

MANUEL

Nestor Company

Centrale d'alarme radio VESTA SmartSeries 640 zones, IP + 4G

Manuel d'installation et d'utilisation

Référence	vesta-047NNZ-SF1
Modèle	HSGW-MAX8
Marque	VESTA

Source: <https://vesta-guide.gitbook.io/vesta-guide/vesta-047nnz-sf1>

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 centrale d'alarme VESTA SmartSeries (modèle HSGW-MAX8 de Climax Technology, numéro fournisseur PKB1HSGWM8B4GSL02) est une centrale d'intrusion radio destinée aux habitations et aux petits bâtiments professionnels. Associée à des détecteurs, sirènes, claviers et télécommandes radio VESTA, elle constitue un système d'alarme complet : lorsqu'un détecteur repère un intrus, il transmet un signal radio à la centrale, qui déclenche l'alarme et transmet l'événement au centre de télésurveillance ainsi qu'à l'application de l'utilisateur.

La centrale gère jusqu'à 640 zones radio, réparties sur 8 secteurs (partitions) de 80 zones chacun. Elle est certifiée EN 50131 Grade 2 et communique en double voie : par le réseau filaire (IP/Ethernet) et par le réseau mobile (4G). Le wifi est disponible en option au moyen d'un dongle USB. Pour la domotique, la centrale peut être étendue avec un dongle Z-Wave permettant d'intégrer interrupteurs, variateurs, modules de volets et thermostats au système.

Cette version se distingue par sa prise en charge de la vérification visuelle : les caméras PIR (PIRCAM) capturent une série d'images en cas d'alarme et les transmettent à l'application et au centre de télésurveillance. Un opérateur peut ainsi évaluer visuellement une alarme avant toute intervention.

La centrale se programme entièrement depuis l'application SmartHomeSec (iOS et Android) ou depuis un navigateur web. Aucun écran ni clavier local n'est nécessaire sur l'appareil : l'utilisateur final commande le système via l'application, un clavier radio, une télécommande ou un badge NFC.

2. Éléments et raccordements

La centrale est un modèle mural livré avec son support de fixation. À l'intérieur et à l'arrière du boîtier se trouvent :

- **Port Ethernet** — pour la liaison IP filaire avec le routeur du client.
- **Logement micro-SIM** — pour la carte SIM de la liaison 4G. Le code PIN doit être désactivé au préalable.
- **Port USB** — pour les dongles optionnels, tels que le dongle wifi ou le dongle Z-Wave (VESTA-240).
- **Connecteur mini-USB** — raccordement rapide pour une batterie externe de grande capacité.
- **Bouton d'apprentissage/réinitialisation (learn/reset)** — pour l'apprentissage local des périphériques et pour la réinitialisation d'usine.
- **Interrupteur de batterie** — placez-le sur ON pour activer la batterie de secours interne. Cette étape est obligatoire pour la conformité à la norme EN.
- **Prise pour l'adaptateur d'alimentation.**
- **LED d'état** — indiquent l'état des secteurs et l'état du système (défaut, alarme, mémoire d'alarme, enregistrement réseau).
- **Sirène et buzzer intégrés** — pour la signalisation en cas d'alarme et pendant les temporisations d'entrée et de sortie.

- **Autoprotection (tamper)** — un contact situé dans le support mural. Dès que la centrale est retirée de son support, elle envoie un signal d'autoprotection.
- **Support de fixation avec trous de montage et vis.**

L'adresse MAC figure sur une étiquette apposée sur le côté du boîtier. Cette adresse est nécessaire pour enregistrer la centrale.

