Poste de porte modulaire

Manuel d'utilisation

V1.0.0

Avant-propos

Général

Ce manuel présente la configuration de la platine de rue de la villa (ci-après dénommée "VTO") sur l'interface Web.

Consignes de sécurité

Les mots-indicateurs catégorisés suivants avec une signification définie peuvent apparaître dans le manuel.

Mots-clés	Sens
 MISE EN GARDE	Indique un risque potentiel qui, s'il n'est pas évité, pourrait entraîner des dommages matériels, une perte de données, une baisse des performances ou un résultat imprévisible.
 REMARQUE	Fournit des informations supplémentaires comme emphase et complément au texte.

Historique des révisions

Version	Contenu de la révision	Date de sortie
V1.0.0	Première sortie.	janvier 2021

À propos du manuel

- Le manuel est pour référence seulement. En cas d'incohérence entre le manuel et le produit réel, le produit réel prévaudra.
- Nous ne sommes pas responsables des pertes causées par des opérations non conformes au manuel. Le
- manuel serait mis à jour conformément aux dernières lois et réglementations des juridictions concernées. Pour des informations détaillées, reportez-vous au manuel papier, au CD-ROM, au code QR ou à notre site Web officiel. En cas d'incohérence entre le manuel papier et la version électronique, la version électronique prévaudra.
- Tous les designs et logiciels sont sujets à changement sans préavis écrit. Les mises à jour du produit peuvent entraîner des différences entre le produit réel et le manuel. Veuillez contacter le service clientèle pour obtenir le programme le plus récent et la documentation complémentaire.
- Il peut toujours y avoir des écarts dans les données techniques, les fonctions et la description des opérations, ou des erreurs d'impression. En cas de doute ou de litige, nous nous réservons le droit d'explication finale.
- Mettez à niveau le logiciel du lecteur ou essayez un autre logiciel de lecteur grand public si le manuel (au format PDF) ne peut pas être ouvert.
- Toutes les marques commerciales, les marques déposées et les noms de société dans le manuel sont la propriété de leurs propriétaires respectifs.
- Veuillez visiter notre site Web, contacter le fournisseur ou le service client en cas de problème lors de l'utilisation de l'appareil.
- En cas d'incertitude ou de controverse, nous nous réservons le droit d'explication finale.

Mesures de sécurité et avertissements importants

La description suivante est la méthode d'application correcte du VTO. Lisez attentivement le manuel avant utilisation, pour éviter tout danger et perte de propriété. Se conformer strictement au manuel lors de l'utilisation et le conserver correctement après l'avoir lu.

Exigences de fonctionnement

- N'exposez pas l'appareil à la lumière directe du soleil ou à une source de chaleur. N'installez
- pas l'appareil dans un environnement humide ou poussiéreux. Installez l'appareil
- horizontalement à des endroits stables pour l'empêcher de tomber.
- Ne faites pas couler ou éclabousser de liquide sur l'appareil, et ne placez pas sur l'appareil un objet rempli de
- liquide. Installez l'appareil dans des endroits bien ventilés et ne bloquez pas son ouverture de ventilation.
- Utilisez l'appareil uniquement dans la plage d'entrée et de sortie
- nominale. Ne démontez pas l'appareil vous-même.
- Transportez, utilisez et stockez l'appareil dans la plage d'humidité et de température autorisée.

Exigences d'alimentation

- Utilisez des fils électriques recommandés dans votre région et conformes à ses spécifications nominales.
- Utilisez une alimentation électrique conforme aux exigences SELV (très basse tension de sécurité) et fournissez une alimentation avec une tension nominale conforme à la source d'alimentation limitée de la norme IEC60950-1. Pour connaître les exigences spécifiques en matière d'alimentation électrique, consultez l'étiquette sur l'appareil.
- Le coupleur d'appareil est un dispositif de déconnexion. Lors d'une utilisation normale, gardez un angle qui facilite l'utilisation.

Table des matières

1 Initialisation du VTO

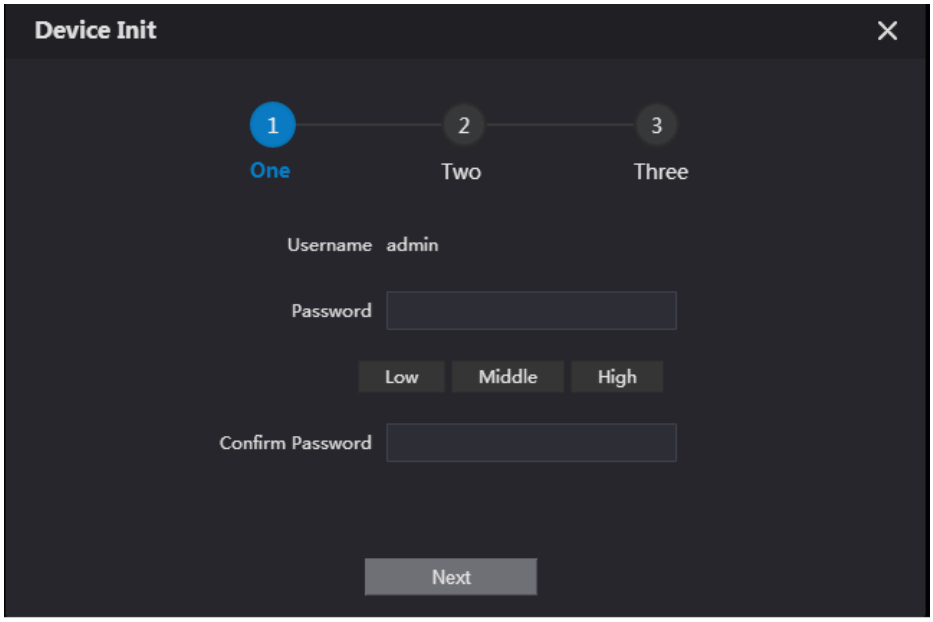
Pour la première connexion ou après la réinitialisation du VTO, vous devez l'initialiser sur l'interface Web.

Step 1 Allumez le VTO.

Step 2 Entrez l'adresse IP par défaut (192.168.1.108) du VTO dans la barre d'adresse du navigateur.

Assurez-vous que l'adresse IP de votre PC se trouve dans le même segment de réseau que le VTO.

Figure 1-1 Initialisation de l'appareil



Step 3 Entrez et confirmez le mot de passe, puis cliquez sur**Prochain**. Entrez

Step 4 une adresse e-mail pour réinitialiser le mot de passe.

Step 5 Cliquez sur**Prochain**, puis cliquez sur**D'ACCORD**.

2 Connexion et réinitialisation du mot de passe

2.1 Connexion

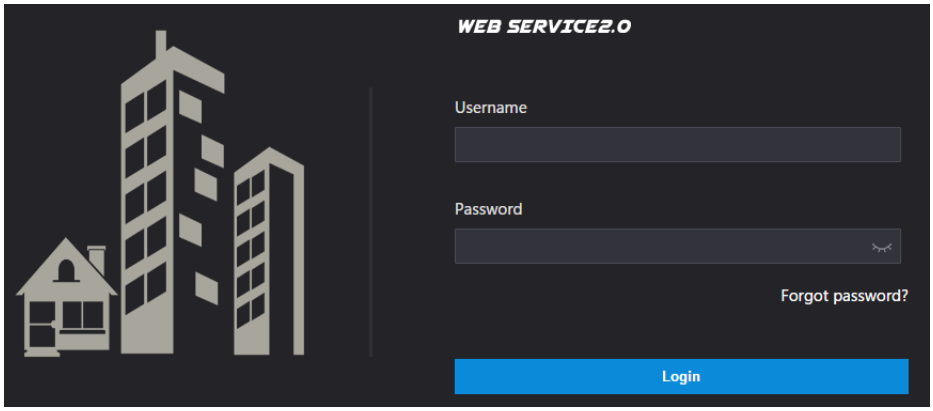
Avant de vous connecter, assurez-vous que le PC se trouve dans le même segment de réseau que le VTO.

Step 1 Accédez à l'adresse IP du VTO dans le navigateur.

Pour la première connexion, entrez l'adresse IP par défaut. Si vous avez plusieurs VTO, nous vous recommandons de changer l'adresse IP par défaut (**Réseau > Basique**) pour éviter les conflits.

Step 2 Entrez "admin" comme nom d'utilisateur et le mot de passe que vous avez défini lors de l'initialisation, puis cliquez sur **Connexion**.

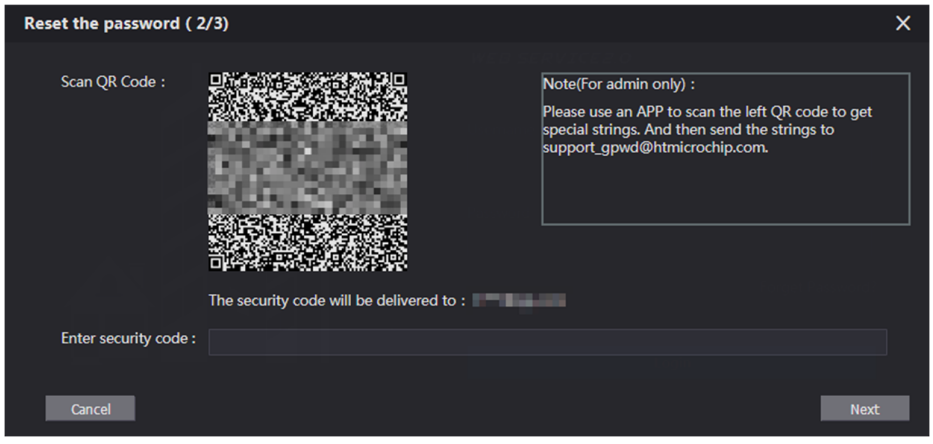
Figure 2-1 Interface de connexion



2.2 Réinitialiser le mot de passe

Step 1 Sur l'interface de connexion, cliquez sur**Mot de passe oublié?**, puis cliquez sur**Prochain**.

Figure 2-2 Réinitialiser le mot de passe (2/3)



Step 2 Scannez le code QR, puis vous obtiendrez une chaîne de chiffres et de lettres.

Step 3 Envoyez la chaîne à l'e-mail : support_gpwd@htmicrochip.com , puis le code de sécurité sera envoyé à l'adresse e-mail configurée lors de l'initialisation.

Step 4 Entrez le code de sécurité dans la zone de saisie, puis cliquez sur**Prochain**.

- Si vous n'avez pas défini d'adresse e-mail lors de l'initialisation, contactez votre fournisseur ou service client pour obtenir de l'aide.
- Le code de sécurité ne sera valide que pendant 24 heures après réception.
- Si vous saisissez le mauvais code de sécurité 5 fois consécutives, votre compte sera verrouillé pendant 5 minutes.

Step 5 Entrez et confirmez le nouveau mot de passe, puis cliquez sur**D'ACCORD**.

3 Interface principale

Figure 3-1 Interface principale

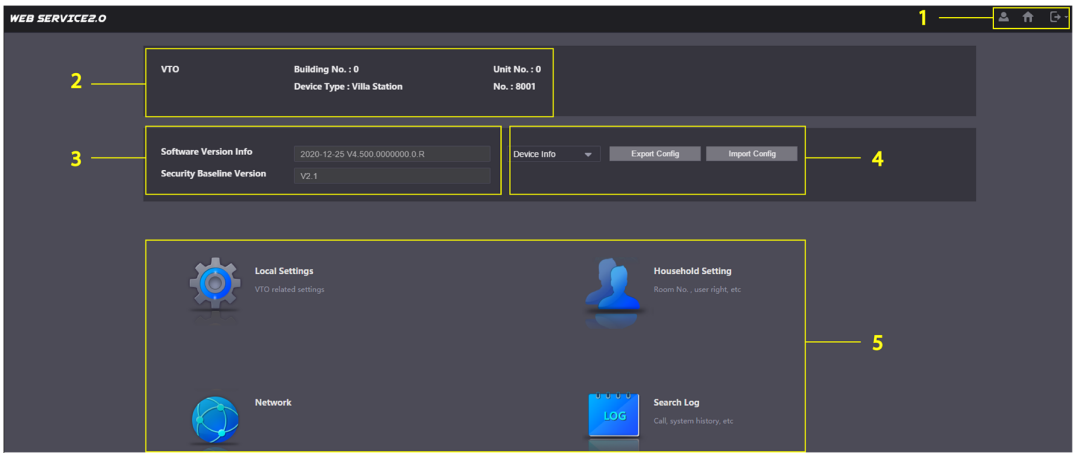


Tableau 3-1 Présentation de l'interface principale

Non.	Fonction	La description
1	Fonction générale	● : Modifiez le mot de passe et votre adresse e-mail. ● : Accédez à l'interface principale. ● : Déconnectez-vous, redémarrez le VTO ou restaurez le VTO aux paramètres d'usine. Si vous restaurez le VTO aux paramètres d'usine, toutes les données, à l'exception du stockage externe, seront supprimées. Vous pouvez formater la carte SD pour supprimer les données qu'elle contient.
2	Informations VTO	Afficher les informations du VTO et du système.
3	Informations système	
4	Configuration gestionnaire	Exportez ou importez la configuration VTO ou les informations utilisateur.
5	Fonction	Configurez les paramètres pour différentes fonctions. L'interface et la fonction peuvent varier selon le type d'appareil que vous avez configuré pour le VTO. L'interface et la fonction réelles prévaudront.

