
Centrale d'alarme radio VESTA SmartHub EX 640 zones, IP + Wi-Fi + 4G

Manuel d'installation et d'utilisation

Référence	Vesta-470
Modèle	HSGW-EX
Marque	VESTA

Source: <https://vesta-guide.gitbook.io/vesta-guide/vesta-470>

Ce manuel a été rédigé par Nestor Company sur la base de la documentation officielle du fabricant. Sous réserve de modifications techniques et d'erreurs typographiques.

Nestor Company · E3-laan 93, 9800 Deinze · nestorcompany.be

1. Description du produit

La VESTA SmartHub EX (HSGW-EX) est une centrale d'alarme radio de la gamme SmartSeries de Climax Technology. Associée aux détecteurs, sirènes, claviers et télécommandes radio VESTA, elle constitue un système d'alarme anti-intrusion complet pour les habitations, les commerces et les environnements professionnels de taille moyenne. La centrale gère 640 zones réparties sur 8 partitions (areas), ce qui vous permet de découper un bâtiment en parties armées et désarmées séparément.

La communication s'effectue par trois voies : IP filaire (Ethernet), Wi-Fi et réseau mobile 4G. Les événements sont transmis au centre de télésurveillance en CID ou en SIA et, en parallèle, au client final par e-mail, SMS et notification push. La programmation et l'exploitation se font depuis l'application SmartHomeSec et depuis un navigateur web : en local sur la page web de la centrale, ou à distance via le portail SmartHomeSec. Associée à des caméras PIR (PIRCAM), la centrale assure la levée de doute vidéo : lors d'une alarme, les images sont transmises à l'application et au centre de télésurveillance.

La centrale offre également des fonctions de domotique et d'automatisation. Vous pouvez créer jusqu'à 100 règles et 50 scènes, par exemple pour capturer une image à l'ouverture d'un contact de porte ou pour commander un relais.

Remarque : depuis février 2025, VESTA utilise le nouveau portail portal.vestasecurity.eu. Utilisez ce portail pour l'enregistrement et la gestion de la centrale.

2. Éléments et raccordements

- **Port Ethernet** — pour la liaison IP filaire avec le routeur du client.
- **Logement micro-SIM** — pour la carte SIM du réseau mobile (4G). Le code PIN de la carte doit être désactivé au préalable et la carte doit disposer d'un forfait data.
- **Port USB** — pour les dongles optionnels, par exemple un dongle Wi-Fi, Z-Wave ou ZigBee. N'insérez et ne retirez jamais un dongle lorsque la centrale est sous tension.
- **Alimentation et raccordement de batterie externe** — pour le bloc d'alimentation fourni et pour une batterie externe haute capacité servant d'alimentation de secours longue durée.
- **Batterie de secours interne et interrupteur de batterie** — l'interrupteur doit être sur ON pour satisfaire à la norme EN applicable.
- **Bouton d'apprentissage / reset** — pour apprendre des périphériques en local et pour réinitialiser la centrale.
- **Sirène et haut-parleur intégrés** — pour le signal d'alarme et les messages vocaux.
- **Autoprotection (tamper)** — la centrale signale l'ouverture du boîtier et l'arrachement du support mural au centre de télésurveillance et à l'application.

- **LED d'état** — indiquent l'état du système (armé, désarmé, défaut, alarme en mémoire, mode apprentissage et test de couverture).
- **Étiquette avec adresse MAC** — toujours située sur un côté de la centrale. L'adresse MAC est nécessaire pour enregistrer la centrale.

3. Caractéristiques techniques

Caractéristique	Valeur
Modèle	HSGW-EX (VESTA SmartHub EX)
Fabricant	Climax Technology
Référence fournisseur	HSGW-EX-S13-DT45-BYD-SF1-2W-868
Nombre de zones	640 zones radio
Partitions (areas)	8
Communication	IP (Ethernet), Wi-Fi, 4G
Protocole radio	VESTA 868 MHz, protocole SF1 bidirectionnel
Transmission	CID/SIA, e-mail, SMS, notification push
Programmation	Navigateur web et application (SmartHomeSec)
Levée de doute vidéo	Oui, via caméras PIR (PIRCAM)
Automatisation	100 règles et 50 scènes
Code installateur par défaut	7982
Accès web local par défaut	Utilisateur admin, port 80

4. Fonctionnement et fonctions

La centrale reçoit les signaux des détecteurs radio et décide de la réaction en fonction du type de zone (l'attribut de zone). Ainsi, *Interior* est une zone instantanée et *Entry* une zone temporisée. Vous attribuez ces caractéristiques dans la section **Response on arming**, qui définit le comportement de la zone lorsque le système est armé.