3. Caractéristiques techniques

Caractéristique	Valeur
Modèle (nc_type)	HSGW-MAX8
Fabricant	Climax Technology
Numéro fournisseur	PKB1HSGWM8B4GSL02
Nombre de zones radio	640
Répartition	8 secteurs (partitions) de 80 zones
Communication	IP (Ethernet) et 4G ; wifi en option via dongle USB
Antenne externe	Raccordement rapide pour antenne GSM externe (VESTA-274 recommandée, non fournie)
Formats de transmission	Contact ID (CID), SIA DC-09 (également avec chiffrement AES), CSV, Manitou, e-mail (SMTP), SMS, notification push
Destinations de transmission	Réparties en groupes 1 à 5, avec 1, 3, 5, 10 ou 99 tentatives
Vérification visuelle	Caméras PIR (PIRCAM) ; photos via SMTP, HTTP ou Manitou
Domotique	Z-Wave via le dongle VESTA-240 (non fourni)
Automatisation	100 règles et 50 scénarios
Programmation	Interface web et application SmartHomeSec (iOS/Android)
Code installateur par défaut	7982
Accès web local	Utilisateur admin, port 80
Norme	EN 50131 Grade 2

4. Fonctionnement et fonctions

Zones et attributs de zone. Chaque détecteur appris reçoit un numéro de zone au sein d'un secteur. Le comportement de la zone se définit par son attribut dans la rubrique *Réponse à l'armement*. Une zone de type *Intérieur* génère une alarme instantanée ; une zone de type *Entry* déclenche d'abord la temporisation d'entrée. Une affectation correcte des zones constitue l'étape la plus importante de la programmation : elle détermine si un détecteur génère une alarme en armement total, en armement partiel, ou en permanence (zones 24 heures).

Temporisations d'entrée et de sortie et durée de sirène. Dans le menu *Réglages > Centrale > Sécurité*, vous définissez la durée de la sirène en cas d'alarme ainsi que les temporisations d'entrée et de sortie. Le même écran propose une option qui retarde de 30 secondes la transmission de l'alarme ; il est conseillé de la laisser désactivée.

Autoprotection (tamper). La centrale ainsi que les détecteurs et sirènes raccordés sont protégés contre l'ouverture et l'arrachement du mur. Pour les travaux de montage, vous pouvez désactiver temporairement l'autoprotection des sirènes ; la centrale la réactive automatiquement après une heure.

Supervision et interférences. La centrale contrôle que tous les périphériques radio se signalent périodiquement et détecte les tentatives de brouillage ou les interférences radio sur la bande 868 MHz. Ces deux événements peuvent être transmis au centre de télésurveillance.

Mémoire d'alarme et défauts. Après une alarme, l'événement reste enregistré dans la mémoire d'alarme jusqu'à sa consultation. En présence d'un défaut, le système refuse de s'armer ; vous pouvez soit corriger le défaut, soit forcer l'armement.

Règles d'automatisation. La centrale peut exécuter jusqu'à 100 règles et 50 scénarios. Vous pouvez ainsi faire capturer une image par une caméra PIR dès l'ouverture d'un contact de porte, ou commander un relais lors d'un événement déterminé.

5. Raccordement et mise en service

1. Desserrez les deux vis qui fixent le boîtier au support mural et retirez le support.
2. Retirez la vis du capot arrière pour accéder aux raccordements.
3. Raccordez le câble Ethernet au port Ethernet de la centrale.
4. Insérez une carte micro-SIM active dans son logement. Désactivez au préalable le code PIN de la carte SIM.
5. Placez l'interrupteur de batterie sur ON.
6. Raccordez l'adaptateur d'alimentation au secteur.
7. Rangez soigneusement les câbles, refermez le capot arrière et resserrez la vis.
8. Fixez le support au mur, accrochez-y la centrale et poussez-la vers le bas jusqu'au déclic. Resserrez les deux vis inférieures. Veillez à ce que le contact d'autoprotection soit entièrement comprimé contre le crochet du support.

Attention : pour satisfaire à la norme EN, la centrale doit être fixée au mur. Une pose sur table n'est pas conforme.

Au démarrage, toutes les LED s'allument brièvement. La LED d'état clignote ensuite pendant que la centrale s'enregistre sur le réseau mobile et obtient une adresse IP auprès du routeur.