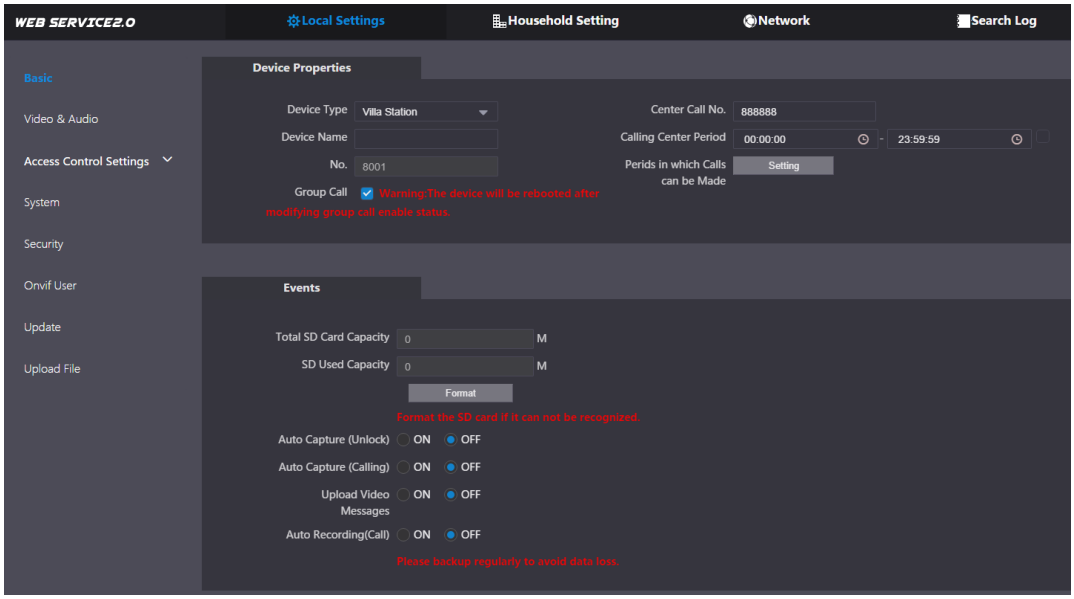
4 paramètres locaux

Ce chapitre présente la configuration détaillée du VTO.

4.1 De base

Step 1 Sélectionner**Paramètres locaux > De base**.

Figure 4-1 De base



Step 2 Configurez les paramètres.

Tableau 4-1 Description des paramètres de base

Paramètre	La description
Type d'appareil	Sélectionner**Villa Station**ou**Petit appartement**comme requis.
Numéro d'appel du centre	Le numéro de téléphone par défaut du centre de gestion est 888888 et vous pouvez le définir sur n'importe quel numéro comportant jusqu'à 9 chiffres.
Nom de l'appareil	Lorsque d'autres appareils surveillent ce VTO, le nom de l'appareil apparaît sur l'image de surveillance.
Période du centre d'appels	Période pendant laquelle le centre de gestion peut être appelé.
Non.	Utilisé pour différencier chaque VTO, et nous vous recommandons de le définir en fonction du numéro d'unité ou de bâtiment, puis vous pouvez ajouter des VTO au serveur SIP en utilisant leurs numéros. Vous pouvez modifier le numéro du VTO lorsqu'il ne fonctionne pas comme serveur SIP.
Périodes pendant lesquelles les appels peuvent être passés	Configurez l'heure si vous souhaitez uniquement recevoir des appels pendant une période spécifique.
Appel de groupe	Activez-le sur le VTO qui fonctionne comme serveur SIP, et lorsqu'un VTH principal reçoit un appel, tous les VTH d'extension recevront également l'appel.

Paramètre	La description
Carte SD totale Capacité	Affiche la capacité totale et utilisée de la carte SD. Vous pouvez cliquer**Format** pour supprimer toutes les données de la carte SD.
Capacité SD utilisée	
Format	
Capture automatique (Ouvrir)	Lorsque la porte est déverrouillée, le VTO prendra deux instantanés et les enregistrera sur la carte SD.
Capture automatique (appel)	Prenez un instantané et enregistrez-le sur la carte SD du VTO lorsque le VTO appelle.
Télécharger une video messages	Lorsqu'il est activé : ● Si une carte SD est insérée à la fois dans le VTH et le VTO, le message vidéo sera enregistré à la fois dans les cartes SD du VTH et du VTO. ● Si une carte SD est insérée uniquement dans le VTH ou le VTO, le message vidéo sera enregistré uniquement dans la carte SD du VTH ou du VTO. ● Si aucune carte SD n'est insérée dans le VTH ou le VTO, aucun message vidéo ne sera enregistré.
Enregistrement automatique (appel)	Enregistrez une vidéo lorsque le VTO est en cours d'appel et enregistrez l'enregistrement sur la carte SD du VTO.

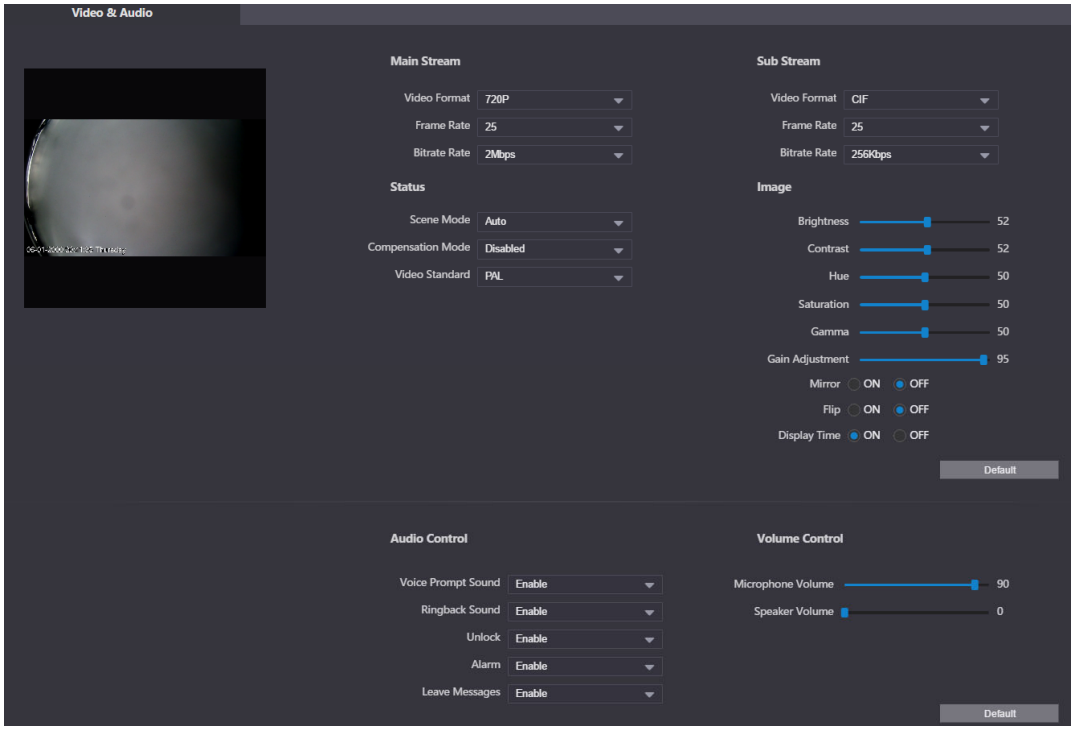
Step 3 Cliquez sur**sauvegarder**.

4.2 Vidéo et audio

Configurez le format et la qualité vidéo, ainsi que l'audio du VTO.

Step 1 Sélectionner**Paramètres locaux > Vidéo et audio**.

Figure 4-2 Vidéo et audio



Step 2 Configurez les paramètres, qui prendront effet en cas de modification.

Tableau 4-2 Description des paramètres vidéo

Paramètre		La description
Principal/Sub Flux	Format vidéo	Sélectionnez une résolution différente selon vos besoins : ● **1080P**: 1920 × 1080. ● **720P**: 1280 × 720. ● **WVGA**: 800 × 480. ● **QVGA**: 320 × 240. **D1**: ● 720 × 480. ● **CAF**: 352 × 288.
	Fréquence d'images	Plus la valeur est élevée, plus la vidéo est fluide, mais elle nécessite plus de bande passante.
	Débit binaire	Plus la valeur est élevée, meilleure est la qualité vidéo, mais cela nécessite plus de bande passante.
Statut	Mode scène	Sélectionnez au besoin en fonction des conditions d'éclairage.**Auto**est sélectionné par défaut.
	Compensation Mode	● **BLC**: Compensation de contre-jour. Améliorer la clarté de la cible dans l'image. ● **WDR**: Large plage dynamique. Améliorez la luminosité des zones sombres et réduisez la luminosité des zones claires pour améliorer l'image. ● **CLH**: Compensation de lumière élevée. Réduisez la luminosité des points forts pour améliorer l'image globale.
	Norme vidéo	Sélectionner**COPAIN**ou**NTSC**selon votre région. **COPAIN**est principalement utilisé en Chine et en Europe, et**NTSC** principalement aux États-Unis et au Japon.
Image	Luminosité	Plus la valeur est élevée, plus l'image est lumineuse.
	Contraste	Une valeur plus élevée pour plus de contraste entre les zones claires et sombres.
	Teinte	Rendre la couleur plus claire ou plus foncée. La valeur par défaut est définie par le capteur de lumière et nous vous recommandons de la conserver par défaut.
	Saturation	Plus la valeur est claire, plus la couleur est épaisse.
	Gamma	Modifie la luminosité de l'image et améliore la plage dynamique de l'image de manière non linéaire. Plus la valeur est élevée, plus l'image est lumineuse.
	Ajustement du gain	Amplifiez le signal vidéo pour augmenter la luminosité de l'image. Si la valeur est trop grande, il y aura plus de bruit dans l'image.
	Miroir	Affiche l'image avec les côtés gauche et droit inversés.
	Retourner	Affiche l'image à l'envers.
	Temps d'affichage	Affiche l'heure et la date actuelles sur l'image vidéo.
l'audio Contrôler	—	Activez ou désactivez chaque type de son.
Le volume Contrôler	Microphone Le volume	Ajustez le volume selon vos besoins.
	Volume du haut-parleur	

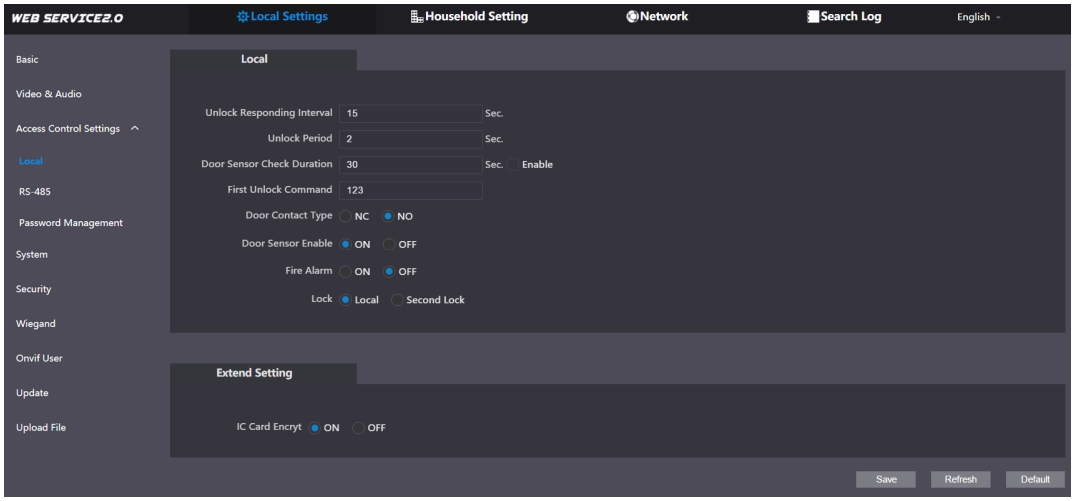
4.3 Paramètres de contrôle d'accès

Cette section explique comment configurer les deux serrures connectées au port de serrure ou au port RS-485 du VTO.

