

# **Station de porte pour villa (version 4.5)**

## **Guide de démarrage rapide**



# Avant-propos

## Général

Ce manuel présente la structure, le processus de montage et la configuration de base de la station de porte pour villa (dénommée ci-après « VTO » ou portier).

## Précautions d'emploi

Les mentions d'avertissement catégorisées suivantes ayant une signification définie apparaîtront dans le manuel.

Mentions d'avertissement	Signification
 <b>DANGER</b>	Indique un danger risquant d'entraîner la mort ou des blessures graves si les instructions données ne sont pas respectées.
 <b>AVERTISSEMENT</b>	Indique une situation moyennement ou faiblement dangereuse qui entraînera des blessures faibles ou modérées si les instructions données ne sont pas respectées.
 <b>ATTENTION</b>	Indique une situation potentiellement dangereuse qui pourra entraîner des dommages de la propriété, des pertes de données, une performance moindre ou des résultats imprévisibles, si les instructions données ne sont pas respectées.
 <b>CONSEILS</b>	Fournit des instructions qui vous permettront de résoudre un problème ou de vous faire gagner du temps.
 <b>REMARQUE</b>	Fournit des informations supplémentaires pour mettre en évidence et compléter le texte.

## Historique des révisions

Version	Description de la révision	Date de sortie
V1.0.0	Date de sortie.	Décembre 2020

## À propos du manuel

- Le manuel est donné uniquement à titre de référence. Si des incohérences existent entre le manuel et le produit réel, vous devrez tenir compte du produit réel.
- Nous ne serons pas tenus responsables de toute perte causée par une utilisation non conforme aux instructions contenues dans ce manuel.

- Le manuel pourra être actualisé selon la réglementation et les lois les plus récentes des régions concernées. Pour des informations détaillées, reportez-vous au manuel au format papier, sur CD-ROM, disponible en numérisant le code QR ou sur notre site Web officiel. Si des incohérences existent entre le manuel au format papier et le manuel au format électronique, vous devrez tenir compte de la version électronique.
- Tous les logiciels et toutes les interfaces présentés ici sont susceptibles d'être modifiés sans préavis écrit. Les mises à jour du produit peuvent apporter des différences entre le produit réel et le manuel. Veuillez contacter le service client pour être informé des dernières procédures et obtenir de la documentation supplémentaire.
- De légères variations ou des erreurs d'impression peuvent apparaître au niveau des caractéristiques techniques, des fonctions et de la description des opérations. En cas d'incertitude ou de désaccord, veuillez vous référer à notre dernière explication.
- Mettez à jour le logiciel de lecture ou essayez un autre logiciel de lecture grand public si le manuel (au format PDF) ne s'ouvre pas.
- Les marques de commerce, les marques déposées et les noms des sociétés dans ce manuel sont de la propriété respective de leurs propriétaires.
- Veuillez visiter notre site Web, contacter le fournisseur ou le service après-vente si un problème survient pendant l'utilisation de l'appareil.
- En cas d'incertitude ou de désaccord, veuillez vous référer à notre dernière explication.

# Précautions et avertissements importants

La méthode décrite ci-après permet une utilisation appropriée de l'appareil. Veuillez lire attentivement le manuel avant de l'utiliser afin d'éviter tout danger et toute perte matérielle. Respectez strictement les instructions d'utilisation de l'appareil contenues dans ce manuel et conservez soigneusement ce dernier après lecture.

## Conditions de fonctionnement

- N'exposez pas l'appareil aux rayons directs du soleil ou à des sources de chaleur.
- N'installez pas l'appareil dans une zone humide ou poussiéreuse.
- Installez l'appareil à l'horizontale et sur une surface stable afin d'empêcher toute chute.
- Évitez d'exposer l'appareil aux déversements ou aux éclaboussures de liquides. Ne placez aucun objet rempli de liquides sur l'appareil.
- Installez l'appareil dans un endroit bien ventilé et empêchez toute obstruction des orifices de ventilation.
- N'utilisez l'appareil que dans la plage d'entrée et de sortie nominale.
- Ne démontez pas l'appareil vous-même.
- Transportez, utilisez et conservez l'appareil dans la plage d'humidité et de température autorisée.

## Besoins énergétiques

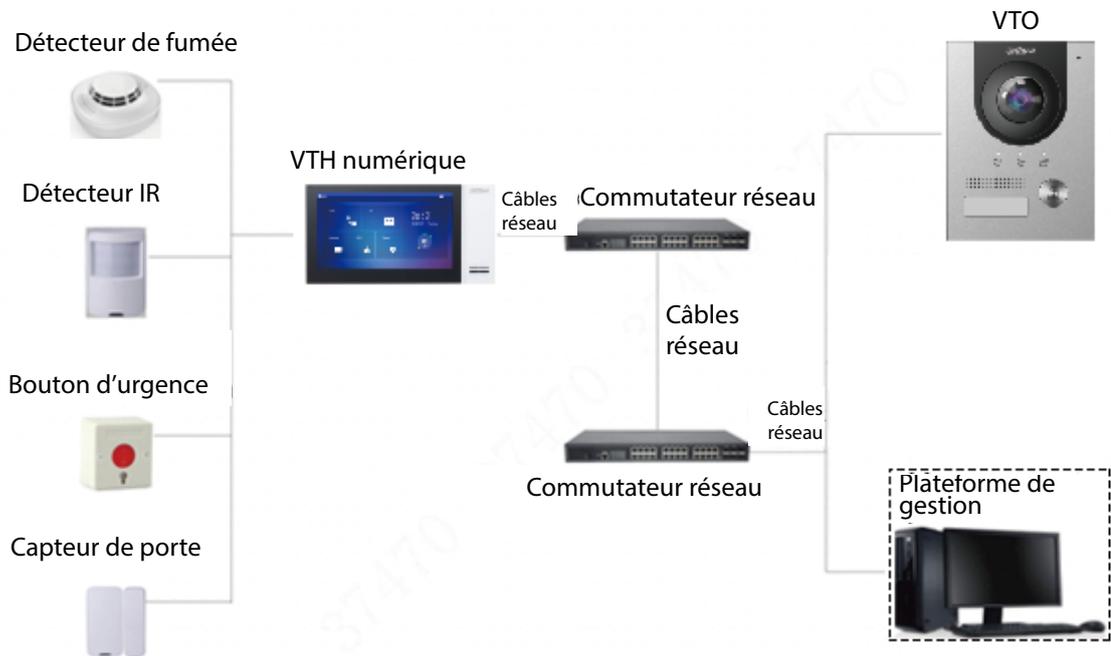
- Le produit doit être installé avec des fils électriques conformes à la réglementation locale.
- Utilisez un bloc d'alimentation conforme ES1, mais qui ne dépasse pas les limites PS2 définies par la norme IEC 62368-1. Pour connaître les exigences spécifiques en matière d'alimentation électrique, reportez-vous aux étiquettes de l'appareil.
- Le coupleur d'appareil est un dispositif de déconnexion. Lors d'une utilisation normale, maintenez l'angle qui garantit un bon fonctionnement.

# Table des matières

<b>Avant-propos</b> .....	<b>I</b>
<b>Précautions et avertissements importants</b> .....	<b>III</b>
<b>1 Schéma du réseau</b> .....	<b>1</b>
<b>2 Illustration</b> .....	<b>2</b>
2.1 VTO2101E-P.....	2
2.1.1 Panneau avant .....	2
2.1.2 Panneau arrière.....	3
2.2 VTO2202F-P-S2/VTO2202F-P/VTO2202F/VTO2201F-P .....	4
2.2.1 Panneau avant .....	4
2.2.2 Panneau arrière.....	5
2.3 VTO2111D-P-S2/VTO1101D-P .....	6
2.3.1 Panneau avant .....	6
2.3.2 Panneau arrière.....	7
2.4 VTO3211D-P-S2.....	8
2.4.1 Panneau avant .....	8
2.4.2 Panneau arrière.....	9
2.5 VTO3221E-P.....	10
2.5.1 Panneau avant .....	10
2.5.2 Panneau arrière.....	11
2.6 VTO2211G-P/VTO1201G-P.....	12
2.6.1 Panneau avant .....	12
2.6.2 Panneau arrière.....	13
<b>3 Installation</b> .....	<b>15</b>
<b>4 Configuration</b> .....	<b>16</b>
4.1 Procédure.....	16
4.2 Outil de configuration.....	16
4.3 Configuration d'un VTO .....	16
4.3.1 Initialisation.....	16
4.3.2 Configuration d'un numéro de VTO .....	17
4.3.3 Configuration des paramètres de réseau .....	18
4.3.4 Configuration du serveur SIP.....	18
4.3.5 Configuration du numéro d'appel et des appels collectifs .....	19
4.3.6 Ajout des VTO.....	20
4.3.7 Ajout du numéro de pièce.....	21
4.4 Mise en service.....	23
4.4.1 VTO appelant un VTH .....	23
4.4.2 VTH surveillant un VTO .....	23
<b>5 EasyViewer Plus</b> .....	<b>26</b>
<b>Annexe 1 Recommandations en matière de cybersécurité</b> .....	<b>27</b>

# 1 Schéma du réseau

Figure 1-1 Schéma du réseau



Dans certaines applications p. ex. pour une villa, le centre ou la plateforme de gestion ne sont habituellement pas nécessaires.