La centrale propose en outre :

- **Temporisation d'entrée et de sortie** — réglable par partition, afin d'entrer et de sortir sans déclencher l'alarme.
- **Mémoire d'alarme** — une alarme reste visible en mémoire jusqu'à sa consultation.
- **Autoprotection et supervision** — sur la centrale et sur tous les périphériques ; la centrale contrôle que chaque appareil radio se signale périodiquement.

- **Signalement de défaut secteur** — avec un délai d'attente réglable avant transmission et un mode d'économie optionnel en cas de coupure.
- **Détection de brouillage** — la centrale détecte et signale les tentatives de brouillage radio.
- **Levée de doute vidéo** — les PIRCAM transmettent les images à l'application et au centre de télésurveillance.

5. Raccordement et mise en service

1. Ouvrez le boîtier selon les indications portées sur la centrale et dégagez les raccords.
2. Raccordez le câble Ethernet au port Ethernet de la centrale et au routeur du client.
3. Si vous utilisez le réseau mobile, insérez une carte micro-SIM opérationnelle dans le logement prévu. Effectuez cette opération centrale hors tension.
4. Placez l'interrupteur de batterie sur **ON**.
5. Raccordez l'alimentation au secteur. La centrale démarre ; toutes les LED s'allument brièvement.
6. Refermez le boîtier et fixez la centrale au mur. Le montage mural est obligatoire pour satisfaire à la norme EN ; veillez à ce que le contact d'autoprotection soit entièrement comprimé contre le support mural.
7. Attendez que la centrale obtienne sa connexion réseau. L'enregistrement sur le réseau mobile peut prendre quelques minutes.

Attention : le code PIN de la carte SIM doit être désactivé avant l'insertion et la carte ne doit contenir aucun SMS. N'insérez jamais la carte SIM au moyen d'un adaptateur.

Remarque : choisissez un emplacement offrant une bonne couverture mobile. N'installez pas la centrale en cave, ni au centre d'un grand bâtiment, ni à proximité immédiate de grandes structures métalliques, de gaines ou d'appareils générant des perturbations radio. En cas de couverture faible, utilisez une antenne GPRS/4G externe.

6. Réseau et communication

Par défaut, la centrale utilise la liaison Ethernet filaire. Le Wi-Fi passe par le module Wi-Fi de la centrale ou, à défaut, par un dongle Wi-Fi USB ; le dongle CUDY-35 (AC650, 2,4 GHz et 5 GHz) est documenté comme compatible avec les centrales VESTA. La voie mobile sert de seconde voie de communication et s'active dès que vous activez la détection SIM.

6.1 Configurer la 4G et l'APN

1. Ouvrez la section **Network Settings** dans l'application installateur ou dans l'assistant de configuration.
2. Si vous passez cette étape, la centrale utilise uniquement la liaison Ethernet.

3. Si vous choisissez **Yes**, vous activez la détection SIM et configurez, si nécessaire, l'APN de l'opérateur de la carte SIM.
4. Validez et attendez que la centrale s'enregistre sur le réseau mobile.

L'APN peut également être configuré par SMS. Envoyez au numéro de la carte SIM insérée dans la centrale la commande suivante :

PROG 7982 GAPN:apn,utilisateur,motdepasse

Le premier paramètre est l'APN, le deuxième le nom d'utilisateur et le troisième le mot de passe. Laissez ces champs vides si l'opérateur n'exige ni nom d'utilisateur ni mot de passe.

6.2 Intervalles de test

Dans **Settings > Panel > Panel**, vous définissez la fréquence des tests de liaison : **GPRS/LTE Test Interval**, **Ethernet Test Interval**, **ARC Polling** pour le signal de vie vers le centre de télésurveillance (en pratique souvent toutes les 3 minutes, toujours en concertation avec le centre) et **Daily Auto Check-in** pour le test quotidien automatique.