4.3.1 Locale

Step 1 Sélectionner**Paramètres locaux > Paramètres de contrôle d'accès**.

Figure 4-3 Local



Step 2 Configurez les paramètres.

Tableau 4-3 Description des paramètres de contrôle d'accès local

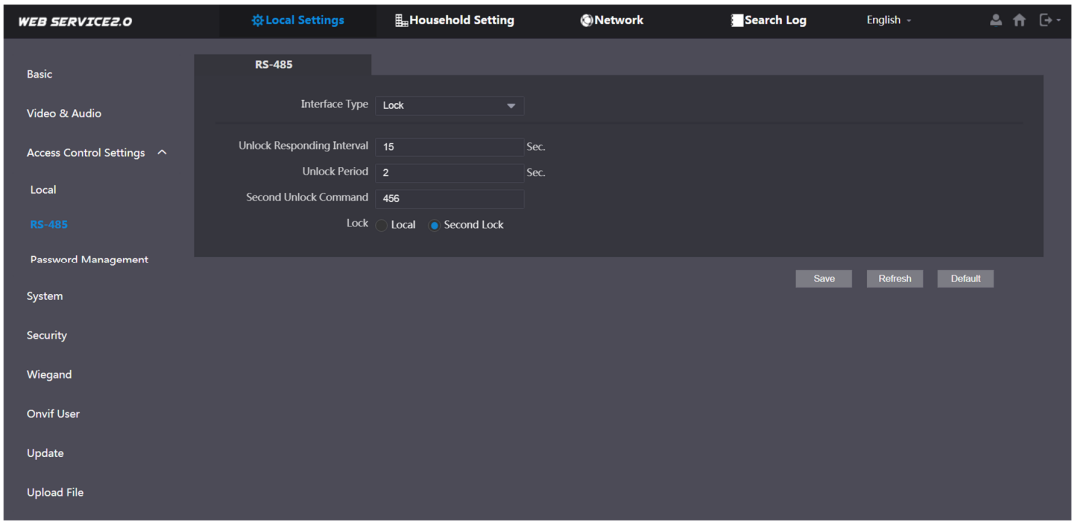
Paramètre	La description
Déverrouiller la réponse Intervalle	La porte ne peut être déverrouillée qu'après l'intervalle.
Déverrouiller la période	Le temps pendant lequel la serrure reste déverrouillée.
Vérification du capteur de porte Durée	● Activez-le et la porte ne sera pas verrouillée tant que les capteurs de porte ne se seront pas contactés. Si la porte est déverrouillée plus longtemps que la**Durée de vérification du capteur de porte**, l'alarme du capteur de porte sera déclenchée et l'alarme sera envoyée au centre de gestion. ● Désactivez-le, puis la porte sera verrouillée après le**Déverrouiller la période**. Vous devez installer un contact de porte pour configurer ce paramètre.
Premier/deuxième déverrouillage Commande	Vous pouvez connecter un téléphone tiers, tel qu'un téléphone SIP, au VTO et utiliser la commande pour ouvrir la porte à distance.
Type de contact de porte	● **NC**: Normalement fermé. ● **NON**: Normalement ouvert.
Activation du capteur de porte	Synchronisez l'état du capteur de porte avec les moniteurs intérieurs (VTH).
Alarme incendie	S'il est activé, vous pouvez connecter un dispositif d'alarme au port qui est à l'origine pour le contact de porte, mais vous ne pouvez pas utiliser la fonction de contact de porte.
Bloquer	Les méthodes non distantes, telles que le mot de passe ou la carte, déverrouilleront le verrou que vous sélectionnez.
Crypter la carte IC	Les cartes d'accès délivrées par le VTO seront cryptées et non clonables.

Step 3 Cliquez sur**sauvegarder**.

4.3.2 RS-485

Sélectionner**Paramètres locaux > Paramètres de contrôle d'accès**, puis configurez les paramètres de la serrure connectée via le port RS-485. Voir Tableau 4-3 pour la description des paramètres.

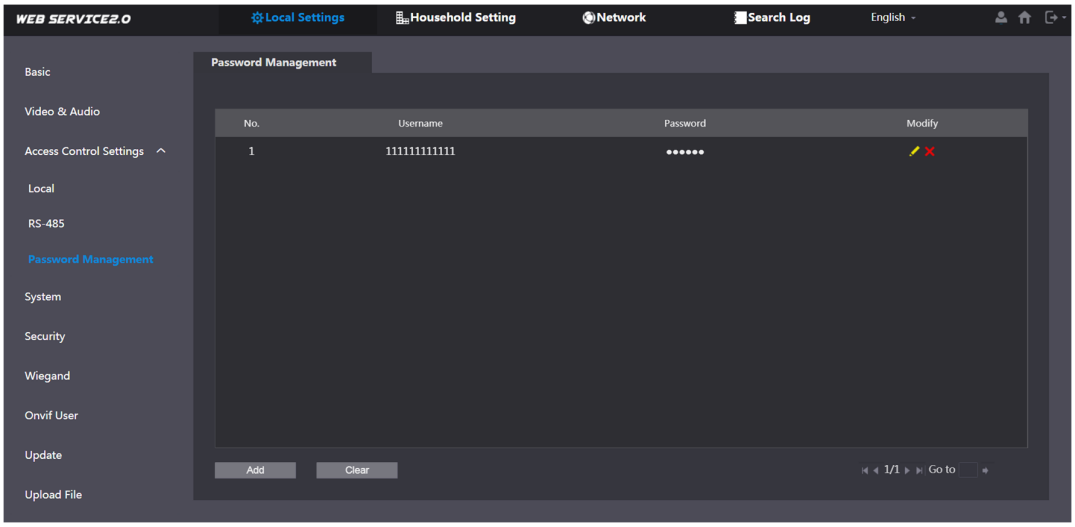
Figure 4-4 Serrure connectée via le port RS-485



4.3.3 Gestion des mots de passe

Ajoutez un nom d'utilisateur et un mot de passe utilisés pour déverrouiller la porte.

Figure 4-5 Gestion des mots de passe

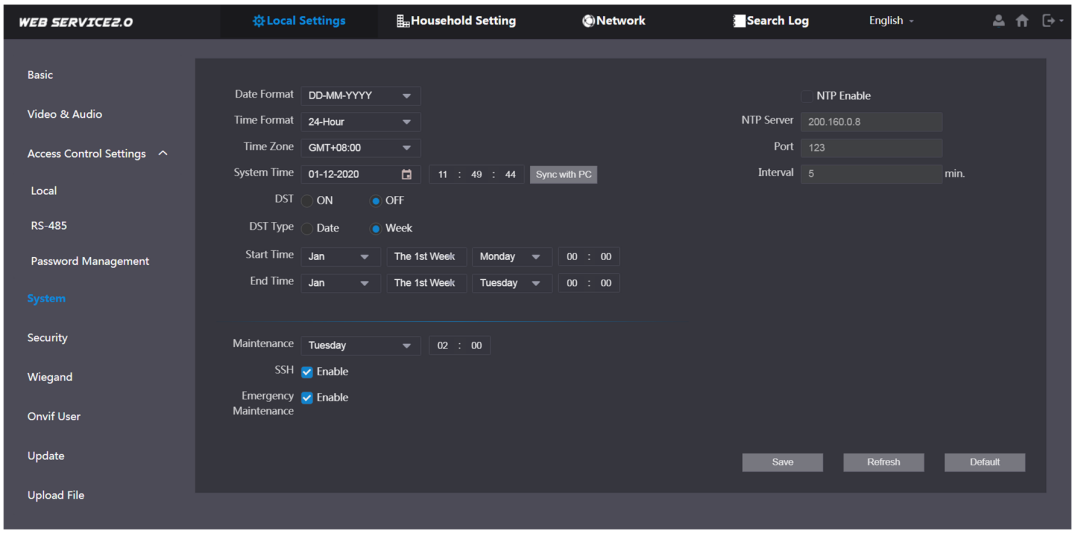


4.4 Système

Configurez les paramètres d'heure, le serveur NTP, etc.

Step 1 Sélectionner**Paramètres locaux > Système**.

Figure 4-6 Système



Step 2 Configurez les paramètres.

Tableau 4-4 Description des paramètres système

Paramètre	La description
Format de date	Sélectionnez un format selon vos besoins.
Format de l'heure	
Le temps du système	La modification de l'heure système peut entraîner des problèmes lors de la recherche de vidéos et de la publication d'informations. Désactivez l'enregistrement vidéo et l'instantané automatique avant de le modifier.
Fuseau horaire	Configurez le fuseau horaire selon vos besoins.
Synchroniser avec le PC	Synchronisez l'heure du système VTO avec votre PC.
heure d'été	Heure d'été. Si cela s'applique à votre région, vous devez l'activer, puis configurer le type d'heure d'été, l'heure de début et l'heure de fin.
Type d'heure d'été	Sélectionner**Date**ou**La semaine**selon vos besoins, puis configurez la période spécifique.
Heure de début	Configurez l'heure de début et l'heure de fin de l'heure d'été.
Heure de fin	
Activer NTP	Activez NTP et entrez l'adresse IP du serveur NTP, puis le VTO synchronisera automatiquement l'heure avec le serveur NTP.
Serveur NTP	
Port	Numéro de port du serveur NTP.
Intervalle	Cycle de mise à jour de l'heure VTO. 30 minutes maximum.
Entretien	Définissez l'heure à laquelle le VTO redémarrera automatiquement.
SSH	Vous pouvez connecter des périphériques de débogage au VTO via le protocole SSH. Nous vous recommandons de le désactiver et d'activer le mode de sécurité et la protection des informations de service sortantes. Voir "4.5 Sécurité". Sinon, le VTO pourrait être exposé à des risques de sécurité et à des fuites de données.
Urgence Entretien	Activez-le pour l'analyse et la réparation des pannes. Cette fonction occupera les ports 8088 et 8087.

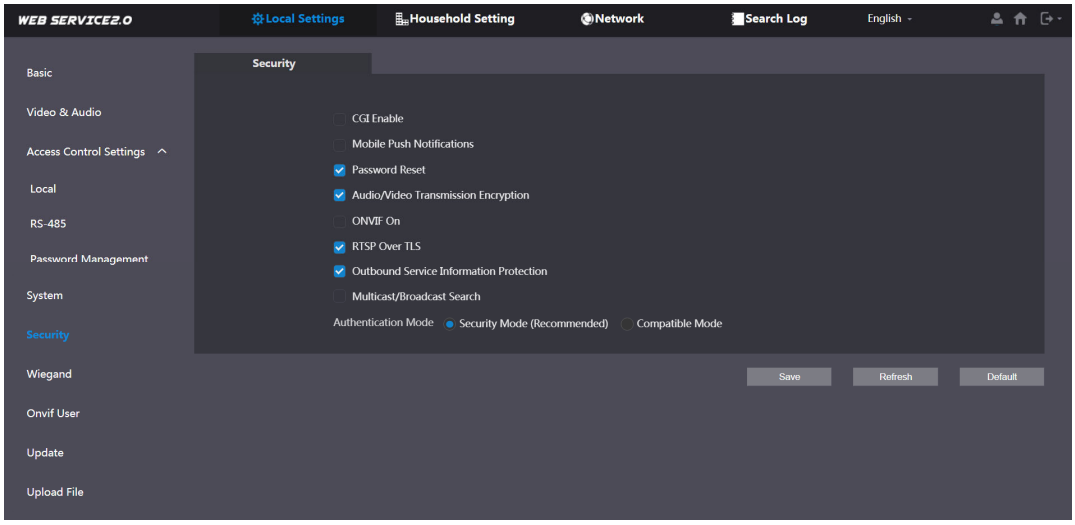
Step 3 Cliquez sur**sauvegarder**.

4.5 Sécurité

Configurez les fonctions qui impliquent la sécurité de l'appareil.

Step 1 Sélectionner**Paramètres locaux > Sécurité**.

Figure 4-7 Sécurité



Step 2 Configurez les paramètres.

