour visualiser le flux vidéo.

Par exemple : **http://IP adresse:80/onvif/device_service**



Note :

- Remplissez l'adresse IP spécifique du téléphone de porte dans l'URL.

17.4. Stream en direct

Si vous voulez vérifier la vidéo en temps réel à partir du portier, vous pouvez aller sur l'interface web du dispositif **Intercom > Live Stream** pour obtenir la vidéo en temps réel ou vous pouvez également entrer l'URL correct sur le navigateur web pour l'obtenir directement.

Pour vérifier la vidéo en temps réel à l'aide d'une URL, vous pouvez saisir l'URL correcte (http://IP_address:8080/video.cgi) sur le navigateur Web si vous souhaitez obtenir la vidéo en temps réel directement au lieu de passer par l'interface Web.

**Note :**

- Pour l'E12W, le chemin d'accès est **Surveillance > Live Stream**.

18. Bûches

18.1. Journaux d'appels

Si vous voulez vérifier les appels, y compris les appels sortants, les appels reçus et les appels manqués pendant une certaine période, vous pouvez vérifier et rechercher le journal des appels sur l'interface Web **Téléphone > Journal des appels**.

Call History						
			All	▼	Hang Up	
Index	Type	Date	Time	Local Identity	Name	Number
1	Dialed	2021-02-04	09:30:33	192.168.31.2 @192.168.31.2	Unknown	192.168.35.1 12@192.168.35.112 5.112
2	Received	2021-02-04	09:29:57	192.168.31.2 @192.168.31.2	192.168.35.112	192.168.35.1 12@192.168.35.112 5.112
3	Dialed	2021-02-04	09:29:06	192.168.31.2 @192.168.31.2	Unknown	192.168.35.1 12@192.168.35.112 5.112

Réglage des paramètres :

- **Historique des appels** : sélectionnez l'historique des appels parmi quatre options : "**Tous**", "**Composé**" "**Reçu**" "**Manqué**" pour le type spécifique de journal d'appels à afficher.
- **Raccrocher** : pour raccrocher l'appel depuis le web.
- **Index** : l'ordre des journaux d'appels.
- **Date** : la date du journal des appels.
- **Heure** : l'heure du journal des appels.
- **Nom/Numéro** : le nom et le numéro du contact.

Note :

- Seule la version R20 V2 prend en charge la fonction Raccrochage.
- Pour E12W, le chemin d'accès est **Intercom > Call Log**.

18.2. Bûches de porte

Si vous souhaitez rechercher et vérifier et importer/exporter les différents types d'historique d'accès aux portes, vous pouvez rechercher et vérifier les journaux de portes sur l'interface web du dispositif **Phone > Door Log**.

Door Log

Door Log

Index	Name	Code	Type	Date	Time	Status	<input type="checkbox"/>
1							<input type="checkbox"/>
2							<input type="checkbox"/>
3							<input type="checkbox"/>
4							<input type="checkbox"/>
5							<input type="checkbox"/>
6							<input type="checkbox"/>
7							<input type="checkbox"/>
8							<input type="checkbox"/>
9							<input type="checkbox"/>
10							<input type="checkbox"/>
11							<input type="checkbox"/>
12							<input type="checkbox"/>
13							<input type="checkbox"/>
14							<input type="checkbox"/>
15							<input type="checkbox"/>

Page 1 ▾
Prev
Next
Delete
Delete All

Import/Export Door Log(.xml)

选择文件
未选择任何文件
Import
Export

Réglage des paramètres :

- **Indexez** : l'ordre des journaux d'appels.
- **Name** : S'il s'agit d'une clé ou d'une carte ajoutée localement, le nom ajouté correspondant sera affiché. S'il s'agit d'une clé ou d'une carte inconnue, l'écran affichera Inconnu.
- **Code** : Si l'ouverture de la porte se fait par code PIN, le code PIN correspondant sera affiché. Si l'ouverture de la porte se fait via des cartes RF, le numéro de la carte correspondante sera affiché, et si la porte est ouverte par commande HTTP, elle sera vide.
- **Type** : Si l'ouverture de la porte se fait par code PIN, **Mot de passe** sera affiché. Si l'ouverture de la porte se fait par carte RF, **Card** sera affiché, et si la porte est ouverte par commande HTTP, **Http** sera affiché.
- **Date** : La date d'ouverture de la porte.
- **C'est le moment** d'ouvrir la porte.
- **Statut** : le résultat de l'ouverture de la porte : **succès** ou **échec**.