7. Enregistrement et accès

7.1 Enregistrer la centrale en tant qu'installateur

1. Connectez-vous en tant qu'installateur dans l'application SmartHomeSec.
2. Appuyez sur le bouton **+** pour ajouter une centrale.
3. Saisissez l'adresse MAC figurant sur le côté de la centrale. Dans le champ **Name**, indiquez le nom de l'abonné ou un autre identifiant reconnaissable.

Attention : la centrale doit être allumée et connectée à Internet. Vous disposez de 15 minutes après la mise sous tension pour enregistrer la centrale.

Une fois enregistrée, la centrale est prête à être configurée. L'application propose un assistant de configuration qui vous guide pas à pas : modèles (**Batch Config**), compte client (**Create Account**), codes utilisateurs (**User PIN**), apprentissage des périphériques (**Add Device**), sécurité (**Security Setting**), paramètres de la centrale (**Panel Settings**), réseau (**Network Settings**) et transmission (**Report Settings**). Vous vous identifiez avec le code installateur par défaut **7982**.

7.2 Se connecter à l'interface web locale

1. Connectez votre ordinateur portable ou votre tablette au même réseau que la centrale.
2. Relevez l'adresse IP locale de la centrale dans le routeur.
3. Saisissez cette adresse IP dans la barre d'adresse de votre navigateur (port 80).
4. Connectez-vous avec l'utilisateur **admin** et le mot de passe par défaut **cX+HsA*7F1**.
5. Initialisez la centrale et définissez immédiatement un nouveau mot de passe robuste.

Attention : si l'interface web n'est pas accessible, redémarrez la centrale et réessayez.

8. Apprentissage des périphériques et configuration des zones

1. Ouvrez **Settings > Devices** dans l'application installateur.
2. Choisissez **Add device**.
3. Sélectionnez le type d'appareil à ajouter, par exemple un détecteur de mouvement.
4. Activez le bouton d'apprentissage de l'appareil. Pour la plupart des détecteurs, une pression brève suffit. Pour les PIRCAM et les claviers, maintenez le bouton enfoncé pendant 3 à 4 secondes ; les claviers s'apprennent également en maintenant * et # enfoncés simultanément pendant 4 secondes.
5. Suivez les instructions affichées. La centrale confirme l'ajout de l'appareil.
6. Sélectionnez l'appareil et validez avec **Submit**.

Sur la page web de la centrale, utilisez le bouton **Learning** : cliquez sur **Start** pour entrer en mode apprentissage, activez l'appareil, puis cliquez sur **Add**. Les appareils appris apparaissent dans la liste **Learned Device**.

Après l'apprentissage, attribuez à chaque zone ses caractéristiques : nom, partition, type de zone et comportement à l'armement. Soyez rigoureux : le type de zone détermine si un détecteur déclenche une alarme instantanée, lance une temporisation d'entrée ou émet un simple carillon.

Avant le montage définitif, effectuez un **test de couverture (walk test)**. Placez la centrale en mode walk test, appuyez sur le bouton de test de chaque appareil et vérifiez la puissance de signal affichée (RSSI). Si le signal est trop faible, déplacez l'appareil ou utilisez un répéteur.

9. Utilisateurs, comptes et codes

La centrale distingue deux types d'accès : les **comptes** pour l'application et le portail web, et les **codes utilisateurs (PIN)** pour armer et désarmer le système.

9.1 Créer un compte client

1. Connectez-vous à la centrale en tant qu'installateur avec le code **7982**.
2. Accédez au menu principal et choisissez **Account list**.
3. Choisissez **Add**, puis **Create an account** pour un nouvel utilisateur.
4. Complétez les données : ID (nom ou adresse e-mail), mot de passe, adresse e-mail et droits.

Il existe deux types de comptes. Le compte **Master** peut créer de nouveaux utilisateurs, ce que le compte **Slave** ne peut pas faire. Créez d'abord le compte Master. Pour chaque compte, vous définissez les droits : demande d'images aux PIRCAM, réception des notifications, automatisation, vues caméra, journal d'événements et partitions (Area 1 à 8) accessibles à l'utilisateur. Vous pouvez également relier la centrale à un compte client existant.