Tableau 4-5 Description des paramètres de sécurité

Paramètre	La description
Activer CGI	Activer l'utilisation de la commande CGI. ⚠ Nous vous recommandons de le désactiver. Sinon, le VTO pourrait être exposé à des risques de sécurité et à des fuites de données.
Poussée mobile Notification	Envoyez des informations à l'application sur le smartphone. ⚠ Nous vous recommandons de le désactiver si vous n'avez pas besoin de cette fonction. Sinon, le VTO pourrait être exposé à des risques de sécurité et à des fuites de données.
Réinitialisation du mot de passe	S'il est désactivé, vous ne pourrez pas réinitialiser le mot de passe.
Audio Video Transmission Chiffrement	Crypter toutes les données lors d'un appel vocal ou vidéo. ⚠ Nous vous recommandons de l'activer. Sinon, le VTO pourrait être exposé à des risques de sécurité et à des fuites de données.
ONVIF activé	Autoriser les appareils tiers à extraire le flux vidéo du VTO via le protocole ONVIF. ⚠

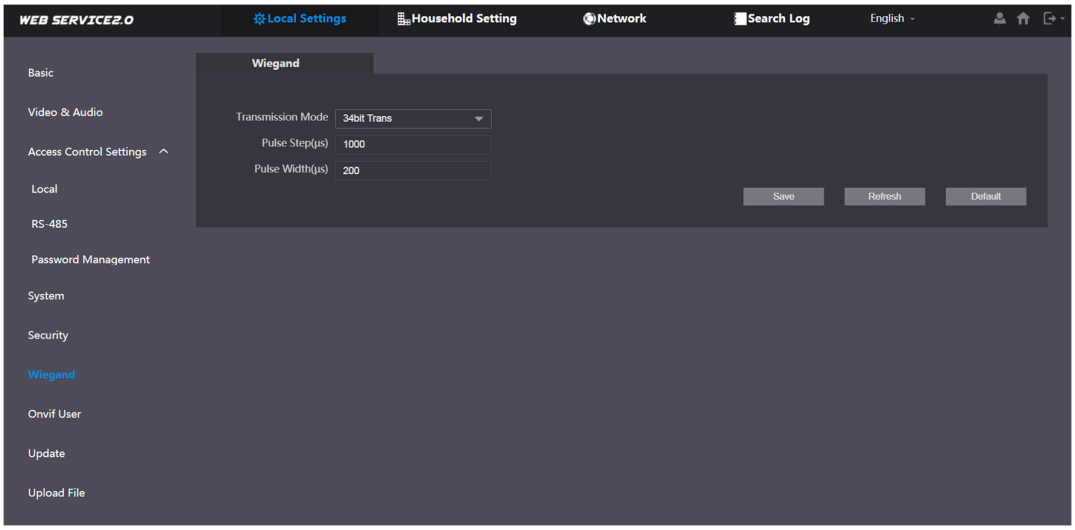
Paramètre	La description
	Nous vous recommandons de le désactiver. Sinon, le VTO pourrait être exposé à des risques de sécurité et à des fuites de données.
RTSP sur TSL	Sortie du flux binaire chiffré via RTSP. ⚠ Nous vous recommandons de l'activer. Sinon, le VTO pourrait être exposé à des risques de sécurité et à des fuites de données.
Service sortant Informations protection	Protégez vos mots de passe. ⚠ Nous vous recommandons de l'activer. Sinon, le VTO pourrait être exposé à des risques de sécurité et à des fuites de données.
Multidiffusion/diffusion Chercher	Activez-le et le VTO sera trouvé par d'autres appareils. ⚠ Nous vous recommandons de le désactiver. Sinon, le VTO pourrait être exposé à des risques de sécurité et à des fuites de données.
Authentification Mode	● **Mode sécurité**(recommandé) : prend en charge la connexion avec l'authentification Digest. ● **Mode compatible**: Utilisez l'ancienne méthode de connexion. ⚠ Nous recommandons le mode de sécurité. Le mode compatible peut exposer le VTO à des risques de sécurité et à des fuites de données.

Step 3 Cliquez sur**sauvegarder**.

4.6 Wiegand

Configurez les paramètres selon vos besoins lorsque vous êtes connecté à d'autres appareils, tels qu'un lecteur de carte avec un port Wiegand.

Figure 4-8 Wiegand



4.7 Utilisateur Onvif

Ajoutez des comptes pour les appareils pour surveiller le VTO via le protocole ONVIF.

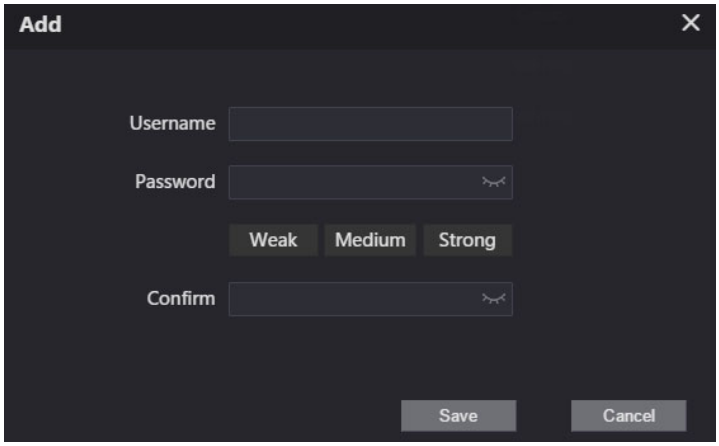
⚠

Si vous supprimez un compte, cela ne peut pas être annulé.

Step 1 Sélectionner**Paramètres locaux > Utilisateur Onvif**. Cliquez

Step 2 sur**Ajouter**.

Figure 4-9 Ajouter un utilisateur ONVIF



Step 3 Entrez les informations, puis cliquez sur**sauvegarder**.

Les appareils ONVIF peuvent désormais surveiller le VTO en utilisant le compte. Voir le manuel de l'utilisateur de l'appareil ONVIF pour plus de détails.

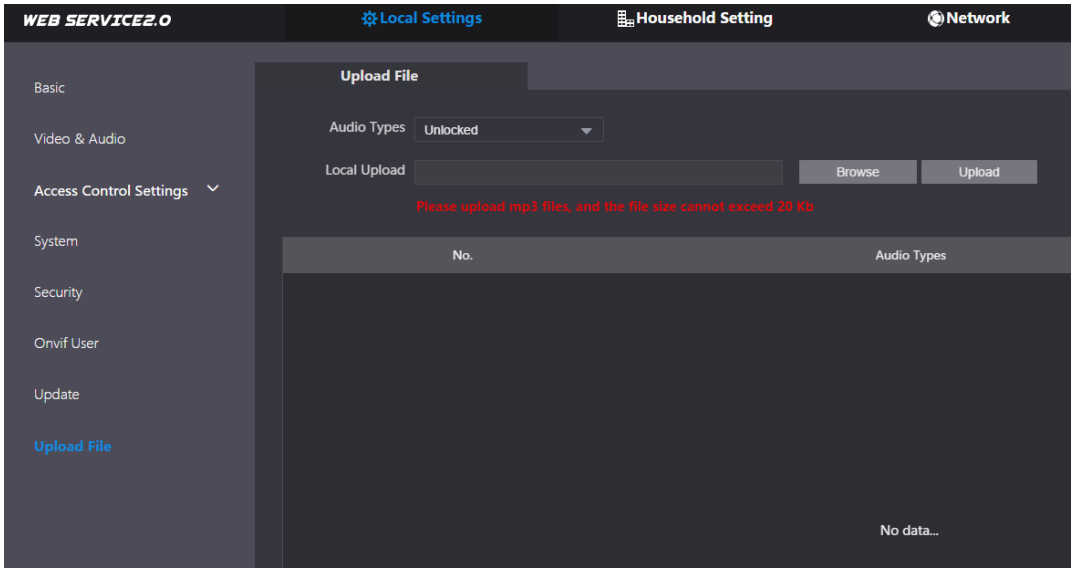
4.8 Téléverser un fichier

Téléchargez un fichier audio pour modifier le son lorsque vous appelez, déverrouillez la porte, etc.

Step 1 Sélectionner**Paramètres locaux > Télécharger un fichier**.

Step 2 Sélectionnez un type audio, puis cliquez sur**Parcourir**pour sélectionner le fichier audio selon vos besoins.

Figure 4-10 Modifier l'invite sonore



Step 3 Cliquez sur**Télécharger**.

5 Milieu familial

Ce chapitre explique comment ajouter, modifier et supprimer des VTO, VTH, VTS et IPC, et comment envoyer des messages du serveur SIP aux VTO et VTH lorsque le VTO fonctionne comme serveur SIP. Si vous utilisez d'autres serveurs comme serveur SIP, consultez le manuel correspondant pour plus de détails.

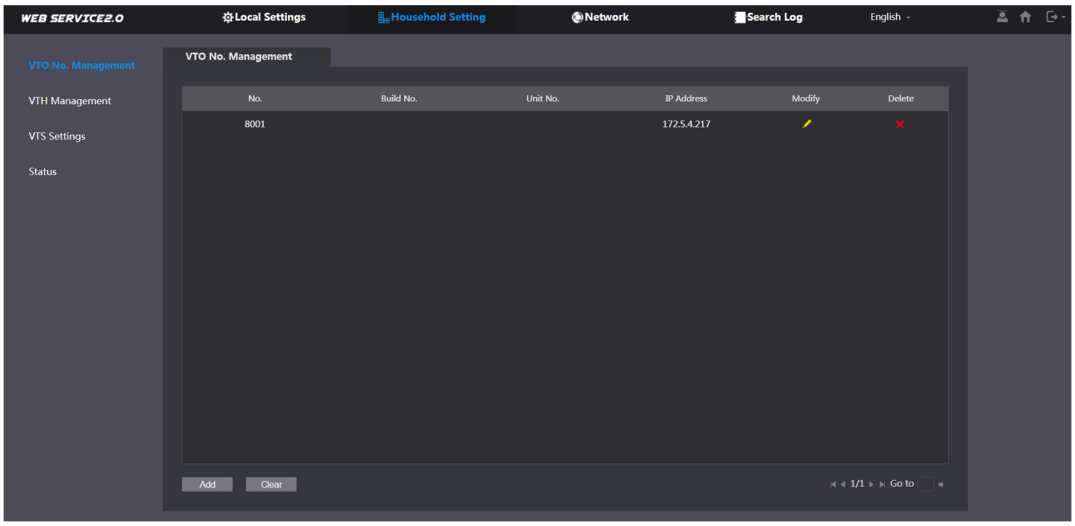
Pour configurer les paramètres du serveur SIP, voir " Serveur SIP" pour plus de détails.

5.1 Gestion des numéros VTO

Vous pouvez ajouter des VTO au serveur SIP, et tous les VTO connectés au même serveur SIP peuvent s'appeler.

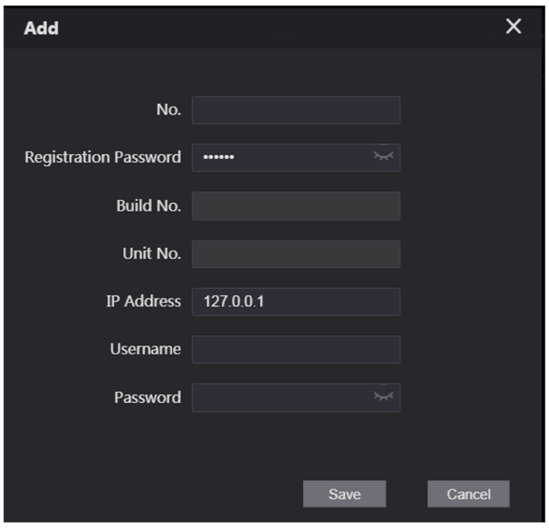
Step 1 Connectez-vous à l'interface Web du VTO fonctionnant comme serveur SIP, puis sélectionnez**Paramètres du ménage > Gestion des numéros VTO**.

Figure 5-1 Gestion VTO



Step 2 Cliquez sur**Ajouter**.

Figure 5-2 Ajouter VTO



Step 3 Configurez les paramètres.

Le serveur SIP doit être ajouté.

Tableau 5-1 Ajouter une configuration VTO

Paramètre	La description
Non.	Le numéro VTO que vous avez configuré. Voir Tableau 4-1 pour plus de détails.
Inscription Mot de passe	Gardez-le par défaut.
Construire n°	Disponible uniquement lorsque d'autres serveurs fonctionnent comme serveur SIP.
N° d'unité	
Adresse IP	Adresse IP du VTO.
Nom d'utilisateur	Nom d'utilisateur et mot de passe de connexion à l'interface Web du VTO.
Mot de passe	

Step 4 Cliquez sur**sauvegarder**.

Cliquez sur ou modifier ou supprimer un VTO, ou**Dégager**pour supprimer tous les VTO ajoutés, sauf celui auxquels vous vous êtes connecté ne peuvent pas être modifiés ou supprimés.