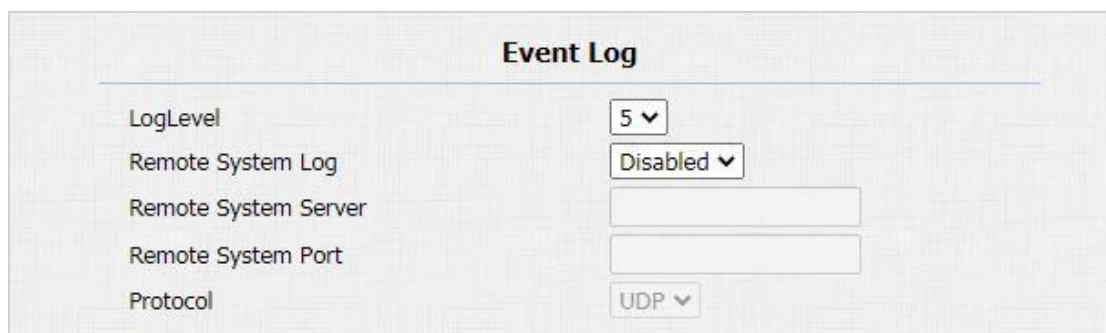
**Note :**

- Seule la version R20 V2 prend en charge la fonction d'importation/exportation.
- Pour F12W, le chemin d'accès est **Contrôle d'accès > Journal de porte**

19. Déboguer

19.1. Journal des événements

Il est utilisé pour exporter les journaux spécifiques au dispositif (appel, émission de carte, ouverture de porte, téléchargement des fichiers de configuration de l'application pour la mise à niveau, configuration du réseau, incidents de piratage, etc.) vers le serveur distant. Pour le configurer sur l'interface web **Upgrade > Advanced > Event Log**.



Event Log	
LogLevel	5 ▾
Remote System Log	Disabled ▾
Remote System Server	<input type="text"/>
Remote System Port	<input type="text"/>
Protocol	UDP ▾

Réglage des paramètres :

- **LogLevel** : sélectionnez les niveaux de journalisation de 1 à 7 niveaux. Le personnel technique d'Akuvox vous indiquera le niveau de journal spécifique à saisir à des fins de débogage. Le niveau de journal par défaut est "5". Plus le niveau est élevé, plus le journal est complet.
- **Journal du système à distance** : sélectionnez "**Activer**" ou "**Désactiver**" si vous souhaitez activer ou désactiver le journal du système à distance.
- **Remote System Server** : entrez l'adresse du serveur distant pour recevoir le **journal de l'appareil**. L'adresse du serveur distant sera fournie par le support technique Akuvox.
- **Port du système distant** : le port du serveur distant.
- **Protocole** : le protocole de transmission par défaut est UDP. Après l'activation de la fonction d'exportation des journaux à distance, la boîte déroulante permet de choisir entre les deux protocoles de transmission UDP et TCP.

**Note :**

- Seule la version R20 V2 prend en charge la fonction de journal des événements.

19.2. Journal du système

Le journal du système du portier peut être utilisé à des fins de débogage. Si vous souhaitez exporter le système vers un PC local ou vers un serveur distant à des fins de débogage, vous pouvez configurer la fonction sur l'interface Web **Upgrade > Advanced > System Log**.

System Log	
LogLevel	3 ▾
Export Log	Export
Remote System Log	Disabled ▾
Remote System Server	<input type="text"/>
Remote System Port	<input type="text"/>

Réglage des paramètres :

- **LogLevel** : sélectionnez les niveaux de journalisation de 1 à 7 niveaux. Le personnel technique d'Akuvox vous indiquera le niveau de journal spécifique à saisir à des fins de débogage. Le niveau de journal par défaut est "3". Plus le niveau est élevé, plus le journal est complet.
- **Exporter le journal** : cliquez sur l'onglet **Exporter** pour exporter le fichier journal de débogage temporaire vers un PC local.
- **Exportation du journal de débogage** : cliquez sur l'onglet **Exportation** pour exporter le fichier journal de débogage vers un PC local.
- **Journal du système à distance** : sélectionnez "**Activer**" ou "**Désactiver**" si vous souhaitez activer ou désactiver le journal du système à distance.
- **Serveur du système à distance** : saisissez l'adresse du serveur à distance qui recevra la

le **journal de l'appareil**. Et l'adresse du serveur distant sera fournie par le support technique d'Akuvox.