## 2 Illustration

### 2.1 VTO2101E-P

#### 2.1.1 Panneau avant

Figure 2-1 VTO2101E-P

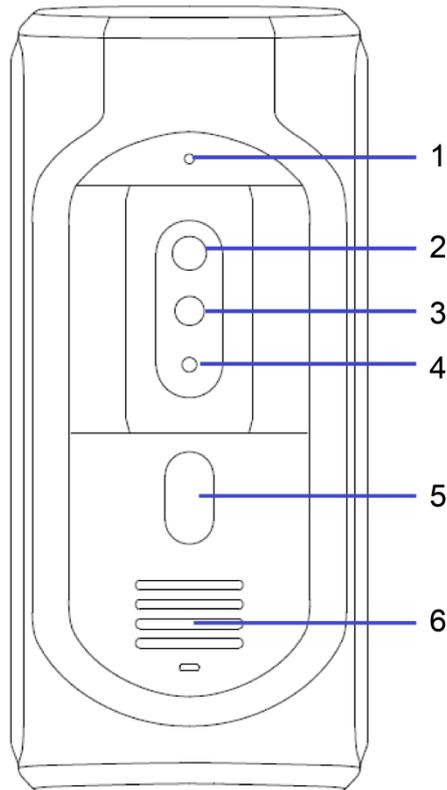


Tableau 2-1 Description du panneau avant

N°	Nom	Description
1	Microphone	—
2	Caméra	—
3	Lumière infrarouge	Apporte une lumière infrarouge supplémentaire à la caméra lorsqu'il fait sombre.
4	Capteur de lumière	Détecte les conditions de luminosité ambiante.
5	Bouton d'appel	Pour appeler les VTH ou le centre de gestion.
6	Haut-parleur	—

## 2.1.2 Panneau arrière

Figure 2-2 VTO2101E-P

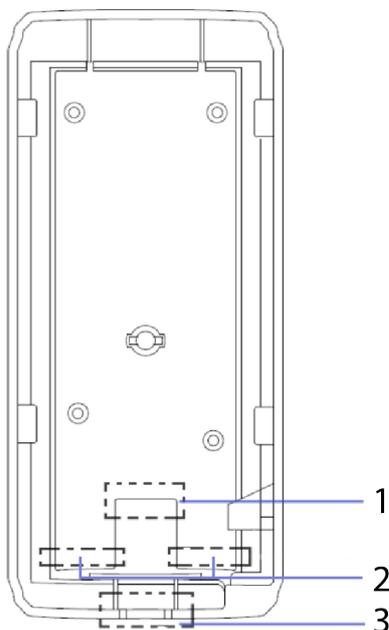
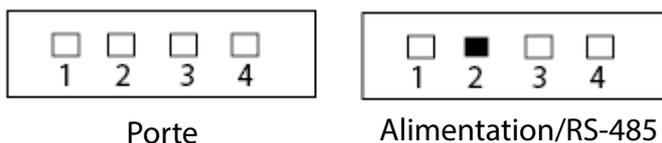


Tableau 2-2 Description du panneau arrière

N°	Nom	Description
1	Port réseau	Permet de connecter le câble réseau.
2	Ports RS-485	Voir la figure et le tableau ci-dessous.
3	Sortie de câble	Faites passer le câble par ce trou.

Figure 2-3 Branchement des câbles



Porte

Alimentation/RS-485

Tableau 2-3 Description du port

PORTE		Alimentation/RS-485	
N°	Nom	N°	Nom
1	NO	1	+12V
2	NC	2	GND
3	COM	3	RS-485A
4	Entrée d'alarme ou déverrouillage (par défaut)	4	RS-485B

## 2.2 VTO2202F-P-S2/VTO2202F-P/VTO2202F/VTO2201F-P

### 2.2.1 Panneau avant

Figure 2-4 Panneau avant

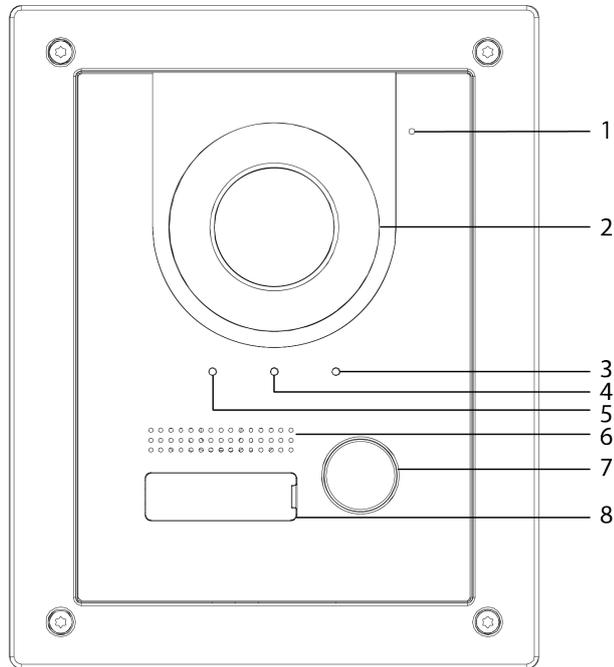


Tableau 2-4 Description du panneau avant

N°	Nom	Description
1	Microphone	—
2	Caméra	—
3	Voyant	Allumé : porte déverrouillée.
4		Allumé : Conversation en cours.
5		Allumé : Appel en cours.
6	Haut-parleur	—
7	Bouton d'appel	Pour appeler d'autres VTH ou le centre de gestion.
8	Étiquette nominative	Nom de l'hôte.

## 2.2.2 Panneau arrière

Figure 2-5 Panneau arrière

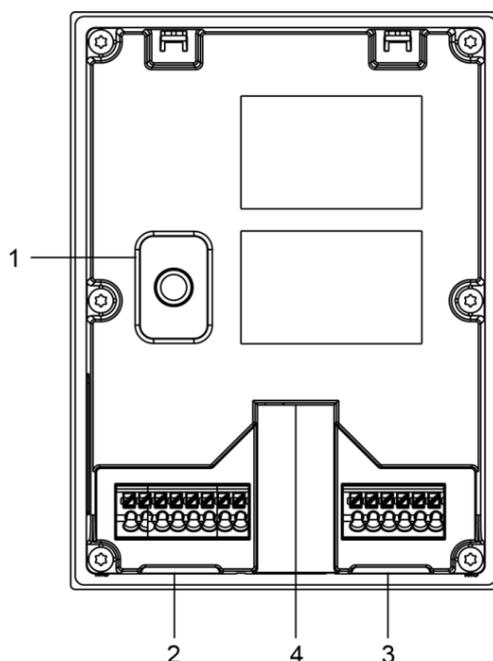


Tableau 2-5 Description du panneau arrière

N°	Nom	Description
1	Contact antisabotage	Lorsque le VTO est retiré de force du mur, une alarme se déclenche et les informations d'alarme sont envoyées au centre de gestion.
2	Port	De gauche à droite : GND +12V_OUT RS485_B RS485_A ALARM_NO ALARM_COM VTO2202F-P-S2 : 2 fils + (48 V) ; VTO2202F-P et VTO2202F : EOC1 (+12 V) ; VTO2201F : +24 V VTO2202F-P-S2 : 2 fils - (GND) ; VTO2202F-P et VTO2202F : EOC2 (GND) ; VTO2201F : GND.
3		De gauche à droite : DOOR_BUTTON DOOR_FB GND DOOR_NC DOOR_COM DOOR_NO
4	Port Ethernet	Pour la connexion au réseau à l'aide d'un câble Ethernet.  Seuls les modèles terminant par « P » prennent en charge la fonction PoE.

## 2.3 VTO2111D-P-S2/VTO1101D-P

### 2.3.1 Panneau avant

Figure 2-6 Panneau avant

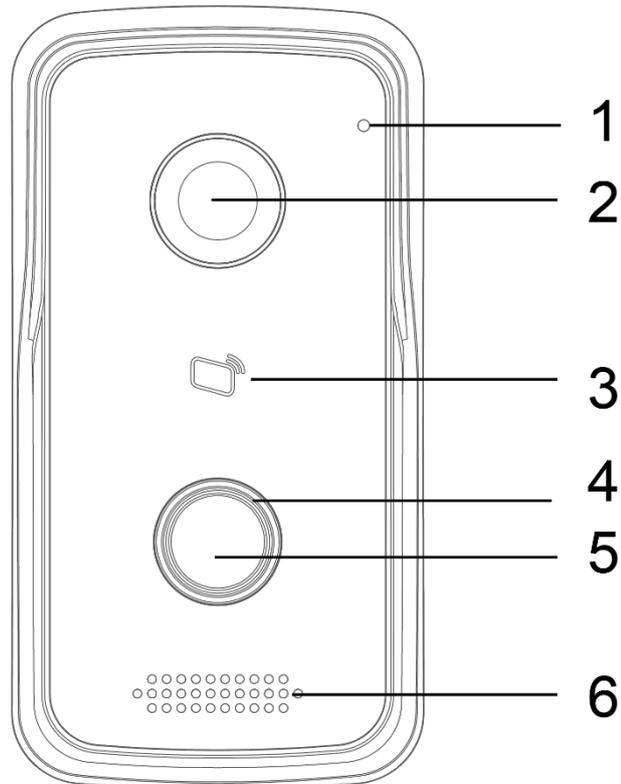


Tableau 2-6 Description du panneau avant

N°	Nom	Description
1	Microphone	—
2	Caméra	—
3	Fenêtre du lecteur de carte	Présenter une carte pour déverrouiller une porte ou l'émettre.
4	Voyant	<ul style="list-style-type: none"><li>● Bleu fixe : mode veille.</li><li>● Bleu clignotant : en appel ou réseau absent.</li></ul>
5	Bouton d'appel	Pour appeler les VTH ou le centre de gestion.
6	Haut-parleur	—