5.2 Gestion VTH

5.2.1 Ajouter un numéro de chambre

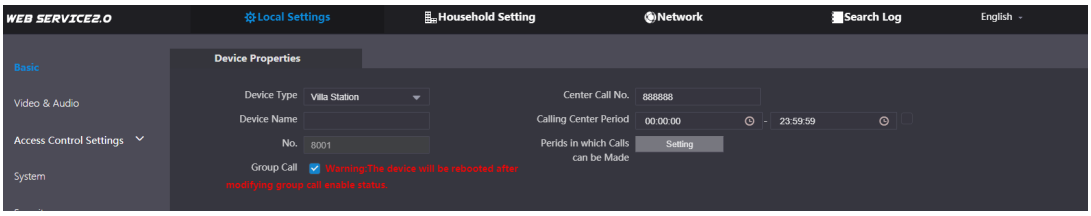
Vous pouvez ajouter le numéro de chambre prévu au serveur SIP, puis configurer le numéro de chambre sur les appareils VTH pour les connecter au réseau. Cette section s'applique lorsque le VTO fonctionne comme serveur SIP, et si vous utilisez d'autres serveurs comme serveur SIP, consultez le manuel correspondant des serveurs pour une configuration détaillée.

Le numéro de chambre peut contenir au maximum 6 chiffres ou lettres ou leur combinaison, et il ne peut pas être le même que n'importe quel numéro VTO.

Utilisation du VTO dans une villa

Step 1 Connectez-vous à l'interface Web du serveur SIP, puis sélectionnez**Paramètres locaux > De base**.

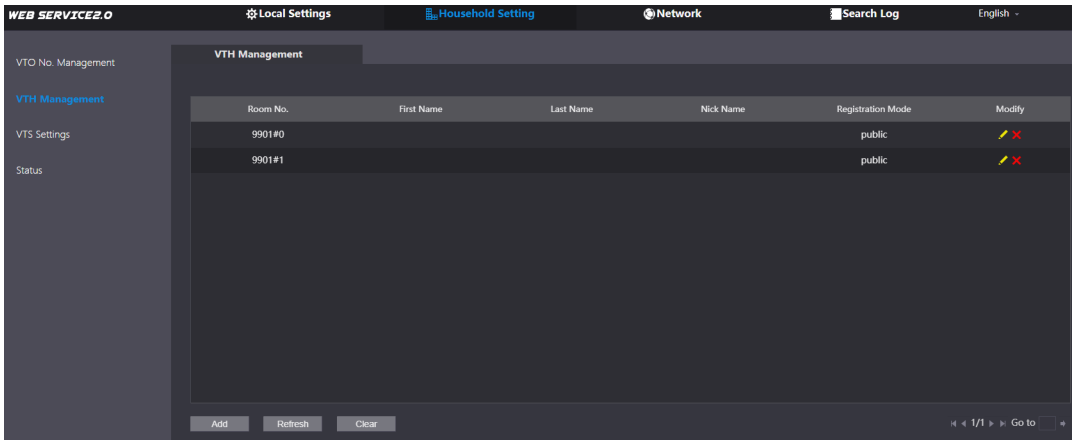
Figure 5-3 Propriétés de l'appareil (1)



Step 2 Régler**Type d'appareil**à**Villa Station**, puis cliquez sur

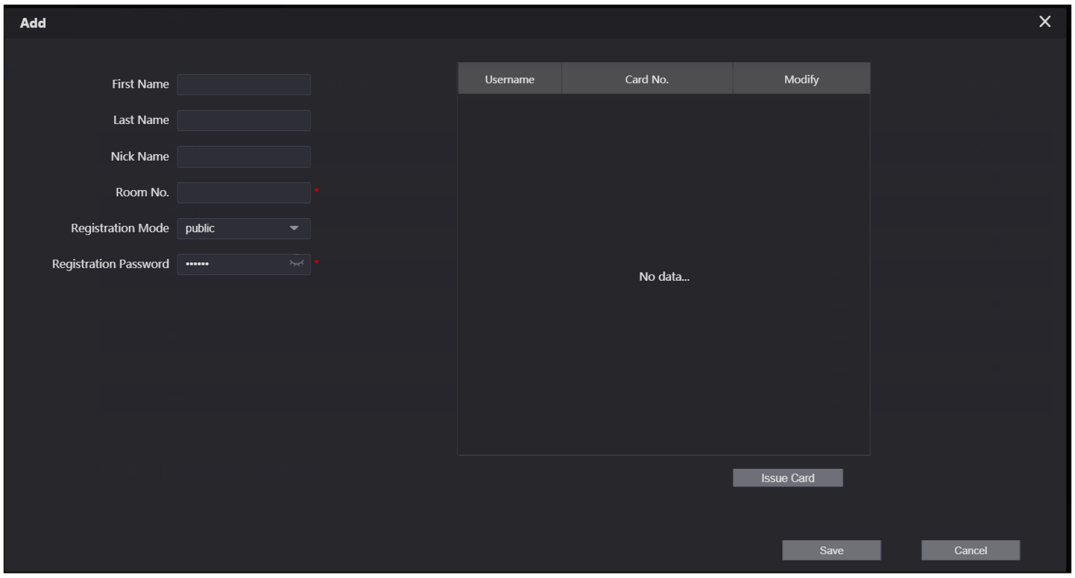
Step 3 **sauvegarder**. Sélectionner**Cadre ménager > Gestion VTH**.

Figure 5-4 Gestion des numéros de chambre



Step 4 Cliquez sur**Ajouter**.

Figure 5-5 Ajouter un numéro de chambre



Step 5 Configurez les paramètres à gauche.

Tableau 5-2 Informations sur la salle

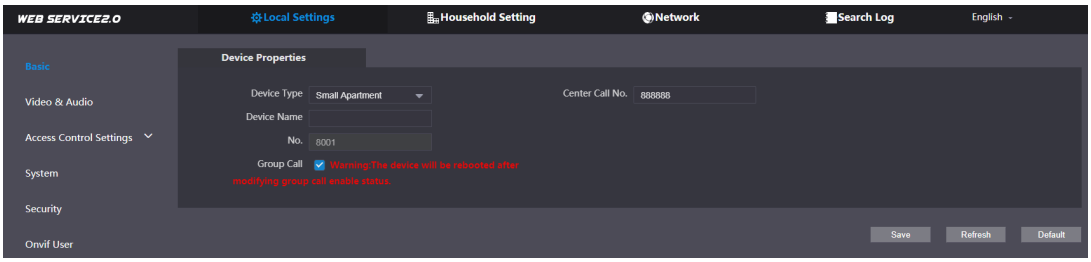
Paramètre	La description
Prénom	Entrez les informations dont vous avez besoin pour différencier chaque pièce.
Nom de famille	
Surnom	
Chambre numéro.	Entrez un numéro de chambre, puis configurez le numéro sur un VTH pour vous connecter pour le connecter au réseau.
Type d'enregistrement	Sélectionner**Publique**.
Inscription Mot de passe	Gardez-le par défaut.

Step 6 Cliquez sur**sauvegarder**.

- Cliquez sur ou pour modifier ou supprimer un numéro de chambre.
- Cliquez sur**Dégager**pour supprimer tous les numéros de chambre.

Step 1 Connectez-vous à l'interface Web du serveur SIP, puis sélectionnez**Paramètres locaux > De base**.

Figure 5-6 Propriétés de l'appareil (2)

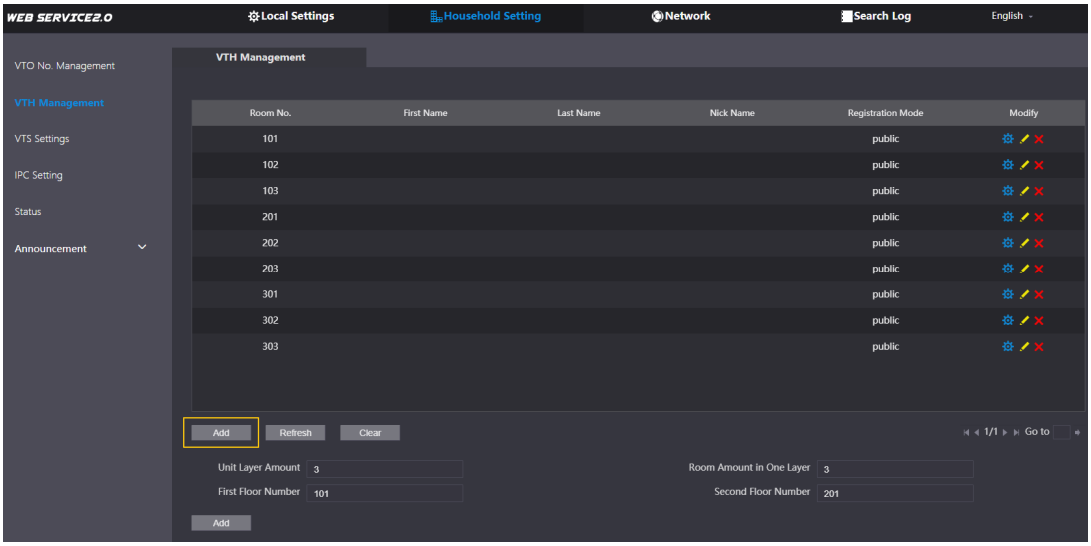


Step 2 Régler**Type d'appareil**à**Petit appartement**, puis cliquez sur**sauvegarder**.

Step 3 Sélectionner**Cadre ménager > Gestion VTH**. Vous pouvez ajouter un seul numéro de chambre ou les ajouter par lots.

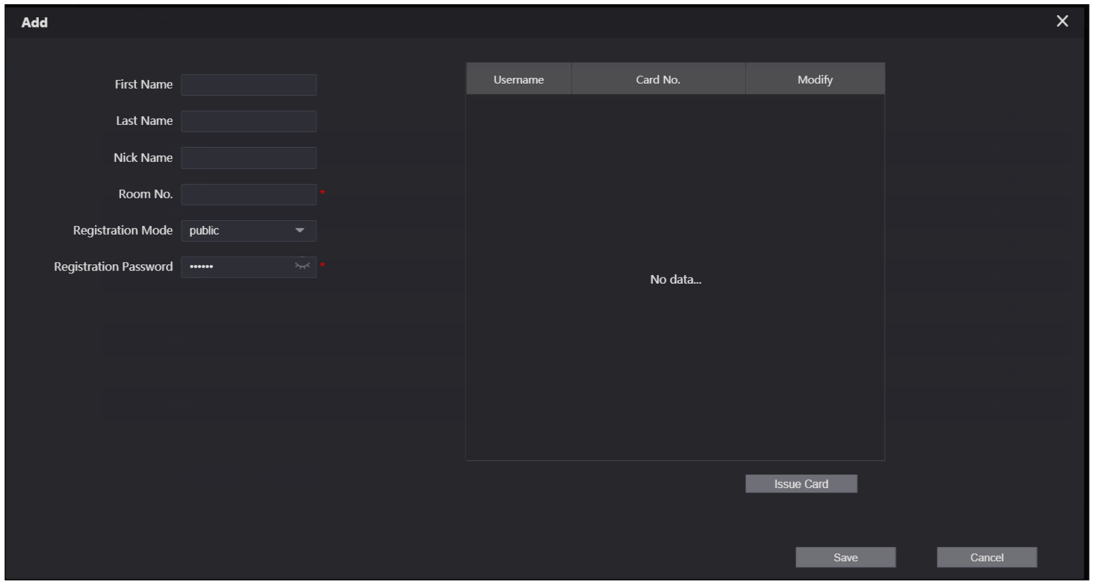
- Ajoutez un numéro de chambre unique.

Figure 5-7 Ajouter des numéros de chambre



1) Cliquez**Ajouter**.

Figure 5-8 Ajouter un seul numéro de chambre

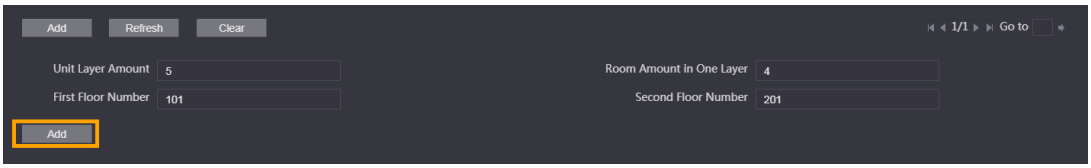


2) Configurez les informations sur la gauche. Voir Tableau 5-2 pour plus de détails.

3) Cliquez**sauvegarder**.

- Ajout de plusieurs numéros de chambre.

Figure 5-9 Ajouter des numéros de chambre par lots



1) Configurez les informations.

- **Montant de la couche unitaire**: Le nombre d'étages de l'appartement. **Montant de la**
- **pièce en une seule couche**: Le nombre de pièces à un étage. **Numéro du premier étage**:
- Le premier numéro de chambre au premier étage. **Numéro du deuxième étage**: Le
- premier numéro de chambre au deuxième étage.