**Note :**

- Pour E12W, le chemin d'accès est le suivant : **Mise à niveau > Diagnostic > Journal du système**.

19.3. PCAP

Le PCAP du portier Akuvox est utilisé pour capturer le paquet de données entrant et sortant des appareils à des fins de débogage et de dépannage. Vous pouvez configurer le PCAP sur l'interface web de l'appareil **Upgrade > Advanced > PCAP** correctement avant de l'utiliser.

PCAP

Specific Port (1-65535)

PCAP

PCAP Auto Refresh Enabled

Paramétrage :

- **Port spécifique** : sélectionnez les ports spécifiques de 1 à 65535 afin que seul le paquet de données du port spécifique puisse être capturé. Vous pouvez laisser le champ vide par défaut.
- **PCAP** : cliquez sur l'onglet **Start** et **Stop** pour capturer une certaine gamme de paquets de données avant de cliquer sur l'onglet **Export** pour exporter les paquets de données vers votre PC local.
- **PCAP Auto Refresh (Rafraîchissement automatique du PCAP)** : sélectionnez "**Enable**" (**Activer**) ou "**Disable**" (**Désactiver**) pour activer ou désactiver la fonction de rafraîchissement automatique du PCAP. Si vous la réglez sur "Enable", le PCAP continuera à capturer des paquets de données

même après que les paquets de données aient atteint leur limite d'utilisation.

Capacité maximale de 1M. Si vous le réglez sur "**Disable**", le PCAP arrêtera la capture de paquets de données lorsque le paquet de données capturé atteindra la capacité maximale de capture de 1Mo.

**Note :**

- Pour l'E12W, le chemin d'opération est : **Mise à jour > Diagnostic > PCAP.**

20. Mise à jour du micrologiciel

Les firmwares de différentes versions pour le portier Akuvox peuvent être mis à jour sur l'interface web du dispositif **Upgrade > Basic**.

Firmware Version	20.0.1.222
Hardware Version	20.0.0.0.0.0.0.0
Upgrade	<input type="button" value="Choose File"/> No File Chosen
	<input type="button" value="Submit"/> <input type="button" value="Cancel"/>

Réglage des paramètres :

- **Mettez à jour** : Choisissez le micrologiciel .rom de votre PC, puis cliquez sur **Soumettre** pour mettre à jour.

21. Sauvegarde

Les fichiers de configuration peuvent être importés ou exportés de l'appareil vers votre PC local sur l'interface Web de l'appareil **Mise à niveau > Avancé > Autres**, si nécessaire.

Others

Config File(.tgz/.conf/.cfg) No file chosen

(Encrypted)

Réglage des paramètres :

- **Exporter le fichier de configuration** : pour exporter le fichier de configuration actuel.
- **Exporter/Importer** : pour exporter le fichier de configuration actuel (crypté) ou importer un nouveau fichier de configuration.



Note :

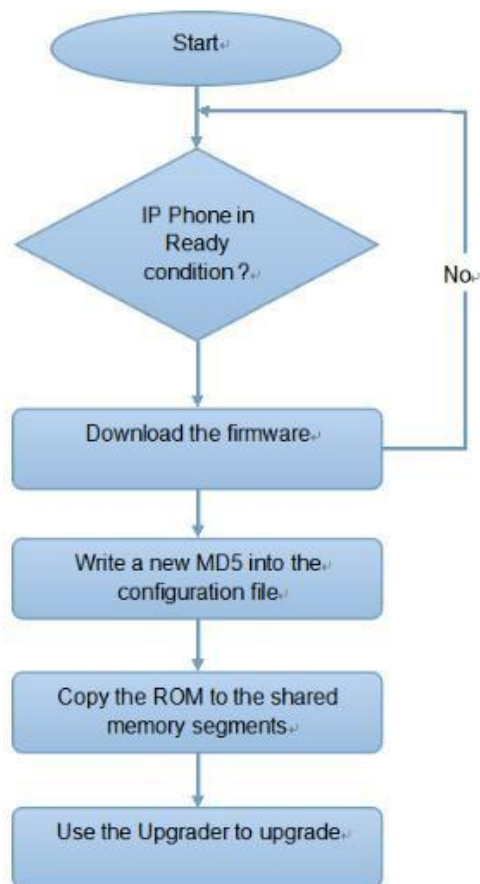
- Pour E12W, le chemin d'accès est le suivant : **Mise à niveau > Diagnostic > Autres**.