9.2 Configurer les codes utilisateurs

Accédez à **Settings > User PIN** et ajoutez, pour chaque utilisateur, un nom et un code. Ce code permet à l'utilisateur d'armer et de désarmer le système depuis l'application ou depuis un clavier.

Attention : si l'installation doit être conforme à la norme PD 6662, le système ne peut pas être désarmé au moyen d'un code saisi sur un clavier. Prévoyez dans ce cas une télécommande, un bouton-poussoir ou un badge utilisé avec un lecteur de badges adapté.

10. Armement et désarmement

Le système comporte trois modes de base : **armement total (away)**, **armement partiel (home/stay)** et **désarmement (disarm)**. Vous commandez le système depuis l'application, un clavier, une télécommande ou un lecteur de badges. Sélectionnez d'abord la partition à commander, puis le mode souhaité ; confirmez avec un code utilisateur valide.

La centrale signale le nouvel état par des messages vocaux et par les LED d'état ; les sirènes confirment par un bip court à l'armement et par deux bips au désarmement. Pendant les temporisations d'entrée et de sortie, des bips de décompte retentissent.

Si des défauts sont présents au moment de l'armement, le système affiche une liste de défauts. Selon le réglage **Arm Fault Type**, vous pouvez exclure les défauts (bypass) ou répéter l'armement dans les 30 secondes pour forcer l'armement.

Dans **Settings > Panel > Security**, vous réglez les principaux paramètres d'alarme : la **durée de sirène** en cas d'alarme et les **temporisations d'entrée et de sortie**. Le même écran comporte une option qui retarde la transmission de l'alarme de 30 secondes ; il est recommandé de la laisser désactivée.

11. Transmission vers le centre de télésurveillance

Accédez à **Settings > Report**. Cette section comporte deux volets : la transmission des **événements** et celle des **images capturées** par les PIRCAM.

11.1 Événements

Saisissez l'URL de transmission du centre de télésurveillance. La centrale prend notamment en charge :

- **Contact ID sur IP** — `ip://numéro_abonné@ip_serveur:port/CID`
- **SIA DC-09 sur IP** — `ip://numéro_abonné@ip_serveur:port/SIA2`
- **SIA DC-09 avec chiffrement AES** — `ip://numéro_abonné@ip_serveur:port/SIA/KEY/clé`
- **SIA DC-09 avec codes d'événement CID** — `ip://numéro_abonné@ip_serveur:port/CID_SIA2`
- **CSV sur IP** — `ip://numéro_abonné@ip_serveur:port/CSV`
- **E-mail** — `mailto:nom@exemple.be`
- **SIA avec numérotation de zone par partition** — `ip://numéro_abonné@ip_serveur:port/SIA2_A`

Avec la notation SIA standard, la centrale transmet les zones 1 à 80 dans chaque partition. Avec la variante à numérotation par partition, la partition 1 transmet les zones 101 à 180 et la partition 8 les zones 801 à 880.

Pour chaque destination, vous choisissez un **niveau** (tous les événements, uniquement les alarmes ou uniquement les états) et un **groupe**. Les groupes sont traités dans l'ordre : groupe 1, puis groupe 2, et ainsi de suite. Si une destination d'un groupe échoue, la centrale essaie la destination suivante du même groupe. Dès qu'une destination aboutit, le groupe est considéré comme réussi. Le groupe 1 est toujours essentiel. Le nombre de tentatives se règle sur 1, 3, 5, 10 ou 99.

Attention : lors de l'enregistrement dans l'application VESTA, l'URL 1 est complétée automatiquement avec les données du Home Portal Server. Ne modifiez pas ces données. Programmez toujours le centre de télésurveillance dans le **groupe 2 ou supérieur**, faute de quoi la transmission vers l'application échouera.

Si votre centre de télésurveillance ne prend en charge aucun protocole standard, VESTA propose la passerelle logicielle **ALARMSPACE**. Elle traduit les événements VESTA dans le format attendu par le centre et s'installe sur un PC Windows ou une machine virtuelle du centre.