2) Cliquez**Ajouter**, puis cliquez sur**Rafraîchir**pour afficher le dernier statut

- Cliquez sur ou pour modifier ou supprimer un numéro de chambre.
- Cliquez sur**Dégager**pour supprimer tous les numéros de chambre.

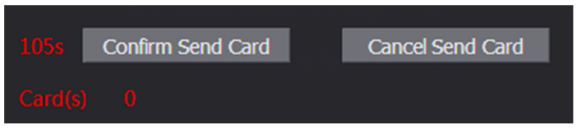
5.2.2 Émission de la carte d'accès

Émettre une carte d'accès pour déverrouiller la porte d'une chambre.

Pour utiliser cette fonction, le VTO doit disposer d'un lecteur de carte.

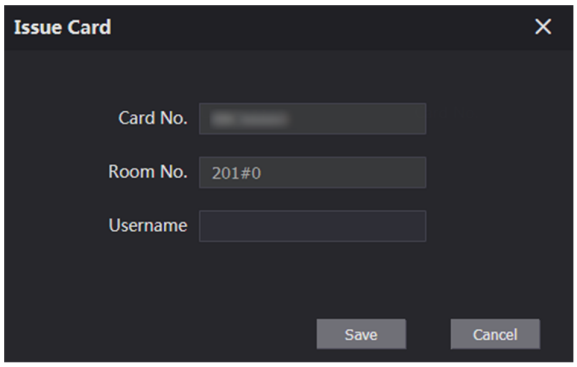
Step 1 Sélectionner**Cadre ménager > Gestion VTH**, Cliquez sur**Ajouter**, puis cliquez sur**Carte d'émission**.

Figure 5-10 Avis de compte à rebours



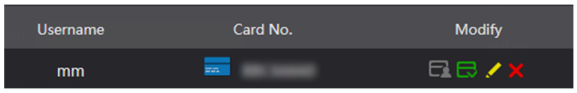
Step 2 Glissez la carte sur le VTO.

Figure 5-11 Carte d'émission



Step 3 Entrez le nom d'utilisateur, cliquez sur**sauvegarder**, puis cliquez sur**Confirmer l'envoi de la carte**.

Figure 5-12 Carte d'accès délivrée



Autres opérations

- Cliquez sur pour le régler sur la carte principale, puis l'icône se transforme en . La carte principale peut être utilisé pour émettre des cartes d'accès pour cette salle sur le VTO.
- Cliquez pour le régler sur perte, puis l'icône se transforme en . La carte perdue ne peut pas être utilisé pour ouvrir la porte.
- Cliquez sur ou pour modifier le nom d'utilisateur ou supprimer la carte.

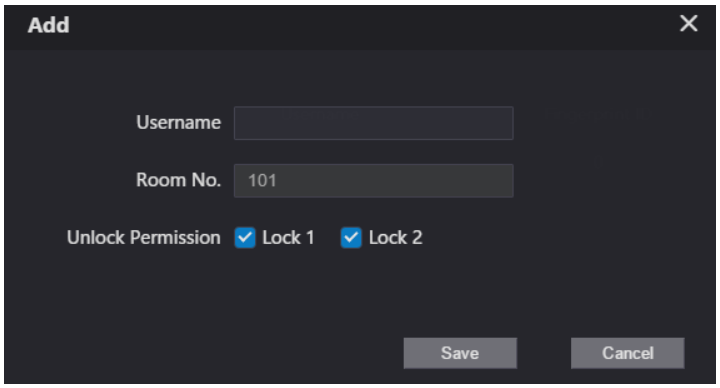
5.2.3 Émission d'empreintes digitales

Émettre des empreintes digitales pour déverrouiller la porte d'une pièce.

Pour utiliser cette fonction, le VTO doit disposer d'un lecteur d'empreintes digitales.

Step 1 Sélectionner**Cadre ménager > Gestion VTH**, Cliquez sur**Ajouter**, puis cliquez sur**Émettre une empreinte digitale**.

Figure 5-13 Émettre une empreinte digitale



Step 2 Entrez un nom d'utilisateur, attribuez une autorisation de déverrouillage si nécessaire, puis cliquez sur**sauvegarder**.

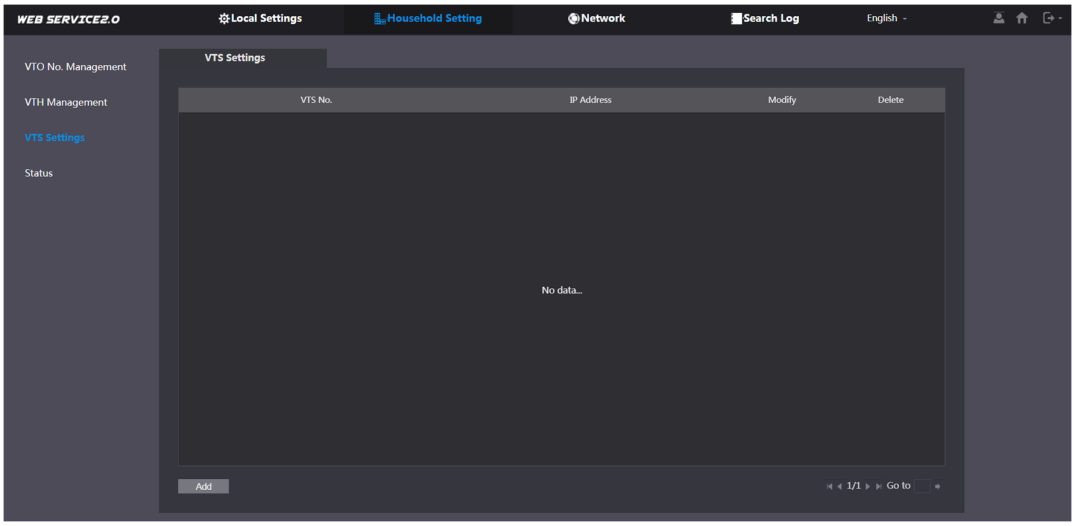
Step 3 Appuyez votre empreinte digitale sur le scanner.

5.3 Gestion VTS

Vous pouvez ajouter un VTS au serveur SIP, puis il peut être utilisé comme centre de gestion. Il peut également gérer, appeler ou recevoir des appels de tous les VTO et VTH du réseau. Voir le manuel de l'utilisateur correspondant pour plus de détails.

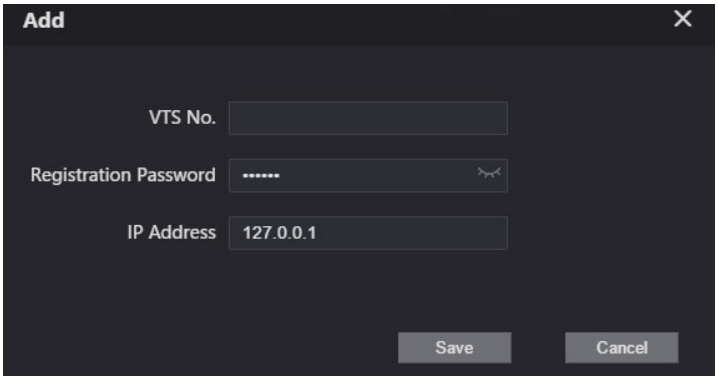
Step 1 Connectez-vous à l'interface Web du VTO fonctionnant comme serveur SIP, puis sélectionnez**Paramètres du foyer > Paramètres VTS**.

Figure 5-14 Gestion VTS



Step 2 Cliquez sur**Ajouter**.

Figure 5-15 Ajouter VTS



Step 3 Configurez les paramètres.

Tableau 5-3 Ajouter une configuration VTS

Paramètre	La description
N° VTS	Le numéro du VTS.
Mot de passe d'enregistrement	Gardez-le par défaut.
Adresse IP	Adresse IP VTS.

Step 4 Cliquez sur**sauvegarder**.

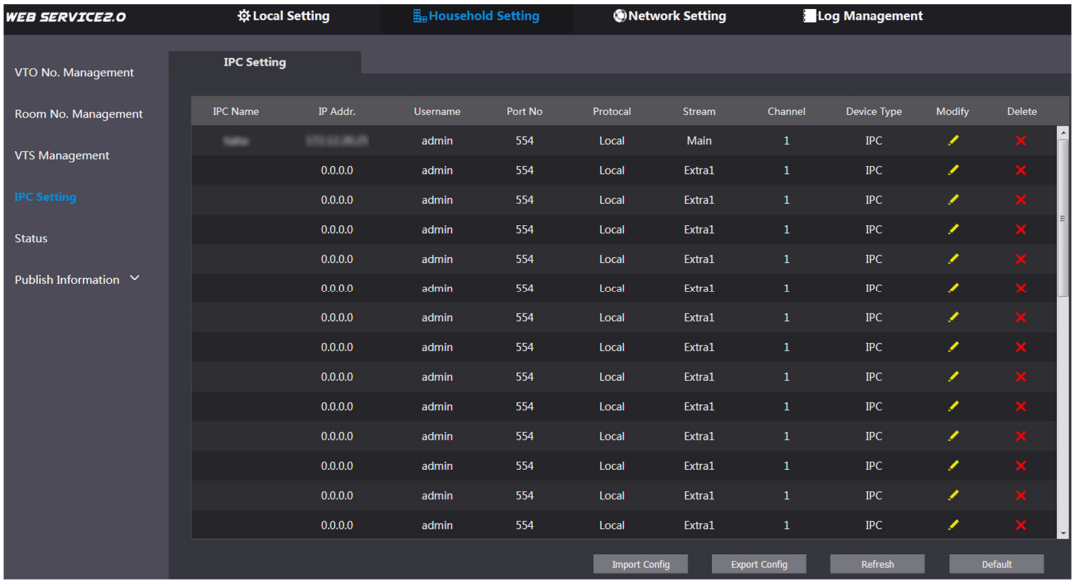
5.4 Paramètre CIB

Vous pouvez ajouter IPC et NVR au VTO fonctionnant comme serveur SIP, puis tous les VTH connectés peuvent les surveiller.

Les interfaces peuvent varier selon les produits. L'interface réelle prévaudra.

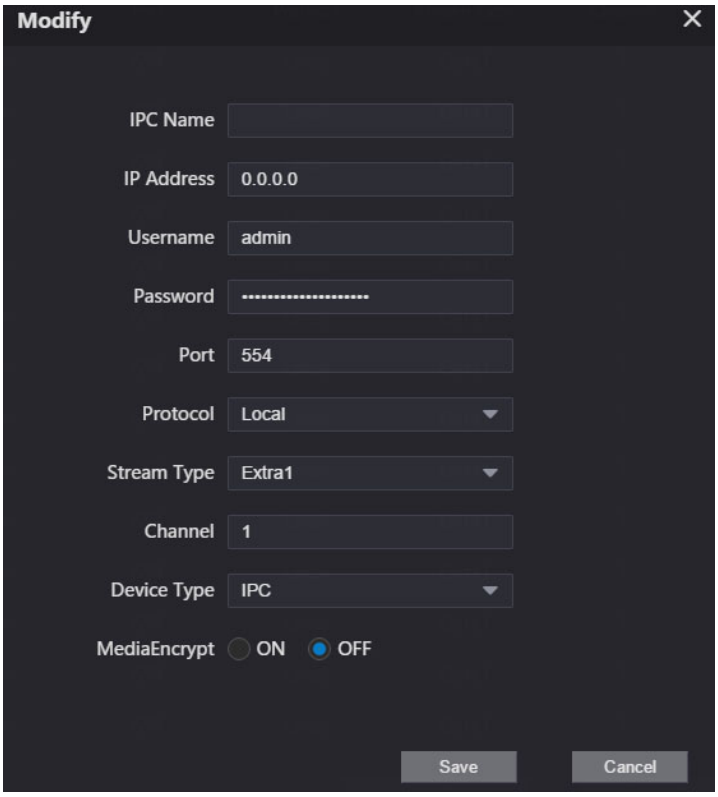
Step 1 Connectez-vous à l'interface Web du VTO fonctionnant comme serveur SIP, puis sélectionnez**Paramètre ménage > Paramètre IPC**.

Figure 5-16 Paramètre CIB



Step 2 Cliquez sur .

Figure 5-17 Ajouter un CIP



Step 3 Configurez les paramètres.

Tableau 5-4 Ajouter une configuration IPC

Paramètre	La description
Nom CIP	Entrez le nom qui identifie l'IPC.
Adresse IP	Adresse IP de l'IPC.
Nom d'utilisateur	Nom d'utilisateur et mot de passe de connexion à l'interface Web de l'appareil.
Mot de passe	
Port	Gardez-le par défaut.
Protocole	Sélectionner**Local**ou**Onvif**.
Type de flux	● **Principal**: Meilleure qualité vidéo mais nécessite plus de bande passante. ● **Extra1**: vidéo plus fluide avec une qualité inférieure, mais nécessite moins de bande passante.
Canaliser	Le nombre de canaux pris en charge par un périphérique.
Type d'appareil	Sélectionnez celui dont vous avez besoin.
MediaEncrypt	Sélectionner**SUR**si l'IPC à ajouter est chiffré.