22. Auto-provisioning via un fichier de configuration

Les configurations et les mises à jour du portier Akuvox peuvent être effectuées sur l'interface web par le biais d'un auto-alimentation unique et d'un auto-alimentation programmé via des fichiers de configuration, ce qui vous évite de définir les configurations nécessaires une par une manuellement sur le portier.

22.1. Principe de l'alimentation

L'auto-alimentation est une fonction utilisée pour configurer ou mettre à niveau les appareils par lots via des serveurs tiers. **DHCP, PNP, TFTP, FTP, HTTPS** sont les protocoles utilisés par les dispositifs d'interphonie Akuvox pour accéder à l'URL de l'adresse du serveur tiers qui stocke les fichiers de configuration et les firmwares, qui seront ensuite utilisés pour mettre à jour le firmware et les paramètres correspondants sur le portier.



22.2. Fichiers de configuration pour l'auto-provisionnement

Les fichiers de configuration ont deux formats pour l'auto-provisionnement. L'un est le fichier de configuration général utilisé pour le provisionnement général et l'autre est le provisionnement de la configuration basée sur le MAC.

La différence entre les deux types de fichiers de configuration est présentée ci-dessous :

- **Provisionnement de la configuration générale** : un fichier général est stocké sur un serveur à partir duquel tous les appareils liés pourront télécharger le même fichier de configuration pour mettre à jour les paramètres sur les appareils. Par exemple : : r000000000020.cfg.
- **Approvisionnement de la configuration basée sur le MAC** : Les fichiers de configuration basés sur le MAC sont utilisés pour le provisionnement automatique sur un appareil spécifique, distingué par son numéro MAC unique. Les fichiers de configuration nommés avec le numéro MAC du dispositif seront automatiquement mis en correspondance avec le numéro MAC du dispositif avant d'être téléchargés pour le provisionnement sur le dispositif spécifique.

Pour obtenir le modèle de fichier de configuration Autop sur **Upgrade > Advanced > Automatic Autop** interface.

Automatic Autop

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

**Note :**

- Si un serveur possède ces deux types de fichiers de configuration, les périphériques IP accéderont d'abord aux fichiers de configuration générale avant d'accéder aux fichiers de configuration basés sur le MAC.

22.3. Programme AutoP

Akuvox vous fournit différentes méthodes Autop qui permettent au portier d'effectuer le provisionnement pour lui-même dans un temps spécifique selon votre planning.

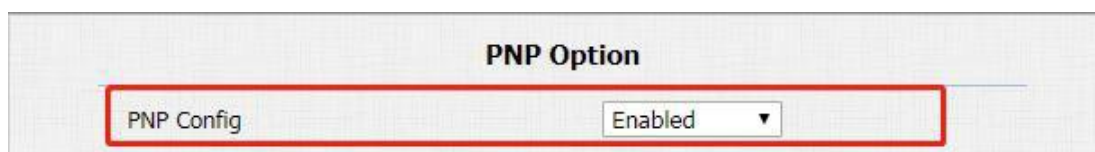
Automatic Autop	
Mode	Power On <input type="button" value="v"/>
Schedule	Sunday <input type="button" value="v"/>
	22 Hour(0~23)
	0 Min(0~59)

Réglage des paramètres :

- **Mode** : sélectionnez "Mise sous tension", "**Répétition**", "**Mise sous tension + Répétition**", "**Répétition horaire**" comme calendrier d'activation automatique. Sélectionnez "**Power on**", si vous voulez que l'appareil exécute Autop à chaque fois qu'il démarre. Sélectionnez "**Répétition**" si vous souhaitez que l'appareil exécute l'opération automatique selon le calendrier que vous avez établi. Sélectionnez "**Mise sous tension + Répétition**", si vous souhaitez combiner le mode **Mise sous tension** et le mode **Répétition** qui permettra à l'appareil d'effectuer une mise sous tension automatique à chaque démarrage ou selon le calendrier que vous avez défini. Sélectionnez "**Répétition horaire**", si vous souhaitez que l'appareil effectue une opération automatique toutes les heures.