L'enregistrement sur le réseau mobile peut prendre jusqu'à dix minutes. Si la LED d'état reste orange après dix minutes et qu'aucun autre défaut n'est signalé, vérifiez la carte SIM, la couverture et la connexion réseau.

6. Réseau et communication

La centrale fonctionne par défaut avec deux voies de communication : Ethernet et 4G. Assurez-vous que les deux voies fonctionnent avant la réception du chantier.

- **IP.** Raccordez de préférence la centrale au routeur par câble. Si vous travaillez avec une adresse IP fixe, vérifiez que tous les paramètres correspondent aux spécifications du réseau.
- **4G.** Configurez l'APN de l'opérateur, faute de quoi la centrale ne pourra pas communiquer avec le cloud SmartHomeSec. Si la couverture est faible, placez la centrale plus haut et à proximité d'un mur extérieur, à l'écart des grandes masses métalliques et des appareils générant des interférences. En couverture limite, utilisez l'antenne externe VESTA-274.
- **Wifi.** Pour une liaison sans fil, utilisez un dongle wifi USB compatible et encodez correctement le SSID et le mot de passe.

Dans le menu *Réglages > Centrale > Centrale*, vous définissez les intervalles de supervision : le polling vers le centre de télésurveillance (le signal de vie, couramment toutes les 3 minutes — à convenir avec votre centre), le test quotidien automatique, l'intervalle de test GPRS/LTE et l'intervalle de test Ethernet. Le même écran regroupe également la signalisation de coupure secteur, la détection de brouillage radio et l'option de conformité PD 6662.

7. Enregistrement et connexion

Enregistrement en tant qu'installateur. Connectez-vous comme installateur dans l'application SmartHomeSec, appuyez sur le bouton + pour ajouter une centrale et saisissez l'adresse MAC figurant sur l'étiquette de la centrale. Dans le champ du nom, indiquez le nom de l'abonné ou un autre identifiant clair.

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

Accès à la programmation. Une fois la centrale enregistrée, ouvrez-la dans l'application en tant qu'installateur. Le code installateur par défaut est **7982**. Modifiez ce code lors de la réception.

Interface web locale. La centrale dispose également d'une interface web locale. Saisissez l'adresse IP de la centrale dans la barre d'adresse d'un navigateur et connectez-vous avec l'utilisateur **admin** et le mot de passe par défaut associé à la centrale. Initialisez la centrale lors de

la première connexion et définissez immédiatement un nouveau mot de passe robuste. Si l'interface web n'est pas accessible, redémarrez la centrale.

8. Utilisateurs et codes

Comptes utilisateurs pour l'application. Il existe deux types de comptes : Master et Slave. Le compte Master peut créer de nouveaux comptes, le compte Slave non. Créez d'abord le compte Master :

1. Ouvrez la centrale dans l'application en tant qu'installateur.
2. Accédez au menu principal du système.
3. Sélectionnez **Liste des comptes**.
4. Sélectionnez **Ajouter**.
5. Sélectionnez **Créer un compte** pour un nouvel utilisateur.
6. Complétez les données de l'utilisateur pour l'accès à l'application.

Codes utilisateurs (PIN). Rendez-vous dans *Réglages > User PIN* et ajoutez un nom et un code par utilisateur. Ce code permet à l'utilisateur d'armer et de désarmer le système depuis l'application ou depuis un clavier.

Remarque : cinq saisies erronées du code PIN en dix minutes verrouillent le clavier pendant quinze minutes.

9. Apprentissage des périphériques

1. Ouvrez la configuration de la centrale dans l'application installateur.
2. Sélectionnez **Périphériques** dans le menu.
3. Sélectionnez **Ajouter un périphérique**.
4. Choisissez le type de périphérique à ajouter, par exemple un détecteur de mouvement.
5. Appuyez sur le bouton d'apprentissage du périphérique jusqu'à ce que la LED clignote.
Consultez le manuel du périphérique pour identifier le bon bouton.
6. Suivez les instructions à l'écran. La centrale confirme l'ajout du périphérique.