Step 4 Cliquez sur**sauvegarder**.

Autres opérations

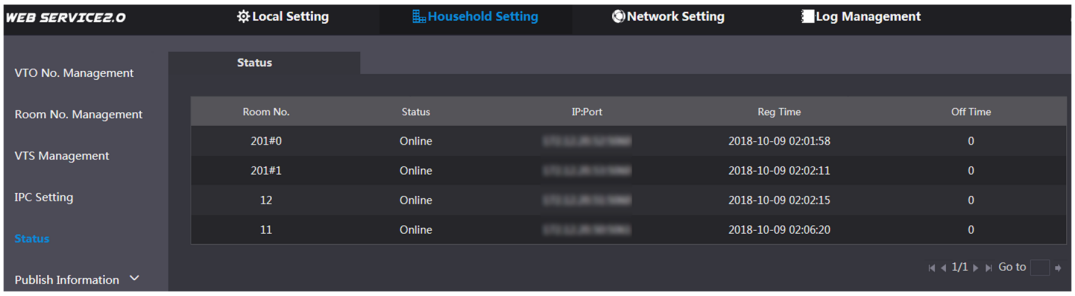
- **Exporter la configuration**: Exportez les informations de l'appareil vers votre PC. **Importer**
- **la configuration**: Importer les informations sur l'appareil.

5.5 Statut

Vous pouvez afficher l'état en ligne et les adresses IP de tous les appareils connectés.

Connectez-vous à l'interface Web du serveur SIP, puis sélectionnez**Paramètres du ménage > Statut**.

Figure 5-18 Statut



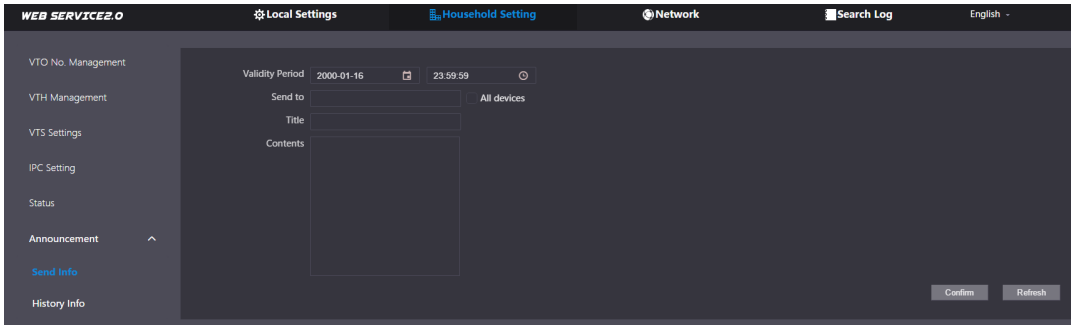
5.6 Publier des informations

Vous pouvez envoyer des messages du serveur SIP aux appareils VTH et afficher l'historique des messages.

5.6.1 Envoyer des informations

Step 1 Connectez-vous à l'interface Web du serveur SIP, puis sélectionnez**Paramètres du foyer > Publier les informations > Envoyer les informations**.

Figure 5-19 Envoyer une information



Step 2 Spécifie le**Période de validité**que le message sera valide.

Step 3 Entrez le numéro VTO ou le numéro VTH, ou sélectionnez**Tous les dispositifs**pour envoyer le message à tous les appareils du réseau, puis entrez le titre et le contenu de votre message.

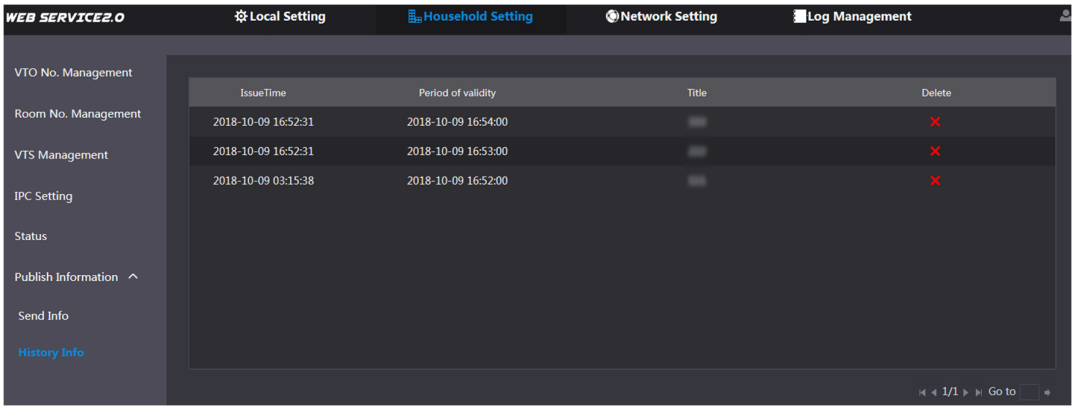
Step 4 Cliquez sur**Confirmer**.

5.6.2 Informations sur l'historique

Vous pouvez afficher les informations des messages envoyés.

Connectez-vous à l'interface Web du serveur SIP, sélectionnez**Paramètres du ménage > Publier des informations > Informations sur l'historique**.

Figure 5-20 Informations sur l'historique



6 Réseau

Ce chapitre explique comment configurer les paramètres réseau.

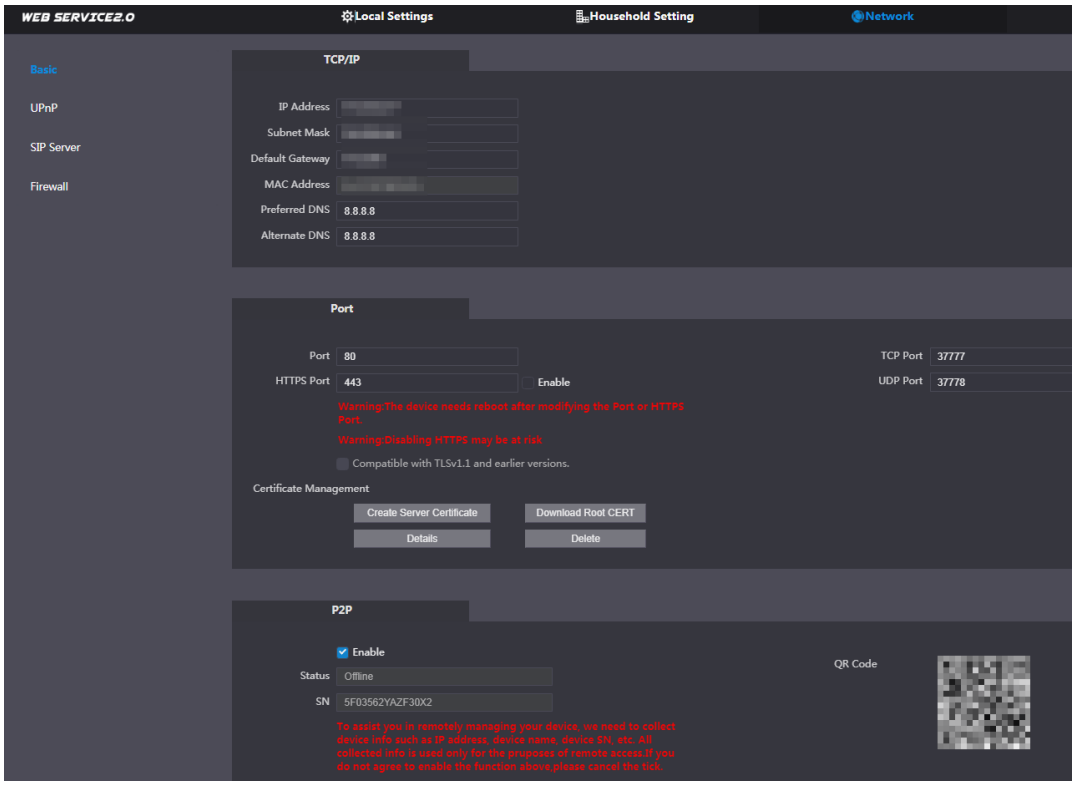
6.1 De base

6.1.1 TCP/IP

Vous pouvez modifier l'adresse IP, le masque de sous-réseau, la passerelle par défaut et le DNS du VTO.

Step 1 Sélectionner**Réseau > Basique**.

Figure 6-1 TCP/IP et ports



Step 2 Configurez les paramètres, puis cliquez sur**sauvegarder**.

Le VTO redémarrera et vous devrez modifier l'adresse IP de votre PC sur le même segment de réseau que le VTO pour vous reconnecter.

6.1.2 Port

Tableau 6-1 Description des paramètres

Paramètre	La description
Port	80 par défaut. S'il est déjà utilisé, choisissez n'importe quel nombre entre 1025 et 65535 selon vos besoins. Vous pouvez entrer*http://Adresse IP VTO : Port*pour vous connecter au VTO.
Port HTTPS	Activez-le et cliquez**sauvegarder**. Vous pouvez maintenant saisir*https://adresse IP VTO : port HTTPS*à

Paramètre	La description
	connectez-vous au VTO.
Port TCP/UDP	Utilisé pour accéder au VTO avec des appareils dans d'autres réseaux. Voir "6.2 UPnP" pour plus de détails.
Créer Serveur Certificat	L'identification numérique unique de VTO pour le protocole SSL. Pour une première utilisation ou après avoir changé l'adresse IP du VTO, vous devez passer par ce processus. ⚠ Si vous supprimez le certificat qui a été créé, il ne peut pas être annulé.
Télécharger la racine CERT	Si vous utilisez un PC qui ne s'est jamais connecté au VTO, vous devez télécharger le certificat racine, double-cliquer pour l'installer, puis vous pouvez utiliser la fonction HTTPS mentionnée ci-dessus. ⚠ Si vous supprimez le certificat qui a été installé, cela ne peut pas être annulé.

6.1.3 P2P

Activez le**P2P**fonction, puis vous pouvez scanner le code QR avec votre téléphone pour ajouter le VTO à l'application sur votre smartphone.

Si vous définissez**Type d'appareil**à**Petit appartement**(voir "4.1 Basique"), le code QR sera déplacé vers **Paramètres du ménage > Gestion VTH.**Cliquez sur de n'importe quel numéro de chambre, puis vous pouvez voir à la fois le numéro de série et le code QR du VTO.

6.2 UPnP

Lorsque le VTO fonctionne comme serveur SIP, vous pouvez configurer la fonction UPnP pour permettre aux périphériques WAN de se connecter au VTO.

Préparation

- Activez la fonction UPnP sur le routeur, puis configurez une adresse IP WAN pour le routeur.
- Connectez le VTO au port LAN du routeur.

6.2.1 Activation des services UPnP

Step 1 Sélectionner**Réseau > UPnP**.

Step 2 Activez les services répertoriés selon vos besoins.

Step 3 Sélectionner**Activer**.

Step 4 Cliquez sur**sauvegarder**.

6.2.2 Ajout de services UPnP

Step 1 Sélectionner**Réseau > UPnP**.

Step 2 Cliquez sur**Ajouter**.

Step 3 Configurez les paramètres selon vos besoins.