22.4. Configuration PNP

Plug and Play (PNP) est une combinaison de support matériel et logiciel qui permet à un système informatique de reconnaître et de s'adapter aux changements de configuration matérielle avec peu ou pas d'intervention de la part de l'utilisateur. Pour effectuer cette configuration sur l'interface web **Upgrade > Advanced > PNP Option**.

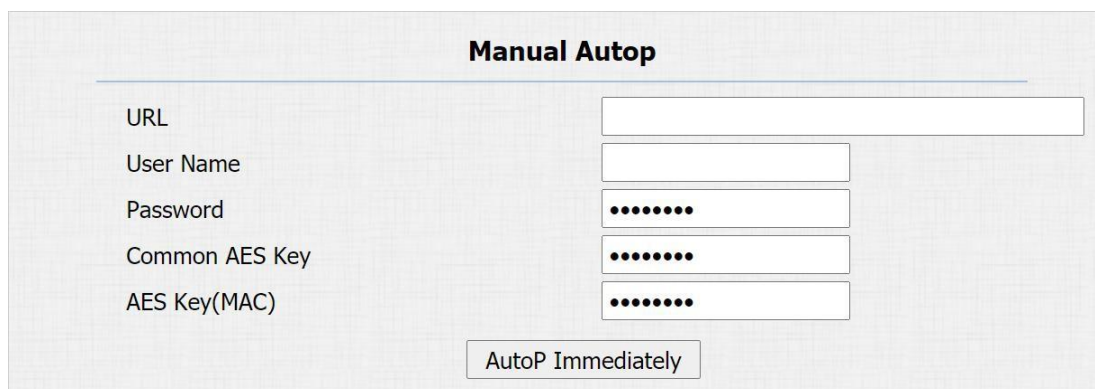


PNP Option

PNP Config Enabled

22.5. Configuration de l'approvisionnement statique

Vous pouvez configurer manuellement une URL de serveur spécifique pour télécharger le micrologiciel ou le fichier de configuration. Si un programme d'auto-alimentation est configuré, le portier effectuera l'auto-alimentation à un moment précis selon le programme d'auto-alimentation que vous avez configuré. En outre, TFTP, FTP, HTTP et HTTPS sont les protocoles qui peuvent être utilisés pour mettre à jour le micrologiciel et la configuration du dispositif.



Manual Autop

URL

User Name

Password

Common AES Key

AES Key(MAC)

AutoP Immediately

Paramétrage :

- **URL** : configurer l'adresse du serveur tftp, http, https, ftp pour le provisionnement.
- **Nom d'utilisateur** : définissez un nom d'utilisateur si le serveur a besoin d'un nom d'utilisateur pour être accessible, sinon laissez-le vide.

- **Mot de passe** : configurez un mot de passe si le serveur a besoin d'un mot de passe pour être accessible, sinon laissez-le vide.

- **Common AES Key (clé AES commune)** : configurez le code AES pour que l'interphone puisse déchiffrer le fichier de configuration général de l'Auto Provisioning.
- **Clé AES (MAC)** : configurer le code AES pour que l'interphone puisse déchiffrer le fichier de configuration de l'auto provisioning basé sur le MAC.

 **Note :**

- AES est un type de cryptage, il doit être configuré uniquement lorsque le fichier de configuration est crypté avec AES, sinon laissez le champ vide.

 **Note :****Format de l'adresse du**

TFTP : tftp://192.168.0.19/

FTP : ftp://192.168.0.19/ (permet une connexion

ftp://username:password@192.168.0.19/(nécessite un nom d'utilisateur

et mot de passe)

HTTP : http://192.168.0.19/ (utiliser le port 80 par défaut)

http://192.168.0.19:8080/ (utiliser d'autres ports, tels que 8080)

 **Conseil :**

- Akuvox ne fournit pas de serveur spécifié par l'utilisateur.
- Veuillez préparer vous-même le serveur TFTP/FTP/HTTP/HTTPS.