## 2.3.2 Panneau arrière

Figure 2-7 Panneau arrière

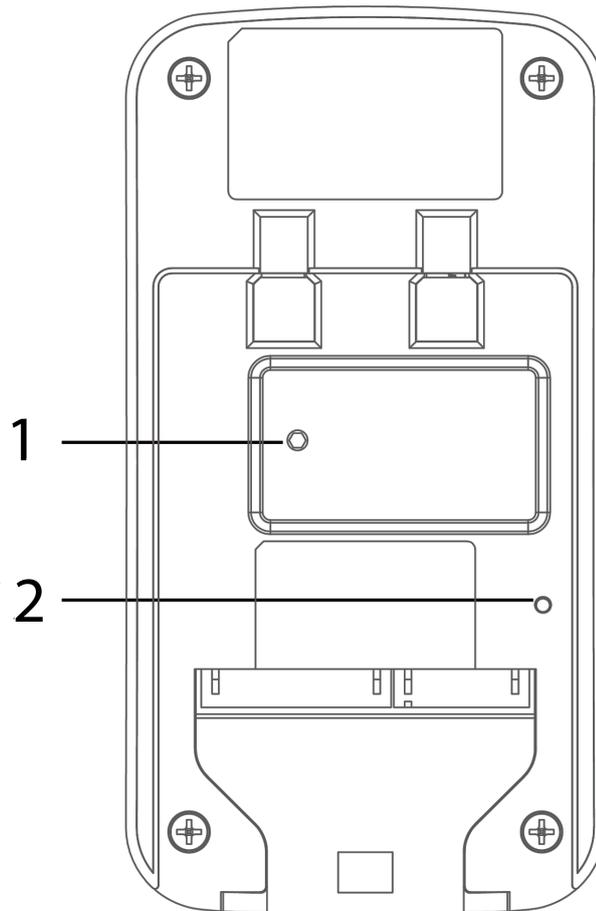


Tableau 2-7 Description du panneau arrière

N°	Nom	Description
1	Contact antisabotage	Lorsque le VTO est retiré de force du mur, une alarme se déclenche et les informations d'alarme sont envoyées au centre de gestion.
2	Réinitialisation	Appuyez et maintenez le bouton enfoncé pendant 10 s pour réinitialiser tous les paramètres.

Figure 2-8 Branchement des câbles

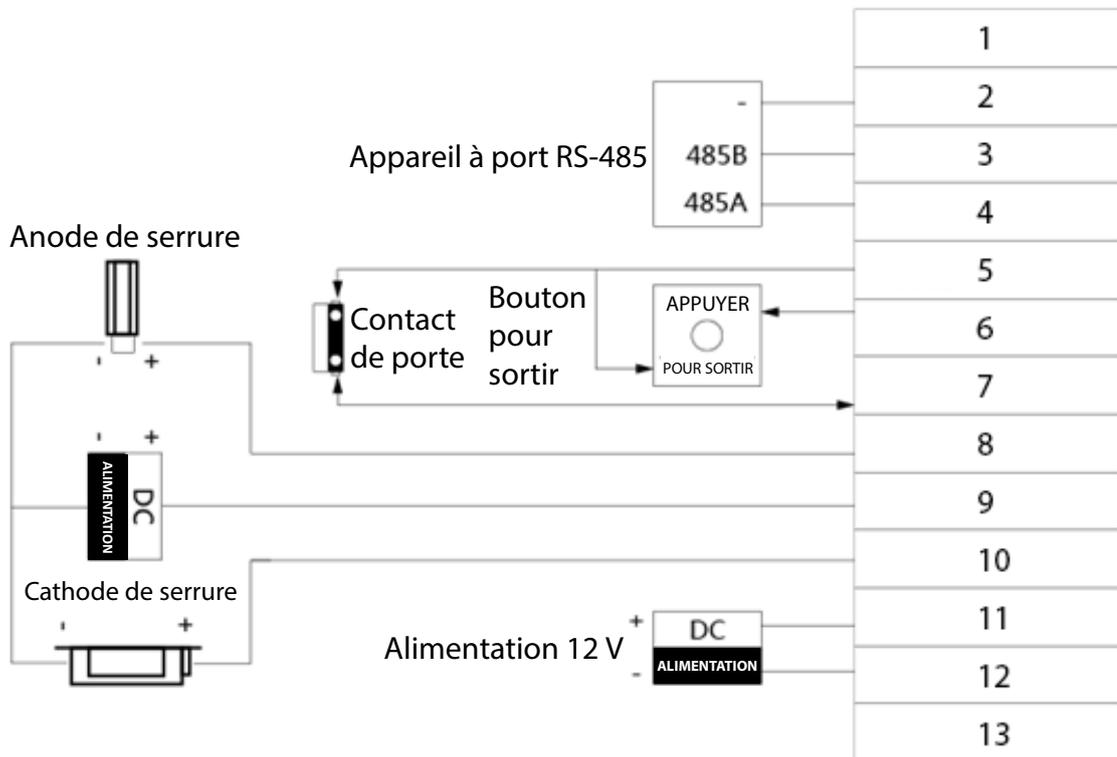


Tableau 2-8 Description du port

N°	Description	N°	Description
1	N/A	8	NC
2	GND	9	COM
3	485_B	10	NO
4	485_A	11	GND
5	GND	12	12 V
6	DÉVERROUILLAGE	13	RÉSEAU
7	RETOUR	—	—

## 2.4 VTO3211D-P-S2

### 2.4.1 Panneau avant

Le nombre de boutons sur le panneau avant varie selon les modèles. Le modèle VTO3211D-P-S2 est équipé d'un bouton, le modèle VTO3211D-P2-S2 est équipé de deux boutons et le modèle VTO3211D-P4-S2 est équipé de quatre boutons. Prenons ici l'exemple du modèle VTO3211D-P4-S2.

Figure 2-9 VTO3211D-P4-S2

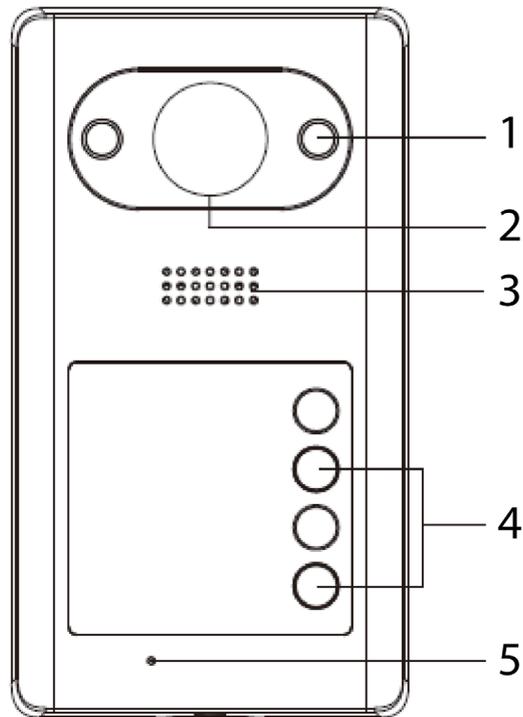


Tableau 2-9 Description du panneau avant

N°	Nom	Description
1	Éclairage IR	Apporte une lumière infrarouge supplémentaire à la caméra lorsqu'il fait sombre.
2	Caméra	—
3	Haut-parleur	—
4	Bouton d'appel	Pour appeler les VTH ou le centre de gestion.
5	Microphone	—

## 2.4.2 Panneau arrière

Figure 2-10 VTO3211D-P4

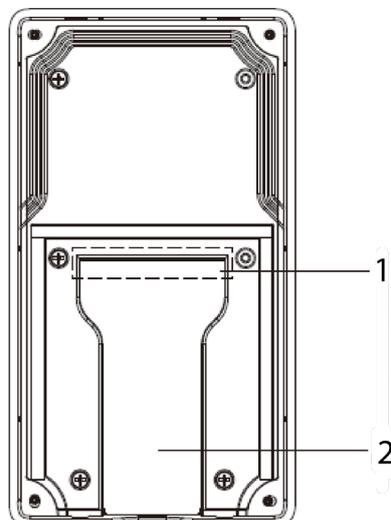


Tableau 2-10 Description du panneau arrière

N°	Nom	Description
1	Ports de câble	Voir la figure et le tableau ci-dessous.
2	Sortie de câble	Faites passer le câble par ce trou.