Attention : pour les caméras PIR et les claviers, l'appui doit durer 3 à 4 secondes. Pour la plupart des autres périphériques, un appui bref suffit.

Après l'apprentissage, définissez pour chaque périphérique le nom, le secteur, le numéro de zone et l'attribut de zone.

Test de marche (walk test). Placez la centrale en mode test de marche avant de monter définitivement les périphériques. Activez chaque périphérique à l'emplacement prévu ; la centrale affiche la force du signal. Si le signal est trop faible, déplacez le périphérique ou utilisez un répéteur. Ne montez les périphériques qu'après un test de marche satisfaisant.

Périphériques Z-Wave. Avec le dongle Z-Wave inséré dans le port USB, vous ajoutez des périphériques domotiques via le menu Z-Wave. Placez la centrale en mode d'ajout et activez le périphérique. Après chaque ajout ou suppression, lancez une redécouverte du réseau (network rediscovery).

10. Armement et désarmement

Le système connaît trois états de base : **armement total** (Away), **armement partiel** (Home) et **désarmé** (Disarm). Vous commandez le système via l'application, un clavier radio, une télécommande ou un badge NFC.

- **Armement total.** Toutes les zones sont surveillées. À l'armement, la temporisation de sortie démarre ; quittez les lieux pendant ce délai.
- **Armement partiel.** Seules les zones périphériques sont surveillées, ce qui permet de circuler à l'intérieur.
- **Désarmement.** À l'entrée par une zone temporisée, la temporisation d'entrée démarre. Désarmez le système pendant ce délai à l'aide d'un code utilisateur valide ou d'un badge, faute de quoi l'alarme se déclenche.

Le désarmement exige toujours un code utilisateur ou un badge. En présence d'un défaut, l'armement est refusé et le défaut est affiché ; corrigez-le ou forcez l'armement.

Remarque : les installations soumises à la norme PD 6662 ne peuvent pas être désarmées par la saisie d'un code sur un clavier. Prévoyez dans ce cas une télécommande ou un badge accompagné d'un lecteur adapté.

11. Transmission vers le centre de télésurveillance

Rendez-vous dans *Réglages > Rapport*. Vous y programmez les destinations pour les événements et, séparément, les destinations pour les photos des caméras PIR.

Une URL de transmission se présente sous la forme `ip://(numéro d'abonné)@(IP du serveur):(port)/(protocole)`. Quelques exemples :

- Contact ID via TCP/IP : `ip://1234@54.183.182.247:8080/CID`
- SIA DC-09 via IP : `ip://1234@54.183.182.247:8080/SIA2`
- SIA DC-09 avec chiffrement AES : `ip://1234@54.183.182.247:8080/SIA/KEY/(clé)`
- E-mail : `mailto:utilisateur@exemple.be`

Pour chaque destination, vous choisissez un **niveau** (tous les événements, uniquement les alarmes, ou uniquement les événements d'état) 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 aboutit, l'ensemble du groupe est considéré comme réussi. Le groupe 1 est toujours essentiel et ne peut pas être modifié.

Attention : lorsque la centrale est enregistrée auprès de l'application VESTA, l'URL 1 est automatiquement complétée avec les données du Home Portal Server. Ne modifiez pas ces données. Programmez toujours le centre de télésurveillance dans le groupe 2 ou supérieur.

Pour les photos, utilisez le SMTP (adresse e-mail du centre de télésurveillance), le HTTP (images en base64) ou le format de votre logiciel de télésurveillance. Si vous utilisez des caméras IP, réglez leur résolution sur 2 MP ou moins.