23. Intégration avec un dispositif tiers

23.1. Intégration via Wiegand

Si vous voulez intégrer le portier Akuvox avec les dispositifs tiers via Wiegand, vous pouvez configurer le Wiegand sur l'interface web.



The screenshot shows a configuration panel titled "Wiegand". It contains two dropdown menus. The first is labeled "WiegandType" and is set to "wiegand-26". The second is labeled "Wiegand Mode" and is set to "Input".

Paramétrage :

- **Wiegand Type** : définit le format de transmission des données Wiegand parmi trois options : **Wiegand 26**, **Wiegand 34**, **Wiegand 58**. Le format de transmission doit être identique entre le portier et le dispositif à intégrer.
- **Mode Wiegand** : réglez le mode de transfert entre l'**entrée** et la **sortie** si le portier est utilisé comme récepteur, réglez-le comme "Entrée" pour le portier et vice versa.

23.2. Intégration via l'API HTTP

L'API HTTP est conçue pour réaliser une intégration en réseau entre un dispositif tiers et le dispositif d'interphonie Akuvox. Vous pouvez configurer la fonction HTTP API sur l'interface web **Intercom > HTTP API** pour l'intégration.

HTTP API	
HTTP API	Enabled
Auth Mode	Digest
User Name	admin
Password	*****
IP01	
IP02	
IP03	
IP04	
IP05	

Submit Cancel

Réglage des paramètres :

- **HTTP API** : sélectionnez "**Enable**" ou "**Disable**" pour activer ou désactiver la fonction HTTP API pour l'intégration d'un tiers. Par exemple, si la fonction est désactivée, toute demande de lancement de l'intégration sera refusée et renverra le statut HTTP 403 interdit.
- **Auth Mode** : choisissez parmi quatre options : "**None**" "**WhiteList**" "**Basic**", "**Digest**" pour le type d'autorisation, qui sera expliqué en détail dans le tableau suivant.
- **Nom d'utilisateur** : entrez le nom d'utilisateur lorsque le mode d'autorisation "**Basic**" et "**Digest**" est sélectionné. Le nom d'utilisateur par défaut est "Admin".
- **Mot de passe** : entrez le mot de passe lors de l'autorisation "**Basic**" et "**Digest**".

est sélectionné. Le nom d'utilisateur par défaut est "Admin".

- **IP01-IP05** : entrez l'adresse IP des dispositifs tiers lorsque l'autorisation "WhiteList" est sélectionnée pour l'intégration.

Veillez vous référer à la description suivante pour le mode d'authentification

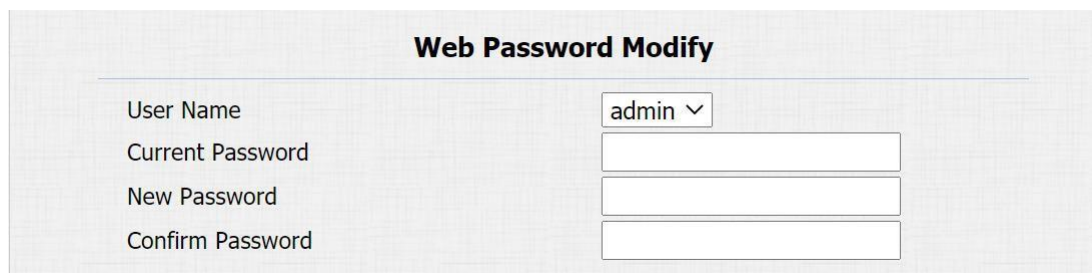
NON	Mode d'autorisation	Description
1	Aucun	Aucune authentification n'est requise pour l'API HTTP car elle n'est utilisée que pour les tests de démonstration.
2	Normal	Ce mode est utilisé par le développeur Akuvox uniquement.
3	Liste blanche	Si ce mode est sélectionné, il vous suffit de renseigner l'adresse IP du périphérique tiers pour l'authentification. La liste blanche est adaptée au fonctionnement en réseau local.
4	Base	Dans le champ Autorisation de l'en-tête de la demande HTTP, utilisez la méthode de codage Base64 pour coder le nom d'utilisateur et le mot de passe.
5	Digest	Méthode de cryptage du mot de passe, supporte uniquement le MD5. MD5(Message-Digest Algorithm) Dans le champ Autorisation de l'en-tête de la requête Http : WWW-Authenticate:Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".