Figure 2-11 Branchement des câbles

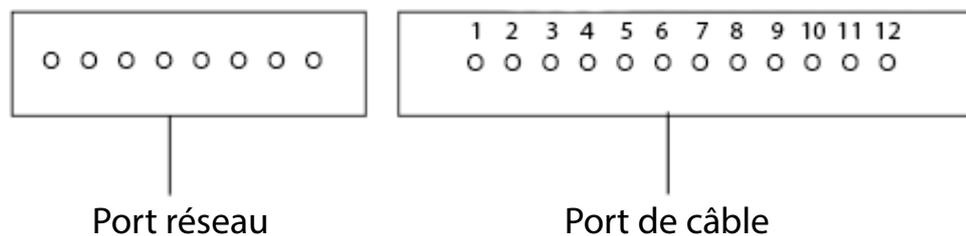


Tableau 2-11 Description du port de câble

N°	Nom	N°	Nom
1	ALM_COM	7	DOOR_FEED
2	ALM_NO	8	DOOR_NC
3	ALM_IN	9	DOOR_COM
4	RS485B	10	DOOR_NO
5	RS485A	11	GND
6	DOOR_OPEN	12	DC 12V

## 2.5 VTO3221E-P

### 2.5.1 Panneau avant

Figure 2-12 Panneau avant

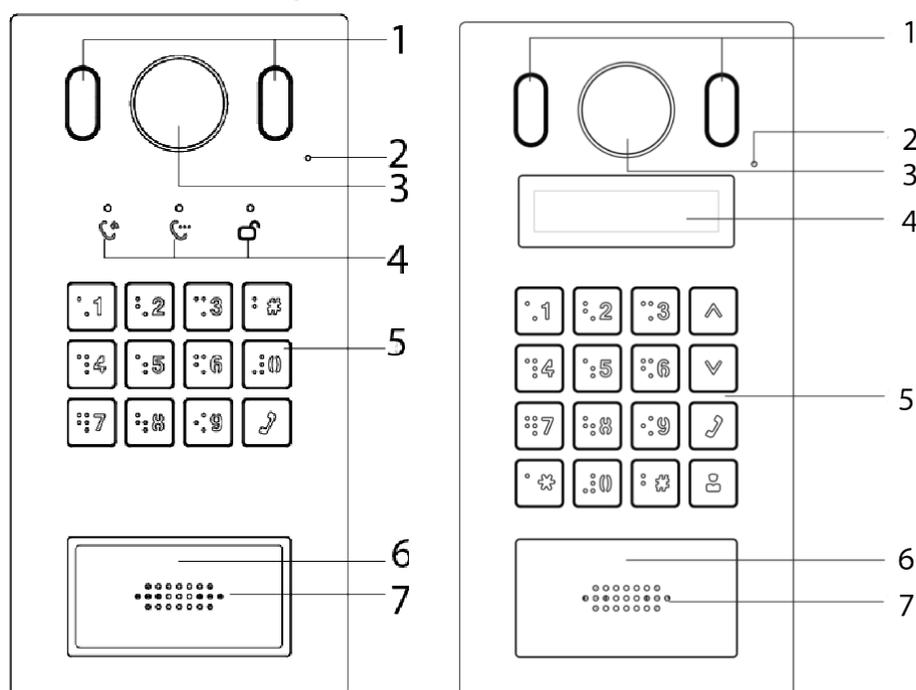


Tableau 2-12 Description du panneau avant

N°	Nom	Description
1	Éclairage	Apporte une lumière supplémentaire à la caméra lorsqu'il fait sombre.
2	Microphone	—
3	Caméra	—
4	Voyants	Indicateur d'activité : en appel, en conversation et déverrouillage.
5	Clavier	—
6	Fenêtre du lecteur de carte	Présentez votre carte à ce niveau pour déverrouiller la porte.
7	Haut-parleur	—

## 2.5.2 Panneau arrière

Figure 2-13 VTO3221E-P

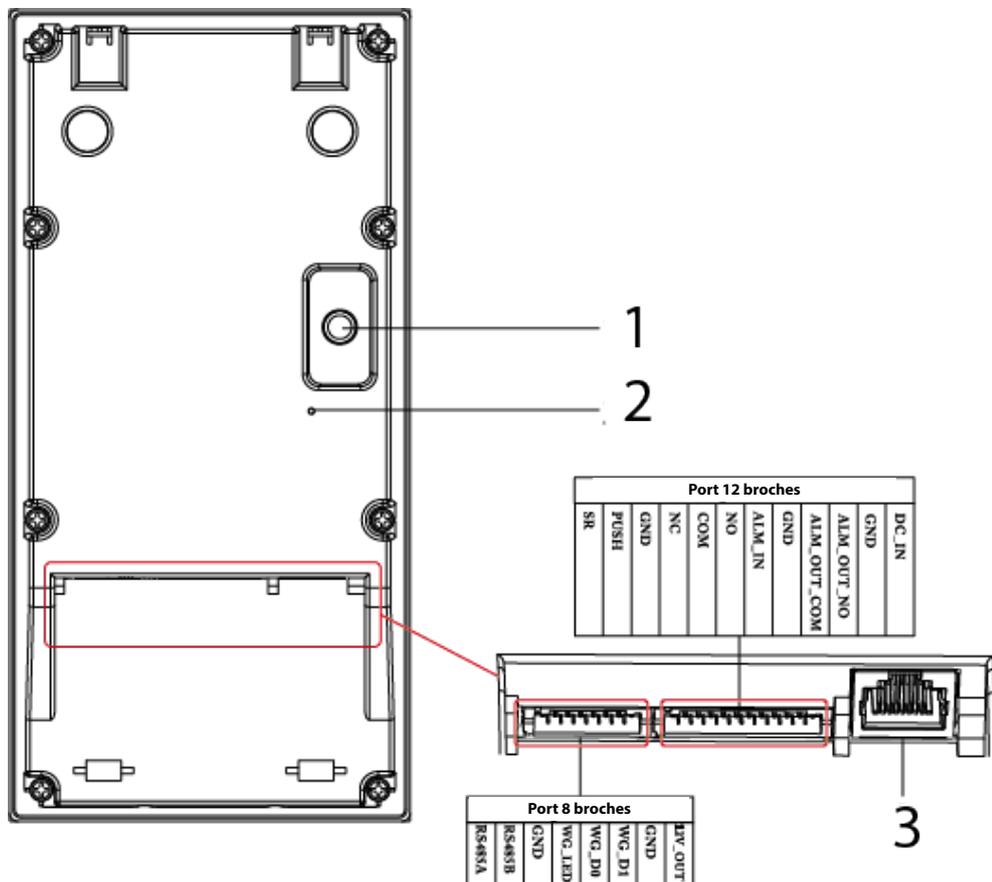


Tableau 2-13 Description du panneau arrière

N°	Nom	Description
1	Contact antisabotage	Lorsque le VTO est retiré de force du mur, une alarme se déclenche et les informations d'alarme sont envoyées au centre de gestion.
2	Bouton de réinitialisation	Appuyez et maintenez le bouton enfoncé pendant 10 s pour réinitialiser tous les paramètres.
3	Port Ethernet	Pour la connexion d'un câble Ethernet.

## 2.6 VTO2211G-P/VTO1201G-P

### 2.6.1 Panneau avant

Figure 2-14 Panneau avant du VTO2211G/VTO1201G

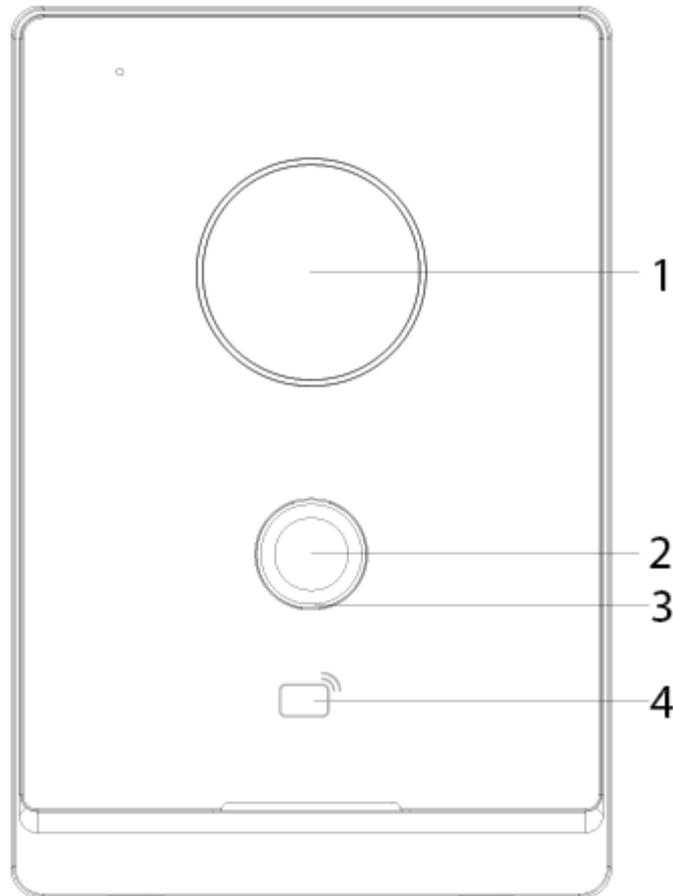


Tableau 2-14 Description du panneau avant

N°	Nom	Description
1	Caméra	—
2	Bouton d'appel	Pour appeler les VTH ou le centre de gestion.
3	Voyant	<ul style="list-style-type: none"><li>● Éteint : l'appareil est en mode veille.</li><li>● Vert fixe : appel en cours.</li><li>● Bleu fixe : Conversation en cours.</li><li>● Jaune-vert : porte déverrouillée par le moniteur (VTH) alors qu'un appel est en cours sur la station de porte (VTO).</li><li>● Rouge-bleu : porte déverrouillée par le moniteur (VTH) alors qu'une conversation est en cours sur la station de porte (VTO).</li><li>● Bleu progressif : réseau déconnecté.</li></ul>
4	Fenêtre du lecteur de carte	Présentez votre carte à ce niveau pour déverrouiller la porte (uniquement pour le modèle VTO2211G-P).