Si votre centre de télésurveillance ne prend en charge aucun des protocoles standard, VESTA propose la passerelle logicielle ALARMSPACE comme couche de traduction. Contactez à cet effet votre représentant VESTA.

12. Entretien et mise à jour du firmware

Maintenez le firmware de la centrale à jour : les mises à jour contiennent des améliorations, des corrections de bugs et des correctifs de sécurité.

1. Rendez-vous dans *Réglages > Centrale*.
2. Sélectionnez **Mise à jour FW**.
3. Sélectionnez dans la liste le firmware portant la version la plus élevée (chiffre le plus élevé et lettre la plus élevée).

Une mise à jour dure environ 3 à 5 minutes en 4G avec une bonne couverture. Avec une couverture faible, elle peut atteindre 8 minutes.

Attention : ne mettez **jamais** la centrale hors tension pendant une mise à jour et ne la débranchez pas. La centrale redémarre automatiquement. Une mise hors tension pendant une mise à jour peut rendre la centrale définitivement inutilisable.

Le module radio dispose également de son propre firmware. Vérifiez dans les réglages de la centrale l'étiquette du firmware RF : si elle commence par BGST, la centrale utilise le protocole SF1 ; si elle commence par BG, il s'agit du protocole F1. Choisissez le fichier correspondant lors de la mise à jour.

Lors d'un entretien périodique, contrôlez la batterie de secours, les contacts d'autoprotection, la force du signal des détecteurs et la transmission vers le centre de télésurveillance. La batterie de secours interne est une pièce d'usure et doit être remplacée par un pack de batteries d'origine.

13. Restauration des réglages d'usine

Ne restaurez les réglages d'usine que si vous souhaitez reconstruire entièrement la centrale. Tous les périphériques appris, les utilisateurs et les réglages sont perdus.

1. Débranchez l'adaptateur d'alimentation et placez l'interrupteur de batterie sur OFF.
2. Maintenez le bouton learn/reset enfoncé et rebranchez l'adaptateur d'alimentation. Toutes les LED s'allument pendant environ 10 secondes.

3. Maintenez le bouton enfoncé encore environ 30 secondes, puis relâchez-le. Après environ 10 secondes, la centrale redémarre et toutes les LED s'allument.
4. Patientez environ 10 secondes ; lorsque toutes les LED s'éteignent, la réinitialisation est terminée.

14. Dépannage

Symptôme	Contrôle
Pas de liaison mobile	La carte SIM est-elle correctement insérée et le code PIN désactivé ? La couverture est-elle suffisante ? Placez la centrale plus haut et près d'un mur extérieur, à l'écart du métal et des sources d'interférences. Envisagez l'antenne externe VESTA-274.
Pas de liaison IP	Le câble Ethernet est-il bien enfiché côté routeur et côté centrale ? Le routeur dispose-t-il d'internet ? En wifi : le SSID et le mot de passe sont-ils corrects ? En IP fixe : tous les paramètres sont-ils corrects ?
Interface web inaccessible	Redémarrez la centrale et réessayez. Vérifiez que vous êtes sur le même réseau local et que l'adresse IP est correcte.
L'enregistrement dans l'application échoue	La centrale doit être sous tension et en ligne ; enregistrez-la dans les quinze minutes suivant la mise sous tension. Vérifiez l'adresse MAC.
Un périphérique ne s'apprend pas	Pour les caméras PIR et les claviers, maintenez le bouton enfoncé 3 à 4 secondes. Contrôlez la pile du périphérique et la distance jusqu'à la centrale.
Un détecteur décroche pendant le test de marche	Rapprochez le périphérique de la centrale ou utilisez un répéteur.
Les images des caméras IP ne passent pas	Réglez la résolution de la caméra sur 2 MP ou moins.
La transmission vers le centre de télésurveillance échoue	Contrôlez l'URL de transmission, le numéro d'abonné, le port et le protocole. Programmez le centre dans le groupe 2 ou supérieur et laissez l'URL 1 inchangée.

15. Support

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