6	Token	Ce mode est utilisé par le développeur Akuvox uniquement.
---	--------------	---

24. Modification du mot de passe

24.1. Modifier le mot de passe de l'interface Web du dispositif

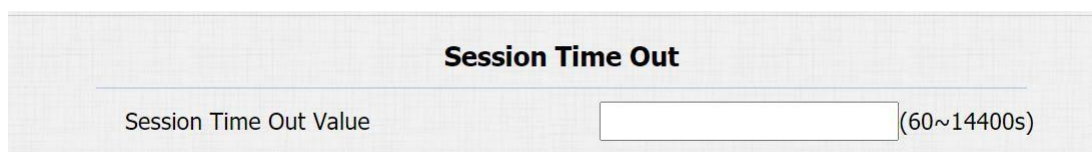
Pour modifier le mot de passe Web par défaut sur l'interface Web **Security > Basic**. Sélectionnez "**admin**" pour le compte administrateur et "**User**" pour le compte utilisateur. Cliquez sur l'onglet **Change Password** pour modifier le mot de passe.



Web Password Modify	
User Name	admin ▾
Current Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

24.2. Configurer la déconnexion automatique de l'interface Web

Il s'agit d'une conception de protection. Lorsqu'il n'y a pas d'opération sur le site Web et que le délai de sortie de la session est atteint, le site Web se déconnecte automatiquement.



Session Time Out	
Session Time Out Value	<input type="text"/> (60~14400s)

Configuration des paramètres :

- **Valeur du délai d'expiration de la session** : Plage de 60 à 14400 secondes. Si aucune opération n'est effectuée pendant cette période, vous devez vous reconnecter au site Web.

25. Redémarrage et réinitialisation du système

25.1. Redémarrer

Si vous souhaitez redémarrer le système de l'appareil, vous pouvez l'opérer sur l'appareil **Mise à niveau** > Interface web de **base** également.

25.2. Réinitialiser

Si vous souhaitez réinitialiser le système de l'appareil aux paramètres d'usine, vous pouvez le faire dans l'interface Web **Upgrade** > **Basic**.

26. Abréviations

ACS : Serveur de configuration automatique

Auto : Automatiquement

AEC : Annuleurs d'échos acoustiques et de lignes configurables

ACD : Distribution automatique

d'appels **Autop** : Provisionnement

automatique **AES** : Advanced

Encryption Standard **BLF** : Busy

Lamp Field (Champ de la lampe
occupée)

COM : Commun

CPE : Customer Premise Equipment

CWMP : CPE WAN Management

Protocol **DTMF** : Dual Tone Multi-
Frequency (multifréquence à double
tonalité)

DHCP : Dynamic Host Configuration Protocol (protocole de configuration dynamique des hôtes)

DNS : Système de noms de domaine

DND : Ne pas déranger

DNS-SRV : Enregistrement de service dans le système des noms de domaine

FTP : Protocole de transfert de fichiers

GND : Terre

HTTP : Protocole de transfert hypertexte

HTTPS : Hypertext Transfer Protocol Secure Socket Layer (protocole de transfert hypertexte).

IP : Internet

Protocol **ID** :

Identification **IR** :

Infrarouge

LCD : Affichage à cristaux

liquides **LED** : Diode

électroluminescente **MAX** :

Maximum

POE : Power Over Ethernet

PCMA : Modulation par code d'impulsions de type A **PCMU** : Modulation par code d'impulsions de type μ **PCAP** : Capture de paquets

PNP : Plug and Play

RFID : Identification par radiofréquence

RTP : Protocole de transport en temps réel **RTSP** : Real Time Streaming Protocol **MPEG** : Moving Picture Experts Group **MWI** : Indicateur de message en attente

NO : Ouverture normale

NC : Connexion normale

NTP : Network Time Protocol (protocole de temps réseau)

NAT : traduction d'adresses de réseau

NVR : enregistreur vidéo en réseau

ONVIF : Open Network Video Interface Forum

SIP : Session Initiation Protocol (protocole d'ouverture de session)

SNMP : Simple Network Management Protocol

STUN : Session Traversal Utilities for NAT

SMTP : Simple Mail Transfer Protocol

SDMC : Centre de gestion des dispositifs SIP

TR069 : Rapport technique 069

TCP : Transmission Control Protocol

TLS : Transport Layer Security **TFTP** : Trivial File Transfer Protocol **UDP** : User Datagram Protocol (protocole de datagramme utilisateur)

URL : Localisateur de ressources

uniformes **VLAN** : Réseau local

virtuel **WG** : Wiegand

27. FAQ

Q1 : Comment obtenir l'adresse IP du R2X ?