## 2.6.2 Panneau arrière

Figure 2-15 Panneau arrière du modèle VTO2211G-P/VTO1201G-P

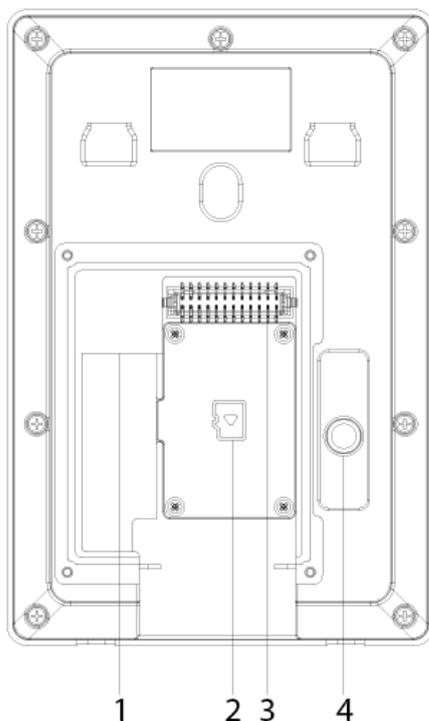
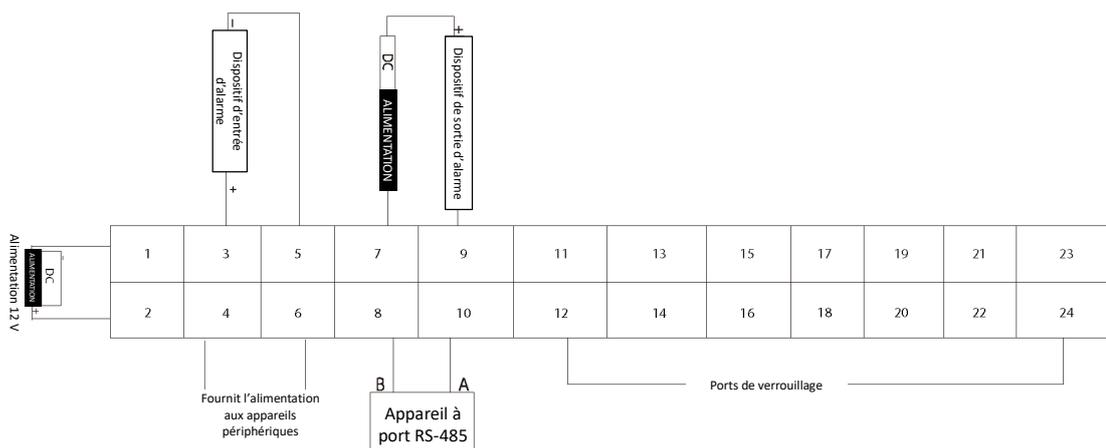


Tableau 2-15 Description du panneau arrière

N°	Description	N°	Description
1	Port réseau	3	Ports
2	Couvercle de la carte SD	4	Contact antisabotage

Figure 2-16 Connexion de câble pour le modèle VTO2211G-P



Les ports 12, 14, 16, 18, 20, 22 et 24 permettent de connecter les serrures.

Tableau 2-16 Description du port

N°	Nom	N°	Nom
1	DC_IN-	13	Non disponible
2	DC_IN+	14	DOOR1_COM

N°	Nom	N°	Nom
3	ALARM_IN	15	Non disponible
4	+12V_OUT	16	DOOR1_NO
5	GND	17	Non disponible
6	GND	18	GND
7	ALARM_NO	19	Non disponible
8	RS485B	20	DOOR1_FB
9	ALARM_COM	21	Non disponible
10	RS485A	22	GND
11	Non disponible	23	Non disponible
12	DOOR1_NC	24	DOOR1_PUSH

Figure 2-17 Connexion de câble pour le modèle VTO1201G-P

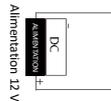
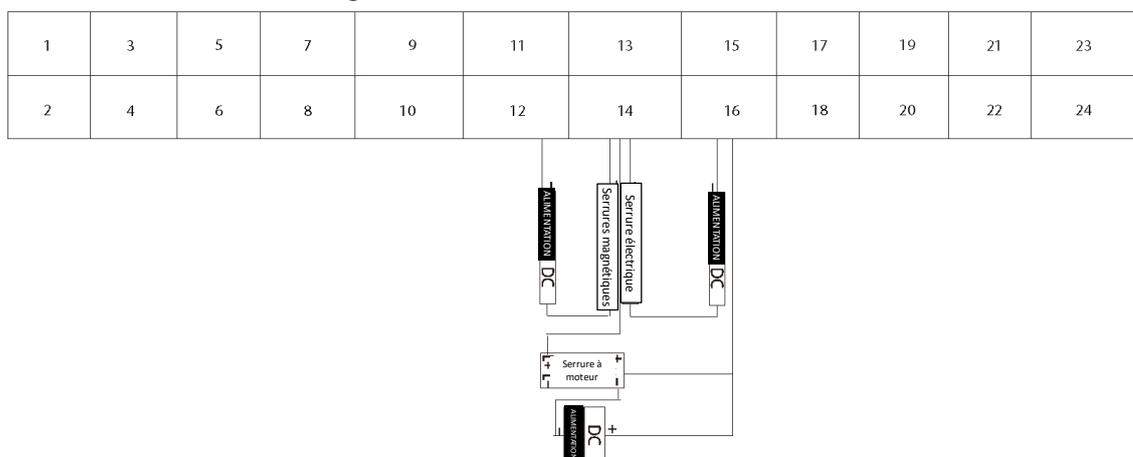
	1	3	5	7	9	11	13	15	17	19	21	23
	2	4	6	8	10	12	14	16	18	20	22	24

Tableau 2-17 Description du port

N°	Nom
1	DC_IN-
2	DC_IN+
3 à 24	Fonction réservée

Figure 2-18 Connexion de câble de serrure

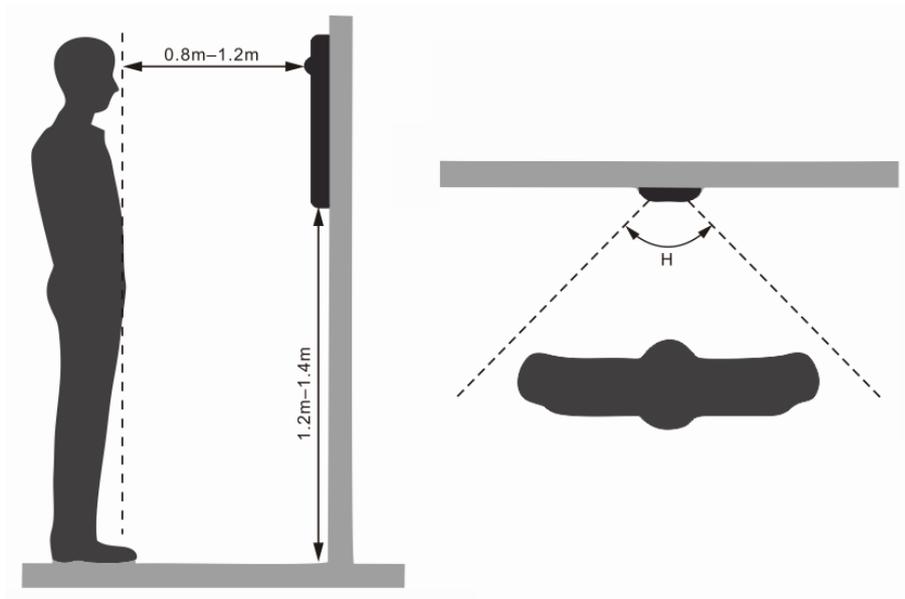


Vous pouvez connecter une serrure magnétique ou électrique le cas échéant. Reportez-vous à la figure précédente pour les règles de connexion au port.

# 3 Installation

- Un personnel compétent doit réaliser l'installation et la configuration de l'appareil. Contactez l'assistance technique si vous avez besoin de réparer un appareil.
- Voir la figure ci-dessous pour l'emplacement d'installation. L'angle de vision horizontal de l'appareil varie en fonction des modèles. Le visage des individus devrait apparaître au centre de la vue de l'appareil.

Figure 3-1 Emplacement d'installation



# 4 Configuration

Ce chapitre présente les configurations de base des moniteurs (VTH) et des portiers (VTO). Reportez-vous au manuel d'utilisation pour les détails.



Les interfaces varient en fonction de la version du logiciel. L'interface réelle prévaut.

## 4.1 Procédure



Avant la configuration, assurez-vous de l'absence de court-circuit circuit ou de circuit ouvert sur chaque appareil.

Étape 1 : Planifiez l'adressage IP et les (servant de numéro de téléphone) pour chaque appareil.

Étape 2 : configurez le VTO. Voir « Configuration d'un VTO ».

Étape 3 : configurez le VTH. Reportez-vous au manuel d'utilisation du VTH.

Étape 4 : vérifiez si tous les paramètres sont corrects. Voir « 4.4 Mise en service ».

## 4.2 Outil de configuration

Téléchargez et utilisez l'outil de configuration « VDPConfig » pour configurer et mettre à jour plusieurs appareils. Pour plus de détails, consultez le manuel d'utilisation correspondant.