11.2 Images

Pour les images, programmez une URL distincte sous **Captured files**. La centrale prend en charge l'envoi au format Manitou (`numéro_abonné@ip:port`), par SMTP (l'adresse e-mail du centre) et par HTTP (images en base64). Pour Sentinel, programmez d'abord les paramètres SMTP sous **Settings > Report**, puis l'adresse e-mail fournie par le centre sous **Captured files**.

Attention : si vous utilisez des caméras IP intégrées à VESTA, réglez leur résolution sur 2 MP ou moins pour garantir un fonctionnement correct.

12. Entretien et firmware

Maintenez toujours la centrale à jour : les mises à jour contiennent des améliorations, des corrections d'anomalies et des correctifs de sécurité.

1. Accédez à **Settings > Panel > FW update**.
2. Sélectionnez dans la liste le firmware portant le numéro de version le plus élevé et la lettre la plus élevée.
3. Lancez la mise à jour et attendez le redémarrage automatique de la centrale.

Sur une liaison 4G avec bonne couverture, une mise à jour dure de 3 à 5 minutes. En couverture faible ou en 2G, elle peut atteindre environ 8 minutes.

Attention : ne mettez en aucun cas la centrale hors tension et ne la débranchez pas pendant une mise à jour. Elle redémarre d'elle-même. Une coupure pendant la mise à jour peut rendre la centrale totalement inopérante.

Contrôlez par ailleurs périodiquement l'état des piles des détecteurs, effectuez un test de couverture après toute modification et vérifiez que les tests parviennent correctement au centre de télésurveillance.

13. Retour aux réglages d'usine

Les réglages et les périphériques se suppriment simplement depuis la page web de la centrale ou depuis l'application. Pour réinitialiser complètement la centrale, utilisez la remise à zéro matérielle au moyen du bouton d'apprentissage / reset situé sur la carte électronique. Pour les centrales HSGW, la procédure est la suivante :

1. Débranchez l'alimentation et placez l'interrupteur de batterie sur **Off**.
2. Maintenez le bouton d'apprentissage / reset enfoncé et rebranchez l'alimentation. Toutes les LED s'allument pendant environ 10 secondes.
3. Maintenez le bouton enfoncé encore environ 30 secondes, puis relâchez-le. La centrale redémarre et toutes les LED s'allument.
4. Après environ 10 secondes, toutes les LED s'éteignent : la réinitialisation est terminée.

Attention : après un retour aux réglages d'usine, tous les réglages, périphériques appris et comptes sont effacés. Vous devez réenregistrer et reprogrammer entièrement la centrale. Vérifiez la procédure exacte pour votre version de firmware avant de réinitialiser.

14. Dépannage

- **La centrale ne se connecte pas.** Vérifiez le câble Ethernet aux deux extrémités, la connexion Internet du routeur, la mise en place de la carte SIM (code PIN désactivé) et l'APN.
- **L'enregistrement échoue.** La centrale doit être allumée et en ligne, et vous ne disposez que de 15 minutes après la mise sous tension. Redémarrez la centrale et réessayez.
- **L'interface web est inaccessible.** Redémarrez la centrale. Vérifiez que votre appareil est sur le même réseau et que vous utilisez la bonne adresse IP et le bon mot de passe.
- **Le centre de télésurveillance ne reçoit pas les événements.** Vérifiez que vous avez choisi le groupe 2 (ou supérieur) et que le numéro d'abonné correspond à celui attribué par le centre.
- **Le centre ne reçoit pas les images.** Vérifiez le protocole et l'URL distincte sous **Captured files**, et abaissez la résolution des caméras IP intégrées à 2 MP.
- **Un détecteur n'est pas reçu.** Effectuez un test de couverture, déplacez le détecteur ou installez un répéteur.
- **Couverture mobile insuffisante.** Placez la centrale plus haut ou plus près d'un mur extérieur, à l'écart des grandes masses métalliques, ou utilisez une antenne GPRS/4G externe.

15. Support

Des questions sur ce produit ou besoin d'aide lors de l'installation ? Contactez Nestor Company — E3-laan 93, 9800 Deinze.