A1 : ✓ Pour les appareils avec un seul bouton - E21/ R20/ R23/ R26 :

Lorsque le E21/ R20/ R23/ R26 s'allume normalement, maintenez le bouton d'appel pendant 5 secondes après que la LED de la statue devienne bleue et il entrera en mode annonce IP. En mode annonce, l'adresse IP sera annoncée de manière répétée. Appuyez à nouveau sur le bouton d'appel pour quitter le mode d'annonce.

✓ Pour les appareils avec un clavier numérique multiple - R27 :

Lorsque le R27 s'allume normalement, appuyez sur "*2396#" pour accéder à l'écran d'accueil et appuyez sur "1" pour accéder à l'écran d'information du système et vérifier l'adresse IP.

✓ Pour les appareils avec écran tactile - X915/R29 :

Pendant qu'il s'allume normalement, dans l'interface de numérotation, appuyez sur "9999", "Touche de numérotation", "3888" et "OK" pour entrer dans l'écran de réglage du système. Allez à l'écran d'information pour vérifier l'adresse IP.

✓ Common method :

Utilisation du Scanner IP Akuvox pour rechercher des appareils Akuvox dans le même réseau LAN.

Q2 : Les appareils Akuvox supportent-ils le codec opus ?

A2 : Pour le moment, seul le téléphone IP vidéo Android R48G d'Akuvox peut supporter le codec audio Opus.

Q3 : Quelle est la plage de température supportée par le portier akuvox ?

A3 : R20/E21/R26/R23/Standard R27/Standard X915 -- 14° à 112°F (-10° à 45°C)

R27/X915 avec support de chauffage --- 40 degrés

R28 -- (-40°C~55°C)

Téléphone intérieur -- 14° à 112°F (-10° à

45°C) Téléphone extérieur -- 32°~104°F

(0~40°C)

Q4 : Les appareils Akuvox supportent-ils le protocole

Modbus ? R4 : Non.

Q5 : Échec de l'importation des données de visage du X915 vers un autre X915 utilisant les données de visage exportées .

A5 : Veuillez confirmer les étapes suivantes

: Le format d'importation est zip ;

1. Après avoir exporté, vous devez dézipper le dossier .tgz, puis refaire le dossier dézippé en .zip.

Q55 : Quelle version d'ONVIF le R20 et le X915 supportent-ils ?

R55 : Profils ONVIF 18.04

Q6

:Est-ce que les téléphones supportent les types de cartes?Prox,Legacy iClass,iClassSE,HID Mifare,HID DESFire,HID SEOS

A6 : Désolé, ils ne sont pas pris en charge. Ils doivent être implémentés via des modifications matérielles.

Q7 : Comment confirmer si mon appareil est de la version matérielle 1 ou de la version matérielle 2 ?

A7 : 1.Label

● **Matériel version 1**



● **Matériel version 2**



- **Version du micrologiciel**

Le micrologiciel est différent entre la version matérielle 1 et la version matérielle 2. Allez sur Web-Status -Firmware Version.
 20.X.X.X est la version 1 du matériel.
 220.X.X.X est la version 2 du matériel.

- **Version du matériel**

Le micrologiciel est différent entre la version matérielle 1 et la version matérielle 2. Allez sur Web-Status -Firmware Version.
 Si la version matérielle est 220.x, alors le dispositif est de la version matérielle 2.

Status	
Product Information	
Model	R20K
MAC Address	0C:11:05:0B:00:6D
Firmware Version	20.30.4.8
Hardware Version	20.9.0.0.0.0.0

28. Nous contacter

Pour plus d'informations sur le produit, veuillez nous rendre visite à l'adresse www.akuvox-france.fr ou n'hésitez pas à nous contacter par

Courriel de vente : contact@akuvox-france.fr

Courriel du support technique : support@akuvox-france.fr

Téléphone : +33 9 81 24 00 06