## 4.3 Configuration d'un VTO

Connectez le VTO à votre ordinateur à l'aide d'un câble réseau. À la première utilisation, vous devez créer un nouveau mot de passe de connexion à l'interface Web.

### 4.3.1 Initialisation

Assurez-vous que l'ordinateur est sur le même segment réseau.

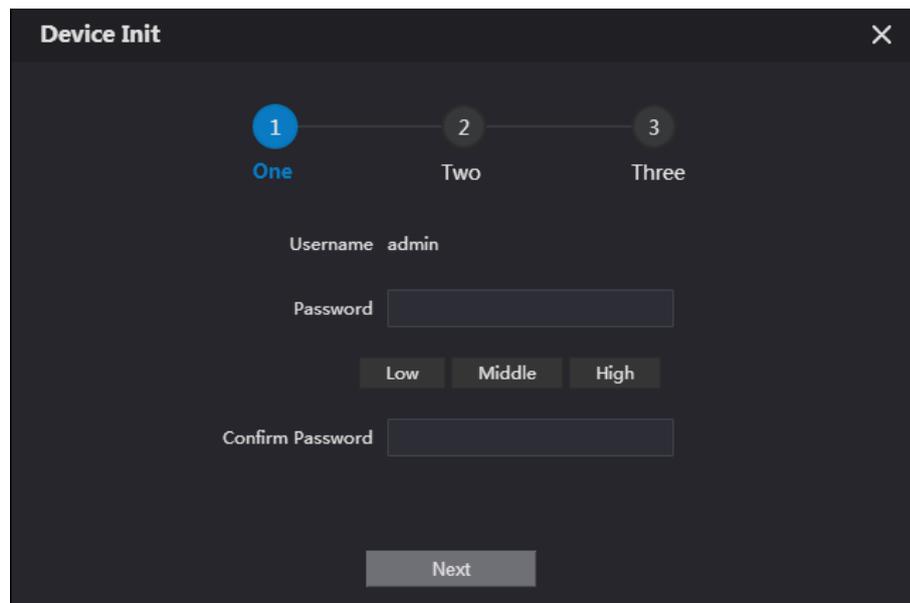
Étape 1 : Mettez sous tension le VTO.

Étape 2 : accédez à l'adresse IP du VTO à l'aide d'un navigateur.



- À la première connexion, saisissez l'adresse IP par défaut (192.168.1.108). Si vous disposez de plusieurs VTO, nous vous recommandons de modifier l'adresse IP par défaut (**Réseau > De Base**) pour éviter les conflits.

Figure 4-1 Initialisation des appareils



Device Init

1 One 2 Two 3 Three

Username admin

Password

Low Middle High

Confirm Password

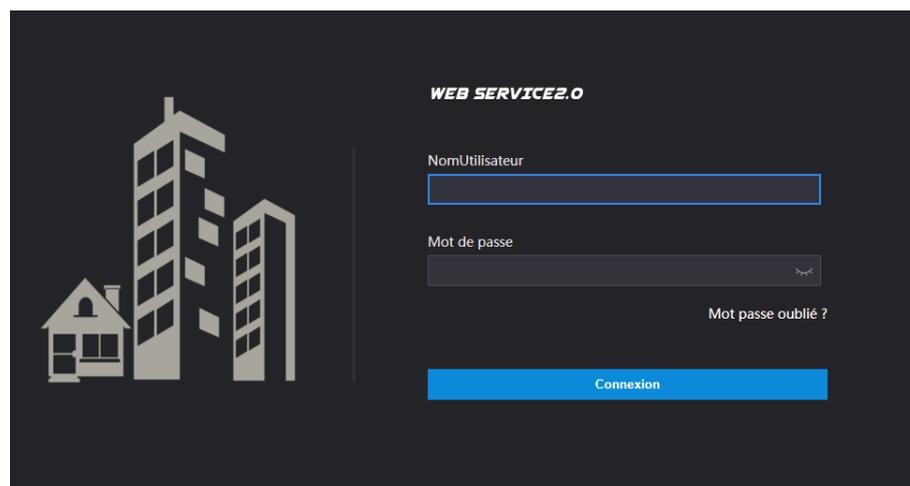
Next

Étape 3 : Saisissez et confirmez votre nouveau mot de passe, puis cliquez sur **Suivant**.

Étape 4 : Sélectionnez **E-mail**, puis saisissez l'adresse e-mail pour réinitialiser le mot de passe.

Étape 5 : Cliquez sur **Suivant**, puis sur **OK** pour accéder à l'interface de connexion.

Figure 4-2 Interface de connexion



WEB SERVICEZ.O

NomUtilisateur

Mot de passe

Mot passe oublié ?

Connexion

### 4.3.2 Configuration d'un numéro de VTO

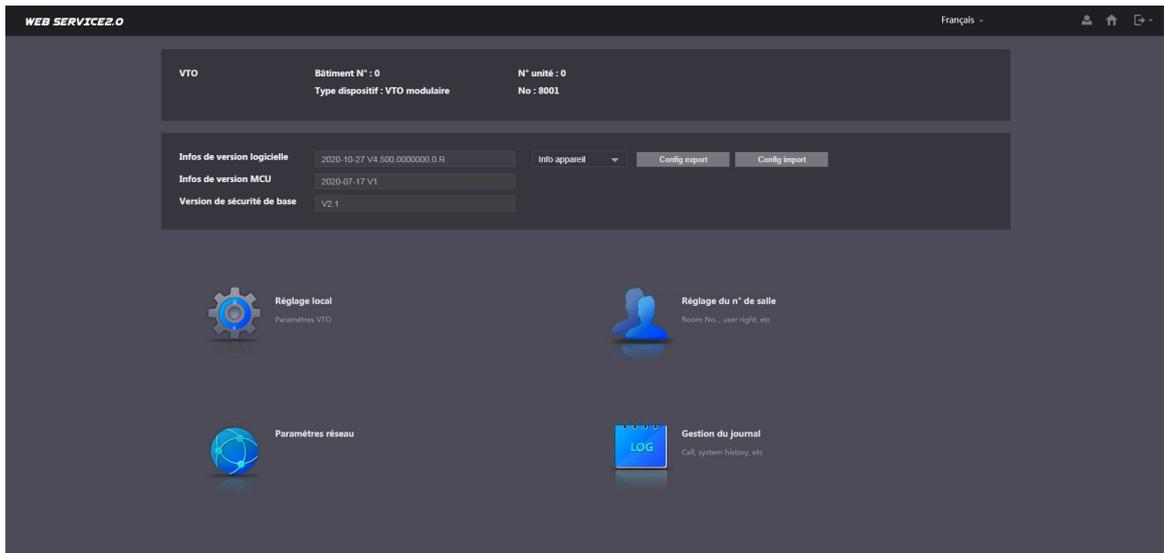
Les numéros permettent de distinguer chaque VTO, nous vous recommandons de les paramétrer en fonction des numéros des unités d'habitation ou du bâtiment.



- Vous pouvez modifier le numéro d'un VTO lorsqu'il ne joue pas le rôle de serveur SIP.
- Un numéro VTO est composé d'un maximum de 5 chiffres et doit être différent d'un numéro de pièce.

Étape 1 : Connectez-vous à l'interface Web du VTO.

Figure 4-3 Interface principale



Étape 2 : Sélectionnez **Réglage local** > **Réglage de base**.

Figure 4-4 Propriétés de l'appareil

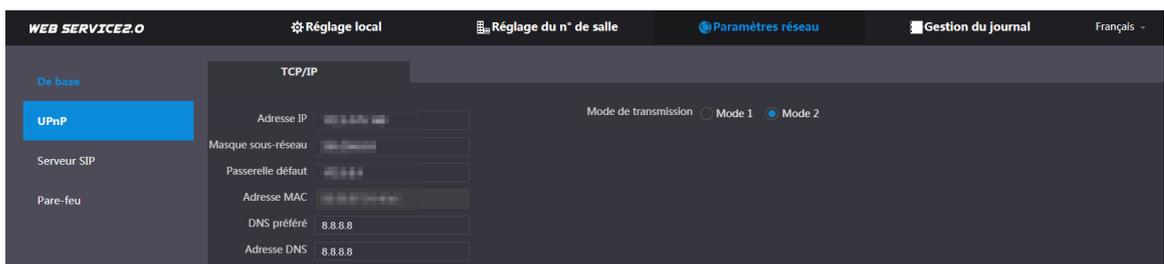


Étape 3 : Saisissez un numéro dans le champ **N°**, puis cliquez sur **Confirmer**.

### 4.3.3 Configuration des paramètres de réseau

Étape 1 : sélectionnez **Réseau** > **De base**.

Figure 4-5 Informations TCP/IP



Étape 2 : Saisissez chaque paramètre, puis cliquez sur **Enreg..**

Le VTO redémarrera automatiquement. Vous devez changer l'adresse IP de votre ordinateur pour qu'il appartienne au même segment réseau que celui du VTO pour la reconnexion.

### 4.3.4 Configuration du serveur SIP

Lorsqu'ils sont connectés au même serveur SIP, tous les VTO et VTH peuvent s'appeler entre eux. Vous pouvez utiliser un VTO ou un autre serveur comme serveur SIP.

Étape 1 : Sélectionnez **Réseau** > **Serveur SIP**.

Figure 4-6 Serveur SIP



Étape 2 : Sélectionnez le type de serveur au besoin.