Figure 6-2 Ajouter un service UPnP

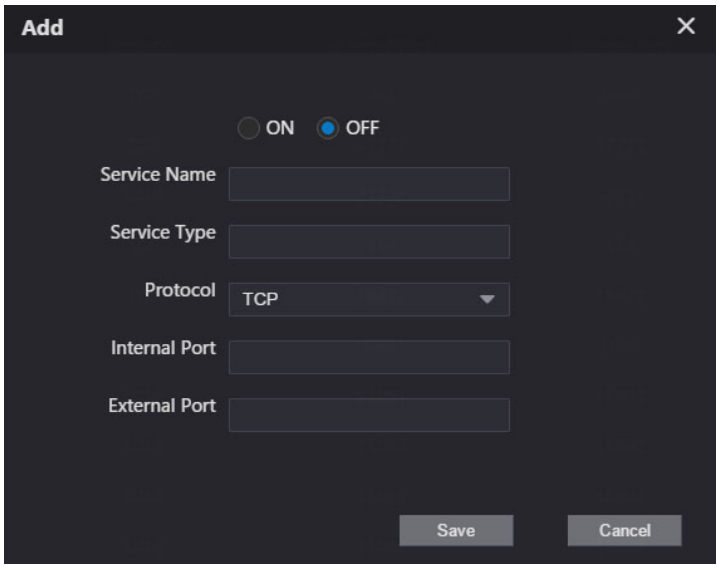


Tableau 6-2 Description des paramètres

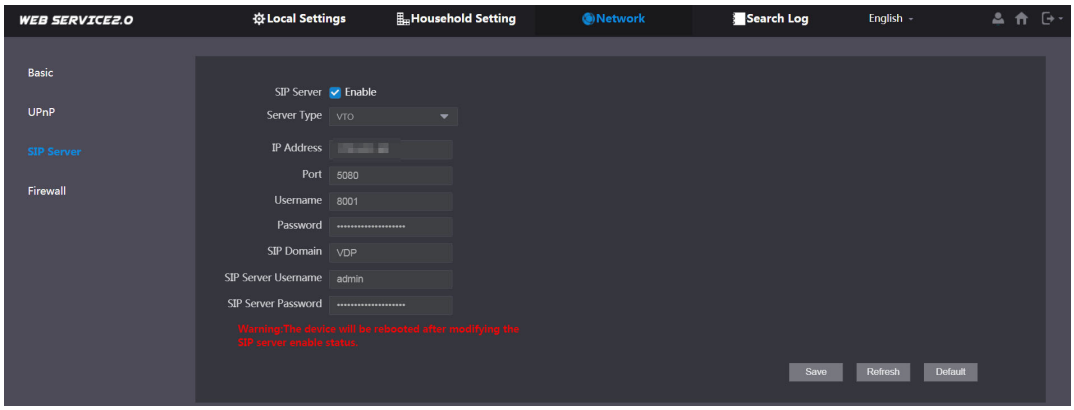
Paramètre	La description
Nom du service	Saisissez les informations nécessaires.
type de service	
Protocole	Sélectionner**TCP**ou**UDP**comme requis.
Port interne	Utilisez le numéro de port de 1024 à 5000. - N'utilisez pas le numéro de port 1–1023 pour éviter les conflits. - Si vous devez configurer cette fonction pour plusieurs appareils, assurez-vous que les ports ne sont pas identiques. - Le numéro de port que vous utilisez ne doit pas être occupé. - Le numéro de port interne et externe doit être le même.
Port externe	

6.3 Serveur SIP

Il doit y avoir un serveur SIP dans le réseau pour que tous les VTO et VTH connectés puissent s'appeler. Vous pouvez utiliser un VTO ou d'autres serveurs comme serveur SIP.

Step 1 Sélectionner**Réseau > Serveur SIP**.

Figure 6-3 Serveur SIP



Step 2 Sélectionnez un type de serveur selon vos besoins.

- Le VTO auquel vous vous êtes connecté en tant que serveur SIP :

  Activer**Serveur SIP**, et cliquez**sauvegarder**, puis le VTO redémarrera. Vous pouvez ajouter des VTO et des VTH à ce VTO. Voir les détails dans « 5 Paramètres du ménage ».

  Si le VTO auquel vous vous êtes connecté n'a pas de serveur SIP, n'activez pas**Serveur SIP**; Par ailleurs la connexion échouera.

- Si un autre VTO fonctionne comme serveur SIP :

  Ne permettent pas**Serveur SIP**. Régler**Type de serveur**à**VTO**, configurez les paramètres, puis cliquez sur **sauvegarder**.

Tableau 6-3 Configuration du serveur SIP

Paramètre	La description
Adresse IP	Adresse IP VTO.
Port	● 5060 par défaut lorsque VTO fonctionne comme serveur SIP. 5080 par ● défaut lorsque la plateforme fonctionne en serveur SIP.
Nom d'utilisateur	Gardez-le par défaut.
Mot de passe	
Domaine SIP	VDP.
Nom d'utilisateur du serveur SIP	Nom d'utilisateur et mot de passe de connexion à l'interface Web du VTO.
Mot de passe du serveur SIP	

- Si d'autres serveurs fonctionnent comme serveur SIP :

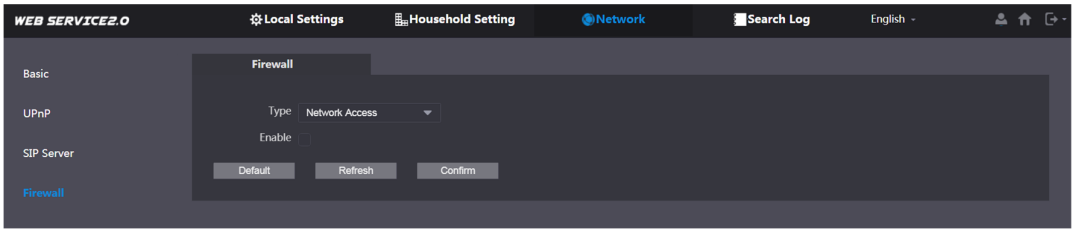
  Sélectionnez le**Type de serveur**au besoin, puis consultez le manuel correspondant pour plus de détails.

6.4 Pare-feu

Vous pouvez activer différents types de pare-feu pour contrôler l'accès réseau au VTO.

Step 1 Sélectionner**Réseau > Pare-feu**.

Figure 6-4 Pare-feu



Step 2 Sélectionnez un ou plusieurs types de pare-feu, puis activez-les.

Step 3 Configurez les paramètres.

Tableau 6-4 Description du type de pare-feu

Taper	La description
L'accès au réseau	Sélectionnez soit**Liste d'autorisation**ou**Liste de blocage**, puis ajoutez une adresse IP ou un segment autorisé ou non à accéder au VTO.
PING interdit	Le VTO ne répondra pas au ping pour éviter les attaques de ping.
Anti-semi-jointure	Protège les performances VTO en bloquant les paquets SYN excessifs.

7 Gestion des journaux

Sélectionner**Journal de recherche**, puis vous pouvez afficher l'historique des appels, les enregistrements d'alarme, les enregistrements de déverrouillage et divers journaux système, et les exporter vers votre PC si nécessaire.

Si le stockage est plein, les enregistrements les plus anciens seront écrasés. Sauvegardez les enregistrements si nécessaire.

Appendix 1 Recommandations de cybersécurité

La cybersécurité est plus qu'un simple mot à la mode : c'est quelque chose qui concerne chaque appareil connecté à Internet. La vidéosurveillance IP n'est pas à l'abri des cyber-risques, mais prendre des mesures de base pour protéger et renforcer les réseaux et les appareils en réseau les rendra moins vulnérables aux attaques. Vous trouverez ci-dessous quelques conseils et recommandations sur la façon de créer un système de sécurité plus sécurisé.

Actions obligatoires à prendre pour la sécurité de base du réseau de l'appareil : 1.

Utiliser des mots de passe forts

Veuillez vous référer aux suggestions suivantes pour définir des mots de passe :

- La longueur ne doit pas être inférieure à 8 caractères ;
- Inclure au moins deux types de caractères ; les types de caractères comprennent les lettres majuscules et minuscules, les chiffres et les symboles ;
- Ne pas contenir le nom du compte ou le nom du compte dans l'ordre inverse ;
- N'utilisez pas de caractères continus, tels que 123, abc, etc. ;
- N'utilisez pas de caractères superposés, tels que 111, aaa, etc. ;

2. Mettre à jour le micrologiciel et le logiciel client à temps

- Conformément à la procédure standard de l'industrie technologique, nous vous recommandons de maintenir à jour le micrologiciel de votre appareil (tel que NVR, DVR, caméra IP, etc.) pour vous assurer que le système est équipé des derniers correctifs et correctifs de sécurité. Lorsque l'appareil est connecté au réseau public, nous vous recommandons d'activer la fonction "vérification automatique des mises à jour" pour obtenir des informations en temps opportun sur les mises à jour du micrologiciel publiées par le fabricant.
- Nous vous suggérons de télécharger et d'utiliser la dernière version du logiciel client.

Recommandations « agréables à avoir » pour améliorer la sécurité réseau de votre appareil :

1. Protection physique

Nous vous suggérons d'effectuer une protection physique sur l'appareil, en particulier les périphériques de stockage. Par exemple, placez l'appareil dans une salle informatique et une armoire spéciales, et mettez en place une autorisation de contrôle d'accès et une gestion des clés bien faites pour empêcher le personnel non autorisé d'effectuer des contacts physiques tels que l'endommagement du matériel, la connexion non autorisée d'un périphérique amovible (tel qu'un disque flash USB , port série), etc.

2. Changez régulièrement les mots de passe

Nous vous suggérons de changer régulièrement de mot de passe pour réduire le risque d'être deviné ou piraté.

3. Définir et mettre à jour les mots de passe Réinitialiser les informations en temps opportun

L'appareil prend en charge la fonction de réinitialisation du mot de passe. Veuillez configurer les informations associées pour la réinitialisation du mot de passe à temps, y compris la boîte aux lettres de l'utilisateur final et les questions de protection par mot de passe. Si les informations changent, veuillez les modifier à temps. Lors de la définition des questions de protection par mot de passe, il est suggéré de ne pas utiliser celles qui peuvent être facilement devinées.

4. Activer le verrouillage du compte

La fonction de verrouillage du compte est activée par défaut et nous vous recommandons de la conserver pour garantir la sécurité du compte. Si un attaquant tente plusieurs fois de se connecter avec le mauvais mot de passe, le compte correspondant et l'adresse IP source seront verrouillés.

5. Modifier le HTTP par défaut et les autres ports de service

Nous vous suggérons de changer le HTTP par défaut et les autres ports de service en n'importe quel ensemble de nombres entre 1024 et 65535, réduisant ainsi le risque que des personnes extérieures puissent deviner quels ports vous utilisez.

6. Activer HTTPS

Nous vous suggérons d'activer HTTPS, afin que vous visitiez le service Web via un canal de communication sécurisé.

7. Liaison d'adresse MAC

Nous vous recommandons de lier l'adresse IP et MAC de la passerelle à l'appareil, réduisant ainsi le risque d'usurpation ARP.

8. Attribuez raisonnablement des comptes et des privilèges

Selon les exigences commerciales et de gestion, ajoutez raisonnablement des utilisateurs et attribuez-leur un ensemble minimum d'autorisations.

9. Désactivez les services inutiles et choisissez les modes sécurisés

Si ce n'est pas nécessaire, nous vous recommandons de désactiver certains services tels que SNMP, SMTP, UPnP, etc., pour réduire les risques.

Si nécessaire, il est fortement recommandé d'utiliser les modes sans échec, y compris, mais sans s'y limiter, les services suivants :

- SNMP : choisissez SNMP v3 et configurez des mots de passe de chiffrement fort et des mots de passe d'authentification.
- SMTP : choisissez TLS pour accéder au serveur de boîtes aux lettres.
- FTP : choisissez SFTP et configurez des mots de passe forts.
- Point d'accès AP : choisissez le mode de cryptage WPA2-PSK et configurez des mots de passe forts.

10. Transmission cryptée audio et vidéo

Si le contenu de vos données audio et vidéo est très important ou sensible, nous vous recommandons d'utiliser la fonction de transmission cryptée, afin de réduire le risque de vol de données audio et vidéo pendant la transmission.

Rappel : la transmission cryptée entraînera une certaine perte d'efficacité de transmission.

11. Audit sécurisé

- Vérifiez les utilisateurs en ligne : nous vous suggérons de vérifier régulièrement les utilisateurs en ligne pour voir si l'appareil est connecté sans autorisation.
- Vérifier le journal de l'appareil : En consultant les journaux, vous pouvez connaître les adresses IP qui ont été utilisées pour se connecter à vos appareils et leurs opérations clés.

12. Journal réseau

En raison de la capacité de stockage limitée de l'appareil, le journal stocké est limité. Si vous devez enregistrer le journal pendant une longue période, il est recommandé d'activer la fonction de journal réseau pour vous assurer que les journaux critiques sont synchronisés avec le serveur de journal réseau pour le traçage.

13. Construire un environnement réseau sûr

Afin de mieux assurer la sécurité de l'appareil et de réduire les cyber-risques potentiels, nous recommandons :

- Désactivez la fonction de mappage de port du routeur pour éviter un accès direct aux périphériques intranet à partir d'un réseau externe.
- Le réseau doit être partitionné et isolé en fonction des besoins réels du réseau. S'il n'y a pas d'exigences de communication entre deux sous-réseaux, il est suggéré d'utiliser le VLAN, le réseau GAP et d'autres technologies pour partitionner le réseau, afin d'obtenir l'effet d'isolation du réseau.
- Établissez le système d'authentification d'accès 802.1x pour réduire le risque d'accès non autorisé aux réseaux privés.
- Activez la fonction de filtrage des adresses IP/MAC pour limiter la plage d'hôtes autorisés à accéder à l'appareil.