- Si le VTO actuel fonctionne comme serveur SIP, activez l'option **Serveur SIP**, puis cliquez sur **Enreg.**

Le VTO redémarre automatiquement. Ensuite, vous pouvez ajouter d'autres VTO et VTH à cette station de porte. Voir « 4.3.6 Ajout des VTO » et « 4.3.7 Ajout du numéro de pièce ».



Si le VTO actuel ne fonctionne pas comme serveur SIP, n'activez pas l'option **Serveur SIP**. Sinon la connexion à ce VTO échouera.

- Si un autre VTO fonctionne comme serveur SIO, réglez l'option **Type serveur** sur VTO, puis configurez les paramètres.

Tableau 4-1 Configuration du serveur SIP

Paramètres	Description
Adresse IP	Saisissez dans le champ de l'adresse IP du VTO fonctionnant comme serveur SIP.
Port	<ul style="list-style-type: none"> <li>• Le port 5 060 est utilisé par défaut lorsque le VTO sert de serveur SIP.</li> <li>• Le port 5 080 est utilisé par défaut lorsque la plateforme sert de serveur SIP.</li> </ul>
NomUtilisateur	Gardez la valeur par défaut.
Mot de passe	
Domaine SIP	Interphone vidéo de porte (VDP).
Nom utilisateur Serveur SIP	Nom d'utilisateur et mot de passe de connexion à l'interface Web du serveur SIP.
MDP Serveur SIP	

- Si un serveur fonctionne comme serveur SIP, réglez au besoin l'option **Type serveur**, puis reportez-vous au manuel correspondant pour les détails.

## 4.3.5 Configuration du numéro d'appel et des appels collectifs

Pour appeler un VTO, vous devez configurer le numéro d'appel de chaque VTO opérationnel avec un numéro d'appel.

Étape 1 : Sélectionnez **Réglage local** > **Réglage de base**.

Figure 4-7 Propriétés de l'appareil

**Étape 2 :** Dans la zone de saisie du **N°**, saisissez le numéro de la pièce que vous devez appeler, puis cliquez sur **Confirmer** pour enregistrer. Répétez cette opération sur chaque interface Web des VTO. Vous avez la possibilité d'activer la fonction d'appel collectif sur le serveur SIP. Lorsque vous appelez un moniteur (VTH) principal, tous les VTH d'extension reçoivent également l'appel.



- Vous pouvez modifier le numéro du VTO uniquement lorsqu'il ne joue pas le rôle de serveur SIP.
- Lorsque vous activez ou désactivez la fonction d'appel collectif, le VTO redémarre automatiquement.

**Étape 3 :** Connectez-vous à l'interface Web du serveur SIP, puis sélectionnez **Réglage local > Réglage de base**.

**Étape 4 :** Activez l'option **Appeler groupe**, puis cliquez sur **Confirmer**. Le VTO redémarrera automatiquement.

### 4.3.6 Ajout des VTO

Vous pouvez ajouter des VTO à un serveur SIP. Tous les VTO connectés au même serveur SIP peuvent effectuer des appels vidéo entre eux. Ce paragraphe s'applique à un VTO jouant le rôle de serveur SIP. Si vous utilisez un autre serveur comme serveur SIP, reportez-vous au manuel correspondant pour une configuration détaillée.

**Étape 1 :** Connectez-vous à l'interface Web du serveur SIP, puis sélectionnez **Réglage du n° de salle > Gestion VTO**.

Figure 4-8 Gestion VTO

No	Bâtiment N°	N° unité	Adresse IP	Modifier	Supprimer
8001					

**Étape 2 :** Cliquez sur **Ajouter**.

Figure 4-9 Ajouter un VTO

Étape 3 : Configurez les paramètres.



- Ajoutez d'abord le serveur SIP.

Tableau 4-2 Ajoutez des stations de porte (VTO).

Paramètres	Description
No	Numéro du VTO. Voir « 4.3.2 Configuration d'un numéro de VTO ».
Enregistrer MDP	Gardez la valeur par défaut.
Bâtiment N°	Uniquement disponible si d'autres serveurs fonctionnent comme serveur SIP.
N° unité	
Adresse IP	Adresse IP VTO
NomUtilisateur	Nom d'utilisateur et mot de passe de connexion à l'interface Web du VTO.
Mot de passe	

Étape 4 : Cliquez sur **Enreg.** (Save).

### 4.3.7 Ajout du numéro de pièce

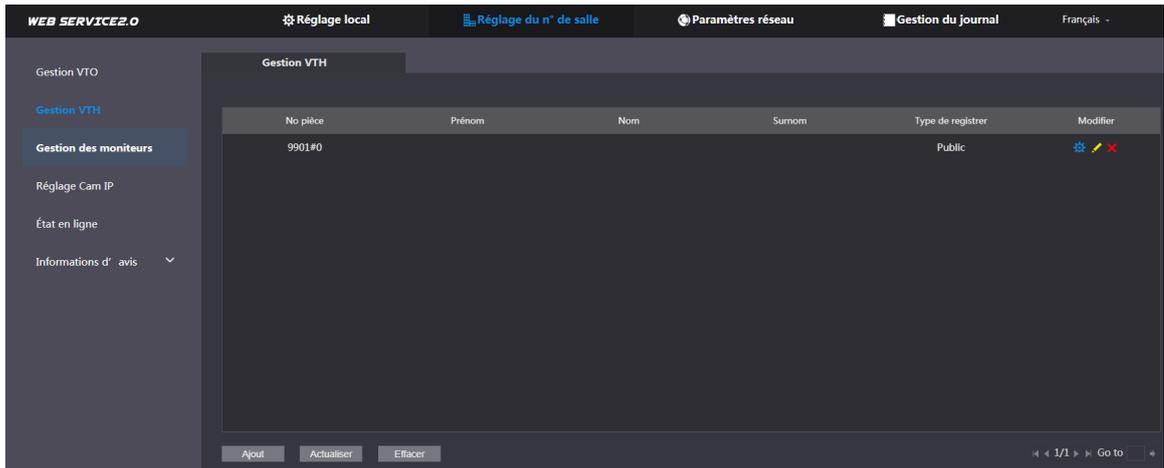
Vous pouvez ajouter le numéro de pièce sur le serveur SIP, puis configurez ce numéro sur les VTH pour établir la connexion au réseau. Ce paragraphe s'applique à un VTO jouant le rôle de serveur SIP. Si vous utilisez un autre serveur comme serveur SIP, reportez-vous au manuel correspondant pour une configuration détaillée.



Le numéro de pièce est composé d'une combinaison de 6 chiffres ou lettres au plus. Il doit être différent pour chaque VTO.

Étape 1 : Connectez-vous à l'interface web du serveur SIP, puis sélectionnez **Réglage du n° de salle > Gestion des numéros de pièce.**

Figure 4-10 Gestion des numéros de pièce



Étape 2 : Cliquez sur **Ajouter**.

Figure 4-11 Ajouter un seul numéro de pièce

Étape 3 : Configurez les informations de la pièce.

Tableau 4-3 Informations de la pièce

Paramètres	Description
Prénom	Ce sont les informations qui permettent de différencier chaque pièce.
Nom	
Surnom	
No pièce	<p>Le numéro de l'unité d'habitation ou pièce.</p>  <ul style="list-style-type: none"> <li>Lorsque vous disposez de plusieurs VTH, le numéro de pièce du VTH principal doit se terminer par #0 et les numéros de pièce pour les VTH d'extension par #1, #2...</li> <li>Vous pouvez configurer jusqu'à 9 VTH d'extension pour un VTH principal.</li> </ul>
Type d'inscription	Sélectionnez <b>Public</b> .
Enregistrer MDP	Gardez la valeur par défaut.

Étape 4 : Cliquez sur **Enreg.**.

Cliquez sur  pour modifier les informations concernant la pièce, puis cliquez sur  pour supprimer la pièce.

## 4.4 Mise en service

### 4.4.1 VTO appelant un VTH

Étape 1 : Composez un numéro de pièce sur le VTO.

Étape 2 : Appuyez sur  sur le VTH pour répondre à l'appel.

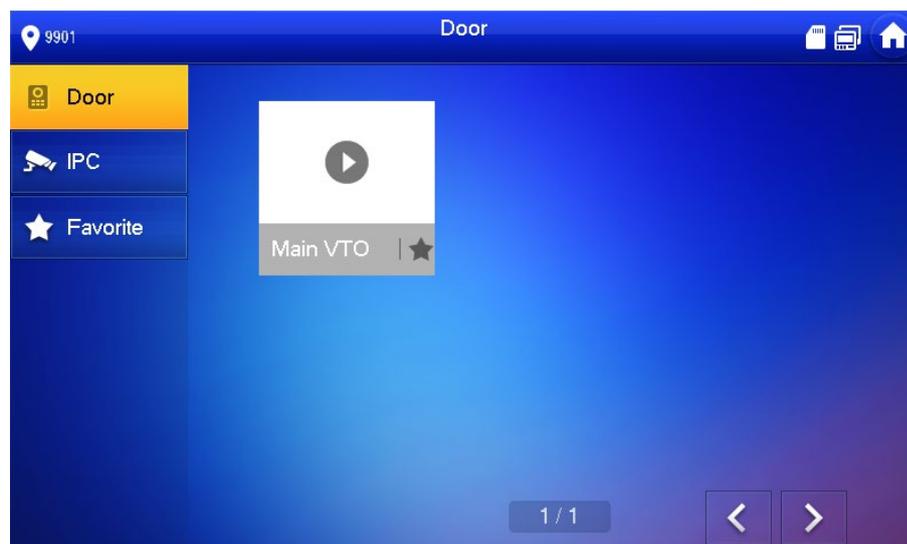
Figure 4-12 Écran d'appel



### 4.4.2 VTH surveillant un VTO

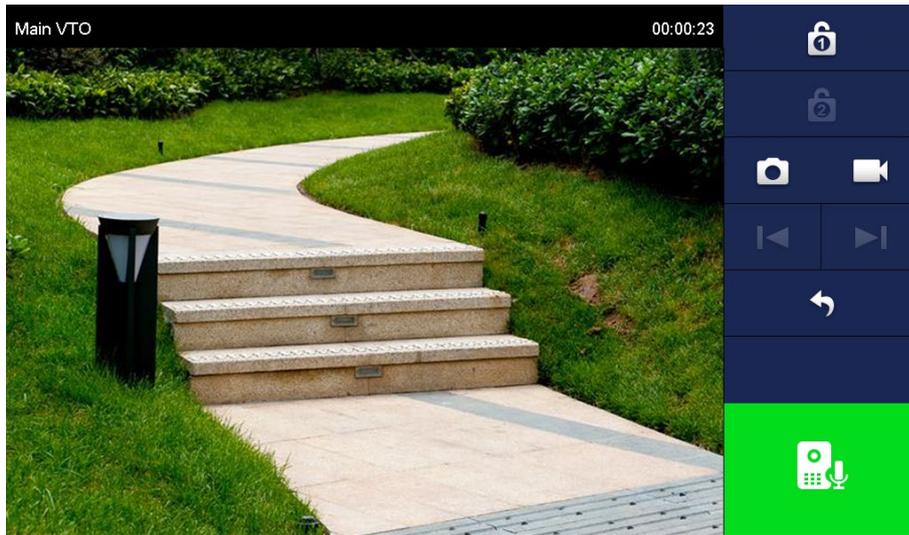
Étape 1 : Dans l'interface principale du VTH, sélectionnez **Moniteur > Porte**.

Figure 4-13 Porte



Étape 2 : Sélectionnez un VTO.

Figure 4-14 Vidéo de surveillance





## 5 EasyViewer Plus

EasyViewer Plus (ci-après dénommée l'application) permet de gérer les appareils, de reproduire des vidéos, de déverrouiller les portes, etc.

Avant d'ajouter le VTO dans l'application, vous devez connecter le VTO au routeur par Wi-Fi ou à l'aide d'un commutateur. Vous devez ensuite modifier manuellement l'adresse IP du VTO pour qu'elle soit sur le même réseau du routeur, si le protocole DHCP n'est pas pris en charge.

Téléchargez l'application de la boutique d'applications sur votre smartphone. Dans l'application, sélectionnez **Réglage > Aide et commentaire** pour afficher les instructions de chaque fonction.

# Annexe 1 Recommandations en matière de cybersécurité

La cybersécurité est plus qu'un mot à la mode : c'est quelque chose qui concerne chaque appareil connecté à Internet. La vidéosurveillance sur IP n'est pas à l'abri des cyberattaques, mais la mise en place de mesures élémentaires pour protéger et renforcer les réseaux et les appareils en réseau les rendra moins vulnérables à des attaques. Nous donnons, ci-après, des conseils et des recommandations pour créer un système de sécurité plus sûr.

## **Actions obligatoires à prendre pour la sécurité réseau d'un équipement de base :**

### **1. Utiliser des mots de passe robustes**

Veillez vous référer aux recommandations suivantes pour définir les mots de passe :

- La longueur du mot de passe doit être d'au moins 8 caractères.
- Ils doivent être composés de deux types de caractères comprenant des lettres majuscules et minuscules, des chiffres et des symboles.
- Ils ne doivent pas être composés du nom du compte dans l'ordre normal ou inversé ;
- Les caractères ne doivent pas se suivre, p. ex. 123, abc, etc.
- Les caractères ne doivent pas se répéter, p. ex. 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 équipement (enregistreurs NVR et DVR, caméra IP, etc.) afin de garantir que votre système est doté des correctifs de sécurité les plus récents. Lorsque l'équipement est connecté au réseau public, il est recommandé d'activer la fonction de vérification automatique de la disponibilité de mises à jour afin d'obtenir rapidement les informations sur les mises à jour du micrologiciel fournies par le fabricant.
- Nous vous conseillons de télécharger et d'utiliser la version du logiciel client la plus récente.

## **Recommandations à suivre pour améliorer la sécurité réseau de votre équipement :**

### **1. Protection matérielle**

Nous vous suggérons de fournir une protection matérielle à vos équipements, en particulier les dispositifs de stockage. Par exemple, placez l'équipement dans une armoire ou une salle informatique spéciale, et appliquez des autorisations de contrôle d'accès et une gestion des clés sur mesure afin d'empêcher tout personnel non autorisé d'entrer en contact physique avec les équipements pour éviter p. ex. d'endommager le matériel, des connexions non autorisées à des équipements amovibles (disque flash USB, port série, etc.).

### **2. Modifier régulièrement votre mot de passe**

Nous vous conseillons de modifier régulièrement vos mots de passe pour réduire les risques qu'ils soient devinés ou déchiffrés.

### **3. Définir et mettre à jour les informations de réinitialisation des mots de passe à temps**

L'équipement prend en charge la fonction de réinitialisation du mot de passe. Veuillez définir les informations relatives à la réinitialisation du mot de passe à temps, y compris l'adresse électronique de l'utilisateur final et les questions de protection du mot de passe. Si les informations changent, veuillez les modifier à temps. Lors de la configuration des questions de protection du mot de passe, il est conseillé de ne pas utiliser des questions (réponses) trop faciles à deviner.

### **4. Activer le blocage de compte**

La fonction de blocage de compte est activée par défaut. Nous vous recommandons de la laisser activée pour garantir la sécurité des comptes. Si un pirate tente de se connecter plusieurs fois avec un mot de passe incorrect, le compte concerné et l'adresse IP de la source seront bloqués.

### **5. Modifier les ports par défaut des services HTTP et d'autres services**

Nous vous conseillons de modifier les ports par défaut du service HTTP et des autres services en les choisissant dans la plage numérique allant de 1 024 à 65 535, ce qui permet de réduire le risque que des étrangers puissent deviner les ports utilisés.

### **6. Activer HTTPS**

Nous vous conseillons d'activer le protocole HTTPS. Vous accéderez ainsi au service Web au moyen d'un canal de communication sécurisé.

### **7. Liaison d'adresse MAC**

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

### **8. Assigner raisonnablement les comptes et les privilèges**

En fonction des besoins d'activité et de gestion, ajoutez de manière raisonnable des utilisateurs et leur assigner un ensemble d'autorisations minimales.

### **9. Désactiver les services inutiles et choisir les modes sécurisés**

S'ils ne sont pas nécessaires et pour réduire les risques, désactivez certains services, tels que SNMP, SMTP, UPnP, etc.

En cas de besoin, il est fortement recommandé d'utiliser les modes sécurisés, y compris, mais sans limitation, les services suivants :

- SNMP : choisissez SNMP v3 et configurez des mots de passe de chiffrement et d'authentification robustes.
- SMTP : choisissez le protocole TLS pour accéder aux serveurs de messagerie.
- FTP : choisissez le protocole SFTP et définissez des mots de passe robustes.
- Point d'accès : choisissez le mode de chiffrement WPA2-PSK et définissez des mots de passe robustes.

### **10. Chiffrement de la transmission audio et vidéo**

Si vos contenus de données audio et vidéo sont très importants ou sensibles, nous vous recommandons d'utiliser la fonction de chiffrement de la transmission, afin de réduire les risques de vol des données audio et vidéo durant la transmission.

Rappel : le chiffrement de la transmission entraînera une certaine baisse de l'efficacité de la transmission.

### **11. Contrôle sécurisé**

- Vérifier les utilisateurs connectés : nous vous conseillons de vérifier régulièrement les utilisateurs connectés afin de savoir si la connexion à l'appareil s'effectue sans autorisation.
- Consulter le journal de l'équipement : en examinant les journaux, vous pouvez connaître les adresses IP utilisées pour la connexion à vos appareils et les principales opérations effectuées.

### **12. Journal réseau**

Comme la capacité de stockage de l'équipement est limitée, le journal stocké sera limité. Si vous devez conserver le journal pour longtemps, il est recommandé d'activer la fonction de journal réseau afin de veiller à ce que les journaux essentiels soient synchronisés avec le serveur de journal réseau pour suivi.

### **13. Construire un environnement réseau sécurisé**

Afin de garantir au mieux la sécurité des équipements et de réduire les cyberrisques, nous vous recommandons de :

- Désactiver la fonction de mappage de ports du routeur pour éviter les accès directs aux appareils Intranet à partir du réseau externe.
- Compartimenter et isoler le réseau en fonction des besoins réseau réels. Si la communication n'est pas nécessaire entre deux sous-réseaux, il est conseillé d'utiliser les technologies de réseau VLAN, GAP et d'autres pour compartimenter le réseau de sorte à obtenir une isolation réseau effective.
- Mettre en place le système d'authentification d'accès 802.1x pour réduire le risque d'accès non autorisés aux réseaux privés.
- Activer le filtrage des adresses IP/MAC pour limiter le nombre d'hôtes autorisés à accéder à l'équipement.